REPUBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
DIRECCION GENERAL DE ESTUDIOS DE POSTGRADO
POSTGRADO EN SISTEMAS DE INFORMACION

MODELO DE AUDITORÍA Y CONTROL DE INFORMACION Y TECNOLOGIAS RELACIONADAS CASO: BANCO SOFITASA

Proyecto de Trabajo Especial de Grado para optar al Titulo de Especialista en Sistemas de Información

Autor: Elixender Lamprea L.

Tutor: Jaime A. Vélez Laguado

San Cristóbal, Julio de 2004

REPUBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD CATÓLICA ANDRÉS BELLO

MODELO DE AUDITORÍA Y CONTROL DE INFORMACION Y TECNOLOGIAS RELACIONADAS

Autor: Elixender Lamprea L.

San Cristóbal, Julio de 2004

APROBACIÓN DEL TUTOR

En mi carácter de Tutor del Trabajo Especial de Grado, presentado por el ciudadano Elixender Lamprea León, para optar al grado de Especialista en Sistemas de Información, considero que dicho trabajo reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del jurado examinador que se designe.

En la ciudad de San Cristóbal, a los quince días del mes de Septiembre de dos mil cuatro.

_____

Jaime A. Vélez Laguado

C.I.: V-11.499.462

A

Alicia y Manuel,

Desde algún lugar de la eternidad me guían y esperan…

Rubiela y José del Carmén,

Creadores de mi vida;

Gloria Cecilia,

Mi fiel esposa y compañera;

Sergio David, Jean Ibrahim, Gloria Elixandra,

Mis hijos, motores de cada día nuevo;

Todos los que amo…

Elixender.

ÍNDICE DE CONTENIDO

LISTA DE CUADROS

LISTA DE GRAFICOS

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
DIRECCIÓN GENERAL DE ESTUDIOS DE POSTGRADO
ESPECIALIZACIÓN EN SISTEMAS DE INFORMACIÓN

Modelo de Auditoría y Control de Información y Tecnologías Relacionadas Caso: Banco Sofitasa

Trabajo especial de grado, presentado para optar al título de Especialista en Sistemas de Información

Autor: Elixender Lamprea L.
Tutor: Jaime A. Vélez Lagüado
Año: 2004

RESUMEN

El aumento significativo y relevante que el uso de la información tiene para las organizaciones actuales determina que todos los procesos relativos a la producción, administración y gerencia de Tecnologías de Información (TI) deben ser óptimamente controlados para asegurar la calidad de la información, soporte del cumplimiento de los objetivos del negocio. Los procesos de información requieren la aplicación de técnicas y medidas de control que garanticen la reducción de vulnerabilidad a amenazas generadoras de riesgo que pongan en peligro la estabilidad del sistema organizacional y del sistema del negocio. El presente trabajo desarrolla un estudio del problema de control y seguridad de la información y las tecnologías relacionadas, fundamentándose teóricamente en la investigación Cobit (Control Objectives for Information Technology), que resume estos requerimientos siguiendo las mejores prácticas de aceptación internacional en materia de gobierno de las TI. El estudio diagnostica el problema en el Banco Sofitasa, una organización que fundamenta sus procesos de negocio en los procesos de información y TI, con una alta infraestructura tecnológica, determinándose la factibilidad de aplicación del Modelo Metodológico de Auditoría de Información y Tecnologías Relacionadas, propuesto como proyecto factible por la presente investigación. El modelo propuesto, fundamentado en el Marco Referencial COBIT, intenta principalmente la promoción de la cultura de control y seguridad de TI en las organizaciones, suministrando una sencilla, práctica y sistémica manera de evaluar los procesos de TI, permitiendo determinar índices de evaluación de procesos, objetivos de control, riesgos asociados y aplicar guías y procedimientos de auditoria para facilitar la emisión de los informes de opinión.

INTRODUCCION

Las organizaciones actuales requieren mantenerse activas y efectivas en la competencia global; las presiones del entorno, producto del avance tecnológico, las estrategias competitivas, las exigencias de los clientes y todas las variables endógenas y exógenas, determinan un singular juego de oportunidades y amenazas que deben ser oportunamente valoradas. En todo esto, la información y las tecnologías relacionadas que la soportan, producto de las operaciones del negocio, poseen un singular y alto grado de importancia y relevancia como activos de gran valor para la organización y la empresa. Esa información y los procesos de Tecnología de la Información que la planifican y organizan, la generan y administran, y la gerencian y evalúan, deben ser controlados a través de la implantación de técnicas de control efectivas, en procura del cumplimiento de objetivos de control que garanticen la calidad y satisfacción de los procesos alineados con los objetivos del negocio.

La complejidad creciente de las plataformas informáticas, múltiples sistemas de hardware y software, redes globales de comunicación de datos, comercio y negocio electrónico, capacidad de delinquir de los usuarios, generan nuevas amenazas de riesgo para los sistemas de información del negocio. Por todo esto, es necesario, como parte de los planes en materia de gobierno de TI, establecer en las organizaciones una estructura de relaciones y procesos dirigida a controlar la información para alcanzar los objetivos del negocio, adicionando valor mientras se mantiene un balance equilibrado de los riesgos sobre la Tecnología de Información y sus procesos.

La presente investigación plantea en el Capitulo I, un estudio del problema de control y seguridad de la información y las tecnologías relacionadas; en el Capitulo II

se presenta un estudio documental de antecedentes de investigación en esta línea y bases teóricas, resaltando el papel fundamental de la investigación adelantada desde el año 1996 por la ISACF (Información System Audit and Control Foundation) y el IT Governance Institute que ha producido el proyecto COBIT, resumiendo las mejores prácticas de aceptación universal para el tratamiento del problema de control de TI. En el Capitulo III se presenta el Marco Metodológico de la presente investigación, aplicada como caso de estudio real, al Banco Sofitasa, una organización bancaria de reconocida trayectoria y estructura organizacional, que por la complejidad y madurez de sus proyectos informáticos, gobernados desde la Vicepresidencia de Tecnología y en coordinación con la Gerencia de Auditoría de Sistemas permitió la aplicación de los instrumentos para la presente investigación y la realización del diagnostico situacional referido al problema en estudio.

Finalmente, en el Capitulo IV, se presenta la propuesta factible de desarrollo del *Modelo Metodológico de Auditoría de Información y Tecnologías Relacionadas* que fundamentado en el proyecto COBIT, propone la aplicación de una serie de métodos y técnicas a través de varias fases, para el tratamiento del problema de evaluación y auditoría, facilitando la comprensión y promoción de la estructura COBIT como modelo practico a seguir. Se incluye, el diseño lógico y físico del prototipo estructural de software que permite visualizar el enfoque metodológico para el desarrollo de una aplicación orientada al uso de los usuarios finales en las áreas gobierno y auditoría de TI.

CAPITULO I

EL PROBLEMA

Contexto o Marco Referencial

Para resaltar la relevancia y significado que los procesos de información y las tecnologías relacionadas tienen para las organizaciones actuales en procura del logro de los objetivos del negocio, resulta muy apropiada la mención de O'Brien (1998) a este aspecto: "La tecnología de la información se ha convertido en una necesidad estratégica, crea en ella, actué con base en ella o conviértase en un acontecimiento tangencial en la historia".

La revolución tecnológica aplicada a la gestión de la información ha crecido a pasos agigantados en los últimos años. Las organizaciones como sistemas abiertos que son, están relacionadas con su entorno; las empresas y organizaciones están sometidas a presiones e influencias de órdenes económicos, industriales y sociales en los que se encuentran inmersas; en consecuencia, si las tendencias tecnológicas y los entornos económicos e industriales cambian, deben adaptarse rápidamente a las nuevas circunstancias para sobrevivir. Como cita Rodríguez (1998) en la presentación de Piattini y Del Peso (1998) "Una de las tendencias actuales más significativas es la que nos ha dirigido desde una Sociedad Industrial hacia una llamada Sociedad de Información".

Los cambios suceden muy rápido respecto a los procesos de adaptación de las organizaciones; están afectando al mundo entero, y su comprensión es fundamental para las organizaciones de todo tipo, particularmente en el contexto de los *Sistemas de Información* (SI) y *Tecnologías de la Información y las Comunicaciones* (TIC).

Aunque los avances tecnológicos han sido constantes y espectaculares, en los últimos veinte años se ha producido una verdadera revolución tecnológica de gran impacto para la propia industria informática, así como de consecuencias importantes para el resto de los sectores.

En consecuencia, cada vez, un mayor número de organizaciones considera que la información y la tecnología asociada a ella representan sus activos más importantes. De igual modo que se exige para los otros activos de la empresa, los requerimientos de calidad, controles, seguridad e información sobre los procesos de datos e información y sobre la tecnología relacionada son indispensables.

En este sentido, la gerencia debe establecer un sistema de *Control Interno* adecuado que minimice los riesgos producidos por la aplicación de la tecnología informática. Tal sistema debe soportar debidamente los procesos del negocio a través de la garantía de seguridad de los sistemas de información. Por lo tanto, el nivel o estado de la seguridad de información y las tecnologías relacionadas en una organización, es un objetivo a evaluar de primer orden. El cumplimiento de este objetivo, es la función principal de la evaluación y el control informáticos.

Planteamiento del Problema

El continuo y creciente desarrollo de sistemas de información basados en el uso de computadoras y otras tecnologías de procesos, gestión y comunicación de información, ha convertido al computador en una herramienta indispensable en las organizaciones, proporcionándole un control más efectivo sobre sus recursos y operaciones, como también en la ejecución propia de esas operaciones. Sin embargo, esos mismos sistemas tienen cada vez, un mayor número de personas preocupadas debido a que el control computarizado de los activos, el fácil acceso a la información y la creciente dependencia de la tecnología pueden convertir a las organizaciones en entes más vulnerables que nunca, cuestionándose en este sentido en qué medida están sus sistemas de información adecuadamente controlados contra los riesgos informáticos.

A pesar de los grandes adelantos tecnológicos y de su aplicación al procesamiento de datos y gestión de información en lo que se ha llamado Tecnologías de la Información y las Comunicaciones (TIC), la incorporación de este importante recurso a las operaciones y gestión de la información en la organizaciones ha generado una problemática particular que se ha hecho evidente en múltiples organizaciones alrededor del mundo. Como lo cita Rodríguez (1998) presidente de la Organización de Auditoría Informática, Capitulo español de ISACA, (Information Systems Audit And Control Asociation), en la presentación de Piattini y del Peso (1998),

> *"…la situación actual de los sistemas de información en las organizaciones se caracteriza frecuentemente por una falta de asimilación de las nuevas tecnologías, por una infrautilización de los equipos informáticos, por un descontento generalizado de los usuarios, por una obsolescencia de las aplicaciones informáticas actuales, por una falta de planificación de los Sistemas de Información, y por soluciones planteadas parcialmente que, al no estar integradas, producen islotes de mecanización y de procesos manuales, en muchos casos redundantes e/o incoherentes, difíciles de controlar y caros de mantener. En definitiva, por una falta de estándares y metodologías, y por una falta de formación y cultura generalizada, sobre todo en los aspectos de control y de seguridad informática. La auditoría informática ha aportado soluciones, en el pasado, para estos problemas; pero se ha realizado frecuentemente, hasta ahora, solo en grandes empresas y, en la mayoría de los casos, como un complemento de la auditoría financiera…"*

Cada día, son mayores las inversiones en tecnologías de información y mayor la dependencia del negocio de las estructuras informáticas; los sistemas de control y seguridad de la información exigen mayor rigurosidad en áreas tan diversas como la planificación de proyectos, la organización de la unidad de informática, la dirección y gestión de los recursos informáticos, la administración y control de infraestructuras e instalaciones, el desarrollo y mantenimiento de aplicaciones, la explotación de los sistemas de información, las bases de datos, las comunicaciones y redes, la ofimática, la seguridad general y particular, los recursos humanos y la calidad.

La globalización ha impuesto nuevos retos de competencia, las organizaciones se deben reestructurar hacia operaciones cada vez más competitivas y, como

consecuencia deben aprovechar los avances de las tecnologías de los sistemas de información para mejorar su situación competitiva. Hoy en día se habla de reingeniería de negocios y de procesos, de calidad total, de procesos distribuidos, de organizaciones planas, de multiples tipos de sistemas de información: MIS (Management Information System), EIS/DSS (Executive Information System)/Decision Support Systems), ERP (Entreprise Resource Planning), CRM (Customer Relationship Management) y otros, como cambios que generan un impacto en la manera en que operan las organizaciones privadas y públicas. Estos cambios están teniendo y continuaran teniendo implicaciones profundas para la gestión y para las estructuras de control en todas las organizaciones.

Todo lo anterior deriva en qué la previsión, el control, la seguridad, y la reducción de costos, implicados en los sistemas de información mecanizados son una estrategia fundamental de las organizaciones actuales. La automatización de las funciones y procesos de la organización, por su propia naturaleza, genera una mayor dependencia de mecanismos de control en las computadoras y redes desde el punto de vista del hardware y del software. La aplicación de la informática al proceso del negocio crea o genera unos riesgos informáticos de los que hay que proteger y preservar a la organización con un conjunto de controles, y la calidad y eficacia de estos controles es el objetivo central a evaluar para poder identificar los puntos débiles y mejorarlos. Esta es una de las funciones de las Auditoría Informática.

Para estar a la altura de las circunstancias, es necesario que los usuarios se pongan al día en cuanto a la tecnología y entorno de la Auditoría Informática, y para acceder a este nuevo paradigma debe tratarse el problema de minimizar la complejidad de los procesos de evaluación y control de los entornos de aplicación de las tecnologías de la información. En tal sentido, un modelo de registro de planes, recursos, procesos, riesgos, controles y guías de evaluación y control de los sistemas de información y sus tecnologías, favorecerá y facilitara la función de Evaluación y Auditoría Informática en la Organización. En resumen, se plantean entonces los siguientes interrogantes:

¿Conocen los usuarios de Sistemas de Información basados en TI, los elementos involucrados en el control y seguridad de la información?
¿Existen registros de los planes en materia de aplicación de TI?

¿Las soluciones de información basadas en TI se adquieren e implementan en función de los objetivos del negocio?

¿Esta controlada la seguridad del servicio de información para la ejecución de las operaciones del negocio?

¿Existen mecanismos de registro y evaluación de los procesos basados en la aplicación de TI?

¿Como acceder de manera sistémica y sencilla al conocimiento y aplicación, por parte de los usuarios ejecutivos de negocios, profesionales de TI y auditores de sistemas de información, de una estructura que facilite la Auditoría de los procesos de Tecnología Informática en concordancia con los objetivos del negocio?

¿Como saber en que medida de control se encuentra la organización respecto a la planificación, desarrollo, uso y evaluación de la TI?

Objetivos

Objetivo General

Diseñar un modelo metodológico de evaluación y Auditoría aplicable a los procesos de información y tecnologías relacionadas.

Objetivos Específicos

1. Diagnosticar la necesidad de Evaluación y Auditoría Informática en una organización.

2. Seleccionar el enfoque metodológico para desarrollar la propuesta de solución al problema de evaluación y auditoría informática.

3. Diseñar el esquema conceptual del modelo de aplicación de evaluación, auditoría y control de procesos de información y tecnologías afines.

4. Integrar al modelo de auditoría, técnicas de valoración cuantitativa que permitan la obtención de valores de medidas de riesgo y control.

5. Estructurar el diseño lógico de la herramienta automatizada para la aplicación del modelo de auditoría, evaluación y control propuesto.

Importancia y Justificación del Estudio

La importancia del estudio que intenta desarrollar el presente proyecto se fundamenta en cuatro aspectos característicos de la información como activo empresarial y en la conceptualización y aplicación de la estructura de la arquitectura

de información y de los procesos soportados en Tecnología de Información (TI) en las organizaciones actuales. Estos aspectos son:

1. El Valor de la Información en las Organizaciones: si se parte del conocimiento previo de qué la Información representa un activo de singular valor para las organizaciones, y que todos los procesos del negocio se sustentan en el procesamiento de datos y administración de información para soportar la toma de decisiones y mantener la estabilidad y rentabilidad del negocio, es necesario entender que la tecnología relacionada con la información y sus procesos representa un punto de enfoque de especial importancia para la estabilidad empresarial.

Existen principios generalmente aceptados en las buenas practicas, reconocidas internacionalmente por los expertos en la materia de *Control y Auditoría de Información y Tecnologías relacionadas*; por tal razón, toda investigación que esté sustentada en el marco referencial de las mejores prácticas y persiga la aplicabilidad de sus principios, está dotada de una singular importancia.

Las metodologías de Auditoría informática deben cubrir todos los aspectos de la información y de la tecnología que la soporta. *Los Objetivos de Control* deben encararse con referencia a las políticas y estándares de la empresa, el propietario del proceso del negocio debe asegurar que se provee un sistema de control adecuado para el ambiente de tecnología informática.

2. Integración de los Recursos de los Sistemas de Información: el presente estudio esta orientado a obtener un producto, que permitirá aplicar modelos de evaluación y control sobre las diferentes actividades y/o tareas, procesos y áreas de aplicación de las Tecnologías de Información bajo el enfoque de aplicación de los diferentes objetivos de control formulados para cada ámbito integrando los recursos y/o componentes de un sistema de información: personas, datos, software (programas), hardware (equipos y facilidades), redes y comunicaciones, información, actividades, conocimiento y bases de conocimiento, retroalimentación (autocontrol), procedimientos e instalaciones físicas.

3. Requerimientos de información: Los recursos anteriores se integran para satisfacer los requerimientos del negocio en cuanto a la calidad, aspectos financieros

y seguridad (control de riesgos) sobre los criterios de información para optimizar su uso. Comenzando el análisis desde los requerimientos amplios de calidad, financieros y seguridad, se deben contemplar las características de la información que satisfacen los criterios de *efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.*

4. La Estructura de Cobertura Global de la TI: los procesos básicos de información basados en la aplicación de tecnología informática comienzan en las actividades y tareas necesarias para lograr un resultado mensurable. Las actividades tienen un concepto de ciclo de vida mientras que las tareas son consideradas más discretas. El concepto *ciclo de vida* tiene requerimientos típicos de control diferentes de las actividades discretas. Ejemplos de la primera categoría son las actividades de desarrollo de sistemas, administración de la configuración y administración de los cambios. La segunda categoría incluye tareas realizadas en soporte de planeamiento estratégico de Tecnología Informática, evaluación de riesgos, planeamiento de calidad, administración de capacidad y performance. Al más alto nivel, los procesos son agrupados naturalmente en dominios, su agrupamiento natural es a menudo confirmado como dominios de responsabilidad en una estructura organizacional y está en línea con el ciclo de administración o ciclo de vida aplicable a los procesos de Tecnología Informática.

La observancia en todos los aspectos mencionados anteriormente para el diseño de un modelo de auditoría, evaluación y control de los procesos de información y de la tecnología relacionada con estos procesos, permitirá la generación de una estructura conceptual y metodológica de fácil conocimiento y aplicación por parte de los usuarios ejecutivos de negocios, profesionales de TI y auditores de sistemas de información, para saber en que medida de control se encuentra la organización respecto a la planificación, desarrollo, uso y evaluación de la TI y en consecuencia, fortalecer o corregir los planes de acción en concordancia con los objetivos del negocio.

CAPITULO II
MARCO TEORICO

Antecedentes

En el marco de referencia de estudios precedentes sobre el estudio y/o aplicación de modelos o enfoques metodológicos de procesos de evaluación y control de Auditoría orientada a los sistemas de información y a las tecnologías relacionadas con estas áreas del conocimiento, hoy conocidas como tecnologías de la información (TI), se pueden encontrar múltiples referencias que han dado origen a las hoy conocidas Metodologías de Auditoría Informática, de las cuales, se presentará más adelante una referencia teórica a las más importantes por su uso y aporte al desarrollo de esta área del conocimiento denominada Auditoría Informática y como antecedentes, propiamente dichos, se citaran algunos estudios que se han sustentado en la aplicación de dichas metodologías para la solución de problemas de control y evaluación de TI y otros que han provisto aportes para la creación, uso y aplicación de nuevos enfoques, modelos o herramientas de aplicación de las metodologías preexistentes.

García (1990), plantea la problemática de generación de novedosas formas de fraudes, delitos informáticos y fracasos de organizaciones como resultado del creciente uso del recurso computador que incorpora nuevas amenazas y riesgos en el tratamiento de la información y propone que frente a esta situación la respuesta no puede ser no utilizarlo; la solución debe ser canalizar adecuadamente su utilización, reconociendo, identificando, avizorando estas novedosas formas de fraudes y generadoras de fracasos. También plantea la existencia de información previa en obras de Auditoría de Sistemas, revistas especializadas, presentaciones de trabajos en

congresos y seminarios de corte internacional, realizados por importantes figuras del área, destacando aspectos estadísticos de robos y fraudes por computador y contribuyendo a alertar y generar conocimiento en la importante función de Auditoría de Sistemas. Según Garcia (ob. cit.) "…Sin embargo, el Auditor no dispone de una herramienta metodológica que le permita formular y aplicar programas de revisión y auditaje". Junto a esta necesidad, como base conceptual para conformar la motivación de su investigación y presentación de su enfoque metodológico, Garcia presenta su enfoque metodológico en seis fases: (a) organización y planificación del programa de auditoría, (b) identificación y descripción de recursos y procesos, (c) simulación, identificación y descripción de amenazas y riesgos, (d) identificación y descripción de controles, (e) análisis de cobertura, y (f) prueba de los controles.

Este trabajo es importante como antecedente porque se ubica en una época, inicio de la década de los noventa, en la que la Auditoría de Sistemas es incipiente metodológicamente y presenta una opción de aplicación sistémica de evaluación y control de los recursos, procesos, amenazas y riesgos en los sistemas de información para evaluar los controles existentes y proponer una serie de controles pertinentes de acuerdo con el grado de requerimientos de control en los sistemas evaluados. Su aporte, aparte de la intención metodológica, es la clasificación y aplicación del concepto amplio de control en el contexto de los sistemas de información. La desventaja de esta investigación radica en que para su época, los conceptos de sistemas de información gerencial, la estrategia y objetivo del negocio, las tendencias abiertas de las tecnologías de la información y las comunicaciones no son contempladas ni incorporadas en el estudio.

La **ISACF (1996),** Information Systems Audit and Control Foundation, Fundación para el Control y Auditoría de los Sistemas de Información, ha desarrollado y publicado con el apoyo de IT Governance Institute (Instituto para el Gobierno de Tecnologías de Información) el *Proyecto de Investigación COBIT,* acrónimo en ingles de Control Objetives for Information and related Technologies, (Objetivos de Control para la Información y las Tecnologías afines o relacionadas).

COBIT ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnología de Información (TI). *COBIT* es la herramienta innovadora para el gobierno de TI. *COBIT* se fundamenta en los *Objetivos de Control* existentes de la *Information Systems Audit and Control Foundation* (ISACF), mejorados a partir de estándares internacionales técnicos, profesionales, regulatorios y específicos para la industria, tanto existentes como en surgimiento.

Los *Objetivos de Control* resultantes han sido desarrollados para su aplicación en sistemas de información en toda la empresa. El término **"generalmente aplicable y aceptado"** es utilizado explícitamente en el mismo sentido que los Principios de Contabilidad Generalmente Aceptados (PCGA o GAAP por sus siglas en inglés). Para propósitos del proyecto, "*buenas prácticas***"** significa consenso por parte de los expertos. El desarrollo de *COBIT* ha traído como resultado la publicación del Marco Referencial general y de los Objetivos de Control detallados, y le seguirán actividades educativas. Estas actividades asegurarán el uso general de los resultados del Proyecto de Investigación *COBIT*. El desarrollo de *COBIT* ha resultado en la publicación de:

1. *Resumen Ejecutivo:* que consiste en una Síntesis Ejecutiva (que proporciona a la alta gerencia entendimiento y conciencia sobre los conceptos clave y principios de COBIT) y el Marco Referencial que identifica los cuatro dominios de COBIT y los correspondientes 34 procesos de TI
2. *Marco Referencial:* que describe en detalle los 34 objetivos de control de alto nivel e identifica los requerimientos de negocio para la información y los recursos de TI que son impactados en forma primaria por cada objetivo de control
3. *Objetivos de Control:* los cuales contienen declaraciones de los resultados deseados o propósitos a ser alcanzados mediante la implementación de 318 objetivos de control detallados y específicos a través de los 34 procesos de TI definidos en el marco referencial.

4. *Directrices de Auditoría:* las cuales contienen los pasos de auditoría correspondientes a cada uno de los 34 objetivos de control de TI de alto nivel para proporcionar asistencia a los auditores de sistemas en la revisión de los procesos de TI con respecto a los 318 objetivos detallados de control recomendados para proporcionar a la gerencia certeza o una recomendaciones de mejoramiento
5. *Conjunto de Herramientas de Implementación:* el cual proporciona lecciones aprendidas por organizaciones que han aplicado COBIT rápida y exitosamente en sus ambientes de trabajo. El Conjunto de Herramientas de Implementación incluye la *Síntesis Ejecutiva*, proporcionando a la alta gerencia conciencia y entendimiento de COBIT.

Las investigaciones y publicaciones sobre *COBIT* han sido posibles gracias a contribuciones de múltiples organizaciones como Unysis, Unitech Systems, Inc., MIS Training Institute, Zergo, Ltd., y Coopers & Lybrand. El Forum Europeo de Seguridad (European Security Forum –ESF-) amablemente puso a disposición material para el proyecto. Otras donaciones fueron recibidas de capítulos miembros de ISACA de todo el mundo.

En la historia de la investigación *COBIT* muchas fuentes han contribuido al aporte de consolidación de la misma. Entre ellas tenemos: (a) estándares técnicos de ISO, EDIFACT, otros; (b) códigos de conducta establecidos por el Council of Europe, OECD, ISACA, otros; (c) criterios de calificación para sistemas y procesos de TI: ITSEC, TCSEC, ISO 9000, SPICE, TICKIT, Common Criteria, otros; (d) estándares profesionales para control interno y auditoria: COSO, IFAC, AICPA, CICA, ISACA, IIA, PCIE, GAO, otros; (e) requerimientos y prácticas de foros de la industria: ESF, I4 y plataformas auspiciadas por gobiernos como IBAG, NIST, DTI; y (f) requerimientos específicos de industrias emergentes de sectores como banca, comercio electrónico, y manufactura de TI. (Las definiciones de los términos y/o acrónimos citados pueden verse más adelante en la definición de términos.

Estos antecedentes del Proyecto de investigación *COBIT* son importantes, en general, por cuanto presentan el basamento estructural de apoyo de los más recientes trabajos de investigación y aplicación en el área de Auditoría en Tecnologías de la Información, y en particular porque sustentan el desarrollo del presente proyecto de investigación.

Las referencias específicas a los contenidos conceptuales de *COBIT* y a su estructura serán presentadas más adelante en el contenido de las bases teóricas donde se ampliaran suficientemente los conceptos necesarios para soportar su aplicación en el presente estudio.

MEYCOR Cobit Control Self Assessment (CSA), de **Datasec (1999),** ha sido apoyado por el Gobierno de Uruguay en Suramérica. Buscando sacar provecho de la experiencia de los profesionales en el campo de la ciencia y la tecnología y promover la apertura de negocios estratégicos de mercado en esta área, decide apoyar proyectos innovadores en el Programa de Desarrollo Tecnológico (PDT) auspiciado por el Banco Interamericano de Desarrollo (BID).

Después de definir los requerimientos para los procesos de las propuestas, PDT aprobó un proyecto para soportar el desarrollo de software relacionado con el gobierno (gestión) de Tecnologías de Información (TI) basado en el modelo *COBIT* desarrollado por ISACF y el IT Governance Institute. El proyecto de investigación y desarrollo fue completado por *DATASEC S.R.L.,* una firma de consultores y desarrolladores de software. Después de una intensa investigación y acumulación de experiencia con aplicaciones de *COBIT* y metodologías de análisis cualitativo de riesgos como la francesa *MARION* y la inglesa *CRAMM*, el primer producto de software basado en *COBIT* fue llamado *MEYCOR Cobit Control Self Assessment (CSA),* es un software que fue puesto al uso de clientes de la consultoría. Después el mismo ha sido mejorado, siendo utilizado por varias compañías en Uruguay y otras partes. A través de su investigación y desarrollo, Datasec ha impuesto a Meycor CSA los siguientes propósitos:

1. Permitir la funcionalidad Cobit no solo para grandes compañías, sino también para organizaciones de medio y pequeño tamaño.
2. Permitir la entrada en múltiples niveles de usuarios; a causa de la flexibilidad de la herramienta, puede ser introducida en las empresas al nivel de supervisores de operaciones, CIO's, directores, interventores, expertos de seguridad IT, auditores y asesores.
3. Generar automáticamente recomendaciones con enlace a gráficos que permitan a la organización el monitoreo de sus logros en cada proceso *COBIT*.
4. Asegurar una conexión entre objetivos de control con categorías primarias de seguridad en TI y a bajo nivel establecer requisitos de seguridad en múltiples plataformas.
5. Incluir la referencia a guías que permiten la comprobación de respuestas de los usuarios considerando el estado de cada objetivo de control.

Muchas de las organizaciones que han incorporado actividades de gestión de TI han conseguido logros sobresalientes. Entre estas, el Banco de la Republica Oriental del Uruguay (BROU), la institución financiera más importante del país, con más de diez empleados CISA's (Certified Information Systems Audit.) en su plantilla de personal, apoyados en Cobit ha conseguido un valor significativo.

Además de BROU, también se puede citar a Ancap (compañía de aceites), Montevideo Stock Exchange, Tribunal de Cuentas y otras organizaciones que han deposito en el proyecto de Datasec su confianza para darle soporte nacional y seguir la investigación y aplicación de herramientas basadas en la estructura *COBIT* como apoyo a la oportunidad otorgada por PDT y el BID, bajo la tutela del Ministerio de Educación y Cultura de Uruguay.

Este antecedente, respalda la importancia de la estructura *COBIT* en el tratamiento del problema de control en la aplicación de la Tecnología de Información en las organizaciones.

Cubillos (2003), desarrolló el *Modelo de Evaluación de Riesgos AUDIRISK***,** titulado "Evaluacion de Riesgos Operacionales en Procesos de Negocio y Servicios Automatizados" en el cual se habla sobre la identificación y valoración de riesgos potenciales y expresa que para valorar o medir el nivel de exposición a riesgos potenciales en cualquier proceso de negocio o de tecnología de información o sistema sujeto a diseño de controles, es necesario tener en mente los siguientes supuestos:

1. Todos los riesgos aplicables al proceso o sistema sujeto a diseño de controles no son igualmente importantes, desde el punto de vista del impacto que podrían causar en caso de llegar a presentarse. Por consiguiente, para ser eficientes y efectivos en el proceso de diseño de controles, es necesario establecer prioridades para atacar los riesgos asociados con cada proceso o sistema.

2. Los recursos que se asignen para prevenir o mitigar los riesgos potenciales (tiempo, financieros, personas y tecnología) de cada proceso o sistema, deberían aplicarse con mayor énfasis a los riesgos críticos, es decir, a los que podrían generar las pérdidas o problemas operacionales más significativos en caso de presentarse.

3. Para priorizar los esfuerzos de protección que requieren los riesgos potenciales y definir los controles requeridos, es necesaria la participación de los funcionarios de niveles estratégico, táctico y operativo que intervienen en el manejo de las operaciones y la toma de decisiones en el negocio o sistema sujeto a diseño de controles.

Continúa el estudio, explicando que para establecer cuales riesgos pueden presentarse en cada proceso de negocio o sistema de información sujeto a diseño de controles, es necesario utilizar como punto de partida un modelo de riesgos típicos, de los varios que difunden y utilizan las asociaciones internacionales de profesionales en controles y Auditoría, las firmas de consultoría en seguridad, los analistas de riesgos y las firmas de auditores. También pueden utilizarse como punto de partida los diferentes modelos de riesgos existentes como son: (a) el modelo de FitzGerald J. (1991), (b) el modelo de Robert H. Courtney, publicado por el National Bureau of

Standard, (c) el modelo propuesto por el Instituto Canadiense de Contadores Públicos (CICA). (d) el modelo propuesto en el estudio SAC del Instituto de Auditores Internos de USA (IIA) y (e) el modelo *AUDIRISK*, propuesto por AUDISIS, su empresa. Este último utiliza como base el concepto que *"riesgo es el valor de las pérdidas que experimenta una organización como consecuencia de la ocurrencia de una ó más causas de riesgo o amenazas contra la seguridad"*, Cubillos (2003).

El modelo *AUDIRISK* agrupa el universo de riesgos potenciales en ocho (8) categorías de riesgos típicos. Estos son: (a) pérdidas por hurto / fraude, (b) pérdidas por daño y destrucción de activos, (c) pérdidas por sanciones legales, (d) pérdidas por baja credibilidad pública o pobre reputación, (e) pérdidas por desventaja competitiva, (f) pérdidas de ingresos por causas accidentales, (g) pérdidas por exceso de pagos, por causas accidentales, y (h) pérdidas por decisiones erróneas de la gerencia. La aplicabilidad de estas categorías de riesgo está comprobada para cualquier tipo de organización, sin importa r el tamaño, el sector a que pertenezcan y el grado de sofisticación tecnológica que presenten sus operaciones automatizadas.

Una ventaja que ofrece el reducido número de categorías de riesgo de este modelo es la facilidad y simplicidad de análisis. Entre mayor número de riesgos utilice el modelo, mayor será la complejidad del análisis y será menor la eficiencia en el trabajo de diseño o revisión de controles.

Este modelo, como los referenciados por él, permiten valorar y justificar el enfoque y nombre de *"modelo metodológico"* en los trabajos de investigación y desarrollo en esta área de aplicación de metodologías al proceso de Auditoría y Evaluación de Tecnologías de Información y en general en la Auditoría de Sistemas Informáticos.

Arima (1990), en su tesis doctoral de la Facultad de Economía, Administración y Contaduría de la Universidad de Sao Paulo, presenta la propuesta de un modelo metodológico y una herramienta automatizada de Auditoría de sistemas, enmarcado dentro del ciclo de vida del sistema de información de Contabilidad Computarizada

fundamentado en que el objetivo fundamental de la Auditoría de sistemas es como cita textualmente en el resumen "… revisar y evaluar el control interno de un determinado sistema de información…". El desenvolvimiento del modelo lo presenta constituido en seis etapas, a saber: (a) planeación del proyecto de Auditoría de sistemas de información, (b) levantamiento de información del sistema a ser auditado, (c) identificación e inventario de puntos de control, (d) priorización y selección de los puntos de control del sistema en Auditoría; (e) revisión y validación de los puntos de control, y (f) acompañamiento y/o conclusiones de la Auditoría. La propuesta automatizada requirió de un análisis funcional de la metodología que fue compuesta de los siguientes módulos: (a) administración de proyectos de Auditoría, (b) monitoreo de puntos de control, (c) aplicación de técnicas de Auditoría, y (d) gerencia de indicadores de Auditoría. En el modelo metodológico propuesto, los módulos indicados constituyen los programas de computación, aplicaciones, que deben permitir la estructuración y recuperación adecuada de información del banco de datos de la Auditoría, de acuerdo con las necesidades de operacionales del área auditada, también como de la alta administración relacionada.

Esta referencia permite observar que la propuesta de un *modelo metodológico* fundamentado en las variables, relaciones y procedimientos o procesos a desarrollar, puede plasmarse en una herramienta de software que permita demostrar la validez del modelo aplicado a cualquier organización, dado que todas las organizaciones que utilizan sistemas de información basados en TI manejan variables similares.

Bases Teóricas

El basamento teórico de la presente investigación se fundamenta en los conceptos y definiciones relativas o referenciadas al marco de aplicación de las tecnologías de información (TI) en las organizaciones. Si entendemos las TI como el conjunto de todos los elementos necesarios para la generación, establecimiento, uso y

evaluación de sistemas de información, y a esto añadimos todos los elementos necesarios para la evaluación y control de la seguridad de la información y la tecnología relacionada, tendremos todo el marco referencial teórico requerido.

Modelo

"*Un modelo puede ser definido como la representación idealizada de un sistema de la vida real"* UNA (1989). El sistema puede existir físicamente o ser una idea concebida que espera por su ejecución, como es el caso de un modelo propuesto para la evaluación, mediante su aplicación, de un sistema. En el primer caso, el objetivo del modelo es proveer los medios para analizar el comportamiento del sistema. "En el segundo caso, el objetivo es definir la estructura de un sistema futuro que incluya las interrelaciones funcionales entre sus componentes, y entre el sistema y su medio ambiente", UNA (ob. cit).

Los modelos pueden ser icónicos, representan el sistema mediante modelos a escala como un avión en un túnel de viento. Los modelos analógicos como las graficas en un plano cartesiano representan las distancias modeladas de los objetos ubicados relativamente. Los modelos simbólicos o matemáticos emplean símbolos para representar las variables de decisión del sistema y las relaciones entre las variables se representan por medio de funciones.

Un modelo también permite presentar un diseño esquematizado para seguir procesos por una línea de acción predefinida que permitan evaluar el comportamiento del sistema estudiado con la aplicación del modelo, como es el caso de los modelos metodológicos.

Metodología

Según el diccionario de la Lengua de la Real Academia Española (1939) "*método* es el modo de decir o hacer con orden una cosa". Asimismo define la palabra *metodología* como "conjunto de métodos que se siguen en una investigación

científica o en una exposición doctrinal". Esto significa que cualquier proceso científico debe estar sujeto a una disciplina de proceso definida con anterioridad y que es llamada metodología.

La informática ha sido tradicionalmente una materia compleja en todos sus aspectos, por lo que se hace necesaria la utilización de metodologías en cada doctrina que la componen, desde sus diseños de ingeniería hasta el desarrollo del software y la Auditoría de los sistemas de información.

Respecto a la aplicación de metodologías Piattini M., Del Peso E. (1998:45) expresan "Las metodologías usadas por un profesional dicen mucho de su forma de entender y hacer su trabajo, y están directamente relacionadas con su experiencia profesional acumulada como parte del comportamiento humano de acierto/error".

Las metodologías son necesarias para que los equipos de profesionales en áreas especificas del conocimiento alcancen resultados homogéneos tal como si lo hiciera uno solo, por lo que resulta habitual y practico el uso de metodologías siguiendo las practicas desarrolladas por los más expertos, para conseguir resultados homogéneos en equipos de trabajo heterogéneos.

Auditoría

La Auditoría en su acepción más general y original es definida por el diccionario General de la lengua Española VOX como el "Proceso que recurre al examen de libros, cuentas y registros de una empresa para precisar si es correcto el estado financiero de la misma, y si los comprobantes están debidamente presentados".

Este concepto de Auditoría se ajusta más a la aplicación del área contable financiera que a las áreas técnicas como la informática y los sistemas de información, sin embargo, el objetivo de control general de salvaguarda de los activos empresariales esta explicito en él y por tanto es aplicable a la información.

Según Echenique (1985) es frecuente encontrar la palabra *auditoría* empleada incorrectamente y considerada como una evaluación cuyo único fin es detectar errores y señalar fallas; por eso se ha llegado a acuñar la frase "tiene *auditoría*" como

sinónimo de que, desde antes de realizarse, ya se encontraron fallas y por lo tanto se está haciendo la auditoría. El concepto de auditoría es más amplio; no sólo detecta errores, sino que es un examen crítico que se realiza con objeto de evaluar la eficiencia y eficacia de una sección o de un organismo.

Un concepto más actualizado y generalizado, aplicable a los diferentes tipos de Auditoría, es el emitido por Piattini y Del Peso (1998):

> *"Conceptualmente la auditoría, toda y cualquier auditoría, es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas".*

En general, la palabra Auditoría viene del latín auditórius, y de esta proviene auditor, que tiene la virtud de oír, y el diccionario lo define como "revisor de cuentas colegiado". El auditor tiene la virtud de oír y revisar cuentas, pero debe estar encaminado a un objetivo especifico que es la evaluación de la eficiencia y la eficacia de las operaciones del negocio, para señalar cursos alternativos de acción que apoyen la toma de decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.

Esta orientación de la función de auditoría es la que justifica el desarrollo de metodologías y modelos de aplicación de evaluación y auditorías en general y de auditorías de información, en particular, por cuanto, como se conoce, la información constituye un activo de singular valor para las organizaciones.

La descomposición del concepto de Auditoría, permite obtener los elementos fundamentales presentados en el **Cuadro 1**.

Cuadro 1

Elementos Fundamentales del Concepto de Auditoría

Elemento	Característica
1) Contenido:	Una **opinión**
2) Condición:	**Profesional**
3) Justificación:	Sustentada en determinados **procedimientos**
4) Objeto:	Una determinada **información** obtenida en un cierto soporte
5) Finalidad:	Determinar si presenta adecuadamente la realidad o ésta responde a las expectativas que le son atribuidas, es decir, su **fiabilidad**

Nota: Análisis conceptual de elementos tomado de Piattini y Del Peso (1998)

En general y en todo caso, la auditoría es una función que se realiza a posteriori, respecto a procesos o actividades ya ejecutados o realizadas, sobre las que hay que emitir una opinión.

Clases de Auditoría

Los elementos 4) y 5) del concepto anterior presentado en el **Cuadro 1**, distinguen de que clase o tipo de Auditoría se trata. El objeto sometido a estudio, sea cual sea su soporte y la finalidad con que se realiza el estudio, definen el tipo de Auditoría de que se trata. Ilustrativamente, Piattini y Del Peso (1998) presentan la clasificación mostrada en el **Cuadro 2**, a continuación:

Cuadro 2

Clases de Auditoría

Clase	Contenido	Objeto	Finalidad
Financiera	Opinión	Cuentas anuales	Presentan realidad
Informática	Opinión	Sistemas de aplicación, recursos informáticos, planes de contingencia, otros	Operatividad eficiente y según normas establecidas
Gestión	Opinión	Dirección	Eficacia, eficiencia, economicidad
Cumplimiento	Opinión	Normas establecidas	Las operaciones se adecuan a estas normas

Nota: Clasificación tomada de Piattini y Del Peso (1998)

Informática

El concepto de informática es más amplio que el simple uso de equipos de cómputo o bien de procesos electrónicos. Etimológicamente, la palabra informática, deriva del francés *informatique*. Este neologismo proviene de la conjunción de *information* (información), y *automatique* (automática). Según la CIFCA (1983), su creación fue estimulada por la intención de dar una alternativa menos tecnocrática y menos mecanicista al concepto de *proceso de datos.*

Hacia principios de los años setenta ya eran claras las limitaciones de esta definición, sobre todo por el hincapié en el uso de las maquinas. El principal esfuerzo por redefinir el concepto de informática lo realizo en esa época el IBI, Oficina Intergubernamental de Informática, en aquel tiempo órgano asociado a la UNESCO, que formuló la definición: “Aplicación racional, sistemática de la información para el desarrollo económico, social y político….ciencia de la política de la información”, IBI-UNESCO (1975).

Este último concepto tiene especial importancia por el realce y enfoque social del valor de la información, lo cual redunda en la justificación de la necesidad de los procesos de auditoría informática en las organizaciones como mecanismos de control y aseguramiento de la calidad de la información.

Dato e Información

Es común confundir el concepto de dato con el de información. La información es una serie de datos clasificados y ordenados con un objetivo común y con un significado dentro de un contexto particular. El dato se refiere únicamente a un símbolo, signo, abstracción o a una serie de signos, letras o números sin significado de extensión o contexto. El proyecto *COBIT*, ISACF (1996), considera a los datos en sentido más amplio como todos los objetos de información. Considera información interna y externa, estructurada o no, gráficas, sonidos y otras representaciones concretas.

En general la información esta orientada a reducir la incertidumbre del receptor y tiene características de poder duplicarse prácticamente sin costo, y no se gasta, no existe por si misma, sino que debe expresarse en algún objeto explicito (papel, cinta, video, otros); de otra manera puede desaparecer o deformarse como sucede con la comunicación oral, la cual hace que la información deba ser controlada debidamente por medio de adecuados sistemas de seguridad, confidencialidad y respaldo, surgiendo el importante concepto de *control de la información*.

El control de la información debe asegurar que esta pueda comunicarse, y para ello hay que lograr que los medios de seguridad sean llevados a cabo después de un adecuado examen sobre la forma de transmisión, la eficiencia de los canales de comunicación, el transmisor, el receptor, el contenido de la comunicación, la redundancia y el ruido. Todos estos aspectos son relevantes en los procesos de Evaluación y Auditoría de la Información y de las Tecnologías que soportan el proceso de la misma.

COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas)

El proyecto de investigación ***COBIT*** de **ISACF (1996),** representa la base teórica fundamental del presente trabajo sobre el modelo metodológico de auditoría de información y tecnologías relacionadas; en este sentido y tal como se presentó en los antecedentes, los conceptos, aspectos y componentes de la estructura *COBIT* representan la piedra angular. Los demás conceptos o bases teóricas que no se independizan en este trabajo están inmersos en la estructura *COBIT* que se presenta a continuación.

COBIT es una herramienta de gobierno (administración) de TI que ha cambiado la forma en que trabajan los profesionales de TI vinculando tecnología informática y prácticas de control, *COBIT* consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, mini computadoras y ambientes distribuidos. Esta basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos. Según cita la propia ISACF en la publicación oficial del Marco Referencial *COBIT* (Cobit FrameWork) su misión es: *"Investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de información con autoridad, actualizados, de carácter internacional y generalmente aceptados para el uso cotidiano de gerentes de empresas y auditores"*. *COBIT* esta dirigido a múltiples usuarios:

1. **La Gerencia:** para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.
2. **Los Usuarios Finales:** quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.

3. **Los Auditores:** para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido.
4. **Los Responsables de TI:** para identificar los controles que requieren en sus áreas. También puede ser utilizado dentro de las empresas por el responsable de un proceso de negocio en su responsabilidad de controlar los aspectos de información del proceso, y por todos aquellos con responsabilidades en el campo de la TI en las empresas.

Las principales características de *COBIT* son: (a) orientado al negocio, (b) alineado con estándares y regulaciones "de facto", (c) basado en una revisión crítica y analítica de las tareas y actividades en TI, (c) alineado con estándares de control y auditoría como (COSO, IFAC, IIA, ISACA, AICPA), (d) los principios básicos de *COBIT,* **Gráfico 1,** están fundamentados en el enfoque del control en TI que se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con las TI que deben ser administrados por procesos de TI. A continuación se presentan las bases teóricas de la estructura *COBIT* que fundamentan el desarrollo del presente estudio.

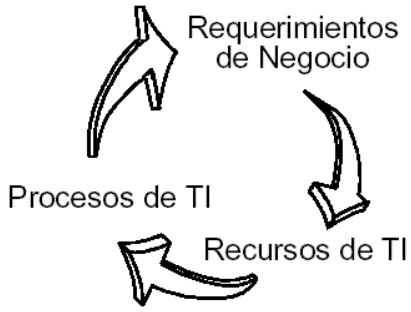


Gráfico 1. Relación de los Principios Básicos de COBIT.
Fuente: Marco Referencial COBIT. ISACF (2000)

Requerimientos de Información COBIT (ob. cit.)

Los *requerimientos de la información* del negocio se definen como los criterios que la información necesita satisfacer para alcanzar los requerimientos del negocio. Estos criterios son: (a) *requerimientos de calidad*: - calidad, costo y entrega -, (b) *requerimientos fiduciarios*: - efectividad y eficiencia operacional, confiabilidad de los reportes financieros y cumplimiento de leyes y regulaciones -, y (c) *requerimientos de seguridad*: - confidencialidad, integridad y disponibilidad -. Estos requerimientos de información del negocio explicados por *COBIT* se definen como:

1. **Efectividad**: La información debe ser relevante y pertinente para los procesos del negocio y debe ser proporcionada en forma oportuna, correcta, consistente y utilizable.
2. **Eficiencia:** Se debe proveer información mediante el empleo óptimo de los recursos (la forma más productiva y económica).
3. **Confiabilidad:** proveer la información apropiada para que la administración tome las decisiones adecuadas para manejar la empresa y cumplir con sus responsabilidades.
4. **Cumplimiento:** de las leyes, regulaciones y compromisos contractuales con los cuales está comprometida la empresa.
5. **Confidencialidad**: Protección de la información sensible contra divulgación no autorizada
6. **Integridad:** Refiere a lo exacto y completo de la información así como a su validez de acuerdo con las expectativas de la empresa.
7. **Disponibilidad:** accesibilidad a la información cuando sea requerida por los procesos del negocio y la salvaguarda de los recursos y capacidades asociadas a la misma.

No todos los anteriores requerimientos de información son satisfechos o tienen impacto en el mismo grado por los diferentes objetivos de control de alto nivel: COBIT clasifica este grado de relación como:

1. **Primario (P):** es el grado al cual el objetivo de control definido impacta directamente el requerimiento de información de interés.

2. **Secundario (S):** es el grado al cual el objetivo de control definido satisface únicamente de forma indirecta o en menor medida el requerimiento de información de interés.
3. **Blanco (vacío):** podría aplicarse; sin embargo, los requerimientos son satisfechos más apropiadamente por otro criterio en este proceso y/o por otro proceso.

Recursos de TI COBIT (op. cit.)

COBIT establece los siguientes recursos en TI necesarios para alcanzar los objetivos de negocio:

1. **Recurso Humano:** Por la habilidad, conciencia y productividad del personal para planear, adquirir, prestar servicios, dar soporte y monitorear los sistemas de Información.
2. **Datos**: Todos los objetos de información. Considera información interna y externa, estructurada o no, gráficas, sonidos y otros objetos.
3. **Aplicaciones:** entendido como los sistemas de información, que integran procedimientos manuales y sistematizados.
4. **Tecnología:** incluye hardware y software básico, sistemas operativos, sistemas de administración de bases de datos, de redes, telecomunicaciones, multimedia, etc.
5. **Instalaciones:** Incluye los recursos necesarios para alojar y dar soporte a los sistemas de información.

Los procesos de negocio requieren de información, la cual a su vez es producida por un conjunto de recursos de TI. Con el fin de asegurar que los requerimientos de negocio para la información son satisfechos, deben definirse, implementarse y monitorearse medidas de control para estos recursos y procesos asociados. Estas relaciones se presentan en el **Gráfico 2** en la página siguiente.

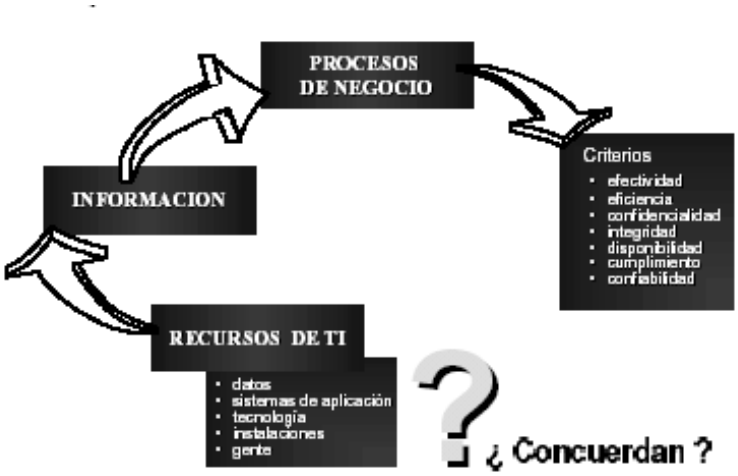


Gráfico 2: Información, Recursos de TI y Procesos del Negocio.
Fuente: Marco Referencial COBIT. ISACF (2000)

Procesos de TI (ob. cit.)

La estructura de COBIT se define a partir de una premisa simple y pragmática: "Los recursos de las Tecnologías de la Información (TI) se han de gestionar mediante un conjunto de procesos agrupados de forma natural para que proporcionen la información que la empresa necesita para alcanzar sus objetivos" (ob. cit.). *COBIT* se divide en tres niveles: Dominios, Procesos y Actividades:

1. **Dominios:** Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.
2. **Procesos**: Conjuntos o series de actividades unidas con delimitación o cortes de control.
3. **Actividades**: Acciones requeridas para lograr un resultado medible. Se definen 34 objetivos de control generales, uno para cada uno de los procesos de las TI. El **Gráfico 3** muestra la relación entre dominios, procesos y actividades.

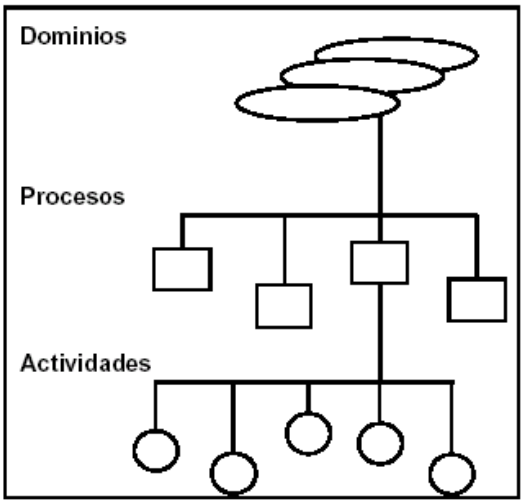


Gráfico 3. Relación de Dominios, Procesos y Actividades COBIT.
Fuente: Marco Referencial COBIT. ISACF (2000)

Dominios COBIT (ob. cit.)

Dominio: Planificación y Organización (PO). Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas. Los procesos de este dominio son:

PO1: Definición de un plan estratégico. Lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, para asegurar sus logros futuros. Su realización se concreta a través un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo, los que deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo, teniendo en cuenta:

1. La definición de objetivos de negocio y necesidades de TI, la alta gerencia será la responsable de desarrollar e implementar planes a largo y corto plazo que satisfagan la misión y las metas generales de la organización.
2. El inventario de soluciones tecnológicas e infraestructura actual, se deberá evaluar los sistemas existentes en términos de: nivel de automatización de negocio, funcionalidad, estabilidad, complejidad, costo y fortalezas y debilidades, con el propósito de determinar el nivel de soporte que reciben los requerimientos del negocio de los sistemas existentes.
3. Los cambios organizacionales, se deberá asegurar que se establezca un proceso para modificar oportunamente y con precisión el plan a largo plazo de tecnología de información con el fin de adaptar los cambios al plan a largo plazo de la organización y los cambios en las condiciones de la TI
4. Estudios de factibilidad oportunos, para que se puedan obtener resultados efectivos

PO2: Definición de la arquitectura de información. Satisfacer los requerimientos de negocio, organizando de la mejor manera posible los sistemas de información, a través de la creación y mantenimiento de un modelo de información de negocio, asegurándose que se definan los sistemas apropiados para optimizar la utilización de esta información, tomando en consideración:

1. La documentación deberá conservar consistencia con las necesidades permitiendo a los responsables llevar a cabo sus tareas eficiente y oportunamente.
2. El diccionario de datos, el cual incorporara las reglas de sintaxis de datos de la organización y deberá ser continuamente actualizado.
3. La propiedad de la información y la clasificación de severidad con el que se establecerá un marco de referencia de clasificación general relativo a la ubicación de datos en clases de información.

PO3: Determinación de la dirección tecnológica. Aprovechar al máximo la tecnología disponible o tecnología emergente, satisfaciendo los requerimientos de

negocio, a través de la creación y mantenimiento de un plan de infraestructura tecnológica, tomando en consideración:

1. La capacidad de adecuación y evolución de la infraestructura actual, que deberá concordar con los planes a largo y corto plazo de tecnología de información y debiendo abarcar aspectos tales como arquitectura de sistemas, dirección tecnológica y estrategias de migración.
2. El monitoreo de desarrollos tecnológicos que serán tomados en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.
3. Las contingencias (por ejemplo, redundancia, resistencia, capacidad de adecuación y evolución de la infraestructura), con lo que se evaluará sistemáticamente el plan de infraestructura tecnológica.
4. Planes de adquisición, los cuales deberán reflejar las necesidades identificadas en el plan de infraestructura tecnológica.

PO4: Definición de la organización y de las relaciones de TI. Prestación de servicios de TI. Esto se realiza por medio de una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas, teniendo en cuenta:

1. El comité de dirección el cual se encargara de vigilar la función de servicios de información y sus actividades.
2. Propiedad, custodia, la Gerencia deberá crear una estructura para designar formalmente a los propietarios y custodios de los datos. Sus funciones y responsabilidades deberán estar claramente definidas.
3. Supervisión, para asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente
4. Segregación de funciones, con la que se evitará la posibilidad de que un solo individuo resuelva un proceso crítico.

5. Los roles y responsabilidades, la gerencia deberá asegurarse de que todo el personal deberá conocer y contar con la autoridad suficiente para llevar a cabo las funciones y responsabilidades que le hayan sido asignadas
6. La descripción de puestos, deberá delinear claramente tanto la responsabilidad como la autoridad, incluyendo las definiciones de las habilidades y la experiencia necesarias para el puesto, y ser adecuadas para su utilización en evaluaciones de desempeño.
7. Los niveles de asignación de personal, deberán hacerse evaluaciones de requerimientos regularmente para asegurar para asegurar una asignación de personal adecuada en el presente y en el futuro.
8. El personal clave, la gerencia deberá definir e identificar al personal clave de tecnología de información.

PO5: Manejo de la inversión. Tiene como finalidad la satisfacción de los requerimientos de negocio, asegurando el financiamiento y el control de desembolsos de recursos financieros. Su realización se concreta a través presupuestos periódicos sobre inversiones y operaciones establecidas y aprobados por el negocio, teniendo en cuenta:

1. Las alternativas de financiamiento, se deberán investigar diferentes alternativas de financiamiento.
2. El control del gasto real, se deberá tomar como base el sistema de contabilidad de la organización, mismo que deberá registrar, procesar y reportar rutinariamente los costos asociados con las actividades de la función de servicios de información
3. La justificación de costos y beneficios, deberá establecerse un control gerencial que garantice que la prestación de servicios por parte de la función de servicios de información se justifique en cuanto a costos. Los beneficios derivados de las actividades de TI deberán ser analizados en forma similar.

PO6: Comunicación de los objetivos y directivas de la alta gerencia. Asegura el conocimiento y comprensión de los usuarios sobre las aspiraciones del alto nivel (gerencia), se concreta a través de políticas establecidas y transmitidas a la

comunidad de usuarios, necesitándose para esto estándares para traducir las opciones estratégicas en reglas de usuario prácticas y utilizables. Toma en cuenta:

1. Los código de ética / conducta, el cumplimiento de las reglas de ética, conducta, seguridad y estándares de control interno deberá ser establecido por la Alta Gerencia y promoverse a través del ejemplo.
2. Las directrices tecnológicas
3. El cumplimiento, la Gerencia deberá también asegurar y monitorear la duración de la implementación de sus políticas.
4. El compromiso con la calidad, la Gerencia de la función de servicios de información deberá definir, documentar y mantener una filosofía de calidad, debiendo ser comprendidos, implementados y mantenidos por todos los niveles de la función de servicios de información.
5. Las políticas de seguridad y control interno, la alta gerencia deberá asegurar que esta política de seguridad y de control interno especifique el propósito y los objetivos, la estructura gerencial, el alcance dentro de la organización, la definición y asignación de responsabilidades para su implementación a todos los niveles y la definición de multas y de acciones disciplinarias asociadas con la falta de cumplimiento de estas políticas.

PO7: Administración de recursos humanos. Maximizar las contribuciones del personal a los procesos de TI, satisfaciendo así los requerimientos de negocio, a través de técnicas sólidas para administración de personal, tomando en consideración:

1. El reclutamiento y promoción, deberá tener como base criterios objetivos, considerando factores como la educación, la experiencia y la responsabilidad.
2. Los requerimientos de calificaciones, el personal deberá estar calificado, tomando como base una educación, entrenamiento y o experiencia apropiados, según se requiera
3. La capacitación, los programas de educación y entrenamiento estarán dirigidos a incrementar los niveles de habilidad técnica y administrativa del personal.

4. La evaluación objetiva y medible del desempeño, se deberá asegurar que dichas evaluaciones sean llevada a cabo regularmente según los estándares establecidos y las responsabilidades específicas del puesto. Los empleados deberán recibir asesoría sobre su desempeño o su conducta cuando esto sea apropiado.

PO8: Asegurar el cumplimiento de los requerimientos externos. Cumplir con obligaciones legales, regulatorias y contractuales. Para ello se realiza una identificación y análisis de los requerimientos externos en cuanto a su impacto en TI, llevando a cabo las medidas apropiadas para cumplir con ellos y se toma en consideración:

1. Definición y mantenimiento de procedimientos para la revisión de requerimientos externos, para la coordinación de estas actividades y para el cumplimiento continúo de los mismos.
2. Leyes, regulaciones y contratos
3. Revisiones regulares en cuanto a cambios
4. Búsqueda de asistencia legal y modificaciones
5. Seguridad y ergonomía con respecto al ambiente de trabajo de los usuarios y el personal de la función de servicios de información.
6. Privacidad
7. Propiedad intelectual
8. Flujo de datos externos y criptografía

PO9: Evaluación de riesgos. Asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI. Para ello se logra la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos y se toma en consideración:

1. Identificación, definición y actualización regular de los diferentes tipos de riesgos de TI de manera de que se pueda determinar como los riesgos deben ser manejados a un nivel aceptable.

2. Definición de alcances, limites de los riesgos y la metodología para las evaluaciones de los riesgos.
3. Actualización de evaluación de riesgos
4. Metodología de evaluación de riesgos
5. Medición de riesgos cualitativos y/o cuantitativos
6. Definición de un plan de acción contra los riesgos para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continúa.
7. Aceptación de riesgos dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y de que tan económico resulte implementar protecciones y controles.

PO10: Administración de proyectos. Establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión. Para ello se realiza una identificación y priorización de los proyectos en línea con el plan operacional por parte de la misma organización. Además, la organización deberá adoptar y aplicar sólidas técnicas de administración de proyectos para cada proyecto emprendido y se toma en consideración:

1. Definición de un marco de referencia general para la administración de proyectos que defina el alcance y los límites del mismo, así como la metodología de administración de proyectos a ser adoptada y aplicada para cada proyecto emprendido. La metodología deberá cubrir, como mínimo, la asignación de responsabilidades, la determinación de tareas, la realización de presupuestos de tiempo y recursos, los avances, los puntos de revisión y las aprobaciones.
2. El involucramiento de los usuarios en el desarrollo, implementación o modificación de los proyectos.
3. Asignación de responsabilidades y autoridades a los miembros del personal asignados al proyecto.

4. Aprobación de fases de proyecto por parte de los usuarios antes de pasar a la siguiente fase.
5. Presupuestos de costos y horas hombre
6. Planes y metodologías de aseguramiento de calidad que sean revisados y acordados por las partes interesadas.
7. Plan de administración de riesgos para eliminar o minimizar los riesgos.
8. Planes de prueba, entrenamiento, revisión post-implementación.

PO11: Administración de calidad. Satisfacer los requerimientos del cliente. Para ello se realiza una planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por parte de la organización y se toma en consideración:

1. Definición y mantenimiento regular del plan de calidad, el cual deberá promover la filosofía de mejora continua y contestar a las preguntas básicas de qué, quién y cómo.
2. Responsabilidades de aseguramiento de calidad que determine los tipos de actividades de aseguramiento de calidad tales como revisiones, Auditorías, inspecciones, etc. que deben realizarse para alcanzar los objetivos del plan general de calidad.
3. Metodologías del ciclo de vida de desarrollo de sistemas que rija el proceso de desarrollo, adquisición, implementación y mantenimiento de sistemas de información.
4. Documentación de pruebas de sistemas y programas
5. Revisiones y reportes de aseguramiento de calidad

Dominio: Adquisición e Implementación (AI). Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes. Sus procesos son:

AI1: Identificación de soluciones automatizadas. Asegurar el mejor enfoque para cumplir con los requerimientos del usuario. Para ello se realiza un análisis claro de las oportunidades alternativas comparadas contra los requerimientos de los usuarios y toma en consideración:

1. Definición de requerimientos de información para poder aprobar un proyecto de desarrollo.
2. Estudios de factibilidad con la finalidad de satisfacer los requerimientos del negocio establecidos para el desarrollo de un proyecto.
3. Arquitectura de información para tener en consideración el modelo de datos al definir soluciones y analizar la factibilidad de las mismas.
4. Seguridad con relación de costo-beneficio favorable para controlar que los costos no excedan los beneficios.
5. Pistas de Auditoría para ello deben existir mecanismos adecuados. Dichos mecanismos deben proporcionar la capacidad de proteger datos sensitivos (ej. Identificación de usuarios contra divulgación o mal uso)
6. Contratación de terceros con el objeto de adquirir productos con buena calidad y excelente estado.
7. Aceptación de instalaciones y tecnología a través del contrato con el Proveedor donde se acuerda un plan de aceptación para las instalaciones y tecnología especifica a ser proporcionada.

AI2: Adquisición y mantenimiento de software de Aplicación. Proporciona funciones automatizadas que soporten efectivamente al negocio. Para ello se definen declaraciones específicas sobre requerimientos funcionales y operacionales y una implementación estructurada con entregables claros y se toma en consideración:

1. Requerimientos de usuarios, para realizar un correcto análisis y obtener un software claro y fácil de usar.
2. Requerimientos de archivo, entrada, proceso y salida.
3. Interfase usuario-maquina asegurando que el software sea fácil de utilizar y que sea capaz de auto documentarse.
4. Personalización de paquetes

5. Realizar pruebas funcionales (unitarias, de aplicación, de integración y de carga y estrés), de acuerdo con el plan de prueba del proyecto y con los estándares establecidos antes de ser aprobado por los usuarios.
6. Controles de aplicación y requerimientos funcionales
7. Documentación (materiales de consulta y soporte para usuarios) con el objeto de que los usuarios puedan aprender a utilizar el sistema o puedan sacarse todas aquellas inquietudes que se les puedan presentar.

AI3: Adquisición y mantenimiento de la infraestructura tecnológica. Proporcionar las plataformas apropiadas para soportar aplicaciones de negocios. Para ello se realizara una evaluación del desempeño del hardware y software, la provisión de mantenimiento preventivo de hardware y la instalación, seguridad y control del software del sistema y toma en consideración:

1. Evaluación de tecnología para identificar el impacto del nuevo hardware o software sobre el rendimiento del sistema general.
2. Mantenimiento preventivo del hardware con el objeto de reducir la frecuencia y el impacto de fallas de rendimiento.
3. Seguridad del software de sistema, instalación y mantenimiento para no arriesgar la seguridad de los datos y programas ya almacenados en el mismo.

AI4: Procedimientos de Desarrollo y Mantenimiento. Asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas. Para ello se realiza un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento y toma en consideración:

1. Manuales de procedimientos de usuarios y controles, de manera que los mismos permanezcan en permanente actualización para el mejor desempeño y control de los usuarios.
2. Manuales de Operaciones y controles, de manera que estén en permanente actualización.

3. Materiales de entrenamiento enfocados al uso del sistema en la práctica diaria.

AI5: Instalación y aceptación de sistemas. Verificar y confirmar que la solución sea adecuada para el propósito deseado. Para ello se realiza una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas y toma en consideración:

1. Capacitación del personal de acuerdo al plan de entrenamiento definido y los materiales relacionados.
2. Conversión / carga de datos, de manera que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo.
3. Pruebas específicas (cambios, desempeño, aceptación final, operacional) con el objeto de obtener un producto satisfactorio.
4. Acreditación de manera que la Gerencia de operaciones y usuaria acepten los resultados de las pruebas y el nivel de seguridad para los sistemas, junto con el riesgo residual existente.
5. Revisiones post implementación con el objeto de reportar si el sistema proporciono los beneficios esperados de la manera mas económica.

AI6: Administración de cambios. Minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores. Esto se hace posible a través de un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de TI actual y toma en consideración:

1. Identificación de cambios tanto internos como por parte de proveedores
2. Procedimientos de categorización, priorización y emergencia de solicitudes de cambios.
3. Evaluación del impacto que provocaran los cambios.
4. Autorización de cambios
5. Manejo de liberación de manera que la liberación de software este regida por procedimientos formales asegurando aprobación, empaque, pruebas de regresión, entrega, etc.

6. Distribución de software, estableciendo medidas de control especificas para asegurar la distribución de software correcto al lugar correcto, con integridad y de manera oportuna.

Dominio: Entrega y Soporte (DS: Delivery & Support). En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación. Comprende los siguientes procesos:

DS1: Definición de niveles de servicio. Establecer una comprensión común del nivel de servicio requerido. Para ello se establecen convenios de niveles de servicio que formalicen los criterios de desempeño contra los cuales se medirá la cantidad y la calidad del servicio y se toma en consideración:

1. Convenios formales que determinen la disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario, plan de contingencia / recuperación, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambio.
2. Definición de las responsabilidades de los usuarios y de la función de servicios de información
3. Procedimientos de desempeño que aseguren que la manera y las responsabilidades sobre las relaciones que rigen el desempeño entre todas las partes involucradas sean establecidas, coordinadas, mantenidas y comunicadas a todos los departamentos afectados.
4. Definición de dependencias asignando un Gerente de nivel de Servicio que sea responsable de monitorear y reportar los alcances de los criterios de

desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento.

5. Provisiones para elementos sujetos a cargos en los acuerdos de niveles de servicio para hacer posibles comparaciones y decisiones de niveles de servicios contra su costo.
6. Garantías de integridad
7. Convenios de confidencialidad
8. Implementación de un programa de mejoramiento del servicio.

DS2: Administración de servicios prestados por terceros. Asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos. Para ello se establecen medidas de control dirigidas a la revisión y monitoreo de contratos y procedimientos existentes, en cuanto a su efectividad y suficiencia, con respecto a las políticas de la organización y toma en consideración:

1. Acuerdos de servicios con terceras partes a través de contratos entre la organización y el proveedor de la administración de instalaciones este basado en niveles de procesamiento requeridos, seguridad, monitoreo y requerimientos de contingencia, así como en otras estipulaciones según sea apropiado.
2. Acuerdos de confidencialidad. Además, se deberá calificar a los terceros y el contrato deberá definirse y acordarse para cada relación de servicio con un proveedor.
3. Requerimientos legales regulatorios de manera de asegurar que estos concuerde con los acuerdos de seguridad identificados, declarados y acordados.
4. Monitoreo de la entrega de servicio con el fin de asegurar el cumplimiento de los acuerdos del contrato.

DS3: Administración de capacidad y desempeño del sistema. Asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado. Para ello se realizan controles de manejo de

capacidad y desempeño que recopilen datos y reporten acerca del manejo de cargas de trabajo, tamaño de aplicaciones, manejo y demanda de recursos y toma en consideración:

1. Requerimientos de disponibilidad y desempeño de los servicios de sistemas de información
2. Monitoreo y reporte de los recursos de tecnología de información
3. Utilizar herramientas de modelado apropiadas para producir un modelo del sistema actual para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de configuración, desempeño y disponibilidad.
4. Administración de capacidad estableciendo un proceso de planeación para la revisión del desempeño y capacidad de hardware con el fin de asegurar que siempre exista una capacidad justificable económicamente para procesar cargas de trabajo con cantidad y calidad de desempeño
5. Prevenir que se pierda la disponibilidad de recursos mediante la implementación de mecanismos de tolerancia de fallas, de asignación equitativos de recursos y de prioridad de tareas.

DS4: Aseguramiento de la Calidad del Servicio. Mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones. Para ello se tiene un plan de continuidad probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio y toma en consideración:

1. Planificación de Severidad
2. Plan Documentado
3. Procedimientos Alternativos
4. Respaldo y Recuperación
5. Pruebas y entrenamiento sistemático y singulares

DS5: Establecimiento de pautas para la seguridad de sistemas. Salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida. Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados y toma en consideración:

1. el acceso lógico junto con el uso de los autenticación y Autorización, recursos de TI deberá restringirse a través de la instrumentación de mecanismos de autenticación de usuarios identificados y recursos asociados con las reglas de acceso
2. Perfiles e identificación de usuarios estableciendo procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario
3. Administración de llaves criptográficas definiendo implementando procedimientos y protocolos a ser utilizados en la generación, distribución, certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas con el fin de asegurar la protección de las mismas
4. Manejo, reporte y seguimiento de incidentes implementado capacidad para la atención de los mismos
5. Prevención y detección de virus tales como Caballos de Troya, estableciendo adecuadas medidas de control preventivas, detectivas y correctivas.
6. Firewalls si existe una conexión con Internet u otras redes de Utilización públicas en la organización

DS6: Identificación e imputación de costos. Asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados. Para ello se realiza un plan completo de entrenamiento y desarrollo y se toma en consideración:

1. Currículo de entrenamiento estableciendo y manteniendo procedimientos para identificar y documentar las necesidades de entrenamiento de todo el personal que haga uso de los servicios de información
2. Campañas de toma de conciencia, definiendo los grupos objetivos, identificar y asignar entrenadores y organizar oportunamente las sesiones de entrenamiento

3. Técnicas de toma de conciencia proporcionando un programa de educación y entrenamiento que incluya conducta ética de la función de servicios de información

DS7: Educación y capacitación de los usuarios. Asegurar un conocimiento correcto de los costos atribuibles a los servicios de TI. Para ello se realiza un sistema de contabilidad de costos que asegure que éstos sean registrados, calculados y asignados a los niveles de detalle requeridos y toma en consideración:

1. Los elementos sujetos a cargo deben ser recursos identificables, medibles y predecibles para los usuarios
2. Procedimientos y políticas de cargo que fomenten el uso apropiado de los recursos de computo y aseguren el trato justo de los departamentos usuarios y sus necesidades
3. Tarifas definiendo e implementando procedimientos de costeo de prestar servicios, para ser analizados, monitoreados, evaluados asegurando al mismo tiempo la economía

DS8: Asistencia y asesoramiento a los clientes de TI. Asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente. Para ello se realiza un Buró de ayuda que proporcione soporte y asesoría de primera línea y toma en consideración:

1. Consultas de usuarios y respuesta a problemas estableciendo un soporte de una función de buró de ayuda
2. Monitoreo de consultas y despacho estableciendo procedimientos que aseguren que las preguntas de los clientes que pueden ser resueltas sean reasignadas al nivel adecuado para atenderlas
3. Análisis y reporte de tendencias adecuado de las preguntas de los clientes y su solución, de los tiempos de respuesta y la identificación de tendencias

DS9: Administración de la configuración. Dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios. Para ello se realizan

controles que identifiquen y registren todos los activos de TI así como su localización física y un programa regular de verificación que confirme su existencia y toma en consideración:

1. Registro de activos estableciendo procedimientos para asegurar que sean registrados únicamente elementos de configuración autorizados e identificables en el inventario, al momento de adquisición
2. Administración de cambios en la configuración asegurando que los registros de configuración reflejen el status real de todos los elementos de la configuración
3. Chequeo de software no autorizado revisando periódicamente las computadoras personales de la organización
4. Controles de almacenamiento de software definiendo un área de almacenamiento de archivos para todos los elementos de software válidos en las fases del ciclo de vida de desarrollo de sistemas

DS10 Administración de problemas e incidentes. Asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir que vuelvan a suceder. Para ello se necesita un sistema de manejo de problemas que registre y dé seguimiento a todos los incidentes, además de un conjunto de procedimientos de escalamiento de problemas para resolver de la manera más eficiente los problemas identificados. Este sistema de administración de problemas deberá también realizar un seguimiento de las causas a partir de un incidente dado.

DS11 Administración de datos. Asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento. Lo cual se logra a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI. Para tal fin, la gerencia deberá diseñar formatos de entrada de datos para los usuarios de manera que se minimicen lo errores y las omisiones durante la creación de los datos.

Este proceso deberá controlar los documentos fuentes (de donde se extraen los datos), de manera que estén completos, sean precisos y se registren apropiadamente. Se deberán crear también procedimientos que validen los datos de entrada y corrijan o

detecten los datos erróneos, como así también procedimientos de validación para transacciones erróneas, de manera que éstas no sean procesadas. Cabe destacar la importancia de crear procedimientos para el almacenamiento, respaldo y recuperación de datos, teniendo un registro físico (discos, disquetes, CDs y cintas magnéticas) de todas las transacciones y datos manejados por la organización, albergados tanto dentro como fuera de la empresa.

La gerencia deberá asegurar también la integridad, autenticidad y confidencialidad de los datos almacenados, definiendo e implementando procedimientos para tal fin.

DS12: Administración de las instalaciones. Proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivos) o fallas humanas lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que provean control de acceso del personal a las instalaciones y contemplen su seguridad física.

DS13: Administración de las operaciones. Asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada. Esto se logra a través de una programación de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades. Para ello, la gerencia deberá establecer y documentar procedimientos para las operaciones de tecnología de información (incluyendo operaciones de red), los cuales deberán ser revisados periódicamente para garantizar su eficiencia y cumplimiento.

Dominio: Monitoreo (M). Todos los procesos de una organización necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad. Este es, precisamente, el ámbito de este dominio. Este dominio comprende los siguientes procesos:

M1: Monitoreo del proceso. Asegurar el logro de los objetivos establecidos para los procesos de TI. Lo cual se logra definiendo por parte de la gerencia reportes e indicadores de desempeño gerenciales y la implementación de sistemas de soporte

así como la atención regular a los reportes emitidos. Para ello la gerencia podrá definir indicadores claves de desempeño y/o factores críticos de éxito y compararlos con los niveles objetivos propuestos para evaluar el desempeño de los procesos de la organización. La gerencia deberá también medir el grado de satisfacción del los clientes con respecto a los servicios de información proporcionados para identificar deficiencias en los niveles de servicio y establecer objetivos de mejoramiento, confeccionando informes que indiquen el avance de la organización hacia los objetivos propuestos.

M2: Evaluación de la adecuación del control interno. Asegurar el logro de los objetivos de control interno establecidos para los procesos de TI. Para ello la gerencia es la encargada de monitorear la efectividad de los controles internos a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias., evaluar su efectividad y emitir reportes sobre ellos en forma regular. Estas actividades de monitoreo continuo por parte de la gerencia deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

M3: Obtención de aseguramiento independiente. Incrementar los niveles de confianza entre la organización, clientes y proveedores externos. Este proceso se lleva a cabo a intervalos regulares de tiempo. Para ello la gerencia deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de implementar nuevos servicios de tecnología de información que resulten críticos, como así también para trabajar con nuevos proveedores de servicios de tecnología de información. Luego la gerencia deberá adoptar como trabajo rutinario tanto hacer evaluaciones periódicas sobre la efectividad de los servicios de tecnología de información y de los proveedores de estos servicios como así también asegurarse el cumplimiento de los compromisos contractuales de los servicios de tecnología de información y de los proveedores de estos servicios.

M4: Provisión de auditoría independiente. Incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas de su implementación, lo que se logra con el uso de Auditorías independientes

desarrolladas a intervalos regulares de tiempo. Para ello la gerencia deberá establecer los estatutos para la función de Auditoría, destacando en este documento la responsabilidad, autoridad y obligaciones de la Auditoría. El auditor deberá ser independiente del auditado, esto significa que los auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado y en lo posible deberá ser independiente de la propia empresa. Esta Auditoría deberá respetar la ética y los estándares profesionales, seleccionando para ello auditores que sean técnicamente competentes, es decir que cuenten con habilidades y conocimientos que aseguren tareas efectivas y eficientes de Auditoría.

Según COBIT, la función de Auditoría deberá proporcionar un reporte que muestre los objetivos de la auditoría, período de cobertura, naturaleza y trabajo de Auditoría realizado, como así también la organización, conclusión y recomendaciones relacionadas con el trabajo de Auditoría llevado a cabo.
Los 34 procesos propuestos se concretan en los objetivos de control de alto nivel detallados anteriormente.

Gobierno de TI (IT Governance)

El Marco referencial *COBIT* y el IT Governance Institute definen el Gobierno de TI como una estructura de relaciones y procesos dirigida a controlar la organización para alcanzar los objetivos del negocio adicionando valor mientras se mantiene un balance equilibrado de los riesgos sobre la Tecnología de Información y sus procesos.

Control

Se define como "las normas, estándares, procedimientos, usos y costumbres y las estructuras organizativas, diseñadas para proporcionar garantía razonable de que

los objetivos empresariales se alcanzaran y que los eventos no deseados se preverán o se detectaran y corregirán" (ob. cit.)

Objetivos de Control

Se define como "la declaración del resultado deseado o propuesto que se ha de alcanzar mediante la aplicación de procedimientos de control en cualquier actividad de TI" (ob. cit.). Los objetivos expuestos en cada uno de los 34 procesos asociados a los 4 dominios explicados anteriormente corresponden a *Objetivos de Control Generales o de Alto Nivel*. Complementariamente, para cada uno de los 34 procesos, se definen de 3 a 30 *Objetivos Detallados de Control Específicos* asociados con cada uno de los procesos de TI. En la versión de *COBIT*(1996) el numero de Objetivos Detallados de Control llegaba a 304; posteriormente en la última versión *COBIT*(2000), el número de estos objetivos llega a 318 con la incorporación de nuevos criterios de control sobre los procesos definidos. Estos objetivos están contenidos en el documento del IT Governance Institute y ISACF denominado "Objetivos de Control Detallados" que complementa al documento "Marco Referencial" que contiene a los Objetivos de Control de Alto Nivel.

La distribución de Objetivos de Control por cada proceso de TI asociado a los diferentes dominios esta definida así: (a) Planificación y Organización – 100 Objetivos -, (b) Adquisición e Implementación – 68 Objetivos, (c) Entrega y Soporte – 126 Objetivos, y (d) Monitoreo con 24 Objetivos para un total de 318 en la versión de *COBIT*(2000).

Todos los objetivos de control han sido definidos de una manera genérica, sin depender de la plataforma o arquitectura técnica, aceptando el hecho real de que diferentes ambientes de TI pueden requerir la cobertura separada de objetivos de control.

El **Gráfico 4**, en la página siguiente, muestra la navegación en cascada de los objetivos de control que facilita su aplicación. Un resumen de los 318 Objetivos de Control Especificos, Versión COBIT(2000), se presenta en el (Anexo D).

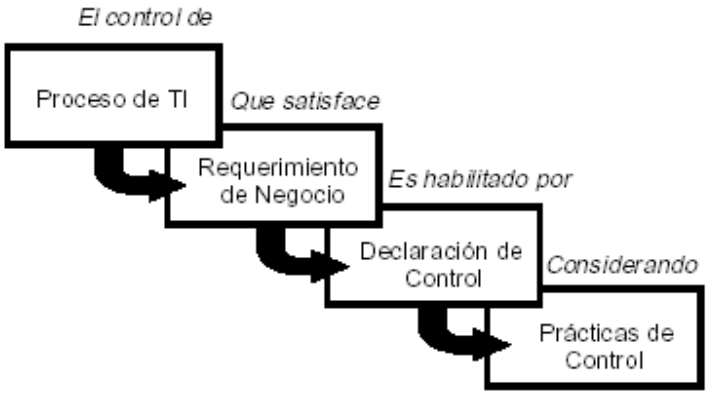


Gráfico 4. Navegación en cascada de Objetivos de Control.
Fuente: Marco Referencial COBIT. ISACF(2000)

En la pagina siguiente, el **Gráfico 5**, indica por proceso y dominio de TI, cuales criterios de información tienen impacto (P)rimario, (S)ecundario o (Vacio) de los 34 objetivos de control de alto nivel, así como una relación de cuales recursos de TI son aplicables.

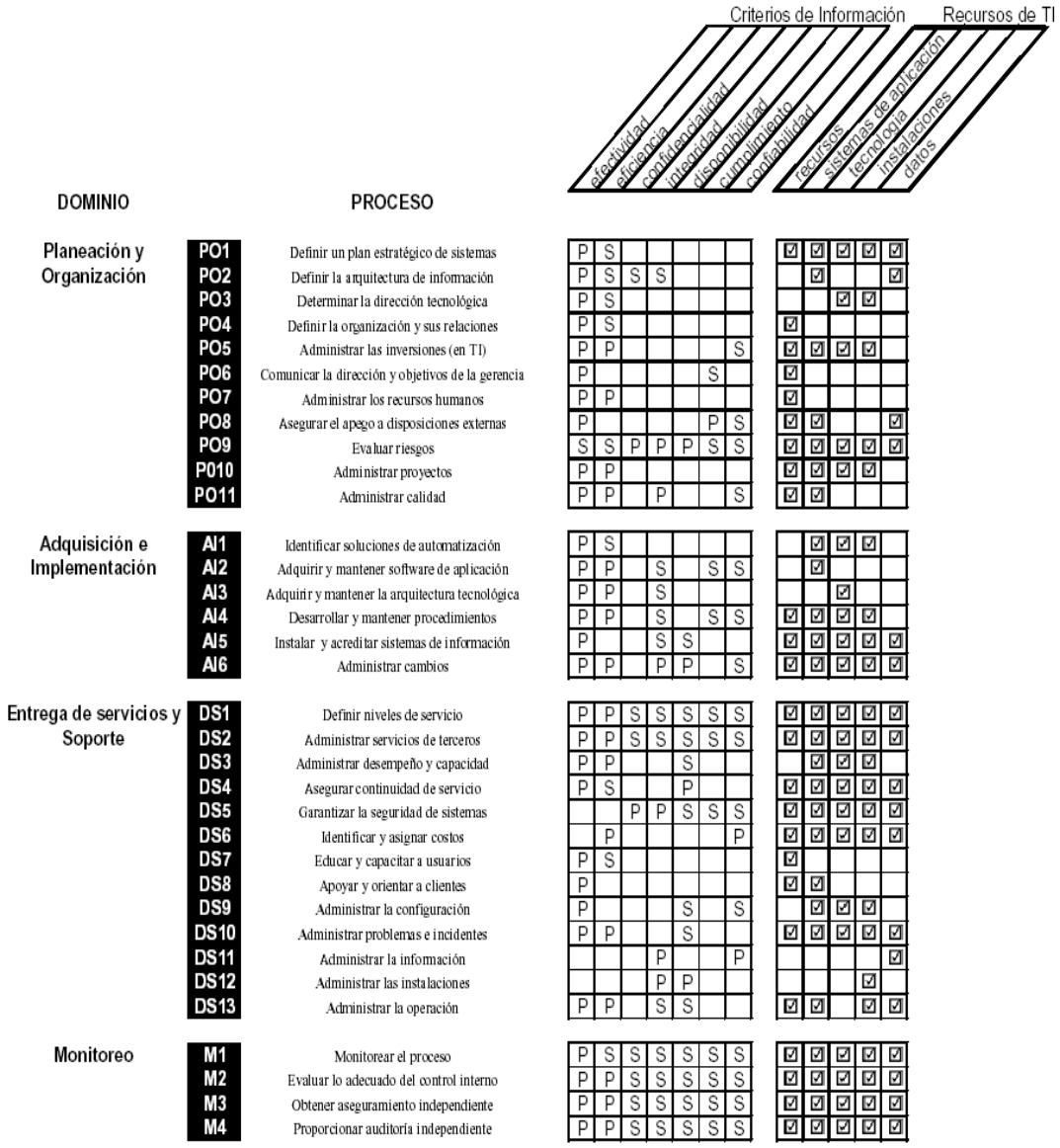


Gráfico 5. Relación de Procesos (Objetivos de Control de Alto Nivel), Criterios de Información y Recursos de TI.
Fuente: Marco Referencial COBIT. ISACF(2000)

Estructura COBIT (ob. cit.)

En resumen, la estructura conceptual de *COBIT* se enfoca desde tres puntos de vista: (a) los recursos de las TI, (b) los criterios empresariales que deben satisfacer la información y (c) los procesos de TI.

Estos tres puntos estratégicos constituyen las dimensiones conceptuales de la estructura *COBIT* y se muestran en el **Gráfico 6**, conocido como Cubo *COBIT,* y en el **Gráfico 7**, que presenta su estructura global con los procesos de TI definidos dentro de los cuatro dominios de agrupación natural de estos procesos.

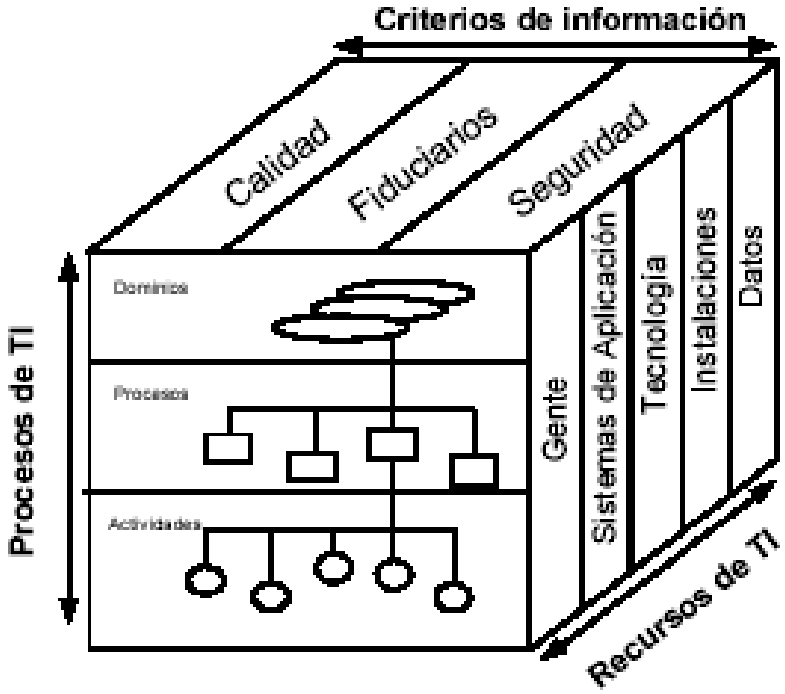


Gráfico 6. Cubo COBIT. Dimensiones Conceptuales de COBIT.
*Fuente***:** Marco Referencial COBIT. ISACF(2000)

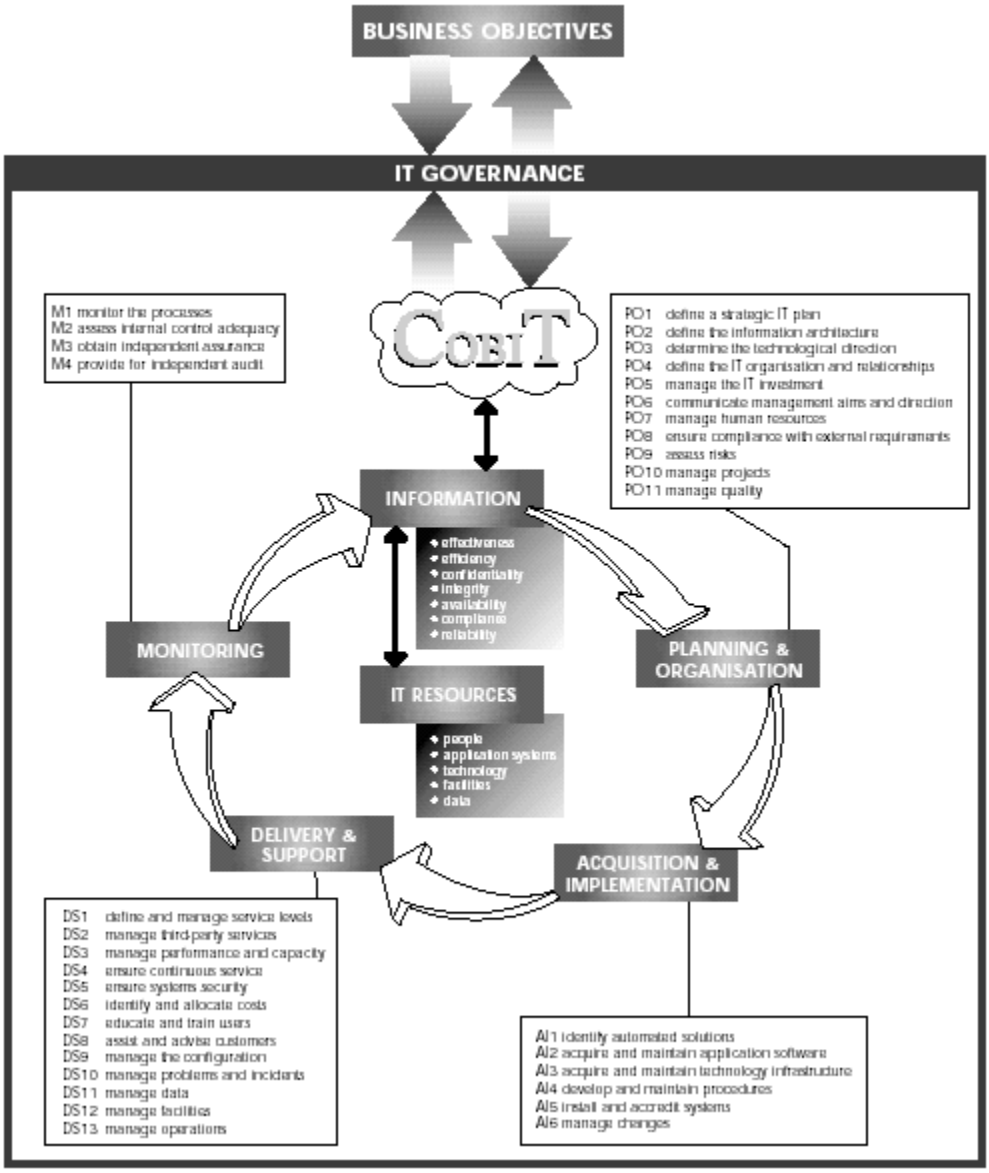


Gráfico 7: Procesos de TI definidos dentro de los Cuatro Dominios y su relación con los Criterios de Información y los Recursos de TI.
*Fuente***:** Marco Referencial COBIT. ISACF(2000)

Guías de Auditoria COBIT (ob. cit.)

Conjunto de pautas para analizar, valorar, apreciar, interpretar, reaccionar e implementar procesos que permitan alcanzar las metas y objetivos mediante la auditoria constante y consistente de los procedimientos. Las Guías de Auditoria perfilan, esbozan y sugieren actividades para desarrollar auditoria de cada uno de los 34 Objetivos de Control de Alto Nivel, mientras sustancian el riego de los objetivos de control no satisfechos. Las guías de auditoría, comprenden fundamentalmente cuatro actividades:

1. **Obtener y comprender:** las actividades del negocio y los controles existentes en el lugar de ejecución. Para ello deben realizarse entrevistas a los gerentes apropiados y al personal de staff para obtener y comprender: (a) Los requerimientos del negocio y los riesgos asociados, (b) La estructura de la Organización, (c) Los roles y responsabilidades, (d) Las políticas y procedimientos, (e) Leyes y regulaciones, (f) Medidas de control en el sitio, (g) Informes gerenciales, (h) Indicadores Claves de Desempeño (**KPI**: Key Performance Indicators).
2. **Evaluar los Controles:** (a) valorar la efectividad o grado en el cual el objetivo de control es alcanzado. Básicamente decidiendo que, en que caso y como evaluarlo. (b) Evaluar la medida de control para los procesos objeto de estudio identificando los criterios y mejores prácticas estándares de la industria, Factores Críticos de Éxito (**CSF**: Critical Success Factors) de las medidas de control y aplicación de juicios de auditoría profesional.
3. **Conformidad de valoración:** (a) asegurar que las medidas de control establecidas corresponden a la prescripción consistentemente y continuamente y concluir sobre el apropiado ambiente de control. (b) Obtener directa o indirectamente evidencia para los ítems y periodos que aseguren que los procedimientos han sido cumplidos. (c) Determinar el nivel de pruebas sustantivas y trabajo adicional requerido para asegurar que los procesos de TI son adecuados a los objetivos del negocio.

4. **Confirmar y verificar riesgos:** (a) desarrollar la confirmación del riesgo del objetivo de control no cumplido por el uso de técnicas analíticas y/o fuentes alternativas de consulta. El objetivo es soportar la opinión y promover a la gerencia para la acción. (b) Los auditores deben ser creativos en encontrar y presentar la información sensitiva y confidencial. (c) Documentar la debilidad de los controles, amenazas y vulnerabilidades. (d) Identificar y documentar el actual y potencial impacto de los riesgos asociados.

Definición de Términos

AICPA Instituto Americano de Contadores Públicos Certificado. (*American Institute of Certified Public Accountants)*

CCEB Criterios comunes para seguridad en tecnología de información. (*Common Criteria for Information Technology Security)*

CICA Instituto Canadiense de Contadores. (*Canadian Institute of Chartered Accountants*)

CISA Auditor Certificado de Sistemas de Información. (*Certified Information Systems Auditor*)

COSO Comité de Organizaciones Patrocinadoras de la Comisión de Intercambio. "Tradeway" (*Committee of Sponsoring Organisations of the Tradeway Commission).*

DRI Instituto Internacional de Recuperación de Desastres. (*Disaster Recovery Institute International*)

DTI Departamento de Comercio e Industria del Reino Unido. (*Department of Trade and Industry of the United Kingdom)*

EDIFACT Intercambio Electrónico de Datos para la Administración, el Comercio y la Industria (*Electronic Data Interchange for Administration, Commerce and Trade*)

EDPAF Fundación de Auditores de Procesamiento Electrónico de Datos (*Electronic Data Processing Auditors Foundation*), ahora **ISACF**.

ESF Foro Europeo de Seguridad (*European Security Forum*), cooperación de 70+ multinacionales europeas principalmente con el propósito de investigar problemas de seguridad y control comunes de TI.

GAO Oficina General de Contabilidad de los EUA. (*U.S. General Accounting Office*)

I4 Instituto Internacional de Integridad de Información. (*International Information Integrity Institute*), asociación similar a ESF, con metas similares, pero con base principalmente en los Estados Unidos y dirigida por el Instituto de Investigaciones de Stanford (*Stanford Research Institute)*

IBAG Grupo Consultivo de Negocios Infosec (*Infosec Business Advisory Group*), representantes de la industria que asesoran al Comité Infosec. Este Comité está compuesto por funcionarios de los gobiernos de la Comunidad Europea y asesora a la Comisión Europea sobre cuestiones de seguridad de TI.

IFAC Federación Internacional de Contadores. (*International Federation of Accountants*)

IIA Instituto de Auditores Internos. (*Institute of Internal Auditors*)

INFOSEC Comité Consultivo para la Comisión Europea en Materia de Seguridad TI. (*Advisory Committee for IT Security Matters to the European Commission*)

ISACA Asociación para la Auditoría y Control de Sistemas de Información. (*Information Systems Audit and Control Asociation)*

ISACF Fundación para la Auditoría y Control de Sistemas de Información. (*Information Systems audit and Control Foundation)*

ISO Organización de Estándares Internacionales. (*International Standards Organisation*)

ISO9000 Estándares de manejo y aseguramiento de la calidad definidos por ISO.

ITIL Biblioteca de Infraestructura de Tecnología de Información. (*Information Technology Infrastructure Library)*

ITSEC Criterios de Evaluación de Seguridad de Tecnología de Información (*Information Technology Security Evaluation Criteria*). Combinación de los criterios de Francia, Alemania, Holanda y Reino Unido, soportadas consecuentemente por la Comisión Europea (ver también TCSEC, el equivalente en los Estados Unidos).

NBS Departamento Nacional de Estándares de los Estados Unidos (*National Bureau of Standards of the U.S.)*

NIST (antes NBS) Instituto Nacional de Estándares y Tecnología. (*National Institute of Standards and Technology*), con base en Washington D.C.

NSW Nueva Gales del Sur, Australia. (*New South Wales, Australia*)

OECD Organización para la Cooperación y el Desarrollo Económico. (*Organisation for EconomicCooperation and Development*)

OSF Fundación de Software Público (*Open Software Foundation*)

PCIE Consejo Presidencial de Integridad y Eficiencia. (*President´s Council on Integrity and Efficiency*)

TCSEC Criterios de Evaluación de Sistemas Computarizados Confiables. (*Trusted Computer System Evaluation Criteria*), conocido también como "*The Orange Book*". Criterios de evaluación de seguridad para sistemas computarizados definidos originalmente por el Departamento de Defensa de los Estados Unidos. Ver también ITSEC, el equivalente europeo.

TickIT Guía para la Construcción y Certificación de Sistemas de Administración de Calidad. (Guide to Software Quality Management System Construction and Certification)

CAPITULO III
MARCO METODOLOGICO

Tipo de Investigación

El estudio que se realizará consiste en una investigación que se ubica en la modalidad conocida como Proyecto Factible, la cual según Barrios (1998), consiste en la investigación, elaboración y desarrollo de una propuesta de un modelo operativo, en este caso, modelo metodológico, viable para la solución de problemas, requerimientos o necesidades de organizaciones o grupos sociales; referido a la formulación de políticas, programas, tecnologías, métodos o procesos. Estos aspectos serán cubiertos en el ambiente de aplicación de Sistemas de Información y las Tecnologías Relacionadas con los procesos de información en las organizaciones actuales.

Diseño de la Investigación

El diseño de la investigación es considerado por Balestrini (1998:118) como "… el plan global que integra de un modo coherente y adecuadamente correcto, técnicas de recogidas de datos a utilizar, análisis previstos y objetivos…". Esta investigación se sustenta en fuentes mixtas por originarse en investigación documental (referencias de materiales impresos y de información publicada en paginas web, documentos y/o bibliografía existente que sirven de base al estudio y al fundamento teórico, principalmente toda la información relacionada con las publicaciones *COBIT*) y de campo (a través de la cual se adquieren conocimientos y datos que no están plasmados en ninguna bibliografía sino que se obtienen estando en

el lugar donde se desarrollaran las actividades, procesos o hechos que fundamentan los conocimientos empíricos).

La investigación documental se centra en el estudio del problema de control de la información y las tecnologías que la soportan dentro de las organizaciones. La investigación de campo esta centrada en el análisis sistemático del problema en una organización especifica; en este estudio se tomará como representante de la realidad a la empresa Banco Sofitasa, con el propósito de interpretar el problema del control de la información en sus procesos, haciendo uso de métodos de diagnostico y evaluación relacionados con la estructura *COBIT*.

Población

Una población es definida por Martínez (2000: 711) como "…conjunto de unidades o elementos que representan una característica común". En este caso de estudio, la población esta representada por los niveles directivos de la más alta gerencia en materia de Tecnología de Información y Auditoría de Sistemas dentro de la Organización objeto de estudio. Esto representa en cierta forma una limitante para el levantamiento de información pero también asegura la calidad de la información recogida por cuanto los usuarios propietarios de los datos requeridos para la investigación representan a su vez las unidades organizacionales que gobiernan la tecnología de información y su evaluación, seguridad y control. La naturaleza de los cargos gerenciales determina una confidencialidad particular de los datos de los procesos a estudiar, por su acceso restringido y su valor estratégico y funcional. Esto determina que la población objeto de estudio este limitada a un número muy reducido de personas por la jerarquía de su ubicación dentro de la organización; las unidades organizacionales hacia las cuales esta orientada la aplicación de las técnicas de recolección de datos son la Vicepresidencia de Tecnología y la Gerencia de Auditoría de Sistemas del Banco Sofitasa, sede San Cristóbal, Estado Táchira. El personal autorizado para suministrar los datos esta limitado a los cargos directivos en cada una de las áreas seleccionadas lo cual no excede las 3 o 4 personas, a lo sumo 2 por cada

área, los cuales no suministraran los datos en forma independientemente sino lo harán en un *workgroup* para suministrar información de consenso sobre los importantes aspectos de *Gobierno de TI.*

Muestra

Una muestra es definida por Martínez (2000:715) como "…una parte de la población o subconjunto de elementos que resulta de la aplicación de algún proceso, generalmente de selección aleatoria, con el objeto de investigar todas o parte de las características de estos elementos."

Por las características expuestas para la población en estudio, el muestreo aleatorio o probabilístico no tiene aplicación, dado el reducido tamaño de la población, la cual además, unida en un workgroup, representa una unidad homogénea de información consensuada; en consecuencia, se opta por aplicar los instrumentos de recolección de datos al grupo directivo como una sola unidad de información tomada como muestra bajo el enfoque de opinión de expertos, en este caso directivos de Tecnología de Información en la organización objeto de estudio, en cuyo caso se le da un tratamiento de censo, definido por Martínez (2000:714) como "la enumeración total de una población en un tiempo dado"

Técnicas e Instrumentos de Recolección de Datos

Las técnicas de recolección de datos son distintas formas o maneras de obtener la información, son ejemplos de técnicas; la observación directa, la encuesta en sus dos modalidades (entrevista o cuestionario), el análisis documental, análisis de contenido entre otras. Los instrumentos según Perdomo (1983:20) "… son el conjunto de elementos o medios de que se sirve el investigador en búsqueda del conocimiento". Los instrumentos de recolección de datos son los medios materiales que se emplean para recoger y almacenar la información, son ejemplos de

instrumentos; los formatos de cuestionario, guías de entrevista, listas de cotejo (checklist), entre otros.

En el presente estudio, se emplean el análisis documental y de contenidos de las referencias bibliográficas y en línea para la sustentación de las bases teóricas de interés para la investigación. En el estudio de campo dentro del Banco Sofitasa, específicamente en la Vicepresidencia de Tecnología, se desarrollaron entrevistas y se aplicaron cuestionarios en el grupo de trabajo bajo los formatos estructurados de listas de cotejo. La entrevista según Tamayo y Tamayo (1986:117) es la "Obtención directa de respuestas de un sujeto por parte del investigador, el cual las anota", la entrevista es del tipo estructurada, ya que facilita la comunicación entre el investigador y el entrevistado a través de la aplicación de un cuestionario predefinido organizado en forma de listas de chequeo o comprobación, de esta forma se obtienen datos directos de las personas que forman parte del proceso, debido a que se tienen preguntas previamente formuladas. Las listas de cotejo o técnicamente como son conocidas en el ámbito de la Auditoría Informática, checklist, son instrumentos estructurados que permitirán valorar las respuestas por pesos de preguntas en escala o por valores duales o binarios (dicotómicos) para obtener de forma más precisa los valores de las variables del estudio.

Para la recolección de datos se han utilizado tres instrumentos denominados: (a) "Checklist para Identificar las Necesidades de Servicios en Evaluación y Auditoria de Información y Tecnologías Relacionadas" (Anexo A), (b) "Autoevaluación del Gobierno de los Procesos de Tecnología de Información" (Anexo B), y (c) "Matriz de Evaluación de Procesos de Tecnología de Información y Grupos de Riesgos Asociados" (Anexo C). El primer instrumento tiene como objetivo determinar un análisis diagnostico de la situación actual de la organización respecto al requerimiento de servicios de evaluación y auditoria de la información y las tecnologías relacionadas. El segundo permite valorar la importancia o relevancia de los 34 procesos *COBIT* y su desempeño en alineación con los objetivos del negocio. Estos valores de relevancia y desempeño, permiten establecer una relación de riesgo de cada proceso; a su vez se identifica por cada proceso, la unidad organizacional

ejecutora, el estado de auditoria y la formalidad estructurada del proceso. El tercer instrumento tiene por finalidad verificar la correspondencia o afinidad de los riesgos estimados por el negocio para los procesos *COBIT* y la clasificación estándar de los grupos de riesgos establecidos por las mejores practicas en materia de evaluación de riesgos.

Análisis e Interpretación de los Datos

Los datos y/o información que se recopiló con la aplicación de las técnicas e instrumentos se organizaron y codificaron para su análisis e interpretación según el tipo de cada uno de ellos; en el caso de las checklist, los datos se clasifican de acuerdo a la categoría de contenido y/o tipo de pregunta, asignándosele una calificación o cuantificación según el tipo de dato. En el caso de las matrices de evaluación, algunos ítems se valoran por respuestas en escala numérica de (1-5) y otros por valores ambivalentes o binarios tipo marcaje X.

En las entrevistas de aplicación de los instrumentos, además de llevar el control de las respuestas del grupo de trabajo entrevistado, también se anotaron los comentarios y observaciones que pudieron realizar los integrantes del grupo de expertos, según su experiencia, afinidad y conocimiento del tema, para posteriormente contrastar la información estructurada con la información complementaria y enriquecer el contexto de aplicación del análisis situacional. Complementariamente, el estudio diagnostico se enriqueció con información proveniente de documentos de la organización pertinente sobre normas, procedimientos, políticas de seguridad y control de la información y las tecnologías relacionadas.

Específicamente, el análisis de cada uno de los instrumentos aplicados permitió obtener los siguientes resultados clasificados por categorías de contenido y áreas de interes. En el Instrumento 1, *"Checklist para Identificar las Necesidades de Servicios de Evaluación y Auditoria de Información y Tecnologías Relacionadas"*, se clasifican los contenidos en las siguientes categorías de datos:

1. **Recurso Humano asignado al área de IT:** 40 personas clasificadas como tecnólogos, ingenieros, especialistas en telecomunicaciones y otros como operadores, transcriptores y personal de apoyo; lo que permite definir a la organización como de tamaño medio respecto a la función de IT.
2. **Plataformas de Hardware y Software:** 4 plataformas de sistemas operativos interconectadas en red, 3 motores de bases de datos, 500 equipos activos de red, servicio de Internet con acceso controlado por perfil de usuario e Intranet para mensajería interna, servidor Exchange de correo electrónico, Firewalls ubicados en diferentes segmentos de la red, 8 servidores de archivos, 2 Mainframes, 500 Microcomputadoras y un Data Warehouse en implementación en la actualidad. Esta arquitectura de Hardware y Software determina que en la organización hay una *alta complejidad* de los procesos de TI.
3. **Sistemas de Información y Aplicaciones**: principalmente cabe resaltar aquí, los 3 grandes sistemas y sus módulos componentes principales, (a) SIAF – Sistema Integral de Administración Financiera, con los módulos de Crédito, Contabilidad, Fideicomiso, Cuentas Corrientes, Cuentas de Ahorro, Cobranza y Política Habitacional -, (b) UNICARD – Sistema de Tarjetas de Crédito -, y (c) SBE – Sistema de Cajeros Automáticos-. Se observa aquí, la relevancia de los sistemas de gestión financiera por la propia naturaleza de la organización que define los objetivos del negocio.
4. **Portafolio de Aplicaciones en Producción y su Importancia**: Esta categoría de datos se valora bajo tres aspectos y modalidades: relevancia (1-Menor relevancia, 5-Mayor), Herramientas de Desarrollo, y existencia de programas fuentes. Los resultados obtenidos permiten determinar en el primer aspecto que todas las aplicaciones son de relevancia para la organización ubicadas en el rango 4 y 5 (Alta importancia, es obvio que de ellas depende la información sensitiva del negocio), en el segundo aspecto se observa que aproximadamente el 66 % de las aplicaciones son desarrolladas en OS/400 y el resto 34% en LINC, esto favorece la

estandarización y compatibilidad de los procesos porque no hay múltiples herramientas de desarrollo. En el tercer aspecto, todas las aplicaciones poseen programas fuentes, lo que significa un aseguramiento de los procesos de mantenimiento de aplicaciones y ausencia de riesgos por procesos de *"caja negra"*, sin conocimiento de código lógico.

5. **Actividades de Procesamiento de Datos:** Esta categoría de datos, de valor ambivalente (marcaje X) permite conocer que en la organización, todas las actividades de procesamiento de datos se desarrollan o ejecutan y que todo el ciclo de aseguramiento de procesos se toma en cuenta, garantizando la continuidad de las operaciones, a saber: (a) Captura de datos, (b) Control de entradas y salidas, (c) Proceso y actualización de archivos, (d) Ayuda de escritorio, (e) Soporte a usuarios, (f) Mantenimiento de hardware, (g) Administración de bases de datos, (h) Administración de seguridad lógica, (i) Planeación estratégica de sistemas, (j) Administración de contratos con terceros, (k) Definición e implementación de políticas de seguridad corporativas, (l) Análisis y diseño de sistemas, (m) Construcción de programas, (n) Mantenimiento de aplicaciones y (o) Aseguramiento de la calidad. El cumplimiento de todas estas actividades reduce la vulnerabilidad de los procesos a eventuales riesgos, quedando pendiente la valoración de cada una de estas actividades.
6. **Servicios Contratados con Terceros:** De las 16 actividades o servicios de procesamiento de datos enumeradas en el punto anterior, solo 3 son desarrolladas con participación de terceros externos (Outsourcing) (a) Mantenimiento de hardware, (b) Programación de aplicaciones, y (c) Planeación de contingencias en sistemas de información, es decir solo el 18,75% de los procesos; estas actividades son controladas por procedimientos internos documentados y estructurados lo que reduce la vulnerabilidad de riesgos.
7. **Servicios de Control Interno y Seguridad de Sistemas de interés:** Según los datos obtenidos en esta categoría, se determina el interés de la dirección

de TI y la dirección de Auditoría de Sistemas de la organización en los servicios de (a) Asesoría para la implantación de estándar COBIT (Control Objectives for Information and Related Technology), (b) Aseguramiento de la calidad del software, y (c) Capacitación en controles y seguridad en sistemas de información. Esta opinión evidencia el requerimiento de la organización en el conocimiento y aplicación de estandares y las mejores prácticas en materia del gobierno de las TI en alineación con los procesos del negocio.

8. **Servicios de Auditoria de Sistemas de interés**: Las respuestas en esta categoría de datos, están en concordancia con las del punto anterior y complementan la justificación del requerimiento de la organización en los servicios de (a) Auditoría al plan de contingencias de sistemas de información (Aseguramiento de la continuidad del negocio) y (b) Asesoría para implantar el enfoque de Auditoría de Sistemas orientada al riesgo.

En el Instrumento 2, *"Autoevaluación del Gobierno de los Procesos de Tecnología de Información"*, se clasifican los contenidos en las categorías definidas por *COBIT* para los 4 dominios y los 34 procesos (Objetivos de Control de Alto Nivel) organizando los datos en 4 grupos de parámetros de evaluación por cada proceso: (a) Pesos de Relevancia y Desempeño, (b) Unidad Organizacional Ejecutora del Procesamiento, (c) Estado del Proceso respecto a Auditoria y Formalización, y (d) Unidad Organizacional Responsable del Gobierno del proceso. Cada uno de los 4 parámetros suministra información particular sobre el diagnostico situacional de los procesos de TI en alineación con los objetivos del negocio de la Organización. Cada parámetro es evaluado de forma particular y combinada. A continuación se exponen los criterios de evaluación de cada grupo de parámetros y los resultados obtenidos:

1. **Relevancia y Desempeño:** particularmente, la relevancia mide la calidad o condición de importancia y significación del proceso de TI en función de su contribución al logro de los objetivos del negocio. Cada proceso es autoevaluado en la escala de (1 – 5) siendo la interpretación cualitativa de

los valores de este rango, la mostrada en el **Cuadro 3**. Particularmente, el desempeño mide el nivel y calidad de cumplimiento (performance) esperado de la ejecución del proceso de TI en el rango (0 – 5), siendo la interpretación la mostrada en el **Cuadro 4**.

Cuadro 3

Valoración de relevancia de los procesos de TI

Relevancias	
Relevancia	**Descripción**
1	No Relevante
2	Poco Relevante
3	Medianamente Relevante
4	Relevante
5	Muy Relevante

Fuente: propia

Cuadro 4

Valoración del desempeño de los procesos de TI

Desempeños		
Desempeño	**Descripción**	**Comentario**
0	No existe	Proceso no Aplicado o no Definido
1	Inicial	Proceso Ad-hoc y Desorganizado
2	Regular	Proceso Rutinario de Curso Regular
3	Definido	Proceso Documentado y Comunicado
4	Gerenciado	Proceso Monitoreado y Evaluado
5	Optimizado	Proceso bajo las Mejores Practicas y Automatizado

Fuente: propia (enfoque de valoración basado en el modelo de madurez que el Software Engineering Institute definió para la madurez de la capacidad de desarrollo de software)

En forma combinada, estos dos valores, relevancia y desempeño, permiten estimar un indicador de fortaleza o debilidad respecto a la vulnerabilidad de riesgo del proceso. Por ejemplo, un proceso valorado con relevancia 5 (muy

relevante) y con desempeño 3 (apenas documentado y comunicado, no monitoreado ni evaluado, no ejecutado bajo las mejores prácticas) es un proceso altamente vulnerable con un alto indicador de riesgo. En cambio, un proceso con relevancia 2 o 3 (poco o medianamente relevante) y desempeño 3 (definido) es un proceso estable, muy poco vulnerable a riesgos. De acuerdo con este análisis valorativo de relevancia y desempeño se obtuvieron los resultados por Dominio *COBIT* presentados en el **Cuadro 5**.

Cuadro 5

Evaluación del Gobierno de los Procesos de TI por Dominio

PROCESOS	REL.	DES.	RIESGO
DOMINIO: PO – Planificación y Organización (11 Procesos)			
5: PO2,PO3,PO9,PO10,PO11	4	4	1 : Moderado
3: PO4,PO5,PO7	4	5	1,25: Bajo
1: PO1	5	3	**0,6: Alto (*)**
1: PO8	5	4	**0,8: Alto**
1: PO6	5	5	1: Moderado
DOMINIO: AI – Adquisición e Implementación (6 Procesos)			
6: Todos	4	4	1: Moderado
DOMINIO: DS – Entrega y Soporte (13 Procesos)			
1: DS6	4	3	**0,75: Alto**
9: DS1,DS5,DS7 a DS13	4	4	1: Moderado
1: DS2	4	5	1,25: Bajo
1: DS4	5	4	**0,8: Alto**
1: DS3	5	5	1: Moderado
DOMINIO: M – Monitoreo (4 Procesos)			
4: Todos	4	4	1: Moderado

Nota: Fuente Propia. Datos tomados del Instrumento No. 2. Los procesos identificados por su nomenclatura COBIT son agrupados y contados en cada dominio por grupos de puntajes de Relevancia y Desempeño iguales. El riesgo autoevaluado se estima como la razón entre el desempeño y la relevancia: < 1: Alto, 1: Moderado, > 1: Bajo.

De acuerdo con los datos obtenidos en el Cuadro 5, puede observarse que la autoevaluación determina al proceso PO1: Planificación y Organización como el proceso más crítico con riesgo Alto, con la mayor relevancia (5) y el menor desempeño (3). Complementariamente, deben considerarse otros indicadores de vulnerabilidad de riesgo como la provisión o ausencia de auditoría (interna y/o externa) del proceso y el grado de formalización del

proceso (existencia de contratos, convenios, acuerdos de niveles de servicio, documentación formal).

2. **Procesamiento:** esta categoría de contenido en el Instrumento 2, permite determinar la Unidad Ejecutora del Proceso de TI entre las unidades de Tecnología, Otras unidades, Terceros o No Informado obteniéndose los siguientes resultados:

Cuadro 6

Unidades Ejecutoras de Procesos de TI

DOMINIOS	PROC.	TI	OTR.	EXT.
PO: Planificación y Organización	11	11	4	1
AI: Adquisición e Implementación	6	6	2	3
DS: Entrega y Soporte	13	13	5	3
M: Monitoreo	4	4	2	1
Total Procesos Ejecutados	34	34	13	6

Nota: Fuente Propia. Datos tomados del Instrumento No. 2. Los 34 procesos definidos por COBIT son ejecutados con participación directa de la Vicepresidencia de TI, El procesamiento de 13 procesos es compartido con otras unidades y 6 procesos comparten su ejecución con terceros externos.

Puede observarse en esta categoría de datos que la Vicepresidencia de Tecnología ejecuta todos los procesos y comparte la ejecución con las unidades usuarias en los procesos PO7 a PO10, AI5, AI6, DS1, DS3 a DS6, M1 y M2, particularmente estos dos últimos con la Gerencia de Auditoria de Sistemas. Los procesos ejecutados por terceros son PO4, "Definición de la Organización y de las relaciones de TI", que merece una referencia especial por cuanto en la actualidad, el Banco Sofitasa, adelanta estudios sobre la alineación del negocio con la estrategia de TI a través de procesos de Outsourcing con firmas especializadas en consultoría del área. El análisis de la ejecución de procesos permite observar que en la organización existe una conciencia especial respecto al valor de aplicación del concepto de Gobierno de TI.

3. **Estado:** en esta categoría de contenido del Instrumento 2, se evidencia la aplicación de procedimientos y programas de Control Interno en todos los procesos de TI (Auditoría Interna) y solo 9 procesos poseen o han recibido Auditoria Externa, lo cual deja una brecha o vació importante en la aplicación de procedimientos de Evaluación y Auditoría bajo enfoques de Gobierno de TI por parte de terceros que puedan apreciar con objetividad el estado actual de la Organización en estos procesos. Finalmente, en esta categoría, se obtiene información sobre el estado de formalización del

proceso, determinándose qué de los 34 procesos, solo 24 poseen documentación formal. En el caso de procesos que hayan sido valorados con Relevancia (4 o 5), la ausencia de formalización implica un alto grado de vulnerabilidad de riesgos, mayor aún cuanto más bajo sea la valoración del desempeño; según esta relación los procesos PO1: "Definición de un plan estratégico de TI y DS6: "Identificación e imputación de Costos", no formalizados y con (5,3) y (4,3) de Relevancia y Desempeño respectivamente representan los Procesos de TI (Objetivos de Control de Alto Nivel) de estado critico respecto al riesgo, y por lo tanto, los procesos sobre los que habría que apuntalar procedimientos de Evaluación y Auditoría. Los valores obtenidos se representan a continuación:

Cuadro 7

Estado de los Procesos de TI respecto a Auditoría y Formalización

DOMINIOS	PROC.	AUI	AUE	FOR.
PO: Planificación y Organización	11	11	1	7
AI: Adquisición e Implementación	6	6	3	5
DS: Entrega y Soporte	13	13	2	8
M: Monitoreo	4	4	3	4
Totales:	34	34	9	24

Nota: Fuente Propia. Datos tomados del Instrumento No. 2. Todos los procesos tienen Auditoría Interna, solo 9 han recibido Auditoría Externa y hay 24 procesos formalizados. En el dominio PO, uno de los procesos no formalizados es el PO1 y en el dominio DS, no esta formalizado el proceso DS6.

4. **Responsables del Gobierno de TI:** en esta categoría de contenido del Instrumento 2, se identifican los responsables del Gobierno de TI para cada uno de los procesos y de acuerdo con los resultados puede calcularse la distribución de responsabilidad de los procesos de TI en las unidades organizacionales responsables, obteniéndose los resultados por dominio presentados en el **Cuadro 8**.

Cuadro 8

Unidades responsables del Gobierno de TI

Unidades Responsables	PO	AI	DS	M	TOT.
Dirección Ejecutiva	2				2
Gerencia de TI	6	5	10		21
Gerencia de Auditoria de Sistemas	1	1	1	4	7
Gerencia de Recursos Humanos	1				1
Gerencia de Seguridad			2		2
Gerencia de Riesgos	1				1
TOTALES	11	6	13	4	34

Nota: Fuente Propia. Datos tomados del Instrumento No. 2. Distribución de responsabilidad del Gobierno de TI para los 34 procesos COBIT.

De estos resultados se determina que el 61.7 % del Gobierno de los procesos de TI, son responsabilidad de la Vicepresidencia de TI, el 20.5 % son responsabilidad de la Gerencia de Auditoria de Sistemas, la Dirección Ejecutiva y la Gerencia de Seguridad, cada una con el 6% y un 2.9% para la Gerencia de Riesgos y la Gerencia de Recursos Humanos.

Con el Instrumento 3, "*Matriz de Evaluación de Procesos de Tecnología de Información y Grupos de Riesgos Asociados"* se encuentra una ratificación por parte de la dirección de tecnología del Banco Sofitasa, de la clasificación establecida por las referencias *COBIT* para los 34 procesos y los grupos de riesgos asociados. Lo importante aquí, es poder establecer la relación específica entre los procesos PO1 y DS6, diagnosticados como los procesos con más alta vulnerabilidad de riesgo, y los riesgos particulares asociados a estos procesos. Estas relaciones se presentan en el **Cuadro 9.**

Cuadro 9.

Riesgos asociados a los Procesos PO1 y DS6 por Grupo de Riesgos

PROCESO	DIRECCION						INTER/INTRA						SOLUCIONES					CLIEN/SERV.					
Número >	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	2	2	2	2
de Riesgo	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3
PO1	**X**		**X**										**X**		**X**			**X**		**X**			**X**
DS6					**X**												**X**						

Nota: Fuente Propia. Datos tomados del Instrumento No. 3. Abstracción de los riesgos asociados a los procesos PO1 y DS6, determinados como más vulnerables en la autoevaluación diagnostica del Gobierno de TI.

De acuerdo con los resultados de la autoevaluación del Gobierno de TI para los procesos definidos por COBIT y los grupos de riesgos asociados se determinan las siguientes relaciones:

1. **Riesgos del Proceso PO1**: (a) De Dirección, 01- Iniciativas de TI alineadas con la estrategia del negocio, 03 - Utilización de la TI para obtener ventajas competitivas; (b) De Soluciones Empresariales, 13 – Fracaso al alcanzar los requerimientos de usuario, 15 - Incompatibilidad con la infraestructura técnica; y (c) De Arquitectura Cliente / Servidor, 18 - Fracaso en los requerimientos de coordinación, 20 - Incompatibilidad con la infraestructura técnica, 23 - Elevados costos de propiedad.

2. **Riesgos del Proceso DS6**: (a) De Dirección, 05 - Reducción de costos de la propiedad de TI; y (b) De Soluciones Empresariales, 17 - Implementación costosa/compleja.

CAPITULO IV

PROPUESTA: MODELO METODOLOGICO DE EVALUACION Y AUDITORIA DE INFORMACION Y TECNOLOGIAS RELACIONADAS

Definición del Modelo Metodológico.

El Modelo Metodológico de Evaluación y Auditoria de Información y Tecnologías Relacionadas considera la definición y aplicación de los siguientes elementos:

1. El Marco Referencial COBIT (*COBIT* Framework) con capacidad definible de relaciones abiertas entre los elementos: procesos, requerimientos o criterios de información y recursos de TI.
2. El conjunto de Objetivos de Control Específicos relacionados con el Marco Referencial *COBIT*.
3. El conjunto de las Guías de Auditoría *COBIT* por Objetivo de Control de Alto Nivel.
4. El Plan de Evaluación y Auditoria definido por el usuario del modelo.
5. Los alcances a ser cubiertos por el proceso de Evaluación y Auditoria.
6. La evaluación de los procesos (Objetivos de Control de Alto Nivel).
7. La evaluación de los Objetivos de Control Específicos detallados por proceso.
8. La información detallada resultado de la aplicación de las Guías de Auditoría por proceso que sustentan el Informe de Evaluación y Auditoria.
9. La opinión del Auditor sobre la aplicación y resultados del Plan de Evaluación y Auditoría con las observaciones y recomendaciones.
10. La emisión del Informe de Evaluación y Auditoría.

Para la definición del Modelo Metodológico de Evaluación y Auditoría de Información y Tecnologías Relacionadas, a continuación se detalla cada uno de los elementos enumerados anteriormente; luego se presenta un esquema general de la aplicación del modelo propuesto reflejando con un diagrama de Flujo de Datos, los diferentes procesos, entidades interfaces, almacenes de datos y flujos de datos. Seguidamente, se presentan el diseño lógico conceptual de la aplicación de software propuesta para la ejecución y validación del modelo con datos de prueba para el Dominio PO: Planificación y Organización, proceso PO1: Definición de un Plan Estratégico de TI.

Elementos del Modelo

1. **Marco Referencial COBIT (CObIT Framework).** Como se explicó en las bases teóricas de la presente investigación, el Marco Referencial *COBIT* presentado por ISACF y el IT Governance Institute(2000), es el fundamento teórico y estructural de la presente propuesta de aplicación metodológica. En resumen, se toman en cuenta: (a) 4 Dominios de procesos de TI: 1-PO: Planificación y Organización, 2-AI: Adquisición e Implementación, 3-DS: Entrega y Soporte, 4-M: Monitoreo; (b) 34 Procesos u Objetivos de Control de Alto Nivel organizados por dominio de correspondencia: 1-PO: 11 procesos, 2-AI: 6 Procesos, 3-DS: 13 procesos, M: 4 procesos; (c) 7 criterios de información del negocio: 1-Efectividad, 2-Eficiencia, 3-Confidencialidad, 4-Integridad, 5-Disponibilidad, 6-Cumplimiento, 7-Integridad; y (d) 5 Recursos de TI: 1-Personas, 2-Datos, 3-Aplicaciones, 4-Tecnología, 5-Instalaciones.
2. **Objetivos de Control Detallados por proceso de TI.** Los 318 Objetivos de Control Específicos organizados por cada dominio y proceso *COBIT* son tomados en cuenta dentro de la Base de Conocimiento del modelo. La carta resumen de este conjunto de Objetivos de Control es presentada en el (Anexo D), en el documento titulado *COBIT 3rd. Edition Control*

Objectives emitido por el Comité Directivo de COBIT – ISACA y el IT Governance Institute.

3. **Guías de Auditoría COBIT**. Para los efectos de aplicación de los Procedimientos de Auditoría posteriores a la evaluación de los procesos de TI, el modelo contempla la referencia, observación y aplicación de las guías de auditoría organizadas por proceso.
4. **Plan de Evaluación y Auditoria**. El modelo permite definidor el Plan de Evaluación y Auditoría a ser desarrollado, indicando el periodo de la auditoria, los usuarios Auditor, Supervisor y Revisor, y las fechas de seguimiento. Este plan permitirá su vinculación con la definición de alcances del proceso de Evaluación y Auditoría.
5. **Alcance del Plan de Evaluación y Auditoria**. El modelo permite definir el alcance, especificando el marco de aplicación del Plan de Evaluación y Auditoría a través de los dominios, procesos (Objetivos de Control de Alto Nivel), criterios de información, recursos de TI por proceso y Objetivos de Control Específicos detallados por proceso.
6. **Evaluación de los procesos (Objetivos de Control de Alto Nivel)**. La evaluación de los procesos seleccionados en el alcance, asociados a sus correspondientes dominios, se logra a través de la relación de dos variables denominadas *Relevancia* (mide el grado de significancia e importancia del proceso asignado por consenso entre el Gobierno de TI y el Auditor) y *Desempeño* (valora el grado de desempeño del proceso tomando en cuenta el modelo de madurez para la capacidad de desarrollo de software definido por el Software Engineering Institute. Estas escalas se representan en los **Gráficos 8 y 9**. Analíticamente, el índice de madurez del proceso se calcula mediante la relación (1):

   (1) $IM = D / R$

Donde el Indice de Madurez (IM), representa una relación directamente proporcional al Desempeño (D) e inversamente proporcional a la Relevancia (R). El dominio de D es [0,5], el dominio de R es [1,5] obteniéndose un rango de [0,5] para IM.

Una vez obtenidos los IM por cada uno de los procesos correspondientes al Dominio evaluado (en caso de la evaluación total del dominio), se obtienen los índices de evaluación del dominio a partir de sus procesos, con las siguientes expresiones analíticas:

(2)	$SR = \Sigma R$	(Sumatoria de Relevancias del Dominio)
(3)	$SRM = 5 * NP$	(Sumatoria de Relevancias Máxima, NP: Número de procesos del Dominio)
(4)	$SD = \Sigma D$	(Sumatoria de Desempeños)
(5)	$SDM = 5 * NP$	(Sumatoria de Desempeños Máxima)
(6)	$IR = SR / SRM$	(Indice de Relevancias)
(7)	$ID = SD / SDM$	(Indice de Desempeños)
(8)	$IMD = ID / IR$	(Indice de Madurez del Dominio)
(9)	$SIM = \Sigma IM$	(Sumatoria de IM de los procesos del Dominio)
(10)	$PIM = SIM / NP$	(Promedio de IM del Dominio)
(11)	$MD = PIM * IMD$	(Madurez del Dominio)

Finalmente, de acuerdo con su IM (Formula 1), los procesos del dominio se clasifican en *procesos críticos* (Riesgo Alto) si IM < 1, *procesos estables* (Riesgo Moderado) si IM = 1, y *procesos aceptables* si IM > 1. Cuanto más cerca esté el valor IM de cero, más crítico y mayor vulnerabilidad a riesgos tendrá. Cuanto más sea IM mayor que uno, más aceptable y seguro será respecto a amenazas que generen vulnerabilidad al riesgo. Estas mismas interpretaciones valen para el análisis del valor MD del dominio total.

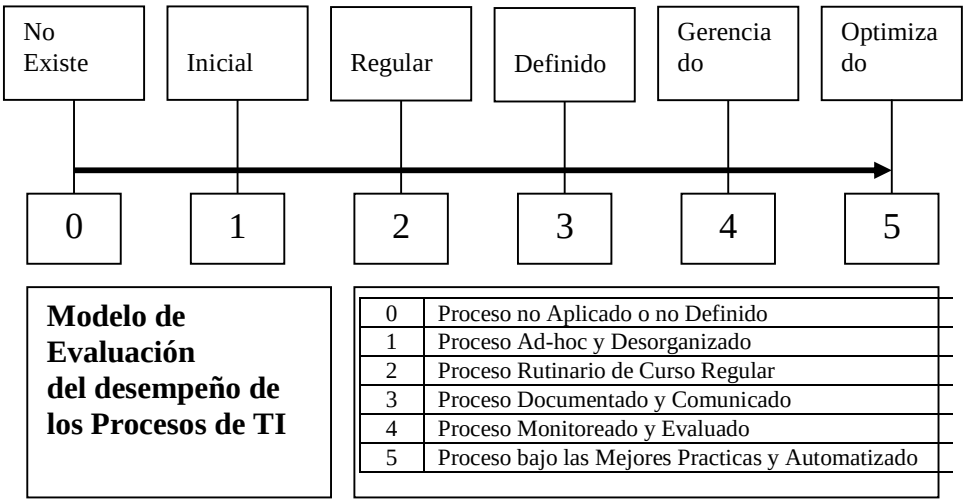


Grafico 8: Escala de evaluación del desempeño de procesos de TI basada en el modelo de madurez definido por el Software Engineering Institute para la capacidad de desarrollo de software.

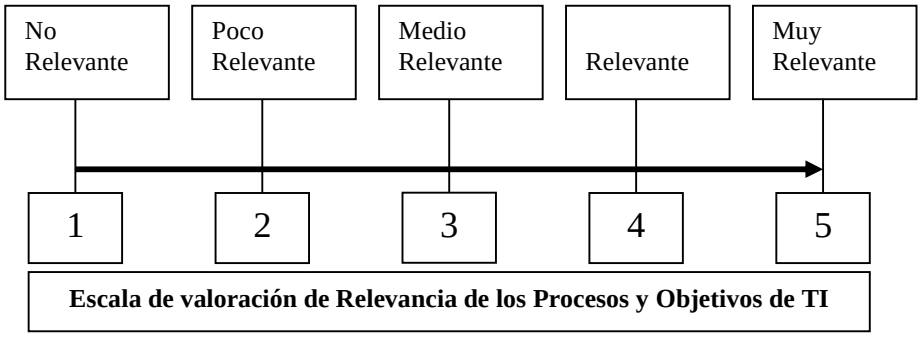


Grafico 9: Fuente propia. Escala de valoración de Relevancia de los procesos y objetivos de TI

7. **Evaluación de los Objetivos de Control Específicos.** La evaluación de los objetivos control específicos detallados por cada proceso seleccionado en el alcance, se obtiene mediante la aplicación de dos variables denominadas *Relevancia* (mide el grado de significancia e importancia del cumplimiento del objetivo de control especifico, para el cumplimiento del objetivo de control de alto nivel del proceso) y *Valoración* (asigna el grado de cumplimiento o ausencia del objetivo de control especifico para el proceso). La escala de Relevancia es la misma utilizada para la evaluación de los procesos y mostrada en el **Gráfico 9**. La escala para la Valoración se representa en el **Gráfico 10**. Analíticamente, el valor del Indice de Evaluación asociado al objetivo de control esta determinado por el producto:

(12) $IE = R * V$

Donde el Indice de Evaluación (IE), representa una relación directamente proporcional a la Relevancia (R) y a la Valoración (V). El dominio de R es [1,5], el dominio de V es [0,1] obteniéndose un rango de [0,5] para IE.

Una vez obtenidos los IE por cada uno de los objetivos correspondientes al proceso evaluado (en caso de la evaluación total del proceso), se obtienen los índices de evaluación del proceso a partir de sus objetivos de control específicos, con las siguientes expresiones analíticas:

(13) $SR = \Sigma R$ (Sumatoria de Relevancias del Proceso)

(14) $SRM = 5 * NO$ (Sumatoria de Relevancias Máxima, NO: Número de Objetivos del Proceso)

(15) $IR = SR / SRM$ (Indice de Relevancias del Proceso)

(16)	SIE = Σ IE	(Sumatoria de IE de los Objetivos del Proceso)
(17)	PIE = SIE / NO	(Promedio de IE del Proceso)
(18)	ICP = PIE / 5,00	(Indice de Control del Proceso → % de Control del Proceso)

Finalmente, de acuerdo con su IE (Formula 12), los objetivos específicos del proceso se clasifican en *objetivos críticos* (Riesgo Alto con Debilidades de Control) si IE < PIE, *objetivos estables* (Riesgo Moderado) si IE = PIE y *objetivos aceptables* (Riesgo Bajo con Fortalezas de Control) si IE > PIE. Cuanto más cerca esté el valor IE de cero, más crítico y generador de vulnerabilidad a riesgos por la falta de control. Cuanto más sea IE cercano a 5,00, más efectivo será el control respecto a amenazas que generen vulnerabilidad al riesgo. Estas mismas interpretaciones valen para el análisis del valor ICP del proceso total.

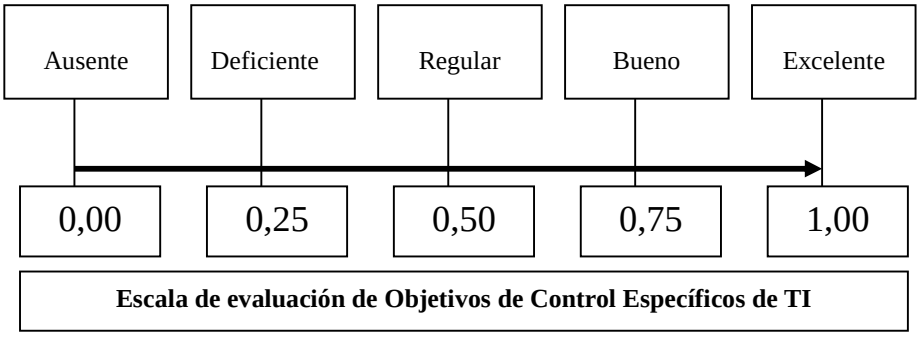


Grafico 10: Fuente propia. Escala de evaluación de los Objetivos de Control específicos de los procesos de TI

8. **Información de aplicación de las Guías de Auditoría**. Con referencia en las Guías de Auditoría *COBIT*, documentadas en el modelo por cada proceso del alcance del plan de auditoría, se registran los resultados de aplicación y desarrollo de los procedimientos de auditoría que sustentan el Informe de Evaluación y Auditoria. El modelo permite el registro de la información de: (a) Obtención y comprensión del negocio mediante el detalle de entrevistas, personas, fechas, temática, comentarios, referencias a instrumentos, cuestionarios, checklist e investigación documental pertinente al alcance de la auditoria, determinación de información sensitiva, indicadores claves de desempeño. referencias a documentos, análisis de entrevistas y observaciones complementarias; (b) Resultados de la evaluación de los controles de Alto Nivel (Procesos por Dominio) y de los Objetivos de Control Específicos por proceso con los indicadores de evaluación obtenidos por la aplicación de los métodos del modelo y estudio de los factores críticos de éxito mediante la aplicación de los principios de auditoria profesional; (c) Conformación de la valoración de la evaluación y auditoría mediante exámenes de pruebas de cumplimiento y sustantivas , correspondencia con las prescripciones, determinación de evidencias y justificativos de las evaluaciones con referencia a los papeles de trabajo de la auditoria; (d) Confirmación y verificación del riesgo con el desarrollo de actividades analíticas y/o complementarias con fuentes de consulta satisfactorias como soporte de la opinión, documentación sobre debilidades, amenazas y vulnerabilidades identificando y documentando las situaciones de impacto de los riesgos actuales y futuros detectados.
9. **Opinión del Auditor**. El modelo facilita el registro de información sobre la aplicación y resultados del Plan de Evaluación y Auditoría por cada proceso (Objetivo de Control de Alto Nivel) asociado a la definición del alcance, indicando las observaciones y recomendaciones para el Informe de Auditoría.
10. **Emisión del Informe**. La emisión del informe de Evaluación y Auditoría en cumplimiento del plan, incorporando el resumen de información contenida en el registro de opinión anterior.

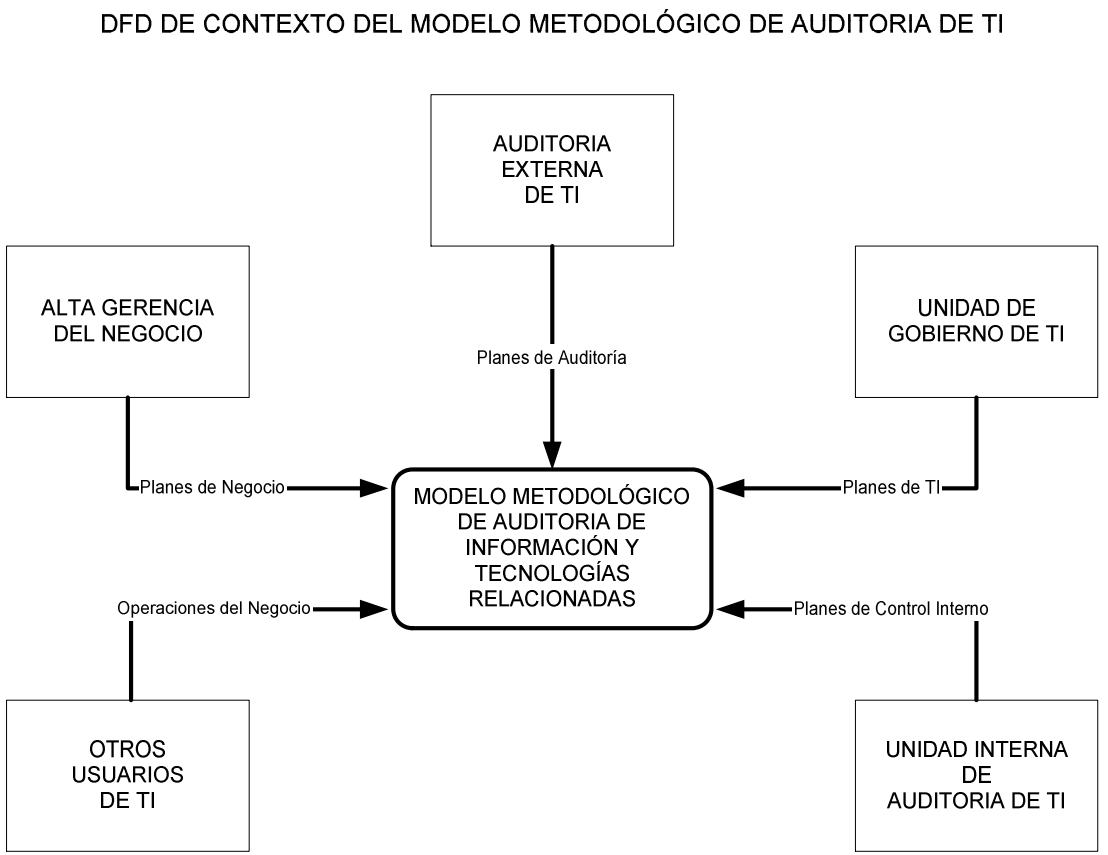


Gráfico 11. Fuente propia, DFD contextual (Nivel 0) del Modelo Metodológico de Evaluación y Auditoría de TI

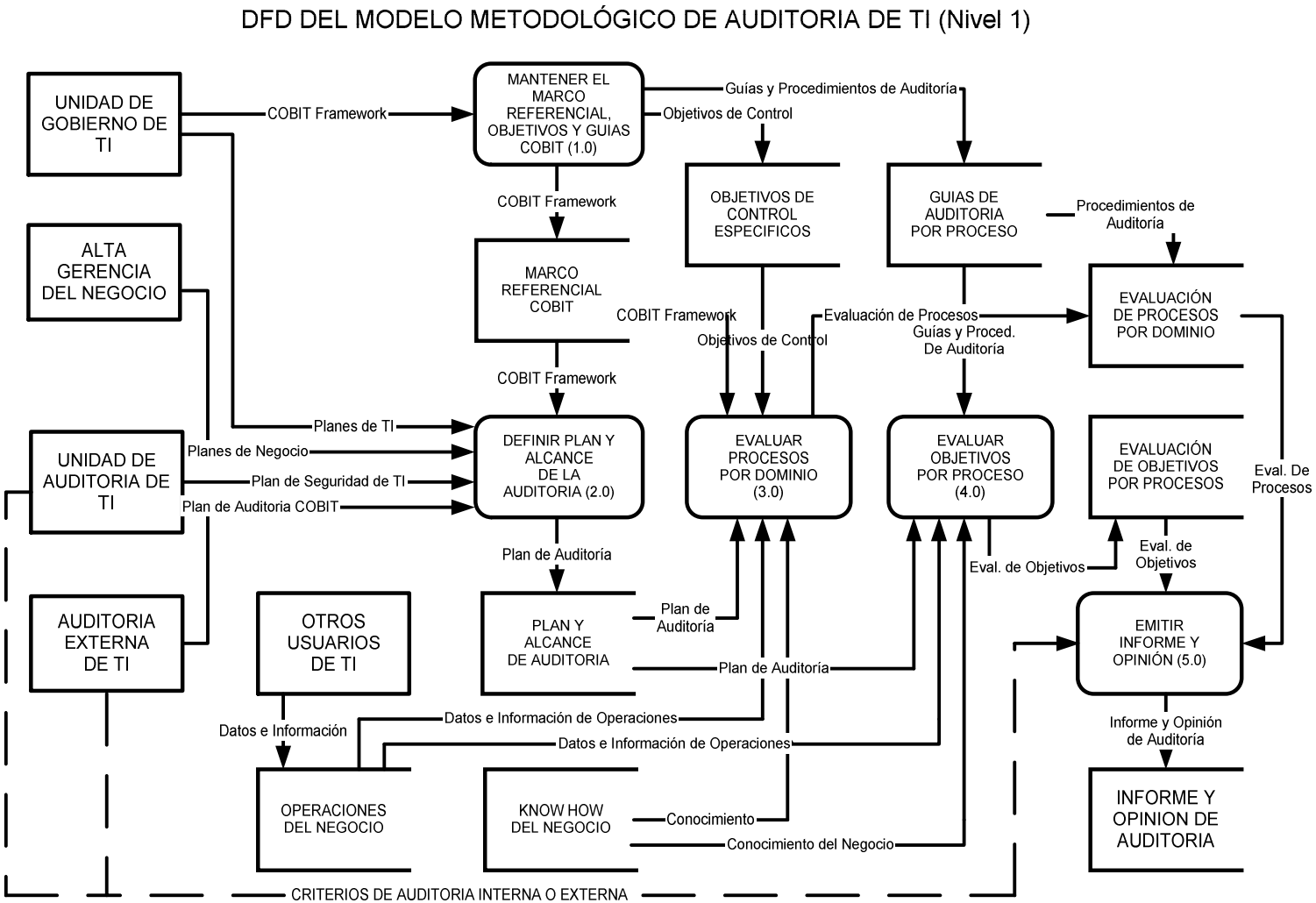


Gráfico 12. Fuente propia, DFD (Nivel 1) del Modelo Metodológico de Evaluación y Auditoría de TI

Diseño de la Propuesta de Software para la Implantación del Modelo

Seguidamente, se presentan el diseño lógico conceptual de la aplicación de software propuesta para la ejecución y validación del modelo. A continuación y en este orden se presenta el modelo lógico de datos a nivel de entidades, el diseño físico de la base de datos (denominada COBIT), el modelo relacional de la base de datos, el diseño de formularios de captura y consulta, e informes de datos y resultados de los procesos de evaluación de procesos (Objetivos de Control de Alto Nivel) y Objetivos de Control Específicos por proceso. Para la implantación física de los componentes de software expuestos en el presente modelo se ha utilizado como herramienta de desarrollo e implantación el software Microsoft Access 2000. La muestra de diseño presentada no intenta representar la totalidad formal de una aplicación para el usuario final, sino la representación factible del modelo de software que puede desarrollarse para satisfacer los requerimientos de aplicación del *Modelo Metodológico de Auditoría de Información y Tecnología Relacionada.* Para facilitar su comprensión y visualización, se alimentaron las estructuras con datos de prueba para el Dominio PO: Planificación y Organización, proceso PO1: Definición de un Plan Estratégico de TI, considerando la importancia de las actividades, tareas y objetivos del proceso de planificación estratégica de TI para la alineación de los objetivos del negocio con los procesos de TI. También como referencia al resultado diagnostico del presente caso de estudio, en el cual los procesos PO1 y DS6 resultaron ser autoevaluados como los procesos más sensibles al riesgo por parte del grupo de trabajo entrevistado. **Es importante,** mencionar en esta parte, que los datos de prueba que se presentan a continuación en el modelo de software, no corresponden estrictamente a la realidad del caso de estudio, los cuales, por la confidencialidad y sensibilidad de la información para la seguridad de la organización Banco Sofitasa, no son utilizados en toda su dimensión.

Modelo Lógico Conceptual de Datos

Entidades

Representación del Marco Referencial COBIT (COBIT Framework):

1. **Dominios:** Dominios COBIT
2. **Procesos:** Procesos (Objetivos de Control de Alto Nivel) por dominio
3. **Criterios:** Criterios o requerimientos de información del negocio indicando tipo de criterio (P)rimario, (S)ecundario
4. **Recursos:** Recursos de TI
5. **Procesos-Criterios:** Criterios de información asociados a procesos
6. **Procesos-Recursos:** Recursos asociados a procesos

Representación del Marco de Control:

7. **Objetivos:** Objetivos de Control Específicos detallados por proceso
8. **Guias-Auditoria:** Guías de Auditoría por proceso

Representación del Modelo integrado al Marco Referencial y de Control:

9. **Planes:** Registro de planes o revisiones de evaluación y auditoría
10. **Alcances:** Registro de procesos y objetivos asociados al plan de auditoria con indicación de la evaluación por objetivo detallado
11. **Evaluación:** Registro de procesos asociados al plan de auditoria con indicación de la evaluación por proceso (Objetivo de Alto Nivel)
12. **Relevancias:** Escala de valores de significancia e importancia de procesos y objetivos detallados por proceso
13. **Desempeño:** Escala de valores del nivel de desempeño o madurez de los procesos u objetivos de control de alto nivel.
14. **Valores:** Escala de valoración del cumplimiento o ausencia de objetivos de control detallados por proceso

Diseño Físico de Entidades (MS Access-2000)

El diseño físico de las entidades para el modelo propuesto se implantó utilizando el manejador de bases de datos de Microsoft Access 2000. Las tablas definidas en el modelo lógico de datos se diseñaron físicamente en una base de datos de nombre **cobit.mdb** como puede observarse en el **Gráfico 12.** Para los efectos de identificación del diseño físico de las tablas contenidas en esta base de datos, todos los esquemas gráficos de las tablas son referidos al Gráfico 12.

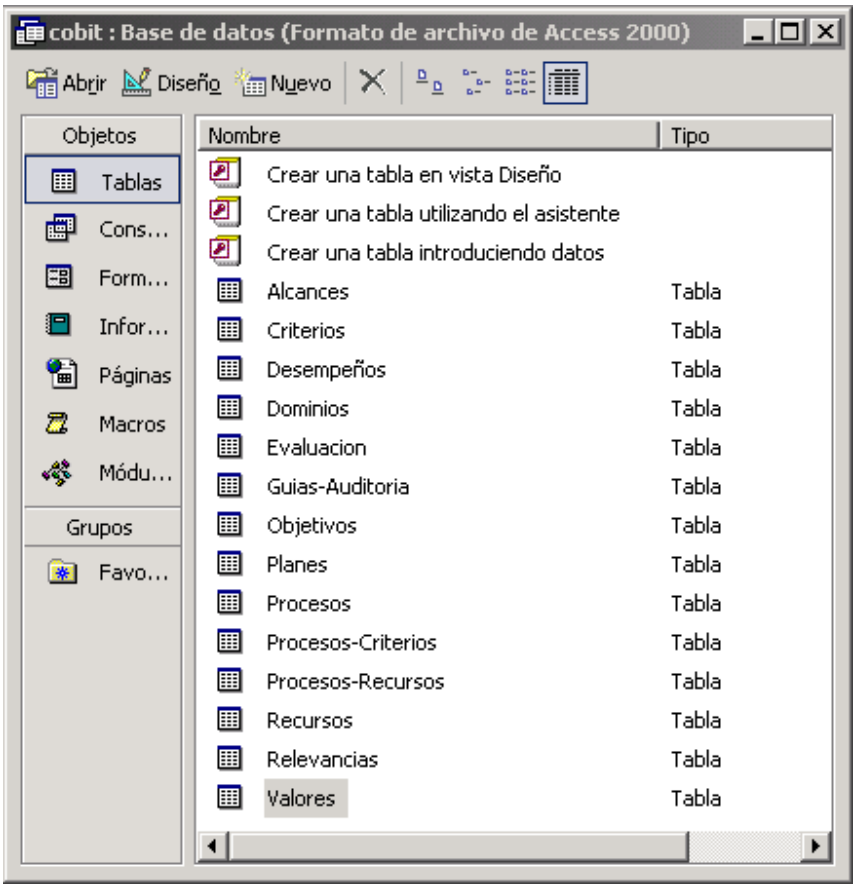


Gráfico 13. Implantación del diseño físico de la base de datos del modelo

Dominios : Tabla

Nombre del campo	Tipo de datos	Descripción
Dominio	Texto	Codigo del dominio
Nombre_Dominio	Texto	Descripción del dominio

Procesos : Tabla

Nombre del campo	Tipo de datos	Descripción
Dominio	Texto	Codigo de dominio
Proceso	Texto	Codigo de proceso
Nombre_Proceso	Texto	Descripción de proceso
Requerimiento	Memo	Requerimientos de información
Posibilidad	Memo	Se posibilita por…
Consideracion	Memo	Toma en consideración…

Criterios : Tabla

Nombre del campo	Tipo de datos	Descripción
Criterio	Texto	Numero de criterio
Nombre_Criterio	Texto	Descripción de criterio

Recursos : Tabla

Nombre del campo	Tipo de datos	Descripción
Recurso	Texto	Numero de recurso
Nombre_Recurso	Texto	Descripción de recurso

Procesos-Criterios : Tabla

Nombre del campo	Tipo de datos	Descripción
Proceso	Texto	Codigo de proceso
Criterio	Texto	Numero de criterio
Tipo-Criterio	Texto	Tipo de criterio (P)rimario - (S)ecundario

Procesos-Recursos : Tabla

Nombre del campo	Tipo de datos	Descripción
Proceso	Texto	Codigo de proceso
Recurso	Texto	Numero de recurso

Objetivos : Tabla

Nombre del campo	Tipo de datos	Descripción
Proceso	Texto	Codigo de proceso
Objetivo	Texto	Codigo de objetivo de control
Nombre-Objetivo	Memo	Descripción del obejtivo de control
Descripción-Control	Memo	Descripción de técnicas de control

Guias-Auditoria : Tabla

Nombre del campo	Tipo de datos	Descripción
Proceso	Texto	Codigo de proceso
Entrevistando-A	Memo	Relación de personal a entrevistar
Obteniendo	Memo	Información que debe obtenerse
Considerando-Si	Memo	Consideraciones sobre la información
Examinando-Que	Memo	Examenes que deben hacerse
Desarrollando	Memo	Actividades que deben desarrollarse
Identificando	Memo	Identificación de situaciones de riesgo

Planes : Tabla

Nombre del campo	Tipo de datos	Descripción
Plan-Auditoria	Texto	Código del plan de auditoría
Empresa	Texto	Descripción de la empresa auditada
Auditor	Texto	Nombre del auditor responsable
Supervisor	Texto	Nombre del supervisor interno
Fecha-Inicio	Fecha/Hora	Fecha de inicio del plan
Fecha-Final	Fecha/Hora	Fecha de finalización del plan
Fecha-Seguimiento	Fecha/Hora	Fecha de la ultima revisión
Revisor	Texto	Nombre del revisor

Alcances : Tabla

Nombre del campo	Tipo de datos	Descripción
Plan	Texto	Código del plan de auditoría
Proceso	Texto	Código del proceso a auditar
Objetivo	Texto	Código del objetivo a evaluar
Valor	Número	Valoración del objetivo evaluado
Relevancia	Número	Relevancia asiganada al objetivo

Evaluacion : Tabla

Nombre del campo	Tipo de datos	Descripción
Plan	Texto	Codigo del plan de auditoría
Proceso	Texto	Codigo del proceso evaluado
Relevancia	Número	Relevancia asignada al proceso
Desempeño	Número	Nivel de desempeño asignado al proceso
Entrevistas	Memo	Detalle de entrevistas realizadas
Obtenciones	Memo	Detalle de la información obtenida
Consideraciones	Memo	Detalle de las consideraciones tomadas en cuenta
Examenes	Memo	Examenes aplicados y papeles de trabajo
Desarrollos	Memo	Actividades desarrolladas
Identificaciones	Memo	Detalle de situaciones ed riesgo identificadas
Opinión	Memo	Resumen de opinión del auditor para el informe

Relevancias : Tabla

Nombre del campo	Tipo de datos	Descripción
Relevancia	Número	Codigo de relevancia de procesos y objetivos
Descripcion	Texto	Descripción de relevancia

Desempeños : Tabla

Nombre del campo	Tipo de datos	Descripción
Desempeño	Número	Codigo del nivel de desempeño de procesos
Descripcion	Texto	Descripción breve del desempeño
Comentario	Texto	Comentario amplio del nivel de desempeño

Valores : Tabla

Nombre del campo	Tipo de datos	Descripción
Valor	Número	Valor de evaluación de objetivos de control
Descripcion	Texto	Descripción de la valoración de evaluación

Diseño Relacional de la Base de Datos

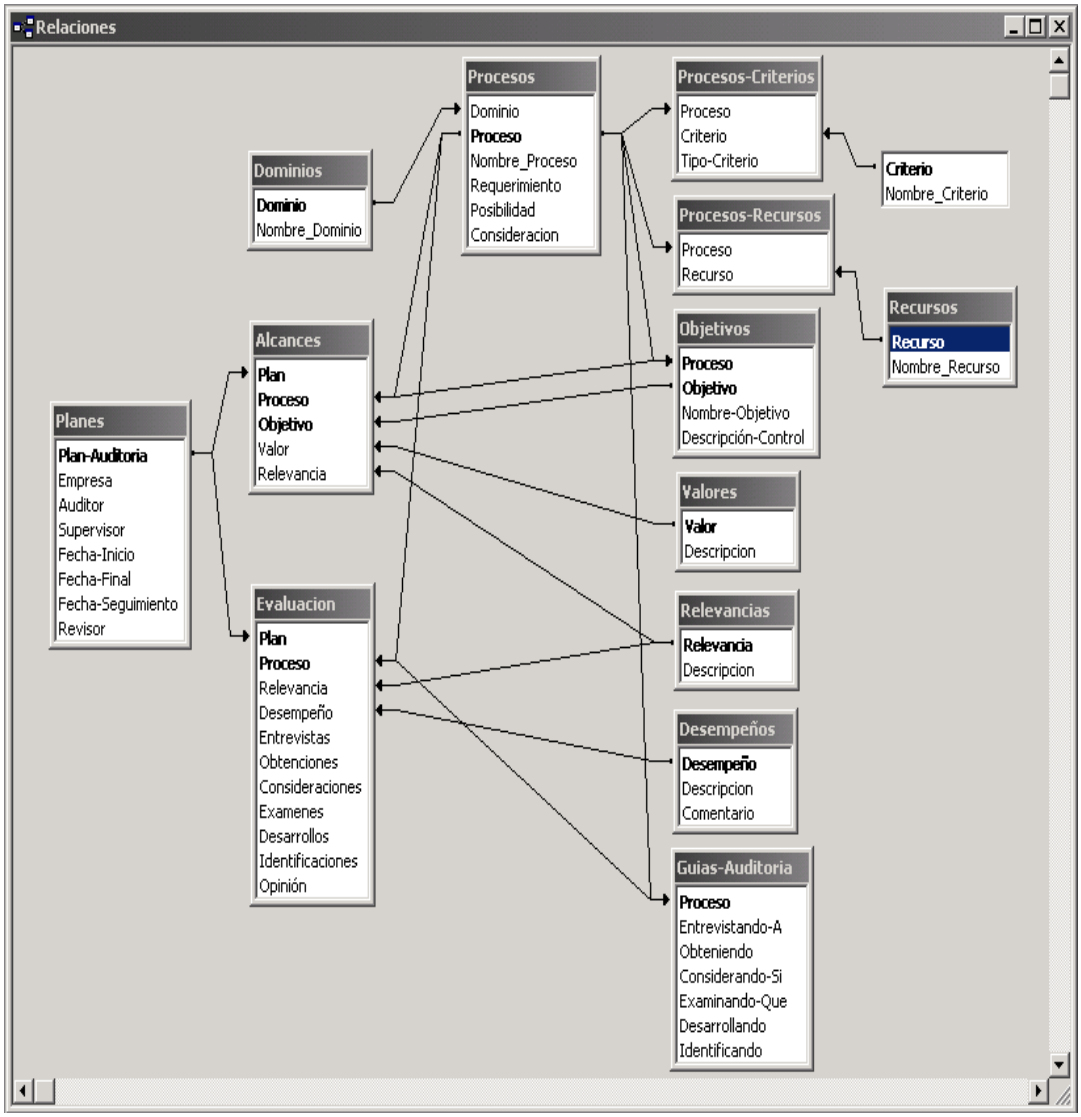


Gráfico 14: Diseño relacional de la base de datos del modelo

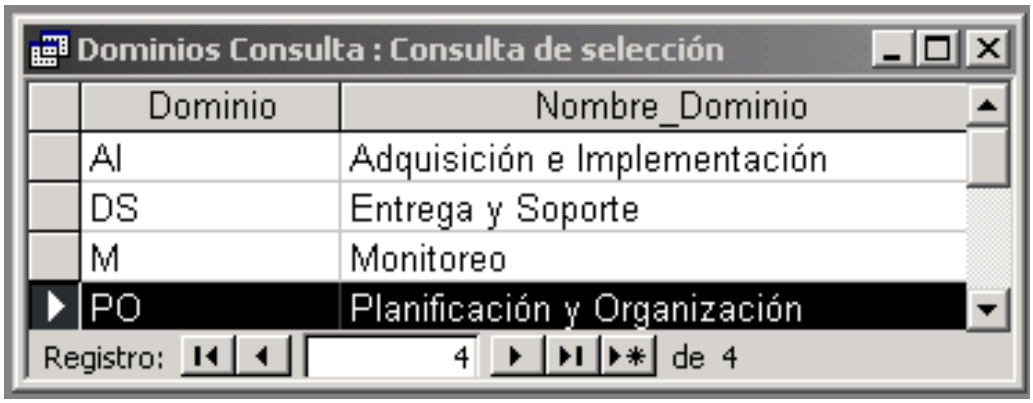
Diseño de Entrada y Salida

Para los efectos de captura de datos de los registros de prueba del modelo se diseñaron formularios de entrada y consulta de datos y en el caso de datos extensos para ciertas categorías de información se diseñaron informes que permiten visualizar y comprender la ejecución del modelo de auditoría y control. Los datos de prueba se relacionaron con el domino PO: Planificación y Organización, proceso PO1: Definición de un Plan Estratégico de TI, para el cual se asignaron en el alcance del modelo los 11 objetivos de control detallados y específicos al proceso en evaluación.

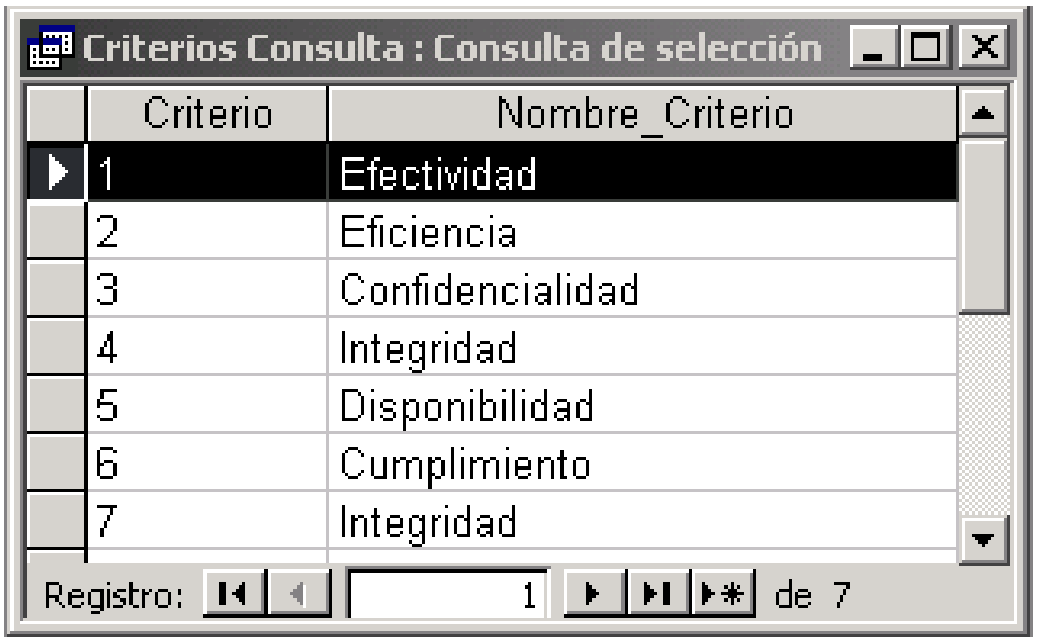
En los formularios que se presentan a continuación, se han hecho abstracciones de algunos registros de entrada para las diferentes categorías de datos e inmediatamente a continuación se presenta un formulario de consulta si son pocos los registros contenidos en la categoría de datos, o un informe si los datos de la categoría son extensos para ser presentados en una consulta. El objeto de las presentaciones siguientes, formularios e informes, es visualizar en la práctica las diferentes relaciones de datos del modelo propuesto y los mecanismos de evaluación y procedimientos de auditoría desde la fase de planificación hasta la fase de opinión pasando por la fase de evaluación y examen.

El orden de exposición de los elementos de entrada y salida se corresponde con el orden de ejecución del modelo según el DFD propuesto en el **Gráfico 11** que se resume en los siguientes procesos generales: (1) Mantenimiento del Marco Referencial COBIT (COBIT Framework): Dominios, Procesos, Criterios, Recursos; Mantenimiento de Objetivos de Control Detallados y Guías de Auditoría; (2) Mantenimiento de Planes de Auditoría; Definición de Alcance de la Auditoría a nivel de Procesos y Objetivos; (3) Evaluación de Procesos por Dominio; (4) Evaluación de Objetivos de Control Específicos Detallados por Proceso; (5) Aplicación de Auditoria según las Guías y Procedimientos y Emitir el Informe y Opinión. (Este último proceso consta del registro de la información y opinión para alimentar el informe).

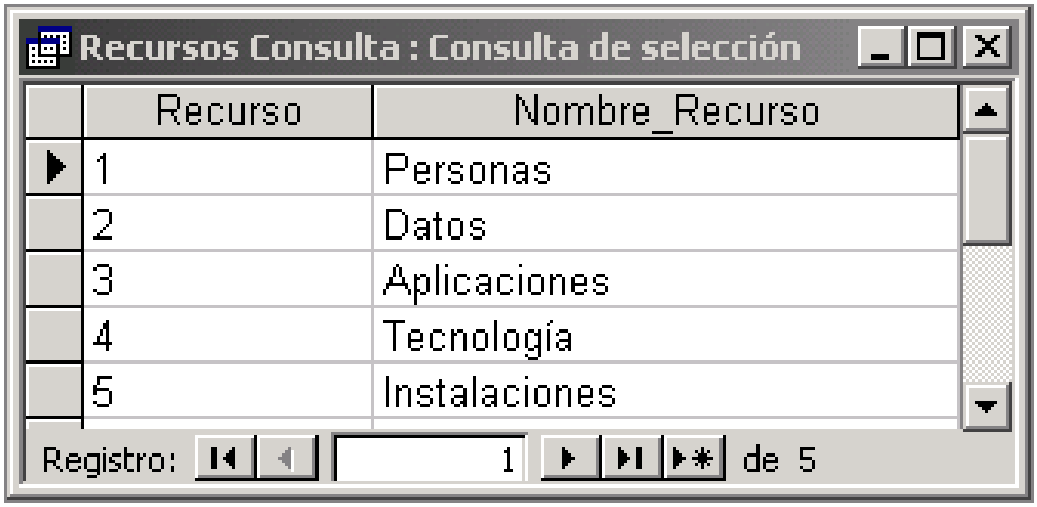
Gráfico 15: Formatos de Entrada / Salida

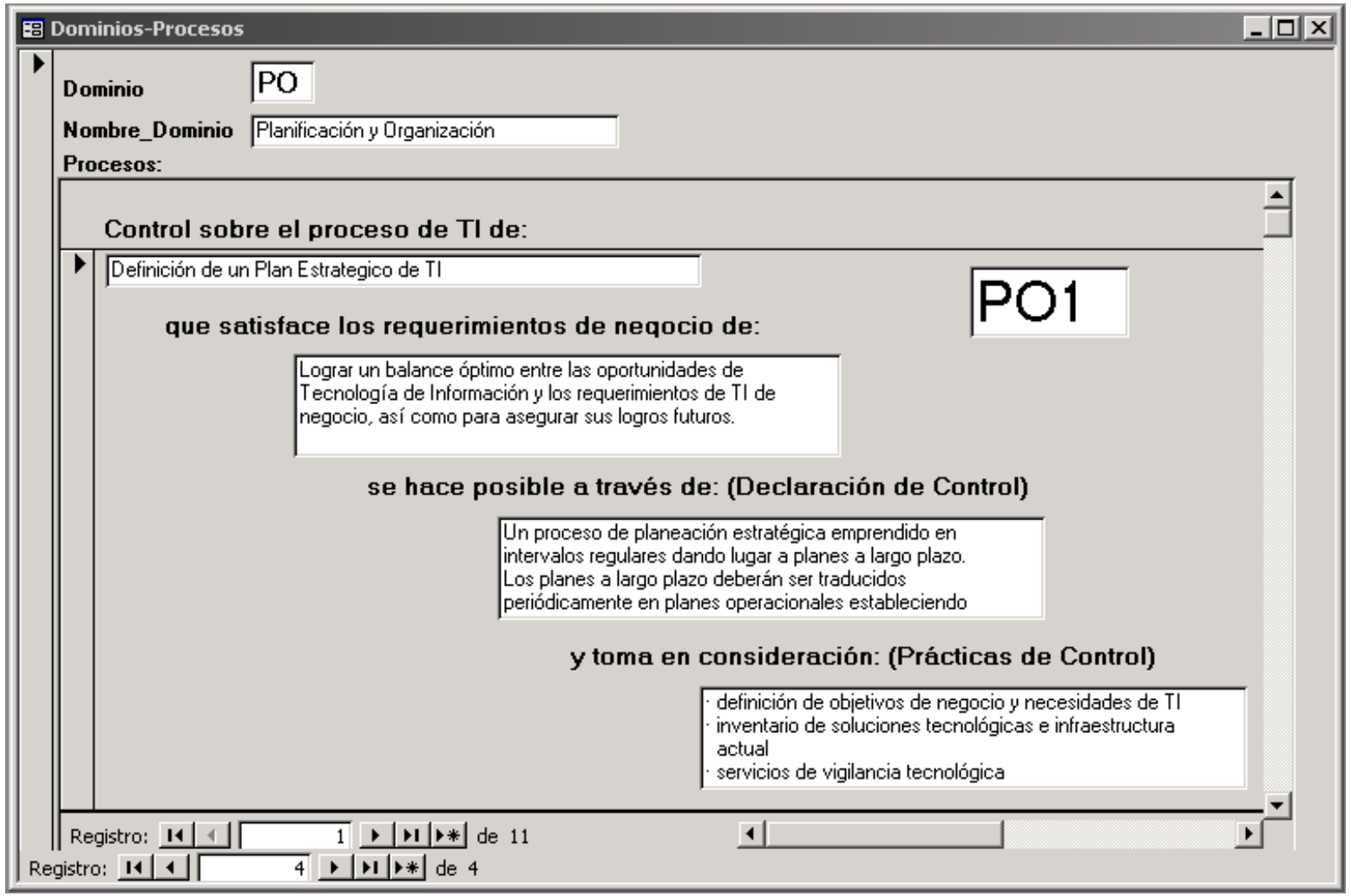


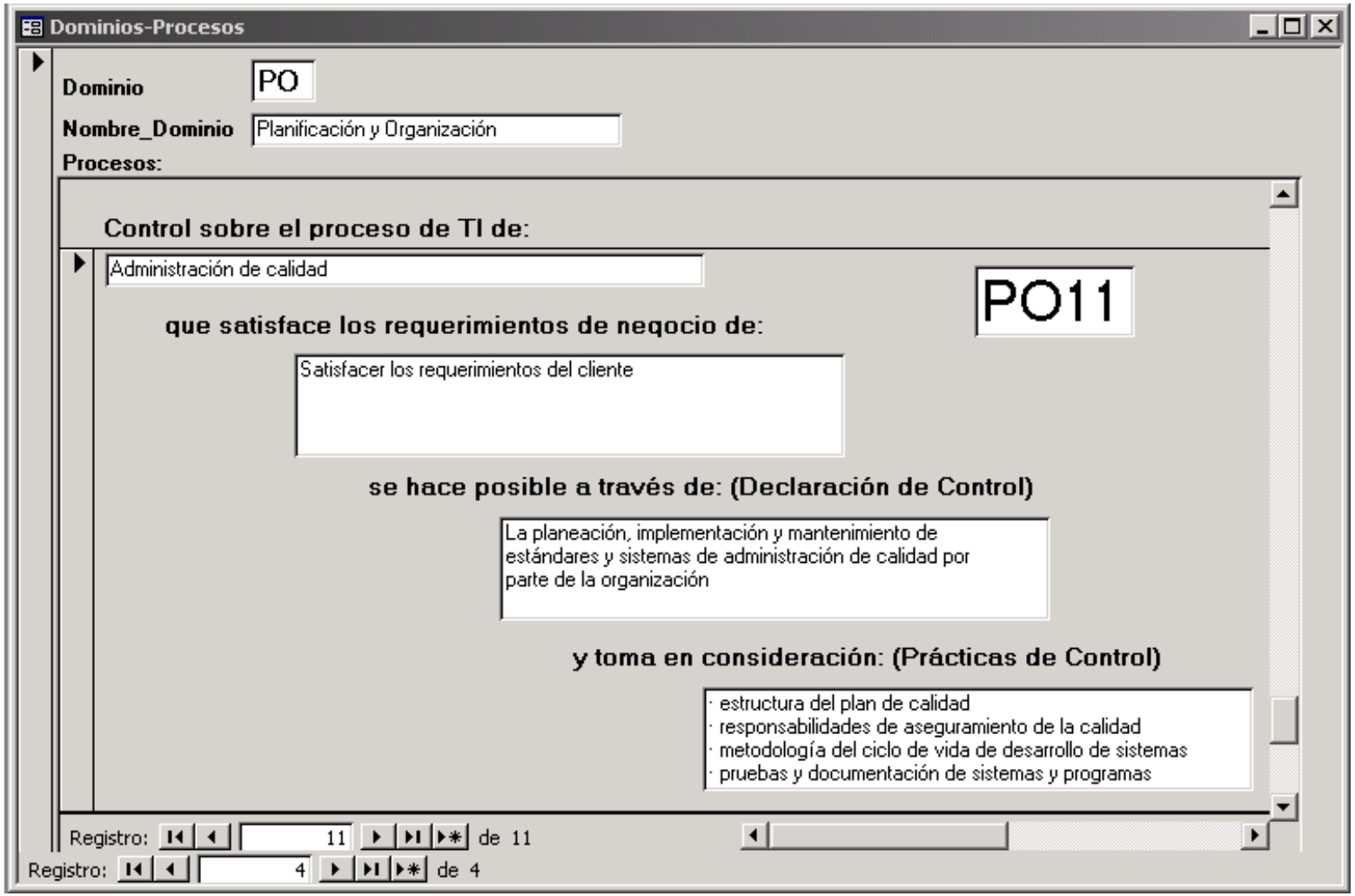

Criterios
Criterio
1
Nombre_Criterio
Efectividad
Registro:
1
de 7

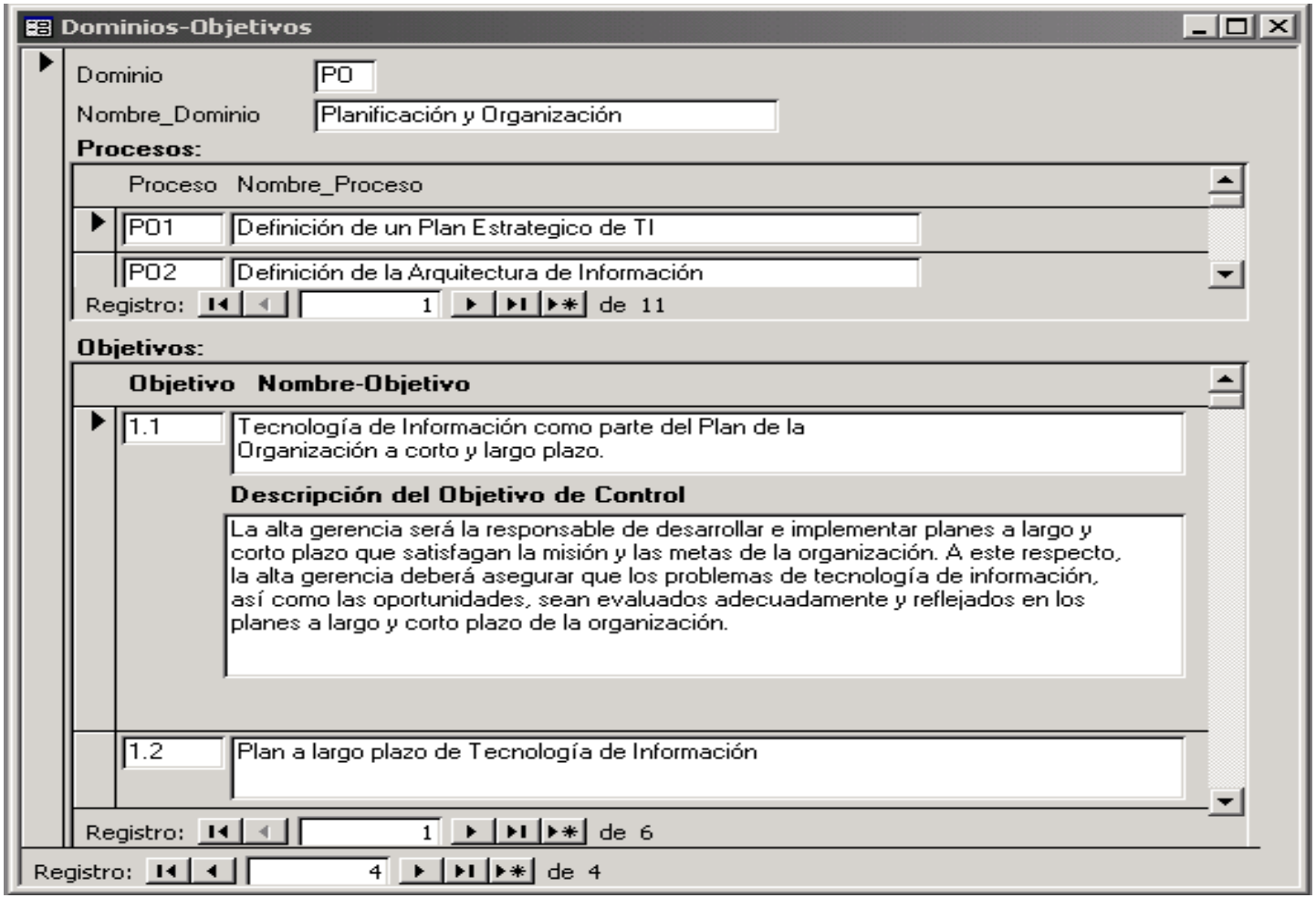

Criterios Consulta : Consulta de selección
Criterio
Nombre_Criterio
1
Efectividad
2
Eficiencia
3
Confidencialidad
4
Integridad
5
Disponibilidad
6
Cumplimiento
7
Integridad
Registro:
1
de 7

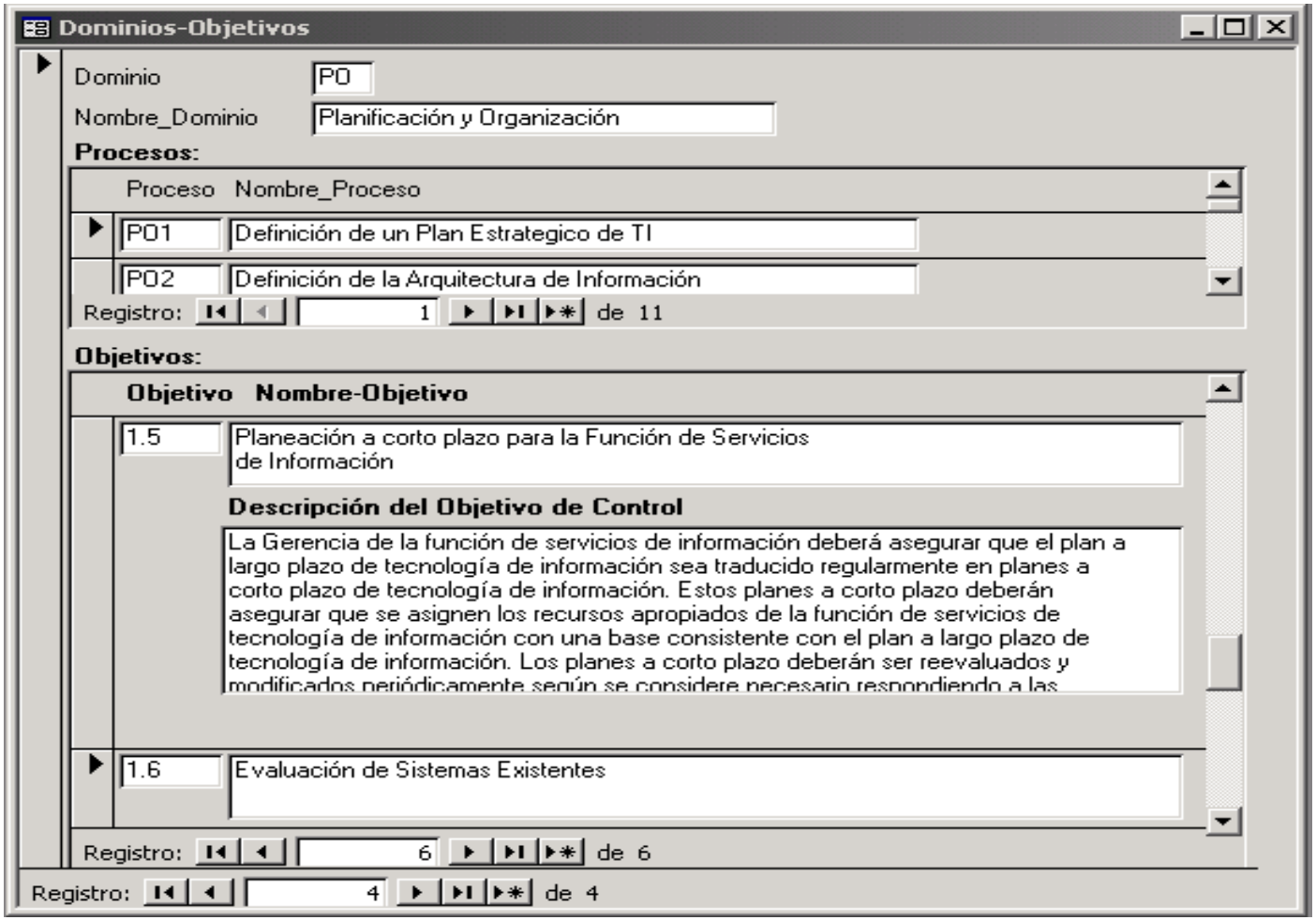

Recursos
Recurso
1
Nombre_Recurso
Personas
Registro:
1
de 5

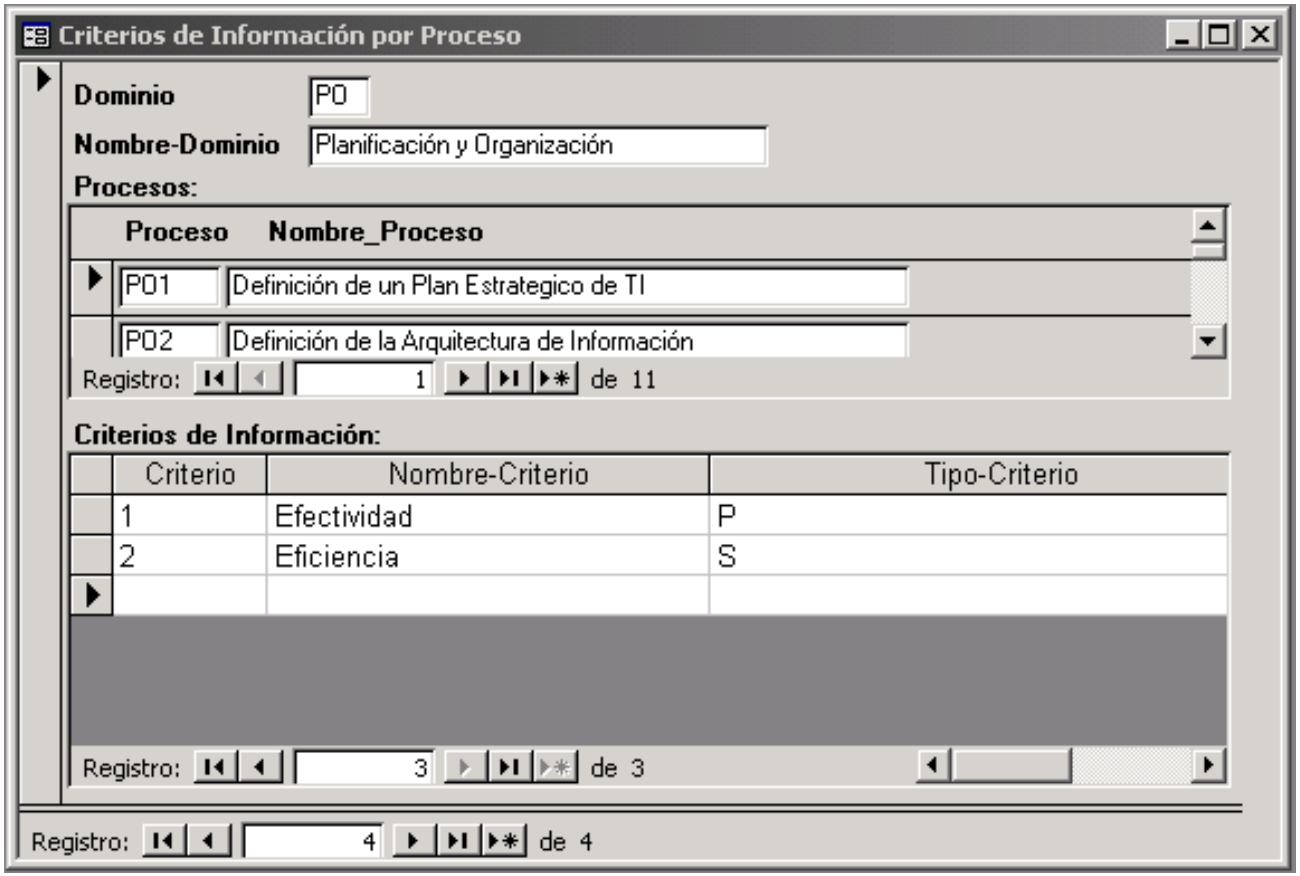

Recursos Consulta : Consulta de selección
Recurso
Nombre_Recurso
1
Personas
2
Datos
3
Aplicaciones
4
Tecnología
5
Instalaciones
Registro:
1
de 5

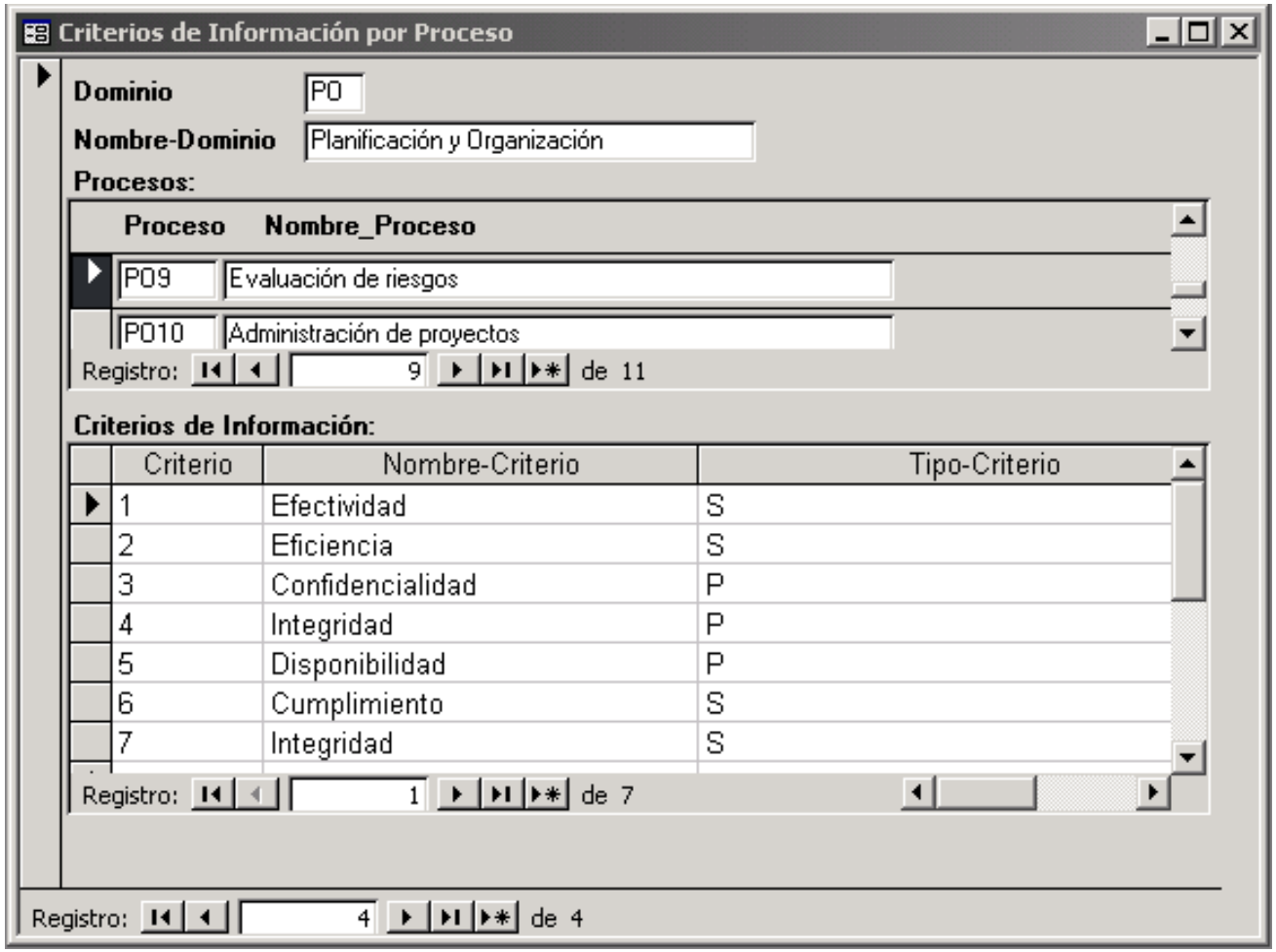

Dominios-Procesos
Dominio
PO
Nombre_Dominio
Planificación y Organización
Procesos:
Control sobre el proceso de TI de:
Definición de un Plan Estrategico de TI
PO1
que satisface los requerimientos de negocio de:
Lograr un balance óptimo entre las oportunidades de Tecnología de Información y los requerimientos de TI de negocio, así como para asegurar sus logros futuros.
se hace posible a través de: (Declaración de Control)
Un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo. Los planes a largo plazo deberán ser traducidos periódicamente en planes operacionales estableciendo
y toma en consideración: (Prácticas de Control)
· definición de objetivos de negocio y necesidades de TI
· inventario de soluciones tecnológicas e infraestructura actual
· servicios de vigilancia tecnológica
Registro: 1 de 11
Registro: 4 de 4


Dominios-Procesos
Dominio
PO
Nombre_Dominio
Planificación y Organización
Procesos:
Control sobre el proceso de TI de:
Administración de calidad
PO11
que satisface los requerimientos de negocio de:
Satisfacer los requerimientos del cliente
se hace posible a través de: (Declaración de Control)
La planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por parte de la organización
y toma en consideración: (Prácticas de Control)
· estructura del plan de calidad
· responsabilidades de aseguramiento de la calidad
· metodología del ciclo de vida de desarrollo de sistemas
· pruebas y documentación de sistemas y programas
Registro: 11 de 11
Registro: 4 de 4


Dominios-Objetivos
Dominio
PO
Nombre_Dominio
Planificación y Organización
Procesos:
Proceso Nombre_Proceso
PO1
Definición de un Plan Estrategico de TI
PO2
Definición de la Arquitectura de Información
Registro: 1 de 11
Objetivos:
Objetivo Nombre-Objetivo
1.1
Tecnología de Información como parte del Plan de la Organización a corto y largo plazo.
Descripción del Objetivo de Control
La alta gerencia será la responsable de desarrollar e implementar planes a largo y corto plazo que satisfagan la misión y las metas de la organización. A este respecto, la alta gerencia deberá asegurar que los problemas de tecnología de información, así como las oportunidades, sean evaluados adecuadamente y reflejados en los planes a largo y corto plazo de la organización.
1.2
Plan a largo plazo de Tecnología de Información
Registro: 1 de 6
Registro: 4 de 4


Dominios-Objetivos
Dominio
P0
Nombre_Dominio
Planificación y Organización
Procesos:
Proceso
Nombre_Proceso
P01
Definición de un Plan Estrategico de TI
P02
Definición de la Arquitectura de Información
Registro:
1
de 11
Objetivos:
Objetivo
Nombre-Objetivo
1.5
Planeación a corto plazo para la Función de Servicios de Información
Descripción del Objetivo de Control
La Gerencia de la función de servicios de información deberá asegurar que el plan a largo plazo de tecnología de información sea traducido regularmente en planes a corto plazo de tecnología de información. Estos planes a corto plazo deberán asegurar que se asignen los recursos apropiados de la función de servicios de tecnología de información con una base consistente con el plan a largo plazo de tecnología de información. Los planes a corto plazo deberán ser reevaluados y
1.6
Evaluación de Sistemas Existentes
Registro:
6
de 6
Registro:
4
de 4

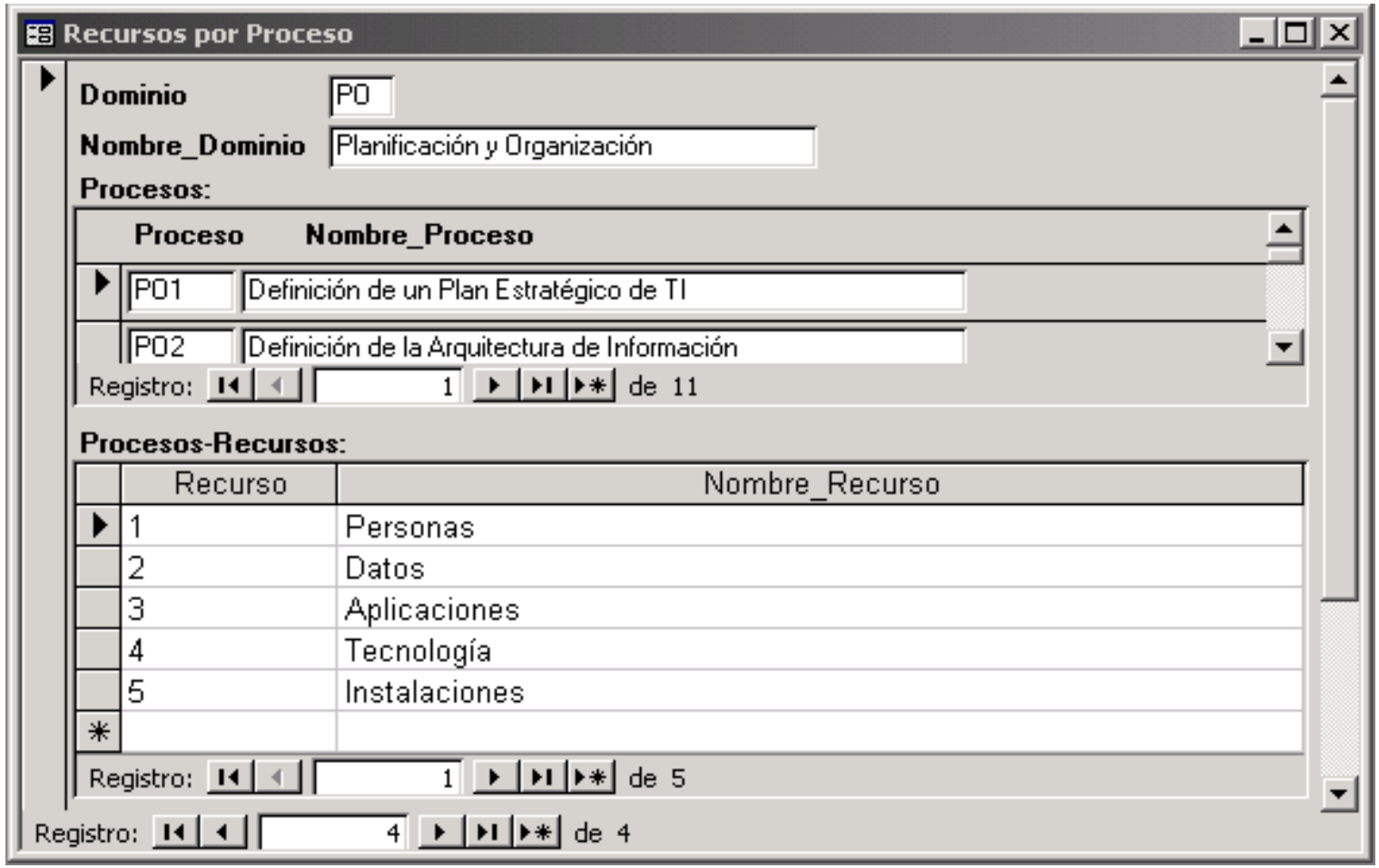

Criterios de Información por Proceso
Dominio
P0
Nombre-Dominio
Planificación y Organización
Procesos:
Proceso
Nombre_Proceso
P01
Definición de un Plan Estrategico de TI
P02
Definición de la Arquitectura de Información
Registro:
1
de 11
Criterios de Información:
Criterio
Nombre-Criterio
Tipo-Criterio
1
Efectividad
P
2
Eficiencia
S
Registro:
3
de 3
Registro:
4
de 4

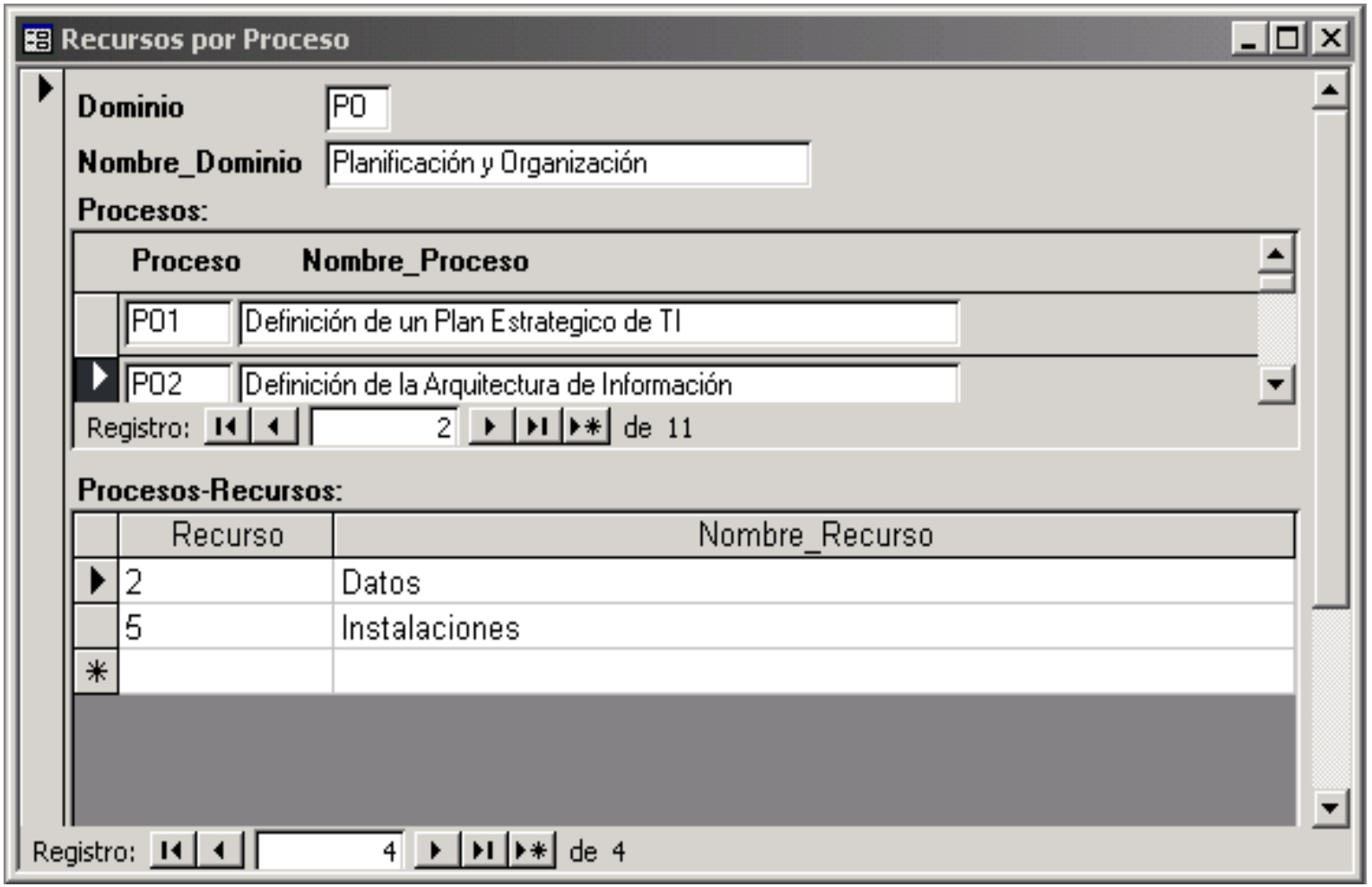

Criterios de Información por Proceso
Dominio
P0
Nombre-Dominio
Planificación y Organización
Procesos:
Proceso
Nombre_Proceso
P09
Evaluación de riesgos
P010
Administración de proyectos
Registro:
9
de 11
Criterios de Información:
Criterio
Nombre-Criterio
Tipo-Criterio
1
Efectividad
S
2
Eficiencia
S
3
Confidencialidad
P
4
Integridad
P
5
Disponibilidad
P
6
Cumplimiento
S
7
Integridad
S
Registro:
1
de 7
Registro:
4
de 4

Criterios de Información por Proceso

Dominio / Procesos	Requerimiento		Criterios	Tipo
PO Planificación y Organización				
PO1	Definición de un Plan Estrategico de TI			
	Lograr un balance óptimo entre las oportunidades de Tecnología de Información y los requerimientos de TI de negocio, así como para asegurar sus logros futuros.			
		1	Efectividad	P
		2	Eficiencia	S
PO2	Definición de la Arquitectura de Información			
	Organizar de la mejor manera los sistemas de información			
		1	Efectividad	P
		2	Eficiencia	S
		3	Confidencialidad	S
		4	Integridad	S
PO3	Determinación de la dirección tecnológica			
	Aprovechar la tecnología disponible o tecnología emergente			
		1	Efectividad	P
		2	Eficiencia	S
PO4	Definición de la organización y de las relaciones de TI			
	Prestación de servicios de TI			
		1	Efectividad	P
		2	Eficiencia	S
PO5	Manejo de la inversión			
	Asegurar el financiamiento y el control de desembolsos de recursos financieros			
		1	Efectividad	P
		2	Eficiencia	P
		7	Integridad	S
PO6	Comunicación de la dirección y aspiraciones de la gerencia			
	Asegurar el conocimiento y comprensión del usuario sobre dichas aspiraciones			
		1	Efectividad	P
		6	Cumplimiento	S

Dominio / Procesos		Requerimiento		Criterios	Tipo
PO7	Administración de recursos humanos				
		Maximizar las contribuciones del personal a los procesos de TI			
			1	Efectividad	P
			2	Eficiencia	P
PO8	Aseguramiento del cumplimiento de requerimientos				
		Cumplir con obligaciones legales, regulatorias y contractuales			
			1	Efectividad	P
			6	Cumplimiento	P
			7	Integridad	S
PO9	Evaluación de riesgos				
		Asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI			
			1	Efectividad	S
			2	Eficiencia	S
			3	Confidencialidad	P
			4	Integridad	P
			5	Disponibilidad	P
			6	Cumplimiento	S
			7	Integridad	S
PO10	Administración de proyectos				
		Establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión			
			1	Efectividad	P
			2	Eficiencia	P
PO11	Administración de calidad				
		Satisfacer los requerimientos del cliente			
			1	Efectividad	P
			2	Eficiencia	P
			4	Integridad	P
			7	Integridad	S


Recursos por Proceso
Dominio
P0
Nombre_Dominio
Planificación y Organización
Procesos:
Proceso
Nombre_Proceso
P01
Definición de un Plan Estratégico de TI
P02
Definición de la Arquitectura de Información
Registro: 1 de 11
Procesos-Recursos:
Recurso
Nombre_Recurso
1
Personas
2
Datos
3
Aplicaciones
4
Tecnología
5
Instalaciones
Registro: 1 de 5
Registro: 4 de 4


Recursos por Proceso
Dominio
P0
Nombre_Dominio
Planificación y Organización
Procesos:
Proceso
Nombre_Proceso
P01
Definición de un Plan Estrategico de TI
P02
Definición de la Arquitectura de Información
Registro:
2
de 11
Procesos-Recursos:
Recurso
Nombre_Recurso
2
Datos
5
Instalaciones
Registro:
4
de 4

Recursos por Proceso

Dominio / Procesos	Posibilidad	Recursos

PO Planificación y Organización

PO1 Definición de un Plan Estratégico de TI

Un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo.
Los planes a largo plazo deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo

1	Personas
2	Datos
3	Aplicaciones
4	Tecnología
5	Instalaciones

PO2 Definición de la Arquitectura de Información

La creación y mantenimiento de un modelo de información de negocios y asegurando que se definan sistemas apropiados para optimizar la utilización de esta información

2	Datos
5	Instalaciones

PO3 Determinación de la dirección tecnológica

La creación y mantenimiento de un plan de Infraestructura tecnológica

3	Aplicaciones
4	Tecnología

PO4 Definición de la organización y de las relaciones de TI

Una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas

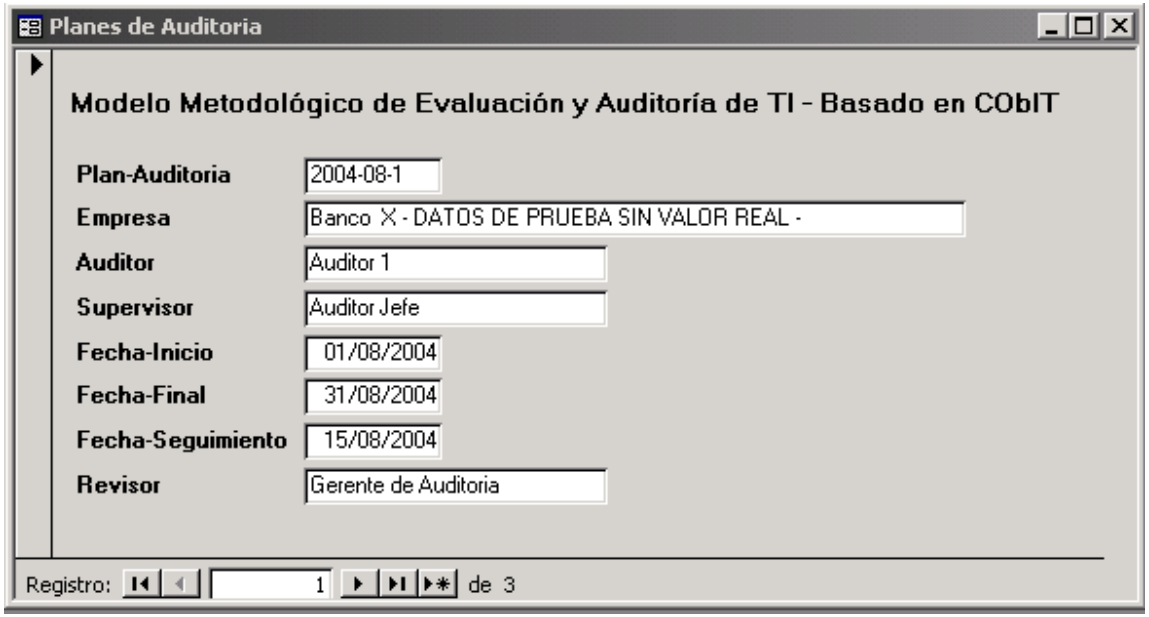
1	Personas

PO5 Manejo de la inversión

Presupuestos periódicos sobre inversiones y operación establecidos y aprobados por el negocio

1	Personas
2	Datos
3	Aplicaciones
4	Tecnología

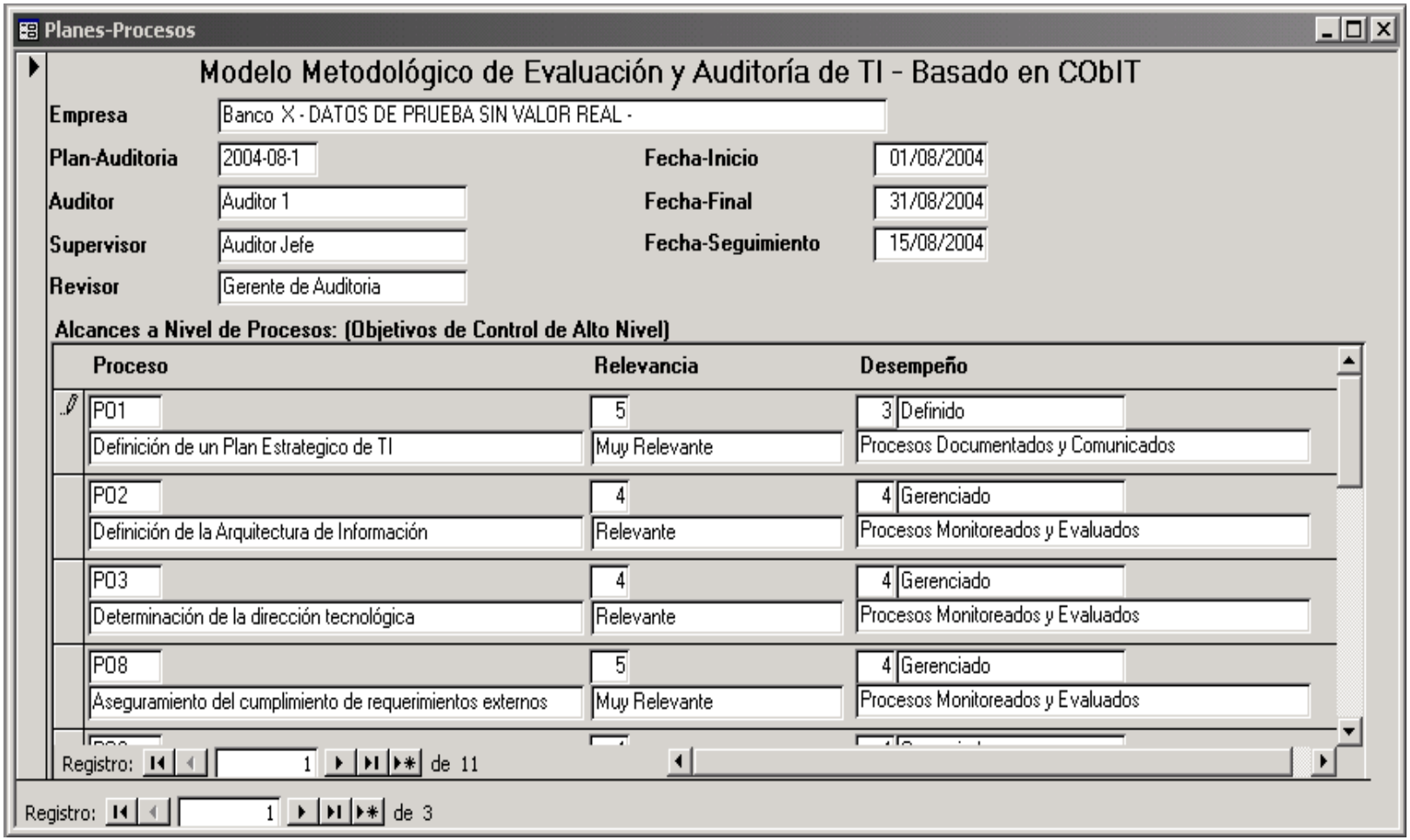
Dominio / Procesos	Posibilidad	Recursos
PO6 Comunicación de la dirección y aspiraciones de la gerencia		
	políticas establecidas y transmitidas a la comunidad de usuarios; además, se necesita estándares para traducir las opciones estratégicas en reglas de usuario prácticas utilizables	
		1 Personas
PO7 Administración de recursos humanos		
	Técnicas sólidas para administración de personal	
		1 Personas
PO8 Aseguramiento del cumplimiento de requerimientos externos		
	La identificación y análisis de los requerimientos externos en cuanto a su impacto en TI, y llevando a cabo las medidas apropiadas para cumplir con ellos	
		1 Personas
		2 Datos
		5 Instalaciones
PO9 Evaluación de riesgos		
	La participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos	
		1 Personas
		2 Datos
		3 Aplicaciones
		4 Tecnología
PO10 Administración de proyectos		
	Identificación y priorización de los proyectos en línea con el plan operacional por parte de la misma organización. Además, la organización deberá adoptar y aplicar sólidas técnicas de administración de proyectos para cada proyecto emprendido	
		1 Personas
		2 Datos
		3 Aplicaciones
		4 Tecnología
PO11 Administración de calidad		
	La planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por	
		1 Personas
		2 Datos
		3 Aplicaciones
		4 Tecnología
		5 Instalaciones



Planes Consulta : Consulta de selección

Plan-Auditoria	Empresa	Auditor	Supervisor	Fecha-Inicio	Fecha-Final	Fecha-Segu	Revisor
2004-08-1	Banco X - DATOS DE PRUEBA SIN VALOR REAL -	Auditor 1	Auditor Jefe	01/08/2004	31/08/2004	15/08/2004	Gerente de Auditori
2004-12-1	Corporación Sur del Lago Azul	Auditor 3	Auditor Jefe	03/01/2005			Gerente de Auditori
2005-01-1	Technology Consulting	Auditor 1	Gerente de Riesgo	15/01/2005			Auditor de Sistema:

Registro: 1 de 3


Planes-Procesos
Modelo Metodológico de Evaluación y Auditoría de TI - Basado en COBIT
Empresa
Banco X - DATOS DE PRUEBA SIN VALOR REAL -
Plan-Auditoria
2004-08-1
Fecha-Inicio
01/08/2004
Auditor
Auditor 1
Fecha-Final
31/08/2004
Supervisor
Auditor Jefe
Fecha-Seguimiento
15/08/2004
Revisor
Gerente de Auditoria
Alcances a Nivel de Procesos: (Objetivos de Control de Alto Nivel)
Proceso
Relevancia
Desempeño
PO1
5
3 Definido
Definición de un Plan Estrategico de TI
Muy Relevante
Procesos Documentados y Comunicados
PO2
4
4 Gerenciado
Definición de la Arquitectura de Información
Relevante
Procesos Monitoreados y Evaluados
PO3
4
4 Gerenciado
Determinación de la dirección tecnológica
Relevante
Procesos Monitoreados y Evaluados
PO8
5
4 Gerenciado
Aseguramiento del cumplimiento de requerimientos externos
Muy Relevante
Procesos Monitoreados y Evaluados
Registro: 1 de 11
Registro: 1 de 3

Evaluación de Procesos

Plan 2004-08-1 **Empresa** Banco X - DATOS DE PRUEBA SIN VALOR -

Auditor: Auditor 1 **Fecha-Inicio** 01/08/2004

Fecha-Final 31/08/2004

Dominio / Proceso		Relevancia	Desempeño	Indice de Madurez
Dominio: PO - Planificación y Organización				
PO1	Definición de un Plan Estratégico de TI	5 Muy Relevante	3 Definido	0,6
			Procesos Documentados y Comunicados	
PO2	Definición de la Arquitectura de Información	4 Relevante	4 Gerenciado	1
			Procesos Monitoreados y Evaluados	
PO3	Determinación de la dirección tecnológica	4 Relevante	4 Gerenciado	1
			Procesos Monitoreados y Evaluados	
PO4	Definición de la organización y de las elaciones de TI	4 Relevante	5 Optimizado	1,25
			Procesos bajo las Mejores Practicas y Automatizados	
PO5	Manejo de la inversión	4 Relevante	5 Optimizado	1,25
			Procesos bajo las Mejores Practicas y Automatizados	
PO6	Comunicación de la dirección y aspiraciones de la gerencia	5 Muy Relevante	5 Optimizado	1
			Procesos bajo las Mejores Practicas y Automatizados	
PO7	Administración de recursos humanos	4 Relevante	5 Optimizado	1,25
			Procesos bajo las Mejores Practicas y Automatizados	
PO8	Aseguramiento del cumplimiento de requerimientos externos	5 Muy Relevante	4 Gerenciado	0,8
			Procesos Monitoreados y Evaluados	
PO9	Evaluación de riesgos	4 Relevante	4 Gerenciado	1
			Procesos Monitoreados y Evaluados	
PO10	Administración de proyectos	4 Relevante	4 Gerenciado	1
			Procesos Monitoreados y Evaluados	
PO11	Administración de calidad	4 Relevante	4 Gerenciado	1
			Procesos Monitoreados y Evaluados	

Evaluación de Procesos

Plan 2004-08-1 **Empresa** Banco X - DATOS DE PRUEBA SIN VALOR -

Auditor: Auditor 1 **Fecha-Inicio** 01/08/2004

Fecha-Final 31/08/2004

Dominio / Proceso	Relevancia	Desempeño	Indice de Madurez
Dominio: PO - Planificación y Organización			
Totales del Dominio:	**43/55**	**43/55**	**11,15**
Indices del Dominio:	**0,78**	**0,78**	**1,00**
Promedio del Dominio:			**1,01**
Madurez del Dominio:			**1,01**

Resumen: (Índices de Madurez de Procesos)

Procesos Críticos: (Riesgo Alto)

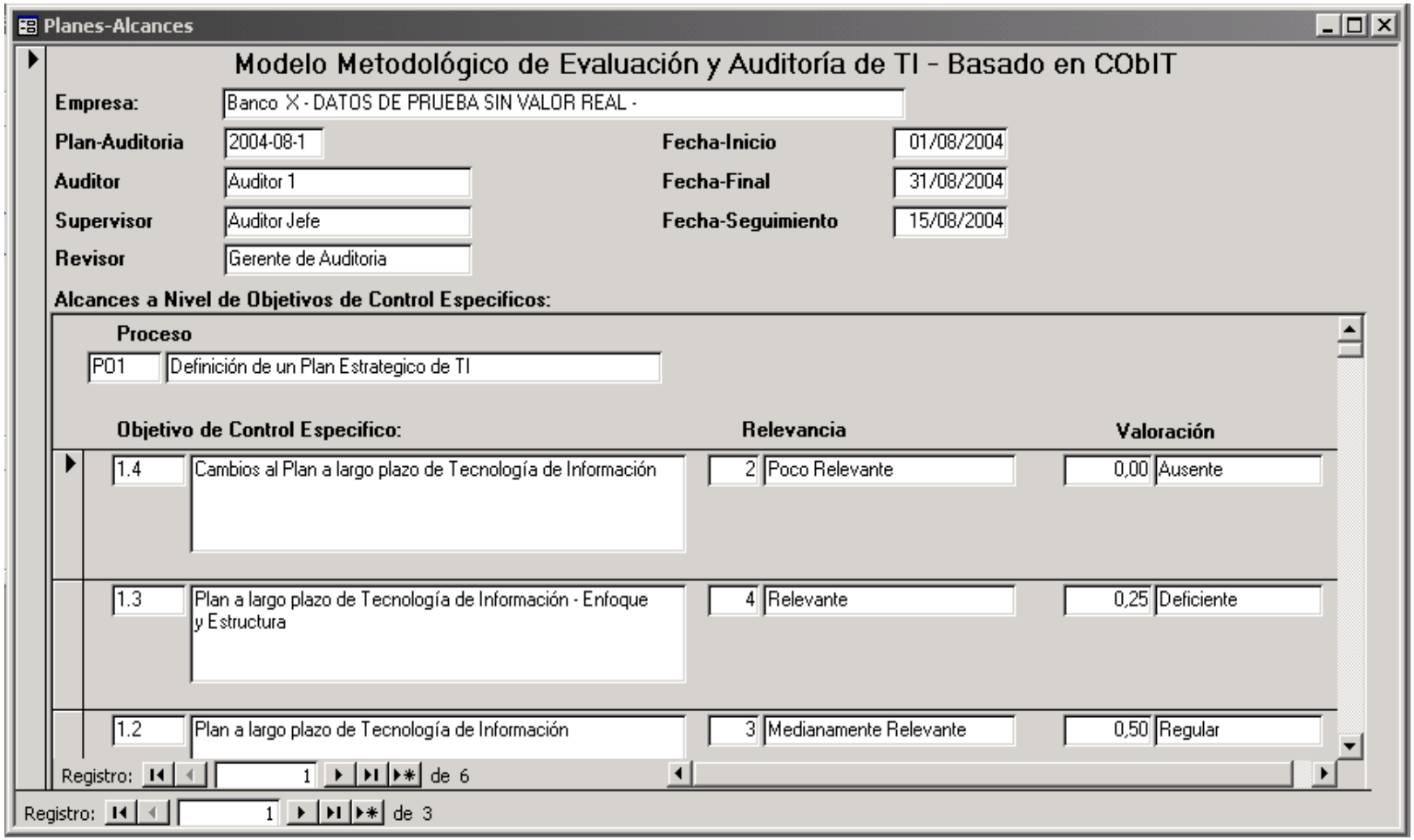
PO1 = 0,6; PO8 = 0,8

Procesos Estables: (Riesgo Moderado)

PO2, PO3, PO6, PO9, PO10, PO11

Procesos Aceptables: (Riesgo Bajo)

PO4, PO5, PO7


Planes-Alcances
Modelo Metodológico de Evaluación y Auditoría de TI - Basado en COBIT
Empresa: Banco X - DATOS DE PRUEBA SIN VALOR REAL -
Plan-Auditoria 2004-08-1
Fecha-Inicio 01/08/2004
Auditor Auditor 1
Fecha-Final 31/08/2004
Supervisor Auditor Jefe
Fecha-Seguimiento 15/08/2004
Revisor Gerente de Auditoria
Alcances a Nivel de Objetivos de Control Especificos:
Proceso
PO1 Definición de un Plan Estrategico de TI
Objetivo de Control Especifico:
Relevancia
Valoración
1.4 Cambios al Plan a largo plazo de Tecnología de Información 2 Poco Relevante 0,00 Ausente
1.3 Plan a largo plazo de Tecnología de Información - Enfoque y Estructura 4 Relevante 0,25 Deficiente
1.2 Plan a largo plazo de Tecnología de Información 3 Medianamente Relevante 0,50 Regular
Registro: 1 de 6
Registro: 1 de 3

Valoración de Objetivos de Control Detallados por Proceso

Plan 2004-08-1 **Empresa** Banco X - DATOS DE PRUEBA SIN VALOR -

Auditor: Auditor 1 **Fecha-Inicio** 01/08/2004

Fecha-Final 31/08/2004

Proceso: PO1 Definición de un Plan Estrategico de TI

Objetivos:		**Relevancia**	**Valoración**	**Indice de Evaluación**
1.1	Tecnología de Información como parte del Plan de la Organización a corto y largo plazo.	5 Muy	0,75 Bueno	3,75
1.2	Plan a largo plazo de Tecnología de Información	3 Medianamente	0,50 Regular	1,50
1.3	Plan a largo plazo de Tecnología de Información - Enfoque y Estructura	4 Relevante	0,25 Deficiente	1,00
1.4	Cambios al Plan a largo plazo de Tecnología de Información	2 Poco	0,00 Ausente	0,00
1.5	Planeación a corto plazo para la Función de Servicios de Información	5 Muy	1,00 Excelente	5,00
1.6	Evaluación de Sistemas Existentes	5 Muy	0,75 Bueno	3,75
Totales del Proceso:		**24/30**		**15,00**
Promedio Valoración de Control del Proceso:		**0,8**		**2,50**

Indice de Control del Proceso: (Promedio / Máximo Control) → 2,50 / 5,00 = 0,5 → 50%

Resumen: (Valoración de Objetivos de Control detallados)

Objetivos por debajo del Promedio: (Críticos) - Debilidades

1.2: 2,50 – 1,50 = 1,00

1.3: 2,50 – 1,00 = 1,50

1.4: 2,50 – 0,00 = 2,50

Objetivos en el Promedio: (Moderados) - Estables

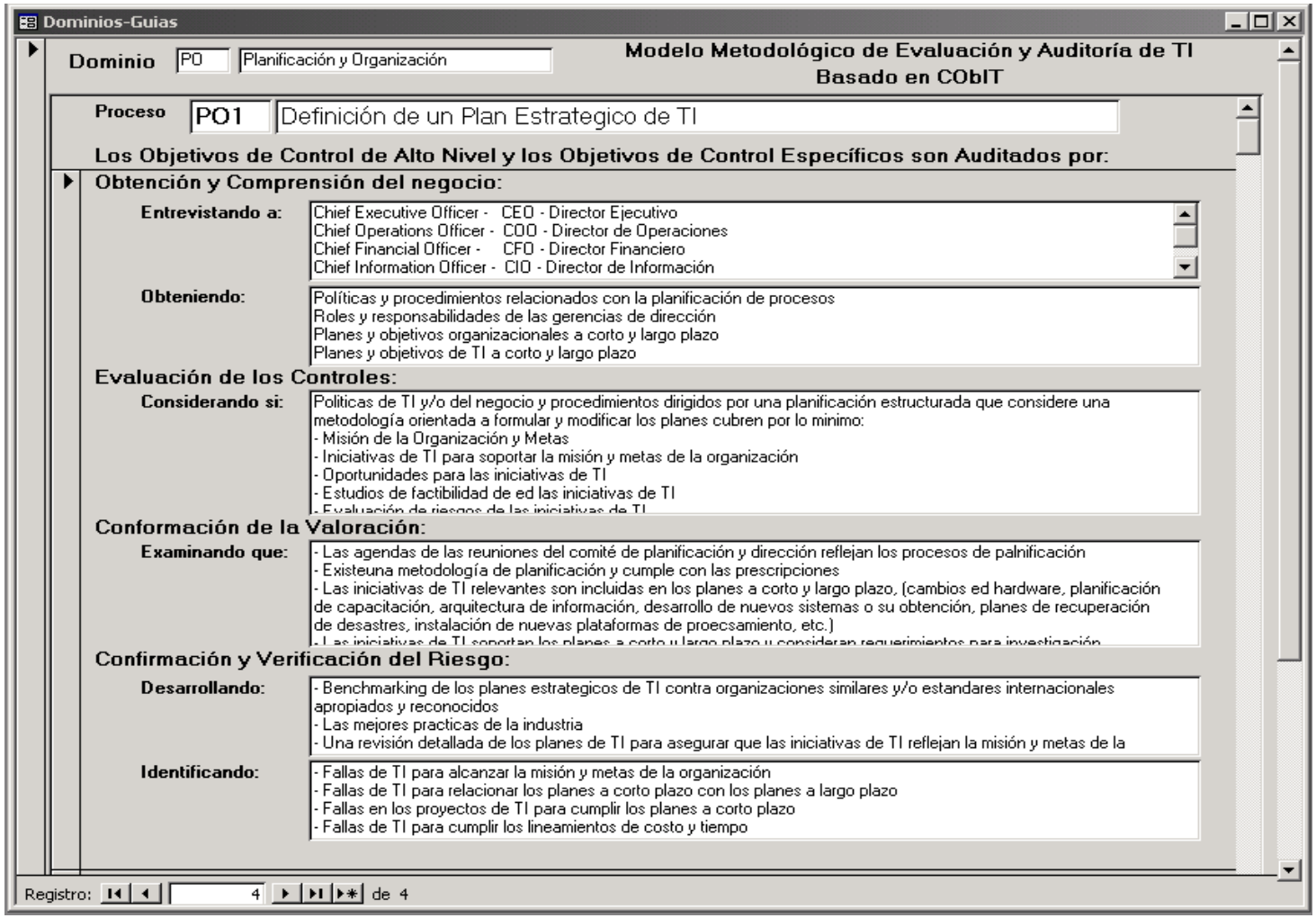
-

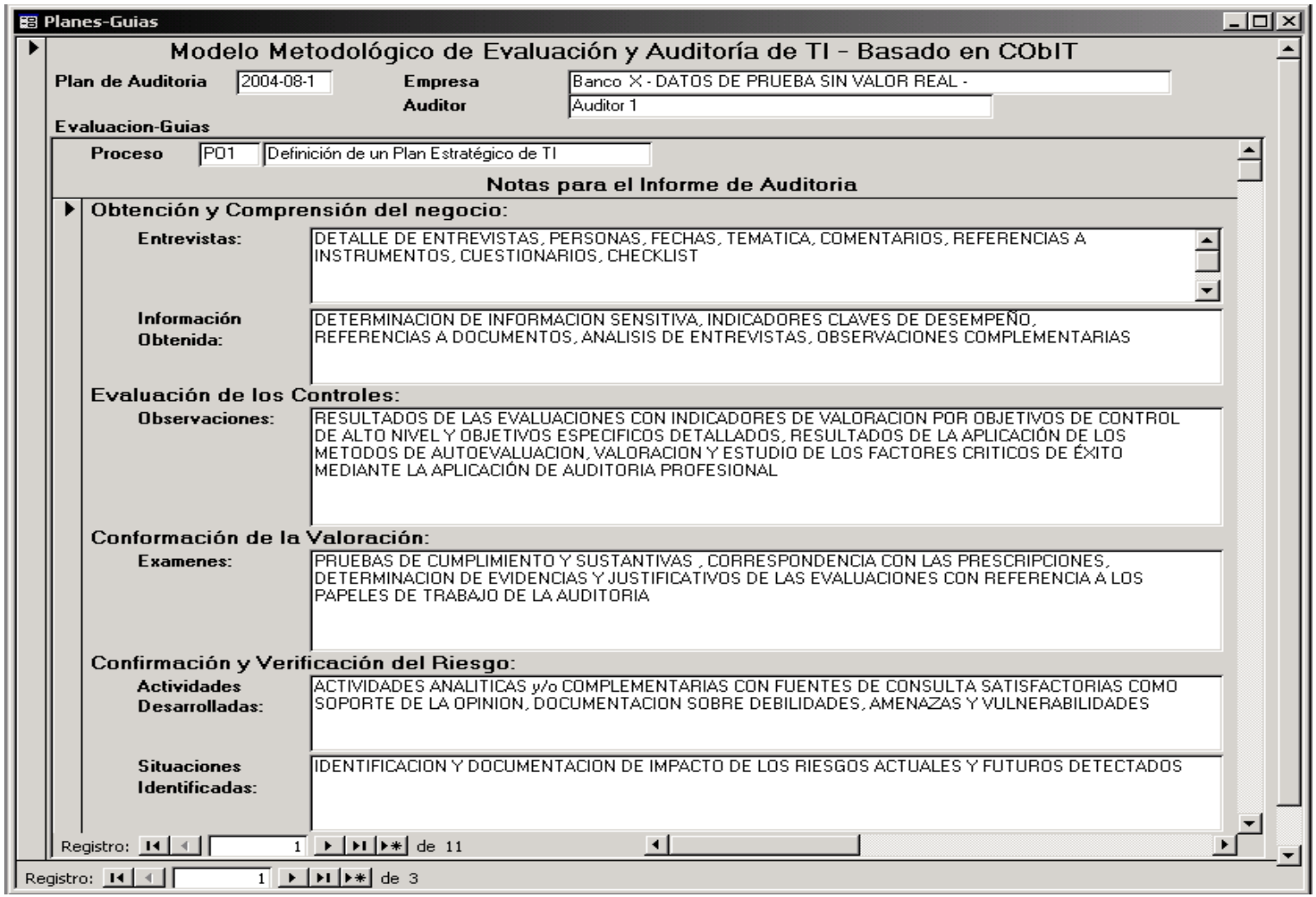
Objetivos por encima del Promedio: (Aceptables) - Fortalezas

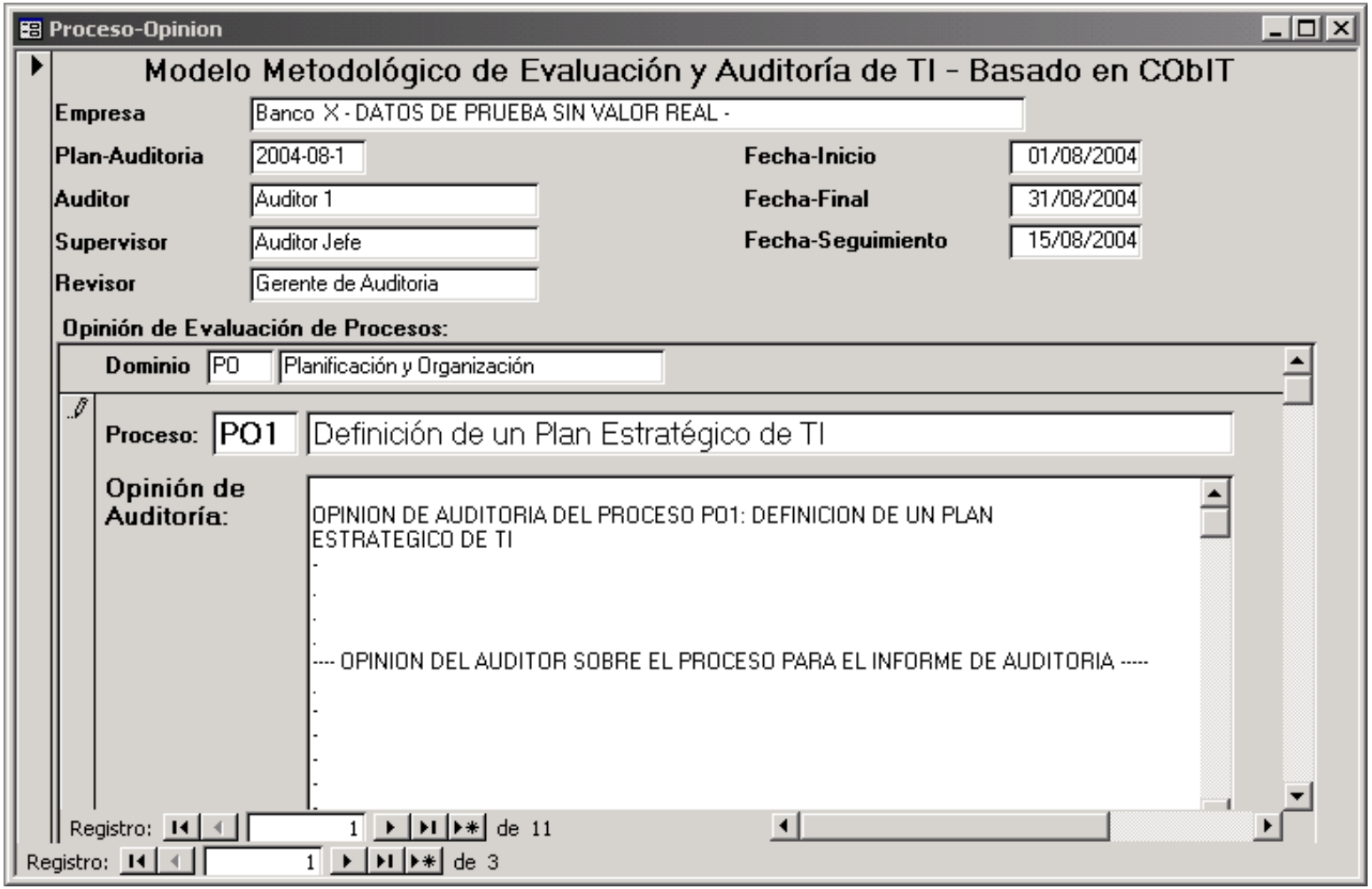
1.1: 3,75 – 2,50 = 1,25

1.5: 5,00 – 2,50 = 2,50

1.6: 3,75 – 2,50 = 1,25


Dominios-Guias
Dominio
PO
Planificación y Organización
Modelo Metodológico de Evaluación y Auditoría de TI
Basado en COBIT
Proceso
PO1
Definición de un Plan Estrategico de TI
Los Objetivos de Control de Alto Nivel y los Objetivos de Control Específicos son Auditados por:
Obtención y Comprensión del negocio:
Entrevistando a:
Chief Executive Officer - CEO - Director Ejecutivo
Chief Operations Officer - COO - Director de Operaciones
Chief Financial Officer - CFO - Director Financiero
Chief Information Officer - CIO - Director de Información
Obteniendo:
Políticas y procedimientos relacionados con la planificación de procesos
Roles y responsabilidades de las gerencias de dirección
Planes y objetivos organizacionales a corto y largo plazo
Planes y objetivos de TI a corto y largo plazo
Evaluación de los Controles:
Considerando si:
Politicas de TI y/o del negocio y procedimientos dirigidos por una planificación estructurada que considere una metodología orientada a formular y modificar los planes cubren por lo minimo:
- Misión de la Organización y Metas
- Iniciativas de TI para soportar la misión y metas de la organización
- Oportunidades para las iniciativas de TI
- Estudios de factibilidad de ed las iniciativas de TI
Conformación de la Valoración:
Examinando que:
- Las agendas de las reuniones del comité de planificación y dirección reflejan los procesos de palnificación
- Existeuna metodología de planificación y cumple con las prescripciones
- Las iniciativas de TI relevantes son incluidas en los planes a corto y largo plazo, (cambios ed hardware, planificación de capacitación, arquitectura de información, desarrollo de nuevos sistemas o su obtención, planes de recuperación de desastres, instalación de nuevas plataformas de proecsamiento, etc.)
Confirmación y Verificación del Riesgo:
Desarrollando:
- Benchmarking de los planes estrategicos de TI contra organizaciones similares y/o estandares internacionales apropiados y reconocidos
- Las mejores practicas de la industria
- Una revisión detallada de los planes de TI para asegurar que las iniciativas de TI reflejan la misión y metas de la
Identificando:
- Fallas de TI para alcanzar la misión y metas de la organización
- Fallas de TI para relacionar los planes a corto plazo con los planes a largo plazo
- Fallas en los proyectos de TI para cumplir los planes a corto plazo
- Fallas de TI para cumplir los lineamientos de costo y tiempo
Registro:
4
de 4


Planes-Guias
Modelo Metodológico de Evaluación y Auditoría de TI - Basado en COBIT
Plan de Auditoria
2004-08-1
Empresa
Banco X - DATOS DE PRUEBA SIN VALOR REAL -
Auditor
Auditor 1
Evaluacion-Guias
Proceso
P01
Definición de un Plan Estratégico de TI
Notas para el Informe de Auditoria
Obtención y Comprensión del negocio:
Entrevistas:
DETALLE DE ENTREVISTAS, PERSONAS, FECHAS, TEMATICA, COMENTARIOS, REFERENCIAS A INSTRUMENTOS, CUESTIONARIOS, CHECKLIST
Información Obtenida:
DETERMINACION DE INFORMACION SENSITIVA, INDICADORES CLAVES DE DESEMPEÑO, REFERENCIAS A DOCUMENTOS, ANALISIS DE ENTREVISTAS, OBSERVACIONES COMPLEMENTARIAS
Evaluación de los Controles:
Observaciones:
RESULTADOS DE LAS EVALUACIONES CON INDICADORES DE VALORACION POR OBJETIVOS DE CONTROL DE ALTO NIVEL Y OBJETIVOS ESPECIFICOS DETALLADOS, RESULTADOS DE LA APLICACIÓN DE LOS METODOS DE AUTOEVALUACION, VALORACION Y ESTUDIO DE LOS FACTORES CRITICOS DE ÉXITO MEDIANTE LA APLICACIÓN DE AUDITORIA PROFESIONAL
Conformación de la Valoración:
Examenes:
PRUEBAS DE CUMPLIMIENTO Y SUSTANTIVAS , CORRESPONDENCIA CON LAS PRESCRIPCIONES, DETERMINACION DE EVIDENCIAS Y JUSTIFICATIVOS DE LAS EVALUACIONES CON REFERENCIA A LOS PAPELES DE TRABAJO DE LA AUDITORIA
Confirmación y Verificación del Riesgo:
Actividades Desarrolladas:
ACTIVIDADES ANALITICAS y/o COMPLEMENTARIAS CON FUENTES DE CONSULTA SATISFACTORIAS COMO SOPORTE DE LA OPINION, DOCUMENTACION SOBRE DEBILIDADES, AMENAZAS Y VULNERABILIDADES
Situaciones Identificadas:
IDENTIFICACION Y DOCUMENTACION DE IMPACTO DE LOS RIESGOS ACTUALES Y FUTUROS DETECTADOS
Registro: 1 de 11
Registro: 1 de 3


Proceso-Opinion
Modelo Metodológico de Evaluación y Auditoría de TI - Basado en CObIT
Empresa
Banco X - DATOS DE PRUEBA SIN VALOR REAL -
Plan-Auditoria
2004-08-1
Fecha-Inicio
01/08/2004
Auditor
Auditor 1
Fecha-Final
31/08/2004
Supervisor
Auditor Jefe
Fecha-Seguimiento
15/08/2004
Revisor
Gerente de Auditoria
Opinión de Evaluación de Procesos:
Dominio
PO
Planificación y Organización
Proceso:
PO1
Definición de un Plan Estratégico de TI
Opinión de Auditoría:
OPINION DE AUDITORIA DEL PROCESO PO1: DEFINICION DE UN PLAN ESTRATEGICO DE TI
---- OPINION DEL AUDITOR SOBRE EL PROCESO PARA EL INFORME DE AUDITORIA -----
Registro: 1 de 11
Registro: 1 de 3

CONCLUSIONES

En las Organizaciones empresariales es evidente la existencia del problema de control de la información y las tecnologías relacionadas con su proceso. Por el singular valor que tiene la información como activo del negocio, se hace necesaria la implantación de un entramado de medidas de control que garanticen el cumplimiento de los criterios de calidad de la información resumidos en: efectividad, eficiencia, confiabilidad, confidencialidad, integridad, disponibilidad

La estructura COBIT (Control Objectives for Información Technology) presenta la referencia más reconocida y aceptada internacionalmente para el uso de las mejores prácticas en el tratamiento del problema de control de los procesos de TI. Su conjunto de elementos permite el diseño de soluciones bajo un enfoque integral de los procesos de información alineados con los objetivos del negocio en lo que se conoce y se promueve como Gobierno de TI.

Se hace posible la difusión, promoción y aplicación de la estructura COBIT en las organizaciones, a través de diseños metodológicos sistémicos de fácil conocimiento y uso para promover la cultura de control y seguridad de la información entre los directivos del negocio, los gerentes administrativos y de gestión, los directores de TI, los auditores de sistemas y los usuarios de las aplicaciones informáticas para lograr organizaciones más eficientes en el uso de la TI.

Con la aplicación de la estructura COBIT, los análisis cualitativos y cuantitativos, obtenidos en la evaluación a nivel de procesos de TI (Objetivos de Alto Nivel) y a nivel de Objetivos de Control Específicos detallados por cada proceso, permiten concluir que existe evidentemente, una relación bien definida entre

dominios, procesos y objetivos detallados que permite la integración de estos elementos en un modelo metodológico de evaluación y auditoría para generar métodos de valoración de riesgos y control.

El Modelo Metodológico de Auditoría de Información y Tecnologías Relacionadas propuesto, permite su aplicación a través de herramientas de software aplicativo de uso sencillo e interactivo. Siguiendo el diseño propuesto, pueden desarrollarse y mejorarse versiones de aplicación de la estructura COBIT.

RECOMENDACIONES

El diseño lógico propuesto que permitió el desarrollo del prototipo presentado para la aplicación del modelo, puede mejorarse y enriquecerse con la definición de otras relaciones de datos y procesos. Pueden desarrollarse aplicaciones de software instalables en configuraciones de escritorio, para su uso *Stand Alone* o pueden desarrollarse aplicaciones bajo arquitectura cliente/servidor para facilitar los procesos colaborativos de evaluación y auditoría en ambientes de Workgroup y Groupware, lo que redundaría en mejorar la cultura organizacional respecto al control y seguridad de los procesos de TI.

Una línea de investigación y desarrollo metodológico de aplicaciones, bajo el enfoque COBIT, debe considerar después de los elementos contemplados en el presente trabajo, variables conducentes a considerar las guías gerenciales COBIT, *Management Audit Guidelines*, que contemplan la extensión y aplicación integral del concepto de Gobierno de TI con la incorporación del modelo de madurez, definido con los siguientes elementos: Factores Críticos de Éxito (Critical Success Factors - CSFs), Indicadores Claves de Objetivos (Key Goal Indicators – KGIs) e Indicadores Claves de Desempeño – KPIs). Estos elementos entregan un marco de referencia especial para responder a las necesidades de la gerencia en materia de planificación y evaluación de los procesos de TI.

REFERENCIAS BIBLIOGRÁFICAS

Arima, H.(1990), Estudio de un Modelo Metodológico Automatizado de Auditoría de Sistemas Computarizados. Tesis doctoral de la Facultad de Economía, Administración y Contaduría de la Universidad de Sao Paulo. Disponible: en la Web http://dedalus.usp.br:4500/ALEPH/POR/USP/USP/TES/FULL/0731774 [Consulta: 2004, Junio]

Balestrini, M. (1998). Como se elabora el Proyecto de Investigación. BL consultores Asociados, Caracas

Barrios, M. (1998). Manual de Trabajos de Grado de Especializaciones y Maestría y Tesis Doctórales**.** Editorial UPEL. Caracas.

CIFCA (1983), Conferencia del Centro de Informática de la Facultad de Contaduría y Administración, Universidad Autónoma de México

Cubillos M. (2003), Modelo de Evaluación de Riesgos AUDIRISK AUDISIS Ltda., Auditoría Integral y Seguridad en Sistemas de Información, Boletín Audideas Año 6 No. 2, Bogotá

Datasec (1999), MEYCOR Cobit Control Self Assessment (CSA); Uruguay. Caso de Estudio en IT Governace Institute. Disponible: en la Web http://www.itgi.org/Template_ITGI.cfm?Section=Case_Studies1&CONTENTID=9195&TEMPLATE=/ContentManagement/ContentDisplay.cfm. [Consulta: 2004 Julio]

Diccionario General de la lengua Española VOX. Disponible en la Web: http://www.diccionarios.com [Consulta: Julio /2004]

Echenique, J.A. (1985), Auditoría Informática. Ed. Mc-Graw Hill.

Fitzgerald, J. (1991), Controles Internos para Sistemas de Computación Editorial Limusa.

Garcia C. (1990), Un enfoque metodológico de Auditoría de sistemas San Cristóbal, UNET – Trabajo de Ascenso Docente

ISACA (1987), General Standars for Information System Auditing, Information System Audit and Control Foundation (ISACA). Illinois, USA.

ISACA(2000) Information System Audit and Control Asociation (ISACA). Disponible en la Web http://www.isaca.org. [Consulta: 2004, Julio, Agosto]

ISACF (1996-2000), COBIT, Control Objectives for Information and Related Technology, Information System Audit and Control Foundation (ISACA), 1996, 1998, 2000. Illinois, 60008, USA

ISACA A.L (2000), Information System Audit and Control Foundation (ISACA), Capítulo America Latina. Disponible en la Web http://www.isaca.cl/cobit.html [Consulta: 2004, Julio-Agosto]

Piattini, M., Del Peso, E.(1998)
AUDITORÍA INFORMATICA, Un enfoque práctico,
Ed. Alfaomega,

O´Brien J. (1998), Sistemas de Información Gerencial,
Ed., Mc Graw Hill

Rodríguez R. (1998), Presentación en Piattini, M., Del Peso, E. (1998)
Ed. Alfaomega,

Tamayo y Tamayo (1986), El Proceso de la Investigación Científica, (ojo)
Fundamentos de Investigación, Grupo Noriega Editores

UNA. (1998), Universidad Nacional Abierta,
AUDITORÍA y EVALUACION DE SISTEMAS, Caracas

ANEXOS

CHECKLIST PARA IDENTIFICAR LAS NECESIDADES
DE SERVICIOS EN EVALUACION Y AUDITORIA DE INFORMACION
Y TECNOLOGIAS RELACIONADAS

Nombre de la Empresa: _____

Cargo de funcionario: _____ Fecha:_____

Nombre de la Unidad de Tecnología de Sistemas de Información:

_____

1. Recurso Humano asignado a la Función de Sistemas de Información.

1.1 Cantidad de personas en el área de Tecnología de Información: _____

1.2 Perfil del personal de sistemas.

Perfil	Cantidad
Tecnólogos en Sistemas	
Ingenieros de Sistemas o Informáticos	
Especialistas en Telecomunicaciones.	
Otros (Indique)	

2. Plataformas de Hardware y Software utilizadas.

Plataforma	Descripción
Sistemas Operativos	
Motores de Bases de Datos	
Otras Herramientas de Desarrollo	
Software de Red.	
Equipos Activos de la Red	
Internet	
Intranet	
Extranet	
Servidores de Correo Electrónico	
Firewalls	
Servidores de Archivo	
Mainframes	
Minicomputares	
Microcomputadores	
E-business	
Business Intelligence	
Data Warehouse	
Otras (indique)	

3. Sistemas de Información que utiliza la empresa.

No	Nombre del S.	Módulos Componentes

4. Portafolio de Aplicaciones o Módulos de Sistemas de Información que están en producción y su importancia para la empresa.

No	Nombre de la Aplicación	Relevancia Para la Empresa (1)	Herramienta de Desarrollo Utilizada	Poseen Programas Fuentes ? (2)

(1) Importancia para los objetivos de la empresa. Utilice un número entre 1 y 5 (1: La menor relevancia; 5: La mayor relevancia).

(2) Conteste SI o NO.

5. Las actividades de procesamiento de datos que se realizan en la empresa.

No	Descripción	Marque con X
1	Grabación (captura de Datos)	
2	Control de Entradas y Salidas.	
3	Producción de información (Procesamiento y actualización de archivos).	
4	Help Desk.	
5	Soporte a usuarios de microcomputadores y LANs.	
6	Mantenimiento de hardware.	
7	Administración de bases de datos (DBA)	
8	Administración de la Seguridad lógica (controles de acceso)	
9	Planeación estratégica de sistemas.	
10	Administración de contratos de terceras partes.	
11	Definición e implementación de políticas de seguridad corporativas.	

12	Análisis y Diseño de Sistemas.	
13	Construcción de Programas (Elaboración de programas de computador).	
14	Mantenimiento de Software Aplicativo	
15	Administración de Telecomunicaciones.	
16	Quality Assurance.	
17	Otras.	

6. Servicios de procesamiento de datos que son contratados con terceros.

No	Descripción	Marque con X
1	Mantenimiento de hardware.	
2	Administración de los Centros de Procesamiento de Datos	
3	Grabación de Datos	
4	Planeación estratégica de sistemas.	
5	Interventoría de proyectos de sistemas.	
6	Planeación de Contingencias en Sistemas de Información.	
7	Análisis y Diseño de Sistemas.	
8	Programación de aplicaciones.	
9	Mantenimiento de Software Aplicativo	
10	Administración y soporte técnico en Telecomunicaciones.	
11	Quality Assurance (Aseguramiento de calidad).	
12	Seguridad en Sistemas de Información.	
13	Otras (indíquelas).	

7. Módulos Componentes del Sistema de Información Comercial (Diligenciar únicamente los pertinentes)

No	Descripción	Marque con X
1	Facturación.	
2	Recaudos	
3	Solicitudes de Servicios	
4	Atención al Suscriptor	
5	Medidores	
6	Financiación de servicios y de deuda	
7	Control de Perdidas y Fraudes	
8	Cartera	
9	Enlace Financiero	
10	Seguridad y Administración del sistema	
11	Estadísticas	
12	Auditoria de Sistemas	
13	Administración de Parámetros Generales	
14	Facturación en sitio	
15	Otros (especifique)	

8. Servicios de Control Interno y Seguridad de Sistemas que son de su interés

No	Descripción	Marque con X
1	Asesoría para implantación de estándar COBIT (Control Objectives for Information and Related Technology).	
2	Diseño e implantación de Controles en operaciones de negocio que se soportan en Sistemas de Información (Aplicaciones de Computador).	
3	Diseño e implantación del Plan de Acción de Prevención y Mitigación de Riesgos (Mapas de Riesgo).	
4	Diseño e implantación de controles en el Desarrollo de Sistemas (especifique)	
5	Aseguramiento de Calidad del Software	
6	Aseguramiento de Calidad de Bases de Datos	
7	Elaboración e Implantación del Plan de Continuidad (Contingencias) en Sistemas de Información.	
8	Ejecución de pruebas de software	
9	Asesoría para implantar modelos de auditoria (Metodología Asistida por computador para Diseño de Controles y Administración de Riesgos en Sistemas de Información).	
10	Capacitación en Controles y Seguridad en Sistemas de Información.	
11	Definición de Políticas, Estándares y Procedimientos de Seguridad en Tecnología de Información	
12	Otros (Especifique)	

9. Servicios de Auditoria de Sistemas que considera de interés y requeridos

No	Descripción	Marque con X
1	Auditoria a la Organización y Funcionamiento de la Informática de la Empresa (Auditoria de Controles Generales de Sistemas de Información)	
2	Auditoría de Sistemas y Aplicaciones en Producción	
3	Auditoria al Sistema de Información Comercial (Unicamente para empresas de Servicios Públicos)	
4	Auditoría al Desarrollo de Sistemas (especifique)	
5	Auditoria al Plan de Contingencias de Sistemas de Información (Continuidad del Negocio)	
6	Desarrollo de Software de Auditoria (Especifique)	
7	Organización e Implantación de la Auditoría de Sistemas.	
8	Asesoría para la adquisición de Software de Auditoría	
9	Capacitación en Auditoría de Sistemas.	
10	Asesoría para implantar el enfoque de Auditoría de Sistemas Orientada al Riesgo.	
11	Otros – Especifique	

AUTOEVALUACION DEL GOBIERNO DE LOS PROCESOS DE TECNOLOGIA DE INFORMACION														
PROCESOS DE TECNOLOGIA DE INFORMACION			**PARAMETROS DE AUTOEVALUACION**											
(Objetivos de Control de Alto Nivel)			**PESOS**		**PROCESAMIENTO**				**ESTADO**			**UNIDAD ORGANIZACIONAL**		
No.	**Serie**	**Descripción de Dominios y Procesos COBIT**	**REL.**	**DES.**	**TI**	**OTR.**	**EXT.**	**N/I**	**AUI.**	**AUE.**	**FOR.**	**RESPONSABLE DEL GOBIERNO**		
	PO:	**DOMINIO: Planificación y Organización**	**1-5**	**1-5**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**DESCRIPCION: (Tabla Anexa)**		
1	PO1	Definición de un plan estratégico de TI												
2	PO2	Definición de la arquitectura de la información												
3	PO3	Determinación de la dirección tecnológica												
4	PO4	Definición de la organización y de las relaciones de TI												
5	PO5	Manejo de la inversión												
6	PO6	Comunicación de los objetivos y directivas de la alta gerencia												
7	PO7	Administración de los recursos humanos												
8	PO8	Aseguramiento del cumplimiento de los requerim. externos												
9	PO9	Evaluación de riesgos												
10	PO10	Administración de proyectos												
11	PO11	Administración de la calidad												
	AI:	**DOMINIO: Adquisición e Implementación**												
12	AI1	Identificación de soluciones automatizadas												
13	AI2	Adquisición y mantenimiento de software de aplicación												
14	AI3	Adquisición y mantenimiento de la infraestructura tecnológica												
15	AI4	Procedimientos de desarrollo y mantenimiento												
16	AI5	Instalación y aceptación de sistemas												
17	AI6	Administración de cambios												
	DS:	**Entrega y Soporte**												
18	DS1	Definición de los niveles del servicio												
19	DS2	Administración de los servicios prestados por terceros												
20	DS3	Administración de la capacidad y desempeño del sistema												
21	DS4	Aseguramiento de la continuidad del servicio												
22	DS5	Establecimiento de pautas para la seguridad de los sistemas												
23	DS6	Identificación e imputación de costos												
24	DS7	Educación y capacitación de los usuarios												
25	DS8	Asistencia y asesoramiento a los clientes de TI												
26	DS9	Administración de la configuración												
27	DS10	Administración de problemas e incidentes												
28	DS11	Administración de datos												
29	DS12	Administración de instalaciones												
30	DS13	Administración de las operaciones												
	M:	**Monitoreo**												
31	M1	Monitoreo de los procesos												
32	M2	Evaluación de la adecuación del control interno												
33	M3	Obtención de aseguramiento independiente												
34	M4	Provisión de auditoría independiente												

PARAMETROS DE AUTOEVALUACION DEL GOBIERNO DE LOS PROCESOS DE TI	
VALORACION DEL PROCESO: (PESO)	
REL.	**Relevancia del Proceso para los objetivos del Negocio** **1: No Relevante, 5: Muy Relevante**
DES.	**Desempeño del Proceso** **1: Deficiente, 5: Excelente**
UNIDAD ORGANIZACIONAL EJECUTORA DEL PROCESO:	
TI	**Gerencia de Tecnologia** **X**
OTR.	**Otra Unidad Ejecutora** **X**
EXT.	**Organización Externa o Terceros.** **X**
N/I	**No Informado** **X**
ESTADO DEL PROCESO:	
AUD.	**Auditado Internamente** **X**
AUE.	**Auditado Externamente** **X**
FOR.	**Formalizado (Contratos, Acuerdos de Servicio, Documentac.)** **X**
UNIDAD ORGANIZACIONAL RESPONSABLE DEL GOBIERNO DE TI:	
01	Alta Gerencia - Dirección Ejecutiva
02	Gerencia de Tecnologia de Información
03	Gerencia de Finanzas
04	Gerencia de Auditoria de Sistemas
05	Gerencia de Recursos Humanos
06	Gerencia de Seguridad
07	
08	
09	
10	

The IT Governance Institute® is pleased to offer you this complimentary download of COBIT®

COBIT provides good practices for the management of IT processes in a manageable and logical structure, meeting the multiple needs of enterprise management by bridging the gaps between business risks, technical issues, control needs and performance measurement requirements. If you believe as we do, that COBIT enables the development of clear policy and good practices for IT control throughout your organisation, we invite you to support ongoing COBIT research and development.

There are two ways in which you may express your support: (1) Purchase COBIT through the association (ISACA) Bookstore (please see the following pages for order form and association membership application. Association members are able to purchase COBIT at a significant discount); (2) Make a generous donation to the IT Governance Institute, which conducts research and authors COBIT.

The complete COBIT package consists of all six publications, an ASCII text diskette, four COBIT implementation/ orientation Microsoft® PowerPoint® presentations and a CD-ROM. A brief overview of each component is provided below. Thank you for your interest in and support of COBIT!

For additional information about the IT Governance Institute, visit *www.itgi.org.*

Management Guidelines

To ensure a successful enterprise, you must effectively manage the union between business processes and information systems. The new *Management Guidelines* is composed of maturity models, critical success factors, key goal indicators and key performance indicators. These *Management Guidelines* will help answer the questions of immediate concern to all those who have a stake in enterprise success.

Executive Summary

Sound business decisions are based on timely, relevant and concise information. Specifically designed for time-pressed senior executives and managers, the COBIT *Executive Summary* explains COBIT's key concepts and principles.

Framework

A successful organization is built on a solid framework of data and information. The *Framework* explains how IT processes deliver the information that the business needs to achieve its objectives. This delivery is controlled through 34 high-level control objectives, one for each IT process, contained in the four domains. The *Framework* identifies which of the seven information criteria (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability), as well as which IT resources (people, applications, technology, facilities and data) are important for the IT processes to fully support the business objective.

Audit Guidelines

Analyze, assess, interpret, react, implement. To achieve your desired goals and objectives you must constantly and consistently audit your procedures. *Audit Guidelines* outlines and suggests actual activities to be performed corresponding to each of the 34 high-level IT control objectives, while substantiating the risk of control objectives not being met.

Control Objectives

The key to maintaining profitability in a technologically changing environment is how well you maintain control. COBIT's *Control Objectives* provides the critical insight needed to delineate a clear policy and good practice for IT controls. Included are the statements of desired results or purposes to be achieved by implementing the 318 specific, detailed control objectives throughout the 34 high-level control objectives.

Implementation Tool Set

The *Implementation Tool Set* contains management awareness and IT control diagnostics, implementation guide, frequently asked questions, case studies from organizations currently using COBIT and slide presentations that can be used to introduce COBIT into organizations. The tool set is designed to facilitate the implementation of COBIT, relate lessons learned from organizations that quickly and successfully applied COBIT in their work environments and assist management in choosing implementation options.

CD-ROM

The CD-ROM, which contains all of COBIT, is published as a Folio infobase. The material is accessed using Folio Views®, which is a high-performance, information retrieval software tool. Access to COBIT's text and graphics is now easier than ever, with flexible keyword searching and built-in index links (optional purchase).

A network version (multi-user) of COBIT 3rd Edition is available. It is compatible with Microsoft Windows NT/2000 and Novell NetWare environments. Contact the ISACA Bookstore for pricing and availability.

See order form, donation information and membership application on the following pages.

We invite your comments and suggestions regarding COBIT. Please visit *www.isaca.org/cobitinput.*

ITGI Contribution Form

Contributor: _____

Address: _____

_____

City _____ State/Province _____

Zip/Postal Code _____ Country _____

Remitted by: _____

Phone: _____

E-mail: _____

For information on the institute and contribution benefits see *www.itgi.org*

Contribution amount (US $):

☐ $25 (donor) ☐ $100 (Silver) ☐ $250 (Gold)

☐ $500 (Platinum) ☐ Other US $_____

☐ Check enclosed payable in US dollars to ITGI

☐ **Charge my:** ☐ VISA ☐ MasterCard ☐ American Express ☐ Diners Club

Card number _____ Exp. Date _____

Name of cardholder: _____

Signature of cardholder: _____

Complete card billing address if different from address on left

_____

_____

_____

U.S. Tax ID number: 95-3080691

Fax your credit card contribution to ITGI at +1.847.253.1443, or mail your contribution to: ITGI, 135 S. LaSalle Street, Department 1055, Chicago, IL 60674-1055 USA

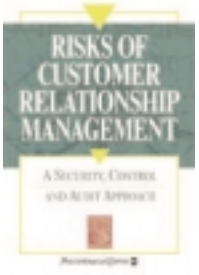
Direct any questions to Scott Artman at +1.847.253.1545, ext. 459, or *finance@isaca.org*.

Thank you for supporting CobiT!

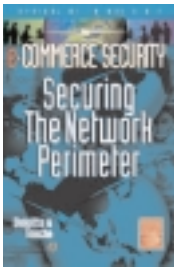
Recent ITGI Research Projects

Security Provisioning:
Managing Access in Extended Enterprises, ISSP
Member - $20 Nonmember - $30

e-Commerce Security
Public Key Infrastructure: Good Practices for Secure Communications, TRS-2
Member - $35 Nonmember - $50



Risks of Customer Relationship Management
A Security, control and Audit Approach, ISCR
Member - $75 Nonmember - $85



e-Commerce Security
Securing the Network Perimeter, TRS-3
Member - $35 Nonmember - $50

e-Commerce Security
Business Continuity Planning, IBCP
Member - $35 Nonmember - $50

For additional information on these publications and others offered through the Bookstore, please visit *www.isaca.org/bookstore*.

Pricing and Order Form

COBIT®
GOVERNANCE, CONTROL *and* AUDIT *for* INFORMATION *and* RELATED TECHNOLOGY

GOVERNANCE INSTITUTE®

	CODE	ISACA Members	Non-Members
Complete COBIT® 3rd Edition©	CB3S CB3SC	$70 (text only) $115 (text and CD-ROM)	 $225 (text and CD-ROM)

Individual components are also available for purchase:

	CODE	ISACA Members	Non-Members
Executive Summary	CB3E	$3	$3
Management Guidelines	CB3M	$40	$50
Framework	CB3F	$15	$20
Control Objectives	CB3C	$25	$30
Audit Guidelines	CB3A	$50	$155
Implementation Tool Set	CB3I	$15	$20

All prices are US dollars. Shipping is additional to all prices.

Name _____ Date _____

ISACA Member: ❑ Yes ❑ No Member Number _____
If an ISACA Member, is this a change of address? ❑ Yes ❑ No

Company Name _____

Address: ❑ Home ❑ Company _____

City _____ State/Province _____ Country _____ Zip/Mail Code _____

Phone Number ( ) _____ Fax Number ( ) _____

E-mail Address _____ Special Shipping Instructions or Remarks _____

_____

Code	Title / Item	Quantity	Unit Price	Total
All purchases are final. ***All prices are subject to change.***			***Subtotal***	
			Illinois (USA) residents, add 8.25% sales tax, or Texas (USA) residents, add 6.25% sales tax	
			Shipping and Handling – see chart below	
			TOTAL	

PAYMENT INFORMATION – PREPAYMENT REQUIRED

❑ Payment enclosed. Check payable in U.S. dollars, drawn on U.S. bank, payable to the Information Systems Audit and Control Association.
❑ Charge to ❑ VISA ❑ MasterCard ❑ American Express ❑ Diners Club
(Note: All payments by credit card will be processed in U.S. Dollars)

Account # _____ Exp. Date _____

Print Cardholder Name _____ Signature of Cardholder _____

Cardholder Billing Address if different than above _____

_____

Shipping and Handling Rates

For orders totaling	Outside USA and Canada	Within USA and Canada
Up to US$30	$7	$4
US$30.01 - US$50	$12	$6
US$50.01 - US$80	$17	$8
US$80.01 - US$150	$22	$10
Over US$150	15% of total	10% of total

Please send me information on: ❑ Association membership ❑ Certification ❑ Conferences ❑ Seminars ❑ Research Projects

ISACA BOOKSTORE
135 SOUTH LASALLE, DEPARTMENT 1055, CHICAGO, IL 60674-1055 USA
TELEPHONE: +1.847.253.1545, EXT. 401 FAX: +1.847.253.1443 E-MAIL: *bookstore@isaca.org*
WEB SITE: *www.isaca.org/bookstore*

PDF

Information Systems Audit and Control Association®

MEMBERSHIP APPLICATION

Please complete both sides
U.S. Federal I.D. No. 23-7067291
www.isaca.org
membership@isaca.org

☐ MR. ☐ MS. ☐ MRS. ☐ MISS ☐ OTHER _____ Date _____
MONTH/DAY/YEAR

Name _____
FIRST MIDDLE LAST/FAMILY

_____
PRINT NAME AS YOU WANT IT TO APPEAR ON MEMBERSHIP CERTIFICATE

Residence address _____
STREET

_____
CITY STATE/PROVINCE/COUNTRY POSTAL CODE/ZIP

Residence phone _____ Residence facsimile _____
AREA/COUNTRY CODE AND NUMBER AREA/COUNTRY CODE AND NUMBER

Company name _____

Business address _____
STREET

_____
CITY STATE/PROVINCE/COUNTRY POSTAL CODE/ZIP

Business phone _____ Business facsimile _____
AREA/COUNTRY CODE AND NUMBER AREA/COUNTRY CODE AND NUMBER

E-mail _____

Send mail to
☐ Home
☐ Business

Form of Membership requested
☐ Chapter Number *(see reverse)*_____
☐ Member at large *(no chapter within 50 miles/80 km)*
☐ Student *(must be verified as full-time)*
☐ Retired *(no longer seeking employment)*

☐ I do not want to be included on a mailing list, other than that for Association mailings.

How did you hear about ISACA?
1 ☐ Friend/Coworker
2 ☐ Employer
3 ☐ Internet Search
4 ☐ IS Control Journal
5 ☐ Other Publication
6 ☐ Local Chapter
7 ☐ CISA Program
8 ☐ Direct Mail
9 ☐ Educational Event

Current field of employment *(check one)*
1 ☐ Financial
2 ☐ Banking
3 ☐ Insurance
4 ☐ Transportation
5 ☐ Retail & Wholesale
6 ☐ Government/National
7 ☐ Government/State/Local
8 ☐ Consulting
9 ☐ Education/Student
10 ☐ Education/Instructor
11 ☐ Public Accounting
12 ☐ Manufacturing
13 ☐ Mining/Construction/Petroleum
14 ☐ Utilities
15 ☐ Other Service Industry
16 ☐ Law
17 ☐ Health Care
99 ☐ Other

Date of Birth _____
MONTH/DAY/YEAR

Level of education achieved
(indicate degree achieved, or number of years of university education if degree not obtained)
1 ☐ One year or less
2 ☐ Two years
3 ☐ Three years
4 ☐ Four years
5 ☐ Five years
6 ☐ Six years or more
7 ☐ AS
8 ☐ BS/BA
9 ☐ MS/MBA/Masters
10 ☐ Ph.D.
99 ☐ Other _____

Certifications obtained (other than CISA)
1 ☐ CISM
2 ☐ CPA
3 ☐ CA
4 ☐ CIA
5 ☐ CBA
6 ☐ CCP
7 ☐ CSP
8 ☐ FCA
9 ☐ CFE
10 ☐ MA
11 ☐ FCPA
12 ☐ CFSA
13 ☐ CISSP
99 ☐ Other _____

Work experience
(check the number of years of Information Systems work experience)
1 ☐ No experience
2 ☐ 1-3 years
3 ☐ 4-7 years
4 ☐ 8-9 years
5 ☐ 10-13 years
6 ☐ 14 years or more

Current professional activity *(check one)*
1 ☐ CEO
2 ☐ CFO
3 ☐ CIO/IS Director
4 ☐ Audit Director/General Auditor
5 ☐ IS Security Director
6 ☐ IS Audit Manager
7 ☐ IS Security Manager
8 ☐ IS Manager
9 ☐ IS Auditor
10 ☐ External Audit Partner/Manager
11 ☐ External Auditor
12 ☐ Internal Auditor
13 ☐ IS Security Staff
14 ☐ IS Consultant
15 ☐ IS Vendor/Supplier
16 ☐ IS Educator/Student
99 ☐ Other _____

Payment due

• Association dues †	$ 120.00	(US)
• Chapter dues *(see following page)*	$ _____	(US)
• New member processing fee	$ 30.00	(US)*
PLEASE PAY THIS TOTAL	$ _____	(US)

† For student membership information please visit *www.isaca.org/student*

* Membership dues consist of association dues, chapter dues and new member processing fee.

Method of payment
☐ Check payable in US dollars, drawn on US bank
☐ Send invoice (Applications cannot be processed until dues payment is received.)
☐ MasterCard ☐ VISA ☐ American Express ☐ Diners Club

All payments by credit card will be processed in US dollars

ACCT # _____

Print name of cardholder _____

Expiration date _____
MONTH/YEAR

Signature _____

Cardholder billing address if different than address provided above:

_____

_____

By applying for membership in the Information Systems Audit and Control Association, members agree to hold the association and the IT Governance Institute, their officers, directors, agents, trustees, and employees and members, harmless for all acts or failures to act while carrying out the purpose of the association and the institute as set forth in their respective bylaws, and they certify that they will abide by the association's *Code of Professional Ethics (www.isaca.org/ethics).*

Initial payment entitles new members to membership beginning the first day of the month following the date payment is received by International Headquarters through the end of that year. No rebate of dues is available upon early resignation of membership.

Contributions, dues or gifts to the Information Systems Audit and Control Association are not tax deductible as charitable contributions in the United States. However, they may be tax deductible as ordinary and necessary business expenses.

Membership dues allocated to a 1-year subscription to the *IS Control Journal* are as follows: $45 for US members, $60 for non-US members. This amount is not deductible from dues.

Make checks payable to:
Information Systems Audit and Control Association

Mail your application and check to:
Information Systems Audit and Control Association
135 S. LaSalle, Dept. 1055
Chicago, IL 60674-1055 USA
Phone: +1.847.253.1545 x470
Fax: +1.847.253.1443

U.S. dollar amounts listed below are for local chapter dues. While correct at the time of printing, chapter dues are subject to change without notice. Please include the appropriate chapter dues amount with your remittance.

For current chapter dues, or if the amount is not listed below, please visit the web site *www.isaca.org/chapdues* or contact your local chapter at *www.isaca.org/chapters*.

Chapter Name	Chapter Number	Dues
ASIA		
Hong Kong	64	$40
Bangalore, India	138	$15
Cochin, India	176	$10
Coimbatore, India	155	$10
Hyderabad, India	164	$17
Kolkata, India	165	⁕
Madras, India (Chennai)	99	$10
Mumbai, India	145	⁕
New Delhi, India	140	$10
Pune, India	159	$17
Indonesia	123	⁕
Nagoya, Japan	118	$130
Osaka, Japan	103	$10
Tokyo, Japan	89	$120
Korea	107	$30
Lebanon	181	$35
Malaysia	93	$10
Muscat, Oman	168	$40
Karachi, Pakistan	148	$15
Manila, Philippines	136	$0
Jeddah, Saudi Arabia	163	$0
Riyadh, Saudi Arabia	154	$0
Singapore	70	$10
Sri Lanka	141	$15
Taiwan	142	$50
Bangkok, Thailand	109	$10
UAE	150	$10
CENTRAL/SOUTH AMERICA		
Buenos Aires, Argentina	124	$35
Mendoza, Argentina	144	⁕
São Paulo, Brazil	166	$25
LaPaz, Bolivia	173	$25
Santiago de Chile	135	$40
Bogotá, Colombia	126	$50
San José, Costa Rica	31	$33
Quito, Ecuador	179	$15
Mérida, Yucatán, México	101	$50
Mexico City, México	14	$65
Monterrey, México	80	$65
Panamá	94	$25
Lima, Perú	146	$15
Puerto Rico	86	$30
Montevideo, Uruguay	133	$100
Venezuela	113	$25
EUROPE/AFRICA		
Austria	157	$45
Belux (Belgium and Luxembourg)	143	$48
Croatia	170	$50
Czech Republic	153	$110
Denmark	96	⁕
Estonian	162	$10
Finland	115	$70
Paris, France	75	⁕
German	104	$80
Athens, Greece	134	$20
Budapest, Hungary	125	$60
Irish	156	$40
Tel-Aviv, Israel	40	⁕
Milano, Italy	43	$53
Rome, Italy	178	$26
Kenya	158	$40
Latvia	139	$10
Lithuania	180	$20
Netherlands	97	$50
Lagos, Nigeria	149	$20
Oslo, Norway	74	$50
Warsaw, Poland	151	$30
Moscow, Russia	167	$0
Romania	172	$50
Slovenia	137	$50
Slovensko	160	$40
South Africa	130	$35
Barcelona, Spain	171	$110
Valencia, Spain	182	$25
Sweden	88	$45
Switzerland	116	$35
Tanzania	174	$40
London, UK	60	$80
Central UK	132	$55
Northern England	111	$50
Scottish, UK	175	$45
NORTH AMERICA		
Canada		
Calgary, AB	121	$0
Edmonton, AB	131	$25
Vancouver, BC	25	$20
Victoria, BC	100	$0
Winnipeg, MB	72	$15
Nova Scotia	105	$0
Ottawa Valley, ON	32	$10
Toronto, ON	21	$25
Montreal, PQ	36	$20
Quebec City, PQ	91	$35
Islands		
Bermuda	147	$0
Trinidad & Tobago	106	$25
Midwestern United States		
Chicago, IL	02	$50
Illini (Springfield, IL)	77	$30
Central Indiana (Indianapolis)	56	$30
Michiana (South Bend, IN)	127	$25
Iowa (Des Moines)	110	$25
Kentuckiana (Louisville, KY)	37	$30
Detroit, MI	08	$35
Western Michigan (Grand Rapids)	38	$25
Minnesota (Minneapolis)	07	$30
Omaha, NE	23	$30
Central Ohio (Columbus)	27	$25
Greater Cincinnati, OH	03	$20
Northeast Ohio (Cleveland)	26	$30
Kettle Moraine, WI (Milwaukee)	57	$25
Quad Cities	169	$0
Northeastern United States		
Greater Hartford, CT (Southern New England)	28	$40
Central Maryland (Baltimore)	24	$25
New England (Boston, MA)	18	$30
New Jersey (Newark)	30	$40
Central New York (Syracuse)	29	$0
Hudson Valley, NY (Albany)	120	$0
New York Metropolitan	10	$50
Western New York (Buffalo)	46	$30
Harrisburg, PA	45	$25
Lehigh Valley (Allentown, PA)	122	$35
Philadelphia, PA	06	$40
Pittsburgh, PA	13	$20
National Capital Area, DC	05	$40
Southeastern United States		
North Alabama (Birmingham)	65	$30
Jacksonville, FL	58	$30
Central Florida (Orlando)	67	$30
South Florida (Miami)	33	$40
West Florida (Tampa)	41	$35
Atlanta, GA	39	$35
Charlotte, NC	51	$35
Research Triangle (Raleigh, NC)	59	$25
Piedmont/Triad (Winston-Salem, NC)	128	$30
Greenville, SC	54	$30
Memphis, TN	48	$45
Middle Tennessee (Nashville)	102	$45
Virginia (Richmond)	22	$30
Southwestern United States		
Central Arkansas (Little Rock)	82	$60
Central Mississippi (Jackson)	161	$0
Denver, CO	16	$40
Greater Kansas City, KS	87	$0
Baton Rouge, LA	85	$25
Greater New Orleans, LA	61	$20
St. Louis, MO	11	$25
New Mexico (Albuquerque)	83	$25
Central Oklahoma (OK City)	49	$30
Tulsa, OK	34	$25
Austin, TX	20	$25
Greater Houston Area, TX	09	$40
North Texas (Dallas)	12	$30
San Antonio/So. Texas	81	$25
Western United States		
Anchorage, AK	177	$20
Phoenix, AZ	53	$30
Los Angeles, CA	01	$25
Orange County, CA (Anaheim)	79	$30
Sacramento, CA	76	$20
San Francisco, CA	15	$45
San Diego, CA	19	$25
Silicon Valley, CA (Sunnyvale)	62	$25
Hawaii (Honolulu)	71	$30
Boise, ID	42	$30
Willamette Valley, OR (Portland)	50	$30
Utah (Salt Lake City)	04	$30
Mt. Rainier, WA (Olympia)	129	$20
Puget Sound, WA (Seattle)	35	$25
OCEANIA		
Adelaide, Australia	68	$0
Brisbane, Australia	44	$16
Canberra, Australia	92	$15
Melbourne, Australia	47	$25
Perth, Australia	63	$5
Sydney, Australia	17	$30
Auckland, New Zealand	84	$30
Wellington, New Zealand	73	$22
Papua New Guinea	152	$0

⁕Call chapter for information

To receive your copy of the *Information Systems Control Journal*, please complete the following subscriber information:

Size of organization (at your primary place of business)
① ☐ Fewer than 50 employees
② ☐ 50-100 employess
③ ☐ 101-500 employees
④ ☐ More than 500 employees

Size of your professional audit staff *(local office)*
① ☐ 1 individual
② ☐ 2-5 individuals
③ ☐ 6-10 individuals
④ ☐ 11-25 individuals
⑤ ☐ More than 25 individuals

Your level of purchasing authority
① ☐ Recommend products/services
② ☐ Approve purchase
③ ☐ Recommend and approve purchase

Education courses attended annually *(check one)*
① ☐ None
② ☐ 1
③ ☐ 2-3
④ ☐ 4-5
⑤ ☐ More than 5

Conferences attended annually *(check one)*
① ☐ None
② ☐ 1
③ ☐ 2-3
④ ☐ 4-5
⑤ ☐ More than 5

Primary reason for joining the association *(check one)*
① ☐ Discounts on association products and services
② ☐ Subscription to *IS Control Journal*
③ ☐ Professional advancement/ certification
④ ☐ Access to research, publications, and education
⑨⑨ ☐ Other_____

One of the most important assets of an enterprise is its information. The integrity and reliability of that information and the systems that generate it are crucial to an enterprise's success. Faced with complex and correspondingly ingenious cyberthreats, organizations are looking for individuals who have the proven experience and knowledge to identify, evaluate and recommend solutions to mitigate IT system vulnerabilities. ISACA offers two certifications to meet these needs.

Certified Information Systems Auditor (CISA)

The CISA program is designed to assess and certify individuals in the IS audit, control and security profession who demonstrate exceptional skill and judgment.

The CISA examination content areas include:

- The IS audit process
- Management, planning and organization of IS
- Technical infrastructure and operational practices
- Protection of information assets
- Disaster recovery and business continuity
- Business application system development, acquisition, implementation and maintenance
- Business process evaluation and risk management

To earn the CISA designation, candidates are required to:

- Successfully complete the CISA examination
- Adhere to the Information Systems Audit and Control Association (ISACA) Code of Professional Ethics
- Submit verified evidence of a minimum number of years of professional information systems auditing, control or security work experience
- Comply with the CISA continuing education program (after becoming certified)

Certified Information Security Manager (CISM)

CISM is a newly created credential for security managers that provides executive management with the assurance that those certified have the expertise to provide effective security management and consulting. It is business-oriented and focused on information risk management while addressing management, design and technical security issues at a conceptual level.

The CISM credential measures expertise in the areas of:

- Information security governance
- Risk management
- Information security program(me) development
- Information security management
- Response management

To earn the CISM designation, information security professionals are required to:

- Successfully complete the CISM examination
- Adhere to the Information Systems Audit and Control Association (ISACA) Code of Professional Ethics
- Submit verified evidence of a minimum number of years of information security experience, with a number of those years in the job analysis domains
- Comply with the CISM continuing education program (after becoming certified)

A grandfathering opportunity, available through 31 December 2003, allows information security professionals with the necessary experience to apply for certification without taking the CISM exam.

CISA®
CERTIFIED INFORMATION SYSTEMS AUDITOR™

CISM
CERTIFIED INFORMATION SECURITY MANAGER™

Being a CISA or a CISM is more than passing an examination. It demonstrates the commitment, dedication and proficiency required to excel in your profession. These certifications identify their holders as consummate professionals who maintain a competitive advantage among their peers. Earning these designations helps assure a positive reputation and distinguishes you among other candidates seeking positions in both the private and public sectors. As a member of ISACA, you have the opportunity to sit for the exams, purchase review materials and attend ISACA conferences to maintain your certifications at a substantially reduced cost.

For more information on becoming a CISA or a CISM, visit the ISACA web site at *www.isaca.org/certification.*

GOVERNANCE INSTITUTE™

COBIT®

3rd Edition

Control Objectives

July 2000

Released by the COBIT Steering Committee and the IT Governance Institute™

The COBIT Mission:

To research, develop, publicise and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors.

American Samoa
Argentina
Armenia
Australia
Austria
Bahamas
Bahrain
Bangladesh
Barbados
Belgium
Bermuda
Bolivia
Botswana
Brazil
British Virgin Islands
Canada
Cayman Islands
Chile
China
Colombia
Costa Rica
Croatia
Curacao
Cyprus
Czech Republic
Denmark
Dominican Republic
Ecuador
Egypt
El Salvador
Estonia
Faeroe Islands
Fiji
Finland
France
Germany
Ghana
Greece
Guam
Guatemala
Honduras
Hong Kong
Hungary
Iceland
India
Indonesia
Iran
Ireland
Israel
Italy
Ivory Coast
Jamaica
Japan
Jordan
Kazakhstan
Kenya
Korea
Kuwait

Information Systems Audit and Control Association

A Single International Source for Information Technology Controls

The Information Systems Audit and Control Association is a leading global professional organisation representing individuals in more than 100 countries and comprising all levels of IT — executive, management, middle management and practitioner. The Association is uniquely positioned to fulfil the role of a central, harmonising source of IT control practice standards for the world over. Its strategic alliances with other groups in the financial, accounting, auditing and IT professions are ensuring an unparalleled level of integration and commitment by business process owners.

Association Programmes and Services

The Association's services and programmes have earned distinction by establishing the highest levels of excellence in certification, standards, professional education and technical publishing.

- *Its certification programme (the Certified Information Systems Auditor™) is the only global designation throughout the IT audit and control community.*
- *Its standards activities establish the quality baseline by which other IT audit and control activities are measured.*
- *Its professional education programme offers technical and management conferences on five continents, as well as seminars worldwide to help professionals everywhere receive high-quality continuing education.*
- *Its technical publishing area provides references and professional development materials to augment its distinguished selection of programmes and services.*

The Information Systems Audit and Control Association was formed in 1969 to meet the unique, diverse and high technology needs of the burgeoning IT field. In an industry in which progress is measured in nano-seconds, ISACA has moved with agility and speed to bridge the needs of the international business community and the IT controls profession.

For More Information

To receive additional information, you may telephone (+1.847.253.1545), send an e-mail (research@isaca.org) or visit these web sites:

www.ITgovernance.org

www.isaca.org

Latvia
Lebanon
Liechtenstein
Lithuania
Luxemburg
Malaysia
Malta
Malawi
Mauritius
Mexico
Namibia
Nepal
Netherlands
New Guinea
New Zealand
Nicaragua
Nigeria
Norway
Oman
Pakistan
Panama
Paraguay
Peru
Philippines
Poland
Portugal
Qatar
Russia
Saudi Arabia
Scotland
Seychelles
Singapore
Slovak Republic
Slovenia
South Africa
Spain
Sri Lanka
St. Kitts
St. Lucia
Sweden
Switzerland
Taiwan
Tanzania
Tasmania
Thailand
Trinidad & Tobago
Tunisia
Turkey
Uganda
United Arab Emirates
United Kingdom
United States
Uruguay
Venezuela
Vietnam
Wales
Yugoslavia
Zambia
Zimbabwe

TABLE OF CONTENTS

Information Systems Audit and Control Foundation
IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: *research@isaca.org*
Web sites: *www.ITgovernance.org*
www.isaca.org

ISBN 1-893209-17-2 (*Control Objectives*)
ISBN 1-893209-13-X (Complete 6 book set with CD-ROM)

Printed in the United States of America.

ACKNOWLEDGMENTS

COBIT STEERING COMMITTEE

Erik Guldentops, S.W.I.F.T. sc, Belgium

John Lainhart, PricewaterhouseCoopers, USA

Eddy Schuermans, PricewaterhouseCoopers, Belgium

John Beveridge, State Auditor's Office, Massachusetts, USA

Michael Donahue, PricewaterhouseCoopers, USA

Gary Hardy, Arthur Andersen, United Kingdom

Ronald Saull, Great-West Life Assurance, London Life and Investors Group, Canada

Mark Stanley, Sun America Inc., USA

SPECIAL THANKS to the ISACA Boston and National Capital Area Chapters for their contributions to the COBIT *Control Objectives*.

SPECIAL THANKS to the members of the Board of the Information Systems Audit and Control Association and Trustees of the Information Systems Audit and Control Foundation, headed by International President Paul Williams, for their continuing and unwavering support of COBIT.

EXECUTIVE OVERVIEW

Critically important to the survival and success of an organisation is effective management of information and related Information Technology (IT). In this global information society—where information travels through cyberspace without the constraints of time, distance and speed—this criticality arises from the:

- Increasing dependence on information and the systems that deliver this information
- Increasing vulnerabilities and a wide spectrum of threats, such as cyber threats and information warfare
- Scale and cost of the current and future investments in information and information systems
- Potential for technologies to dramatically change organisations and business practices, create new opportunities and reduce costs

For many organisations, information and the technology that supports it represent the organisation's most valuable assets. Moreover, in today's very competitive and rapidly changing business environment, management has heightened expectations regarding IT delivery functions: management requires increased quality, functionality and ease of use; decreased delivery time; and continuously improving service levels—while demanding that this be accomplished at lower costs.

Many organisations recognise the potential benefits that technology can yield. Successful organisations, however, understand and manage the risks associated with implementing new technologies.

There are numerous changes in IT and its operating environment that emphasise the need to better manage IT-related risks. Dependence on electronic information and IT systems is essential to support critical business processes. In addition, the regulatory environment is mandating stricter control over information. This, in turn, is driven by increasing disclosures of information system disasters and increasing electronic fraud. The management of IT-related risks is now being understood as a key part of enterprise governance.

Within enterprise governance, IT governance is becoming more and more prominent, and is defined as a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes. IT governance is integral to the success of enterprise governance by assuring efficient and effective measurable improvements in related enterprise processes. IT governance provides the structure that links IT processes, IT resources and information to enterprise strategies and objectives. Furthermore, IT governance integrates and institutionalises good (or best) practices of planning and organising, acquiring and implementing, delivering and supporting, and monitoring IT performance to ensure that the enterprise's information and related technology support its business objectives. IT governance thus enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage.

IT GOVERNANCE

A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes.

Organisations must satisfy the quality, fiduciary and security requirements for their information, as for all assets. Management must also optimise the use of available resources, including data, application systems, technology, facilities and people. To discharge these responsibilities, as well as to achieve its objectives, management must understand the status of its own IT systems and decide what security and control they should provide.

Control Objectives for Information and related Technology (COBIT), now in its 3rd edition, helps meet the multiple needs of management by bridging the gaps between business risks, control needs and technical issues. It provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT's "good practices" means consensus of the experts—they will help optimise information investments and will provide a measure to be judged against when things do go wrong.

Management must ensure that an internal control system or framework is in place which supports the business processes, makes it clear how each individual control activity satisfies the information requirements and impacts the IT resources. Impact on IT resources is highlighted in the COBIT *Framework* together with the business requirements for effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability of information that need to be satisfied. Control, which includes policies, organisational structures, practices and procedures, is management's responsibility. Management, through its enterprise governance, must ensure that due diligence is exercised by all individuals involved in the management, use, design, development, maintenance or operation of information systems. An IT control objective is a statement of the desired result or purpose to be achieved by implementing control procedures within a particular IT activity.

Business orientation is the main theme of COBIT. It is designed to be employed not only by users and auditors, but also, and more importantly, as comprehensive guidance for management and business process owners. Increasingly, business practice involves the full empowerment of business process owners so they have total responsibility for all aspects of the business process. In particular, this includes providing adequate controls.

The COBIT *Framework* provides a tool for the business process owner that facilitates the discharge of this responsibility. The *Framework* starts from a simple and pragmatic premise:

In order to provide the information that the organisation needs to achieve its objectives, IT resources need to be managed by a set of naturally grouped processes.

The *Framework* continues with a set of 34 high-level *Control Objectives*, one for each of the IT processes, grouped into four domains: planning and organisation, acquisition and implementation, delivery and support, and monitoring. This structure covers all aspects of information and the technology that supports it. By addressing these 34 high-level control objectives, the business process owner can ensure that an adequate control system is provided for the IT environment.

IT governance guidance is also provided in the COBIT *Framework*. IT governance provides the structure that links IT processes, IT resources and information to enterprise strategies and objectives. IT governance integrates optimal ways of planning and organising, acquiring and implementing, delivering and supporting, and monitoring IT performance. IT governance enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage.

In addition, corresponding to each of the 34 high-level control objectives is an *Audit Guideline* to enable the review of IT processes against COBIT's 318 recommended detailed control objectives to provide management assurance and/or advice for improvement.

The *Management Guidelines*, COBIT's most recent development, further enhances and enables enterprise management to deal more effectively with the needs and requirements of IT governance. The guidelines are action oriented and generic and provide management direction for getting the enterprise's information and related processes under control, for monitoring achievement of organisational goals, for monitoring performance within each IT process and for benchmarking organisational achievement.

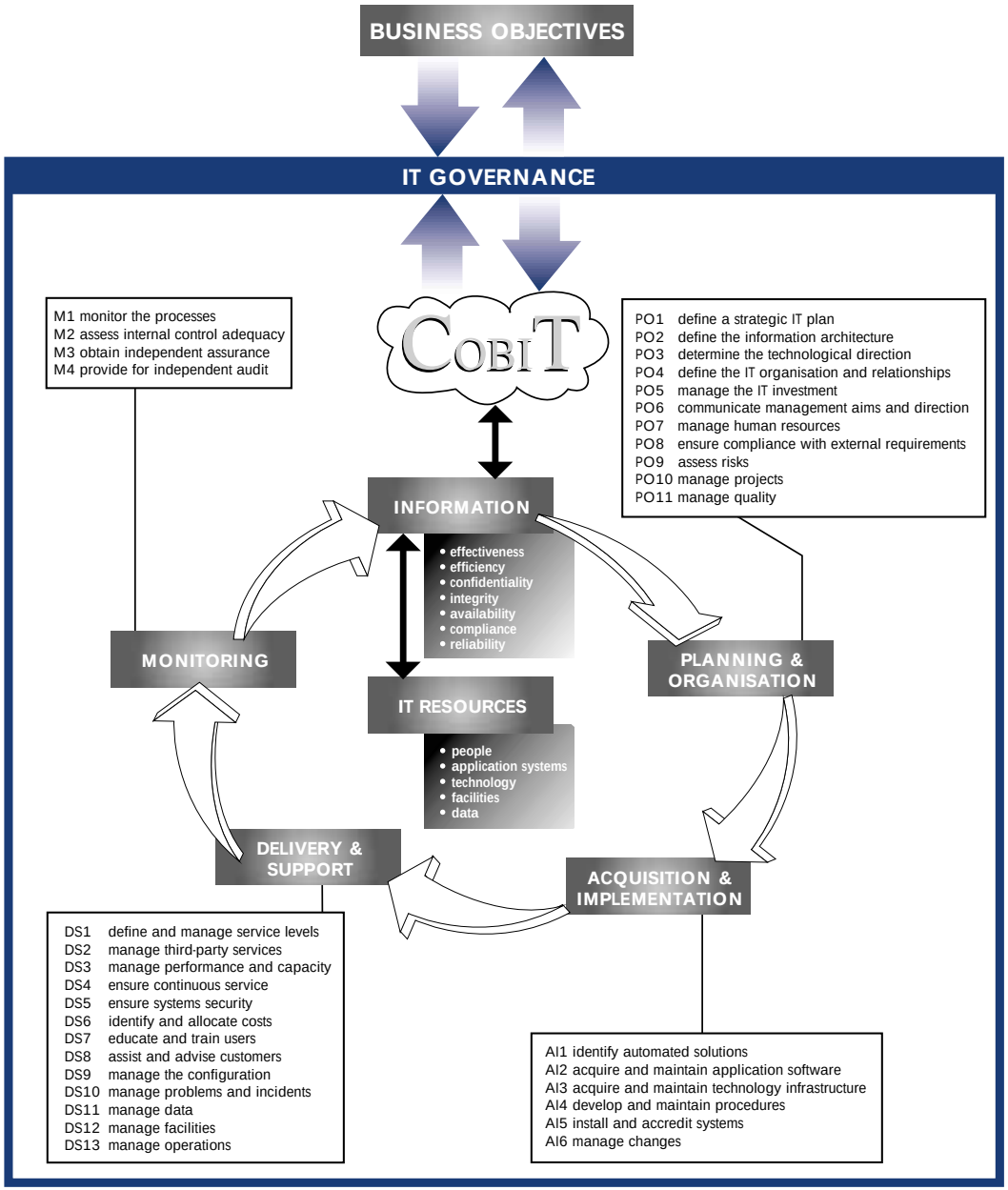
Specifically, COBIT provides **Maturity Models** for control over IT processes, so that management can map where the organisation is today, where it stands in relation to the best-in-class in its industry and to international standards and where the organisation wants to be; **Critical Success Factors**, which define the most important management-oriented implementation guidelines to achieve control over and within its IT processes; **Key Goal Indicators**, which define measures that tell management—after the fact—whether an IT process has achieved its business requirements; and **Key Performance Indicators**, which are lead indicators that define measures of how well the IT process is performing in enabling the goal to be reached.

COBIT's *Management Guidelines* are generic and action oriented for the purpose of answering the following types of management questions: How far should we go, and is the cost justified by the benefit? What are the indicators of good performance? What are the critical success factors? What are the risks of not achieving our objectives? What do others do? How do we measure and compare?

COBIT also contains an *Implementation Tool Set* that provides lessons learned from those organisations that quickly and successfully applied COBIT in their work environments. It has two particularly useful tools—Management Awareness Diagnostic and IT Control Diagnostic—to assist in analysing an organisation's IT control environment.

Over the next few years, the management of organisations will need to demonstrably attain increased levels of security and control. COBIT is a tool that allows managers to bridge the gap with respect to control requirements, technical issues and business risks and communicate that level of control to stakeholders. COBIT enables the development of clear policy and good practice for IT control throughout organisations, worldwide. **Thus, COBIT is designed to be the breakthrough IT governance tool that helps in understanding and managing the risks and benefits associated with information and related IT.**

COBIT IT PROCESSES DEFINED WITHIN THE FOUR DOMAINS



THE COBIT FRAMEWORK

THE NEED FOR CONTROL IN INFORMATION TECHNOLOGY

In recent years, it has become increasingly evident that there is a need for a reference framework for security and control in IT. Successful organisations require an appreciation for and a basic understanding of the risks and constraints of IT at all levels within the enterprise in order to achieve effective direction and adequate controls.

MANAGEMENT has to decide what to reasonably invest for security and control in IT and how to balance risk and control investment in an often unpredictable IT environment. While information systems security and control help manage risks, they do not eliminate them. In addition, the exact level of risk can never be known since there is always some degree of uncertainty. Ultimately, management must decide on the level of risk it is willing to accept. Judging what level can be tolerated, particularly when weighted against the cost, can be a difficult management decision. Therefore, management clearly needs a framework of generally accepted IT security and control practices to benchmark the existing and planned IT environment.

There is an increasing need for **USERS** of IT services to be assured, through accreditation and audit of IT services provided by internal or third parties, that adequate security and control exists. At present, however, the implementation of good IT controls in information systems, be they commercial, non-profit or governmental, is hampered by confusion. The confusion arises from the different evaluation methods such as ITSEC, TCSEC, IS0 9000 evaluations, emerging COSO internal control evaluations, etc. As a result, users need a general foundation to be established as a first step.

Frequently, **AUDITORS** have taken the lead in such international standardisation efforts because they are continuously confronted with the need to substantiate their opinion on internal control to management. Without a framework, this is an exceedingly difficult task. Furthermore, auditors are increasingly being called on by management to proactively consult and advise on IT security and control-related matters.

THE BUSINESS ENVIRONMENT: COMPETITION, CHANGE AND COST

Global competition is here. Organisations are restructuring to streamline operations and simultaneously take advantage of the advances in IT to improve their competitive position. Business re-engineering, right-sizing, outsourcing, empowerment, flattened organisations and distributed processing are all changes that impact the way that business and governmental organisations operate. These changes are having, and will continue to have, profound implications for the management and operational control structures within organisations worldwide.

Emphasis on attaining competitive advantage and cost-efficiency implies an ever-increasing reliance on technology as a major component in the strategy of most organisations. Automating organisational functions is, by its very nature, dictating the incorporation of more powerful control mechanisms into computers and networks, both hardware-based and software-based. Furthermore, the fundamental structural characteristics of these controls are evolving at the same rate and in the same "leap frog" manner as the underlying computing and networking technologies are evolving.

Within the framework of accelerated change, if managers, information systems specialists and auditors are indeed going to be able to effectively fulfil their roles, their skills must evolve as rapidly as the technology and the environment. One must understand the technology of controls involved and its changing nature if one is to exercise reasonable and prudent judgments in evaluating control practices found in typical business or governmental organisations.

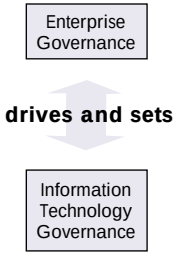
EMERGENCE OF ENTERPRISE AND IT GOVERNANCE

To achieve success in this information economy, enterprise governance and IT governance can no longer be considered separate and distinct disciplines. Effective enterprise governance focuses individual and group expertise and experience where it can be most productive, monitors and measures performance and provides assurance to critical issues. IT, long considered solely an

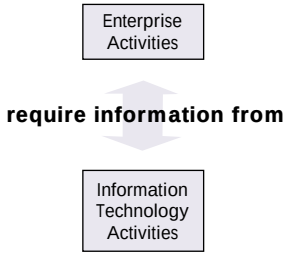
enabler of an enterprise's strategy, must now be regarded as an integral part of that strategy.

IT governance provides the structure that links IT processes, IT resources, and information to enterprise strategies and objectives. IT governance integrates and institutionalises optimal ways of planning and organising, acquiring and implementing, delivering and supporting, and monitoring IT performance. IT governance is integral to the success of enterprise governance by assuring efficient and effective measurable improvements in related enterprise processes. IT governance enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage.

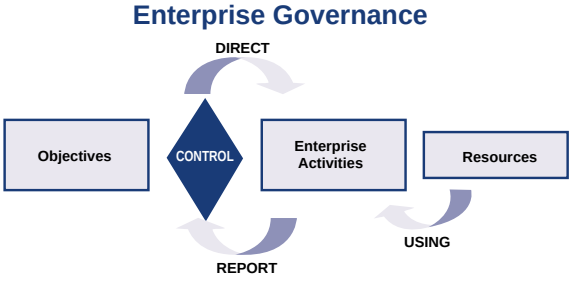
Looking at the interplay of enterprise and IT governance processes in more detail, enterprise governance, the system by which entities are directed and controlled, drives and sets IT governance. At the same time, IT should provide critical input to, and constitute an important component of, strategic plans. IT may in fact influence strategic opportunities outlined by the enterprise.



Enterprise activities require information from IT activities in order to meet business objectives. Successful organisations ensure interdependence between their strategic planning and their IT activities. IT must be aligned with and enable the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining a competitive advantage.

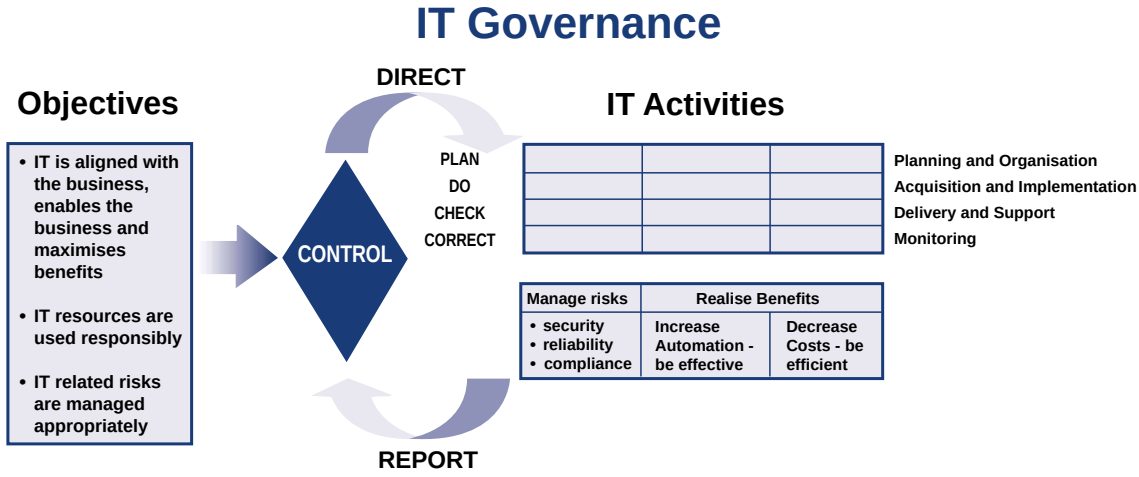


Enterprises are governed by generally accepted good (or best) practices, to ensure that the enterprise is achieving its goals-the assurance of which is guaranteed by certain controls. From these objectives flows the organisation's direction, which dictates certain enterprise activities, using the enterprise's resources. The results of the enterprise activities are measured and reported on, providing input to the constant revision and maintenance of the controls, beginning the cycle again.



THE COBIT FRAMEWORK, *continued*

IT also is governed by good (or best) practices, to ensure that the enterprise's information and related technology support its business objectives, its resources are used responsibly and its risks are managed appropriately. These practices form a basis for direction of IT activities, which can be characterised as planning and organising, acquiring and implementing, delivering and supporting, and monitoring, for the dual purposes of managing risks (to gain security, reliability and compliance) and realising benefits (increasing effectiveness and efficiency). Reports are issued on the outcomes of IT activities, which are measured against the various practices and controls, and the cycle begins again.



In order to ensure that management reaches its business objectives, it must direct and manage IT activities to reach an effective balance between managing risks and realising benefits. To accomplish this, management needs to identify the most important activities to be performed, measure progress towards achieving goals and determine how well the IT processes are performing. In addition, it needs the ability to evaluate the organisation's maturity level against industry best practices and international standards. **To support these management needs, the COBIT *Management Guidelines* have identified specific Critical Success Factors, Key Goal Indicators, Key Performance Indicators and an associated Maturity Model for IT governance, as presented in Appendix I.**

RESPONSE TO THE NEED

In view of these ongoing changes, the development of this framework for control objectives for IT, along with continued applied research in IT controls based on this framework, are cornerstones for effective progress in the field of information and related technology controls.

On the one hand, we have witnessed the development and publication of overall business control models like COSO (Committee of Sponsoring Organisations of the Treadway Commission-Internal Control—*Integrated Framework*, 1992) in the US, Cadbury in the UK, CoCo in Canada and King in South Africa. On the other hand, an important number of more focused control models are in existence at the level of IT. Good examples of the latter category are the Security Code of Conduct from DTI (Department of Trade and Industry, UK), Information Technology Control Guidelines from CICA (Canadian Institute of Chartered Accountants, Canada), and the Security Handbook from NIST (National Institute of Standards and Technology, US). However, these focused control models do not provide a comprehensive and usable control model over IT in support of business processes. The purpose of COBIT is to bridge this gap by providing a foundation that is closely linked to business objectives while focusing on IT.

(Most closely related to COBIT is the recently published *AICPA/CICA SysTrust™ Principles and Criteria for Systems Reliability*. SysTrust is an authoritative issuance of both the Assurance Services Executive Committee in the United States and the Assurance Services Development Board in Canada, based in part on the COBIT *Control Objectives*. SysTrust is designed to increase the comfort of management, customers and business partners with the systems that support a business or a particular activity. The SysTrust service entails the public accountant providing an assurance service in which he or she evaluates and tests whether a system is reliable when measured against four essential principles: availability, security, integrity and maintainability.)

A focus on the business requirements for controls in IT and the application of emerging control models and related international standards evolved the original Information Systems Audit and Control Foundation's *Control Objectives* from an auditor's tool to COBIT, a management tool. Further, the development of IT *Management Guidelines* has taken COBIT to the next level-providing management with Key Goal Indicators (KGIs), Key Performance Indicators (KPIs), Critical Success Factors (CSFs) and Maturity Models so that it can assess its IT environment and make choices for control implementation and control improvements over the organisation's information and related technology.

Hence, the main objective of the COBIT project is the development of clear policies and good practices for security and control in IT for worldwide endorsement by commercial, governmental and professional organisations. It is the goal of the project to develop these control objectives primarily from the business objectives and needs perspective. (This is compliant with the COSO perspective, which is first and foremost a management framework for internal controls.) Subsequently, control objectives have been developed from the audit objectives (certification of financial information, certification of internal control measures, efficiency and effectiveness, etc.) perspective.

AUDIENCE: MANAGEMENT, USERS AND AUDITORS

COBIT is designed to be used by three distinct audiences.

MANAGEMENT:
to help them balance risk and control investment in an often unpredictable IT environment.

USERS:
to obtain assurance on the security and controls of IT services provided by internal or third parties.

AUDITORS:
to substantiate their opinions and/or provide advice to management on internal controls.

THE COBIT FRAMEWORK, *continued*

BUSINESS OBJECTIVES ORIENTATION

COBIT is aimed at addressing business objectives. The control objectives make a clear and distinct link to business objectives in order to support significant use outside the audit community. Control objectives are defined in a process-oriented manner following the principle of business re-engineering. At identified domains and processes, a high-level control objective is identified and rationale provided to document the link to the business objectives. In addition, considerations and guidelines are provided to define and implement the IT control objective.

The classification of domains where high-level control objectives apply (domains and processes), an indication of the business requirements for information in that domain, as well as the IT resources primarily impacted by the control objectives, together form the COBIT *Framework*. The *Framework* is based on the research activities that have identified 34 high-level control objectives and 318 detailed control objectives. The *Framework* was exposed to the IT industry and the audit profession to allow an opportunity for review, challenge and comment. The insights gained have been appropriately incorporated.

GENERAL DEFINITIONS

For the purpose of this project, the following definitions are provided. "Control" is adapted from the COSO Report (*Internal Control—Integrated Framework*, Committee of Sponsoring Organisations of the Treadway Commission, 1992) and "IT Control Objective" is adapted from the SAC Report (*Systems Auditability and Control Report*, The Institute of Internal Auditors Research Foundation, 1991 and 1994).

Control is defined as the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

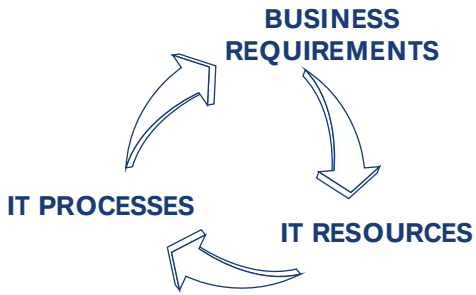
IT Control Objective is defined as a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.

IT Governance is defined as a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes.

THE FRAMEWORK'S PRINCIPLES

There are two distinct classes of control models currently available: those of the "business control model" class (e.g., COSO) and the "more focused control models for IT" (e.g., DTI). COBIT aims to bridge the gap that exists between the two. COBIT is therefore positioned to be more comprehensive for management and to operate at a higher level than technology standards for information systems management. **Thus, COBIT is the model for IT governance!**

The underpinning concept of the COBIT *Framework* is that control in IT is approached by looking at information that is needed to support the business objectives or requirements, and by looking at information as being the result of the combined application of IT-related resources that need to be managed by IT processes.



To satisfy business objectives, information needs to conform to certain criteria, which COBIT refers to as business requirements for information. In establishing the list of requirements, COBIT combines the principles embedded in existing and known reference models:

Quality Requirements	Quality Cost Delivery
Fiduciary Requirements (COSO Report)	Effectiveness and Efficiency of operations Reliability of Information Compliance with laws and regulations
Security Requirements	Confidentiality Integrity Availability

Quality has been retained primarily for its negative aspect (no faults, reliability, etc.), which is also captured to a large extent by the Integrity criterion. The positive but less tangible aspects of Quality (style, attractiveness, "look and feel," performing beyond expectations, etc.) were, for a time, not being considered from an IT control objectives point of view. The premise is that the first priority should go to properly managing the risks as opposed to the opportunities. The usability aspect of Quality is covered by the Effectiveness criterion. The Delivery aspect of Quality was considered to overlap with the Availability aspect of the Security requirements and also to some extent Effectiveness and Efficiency. Finally, Cost is also considered covered by Efficiency.

For the Fiduciary Requirements, COBIT did not attempt to reinvent the wheel—COSO's definitions for Effectiveness and Efficiency of operations, Reliability of Information and Compliance with laws and regulations were used. However, Reliability of Information was expanded to include all information—not just financial information.

With respect to the Security Requirements, COBIT identified Confidentiality, Integrity, and Availability as the key elements—these same three elements, it was found, are used worldwide in describing IT security requirements.

THE FRAMEWORK'S PRINCIPLES, *continued*

Starting the analysis from the broader Quality, Fiduciary and Security requirements, seven distinct, certainly overlapping, categories were extracted. COBIT's working definitions are as follows:

Effectiveness deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.

Efficiency concerns the provision of information through the optimal (most productive and economical) use of resources.

Confidentiality concerns the protection of sensitive information from unauthorised disclosure.

Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.

Availability relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

Compliance deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria.

Reliability of Information relates to the provision of appropriate information for management to operate the entity and for management to exercise its financial and compliance reporting responsibilities.

The IT resources identified in COBIT can be explained/defined as follows:

Data are objects in their widest sense (i.e., external and internal), structured and non-structured, graphics, sound, etc.

Application Systems are understood to be the sum of manual and programmed procedures.

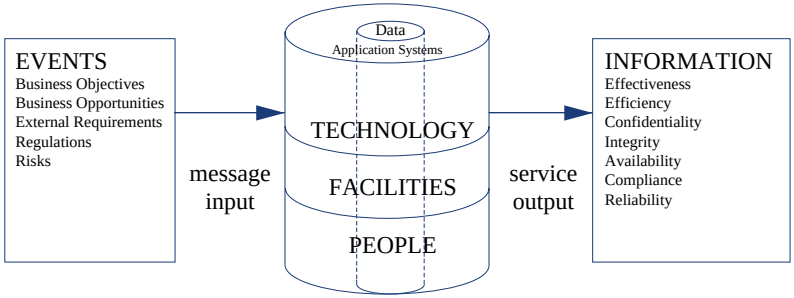
Technology covers hardware, operating systems, database management systems, networking, multimedia, etc.

Facilities are all the resources to house and support information systems.

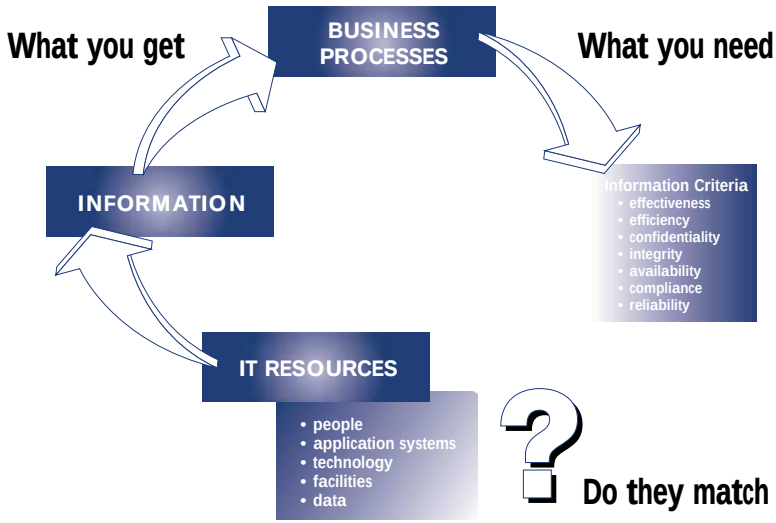
People include staff skills, awareness and productivity to plan, organise, acquire, deliver, support and monitor information systems and services.

Money or capital was not retained as an IT resource for classification of control objectives because it can be considered as being the investment into any of the above resources. It should also be noted that the *Framework* does not specifically refer to documentation of all material matters relating to a particular IT process. As a matter of good practice, documentation is considered essential for good control, and therefore lack of documentation would be cause for further review and analysis for compensating controls in any specific area under review.

Another way of looking at the relationship of IT resources to the delivery of services is depicted below.

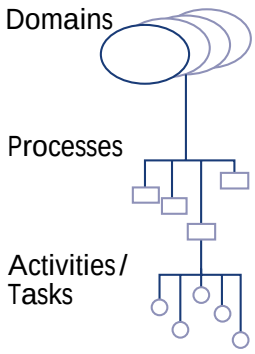


In order to ensure that the business requirements for information are met, adequate control measures need to be defined, implemented and monitored over these resources. How then can organisations satisfy themselves that the information they get exhibits the characteristics they need? This is where a sound framework of IT control objectives is required. The next diagram illustrates this concept.

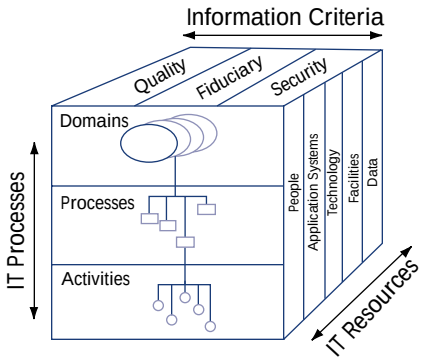


THE FRAMEWORK'S PRINCIPLES, *continued*

The COBIT *Framework* consists of high-level control objectives and an overall structure for their classification. The underlying theory for the classification is that there are, in essence, three levels of IT efforts when considering the management of IT resources. Starting at the bottom, there are the activities and tasks needed to achieve a measurable result. Activities have a life-cycle concept while tasks are more discrete. The life-cycle concept has typical control requirements different from discrete activities. Processes are then defined one layer up as a series of joined activities or tasks with natural (control) breaks. At the highest level, processes are naturally grouped together into domains. Their natural grouping is often confirmed as responsibility domains in an organisational structure and is in line with the management cycle or life cycle applicable to IT processes.



Thus, the conceptual framework can be approached from three vantage points: (1) information criteria, (2) IT resources and (3) IT processes. These three vantage points are depicted in the COBIT Cube.



With the preceding as the framework, the domains are identified using wording that management would use in the day-to-day activities of the organisation—not auditor jargon. Thus, four broad domains are identified: planning and organisation, acquisition and implementation, delivery and support, and monitoring.

Definitions for the four domains identified for the high-level classification are:

Planning and Organisation

This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. Furthermore, the realisation of the strategic vision needs to be planned, communicated and managed for different perspectives. Finally, a proper organisation as well as technological infrastructure must be put in place.

Acquisition and Implementation

To realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure that the life cycle is continued for these systems.

Delivery and Support

This domain is concerned with the actual delivery of required services, which range from traditional operations over security and continuity aspects to training. In order to deliver services, the necessary support processes must be set up.
This domain includes the actual processing of data by application systems, often classified under application controls.

Monitoring

All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain thus addresses management's oversight of the organisation's control process and independent assurance provided by internal and external audit or obtained from alternative sources.

It should be noted that these IT processes can be applied at different levels within an organisation. For example, some of these processes will be applied at the enterprise level, others at the IT function level, others at the business process owner level, etc.

It should also be noted that the Effectiveness criterion of processes that plan or deliver solutions for business requirements will sometimes cover the criteria for Availability, Integrity and Confidentiality—in practice, they have become business requirements. For example, the process of "identify solutions" has to be effective in providing the Availability, Integrity and Confidentiality requirements.

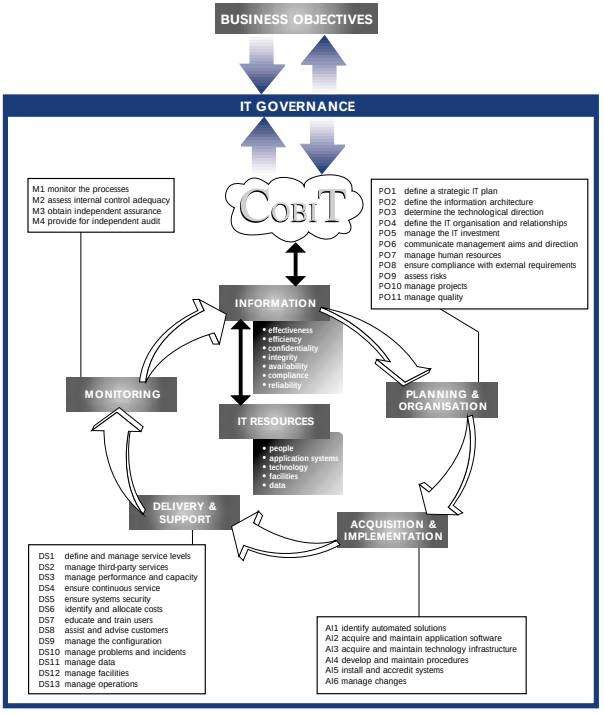
It is clear that all control measures will not necessarily satisfy the different business requirements for information to the same degree.

- **Primary** is the degree to which the defined control objective directly impacts the information criterion concerned.
- **Secondary** is the degree to which the defined control objective satisfies only to a lesser extent or indirectly the information criterion concerned.
- **Blank** could be applicable; however, requirements are more appropriately satisfied by another criterion in this process and/or by another process.

Similarly, all control measures will not necessarily impact the different IT resources to the same degree. Therefore, the COBIT *Framework* specifically indicates the applicability of the IT resources that are specifically managed by the process under consideration (not those that merely take part in the process). This classification is made within the COBIT *Framework* based on a rigorous process of input from researchers, experts and reviewers, using the strict definitions previously indicated.

In summary, in order to provide the information that the organisation needs to achieve its objectives, IT governance must be exercised by the organisation to ensure that IT resources are managed by a set of naturally grouped IT processes. The following diagram illustrates this concept.

COBIT IT PROCESSES DEFINED WITHIN THE FOUR DOMAINS



COBIT HISTORY AND BACKGROUND

COBIT 3rd Edition is the most recent version of Control Objectives for Information and related Technology, first released by the Information Systems Audit and Control Foundation (ISACF) in 1996. The 2nd edition, reflecting an increase in the number of source documents, a revision in the high-level and detailed control objectives and the addition of the *Implementation Tool Set*, was published in 1998. The 3rd edition marks the entry of a new primary publisher for COBIT: the IT Governance Institute.

The IT Governance Institute was formed by the Information System Audit and Control Association (ISACA) and its related Foundation in 1998 in order to advance the understanding and adoption of IT governance principles. Due to the addition of the Management Guidelines to COBIT 3rd Edition and its expanded and enhanced focus on IT governance, the IT Governance Institute took a leading role in the publication's development.

COBIT was originally based on ISACF's *Control Objectives*, and has been enhanced with existing and emerging international technical, professional, regulatory and industry-specific standards. The resulting control objectives have been developed for application to organisation-wide information systems. The term "generally applicable and accepted" is explicitly used in the same sense as Generally Accepted Accounting Principles (GAAP).

COBIT is relatively small in size and attempts to be both pragmatic and responsive to business needs while being independent of the technical IT platforms adopted in an organisation.

While not excluding any other accepted standard in the information systems control field that may have come to light during the research, sources identified are:

Technical standards from ISO, EDIFACT, etc.
Codes of Conduct issued by the Council of Europe, OECD, ISACA, etc.
Qualification criteria for IT systems and processes: ITSEC, TCSEC, ISO 9000, SPICE, TickIT, Common Criteria, etc.
Professional standards for internal control and auditing: COSO, IFAC, AICPA, CICA, ISACA, IIA, PCIE, GAO, etc.
Industry practices and requirements from industry forums (ESF, I4) and government-sponsored platforms (IBAG, NIST, DTI), etc., and
Emerging industry-specific requirements from banking, electronic commerce, and IT manufacturing.

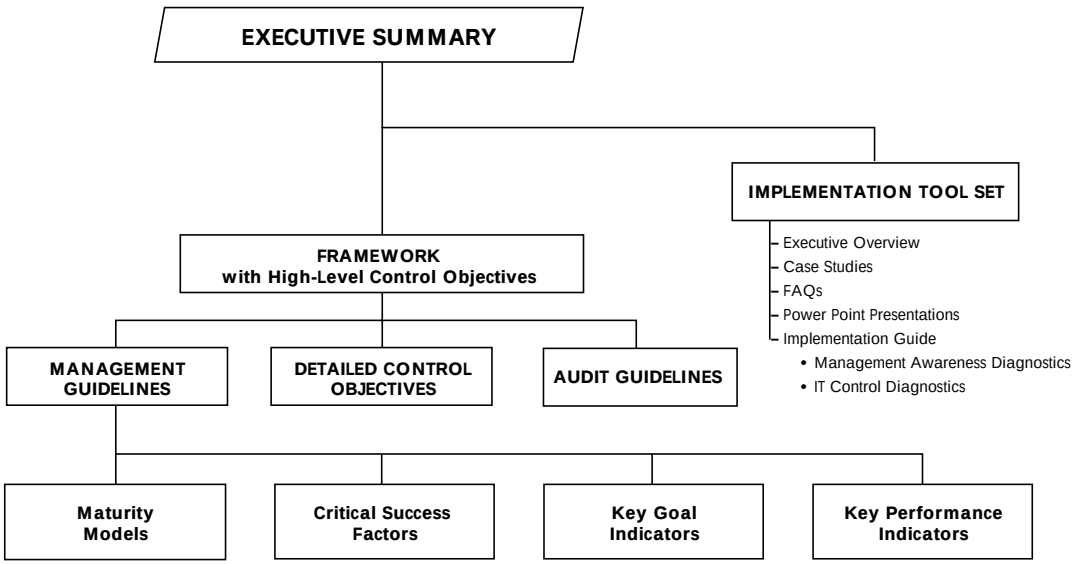
Refer to Appendix II, COBIT Project Description; Appendix III, COBIT Primary Reference Material; and Appendix IV, Glossary of Terms.

COBIT PRODUCT EVOLUTION

COBIT will evolve over the years and be the foundation for further research. Thus, a family of COBIT products will be created and, as this occurs, the IT tasks and activities that serve as the structure to organise control objectives will be further refined, and the balance between domains and processes reviewed in light of the industry's changing landscape.

Research and publication have been made possible by significant grants from PricewaterhouseCoopers and donations from ISACA chapters and members worldwide. The European Security Forum (ESF) kindly made research material available to the project. The Gartner Group also participated in the development and provided quality assurance review of the *Management Guidelines*.

COBIT Family of Products



CONTROL OBJECTIVES
SUMMARY TABLE

The following chart provides an indication, by IT process and domain, of which information criteria are impacted by the high-level control objectives, as well as an indication of which IT resources are applicable.

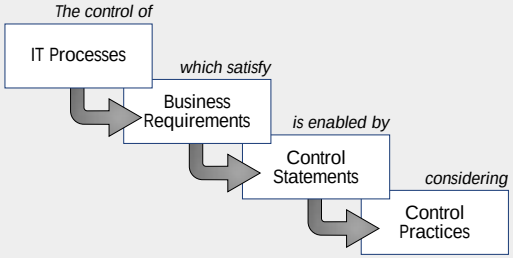
DOMAIN		PROCESS	Information Criteria: effectiveness	efficiency	confidentiality	integrity	availability	compliance	reliability	IT Resources: people	applications	technology	facilities	data
Planning & Organisation	PO1	Define a strategic IT plan	P	S						✔	✔	✔	✔	✔
	PO2	Define the information architecture	P	S	S	S					✔			✔
	PO3	Determine technological direction	P	S								✔	✔	
	PO4	Define the IT organisation and relationships	P	S						✔				
	PO5	Manage the IT investment	P	P					S	✔	✔	✔	✔	
	PO6	Communicate management aims and direction	P					S		✔				
	PO7	Manage human resources	P	P						✔				
	PO8	Ensure compliance with external requirements	P					P	S	✔	✔			✔
	PO9	Assess risks	P	S	P	P	P	S	S	✔	✔	✔	✔	✔
	PO10	Manage projects	P	P						✔	✔	✔	✔	
	PO11	Manage quality	P	P		P			S	✔	✔	✔	✔	
Acquisition & Implementation	AI1	Identify automated solutions	P	S							✔	✔	✔	
	AI2	Acquire and maintain application software	P	P		S		S	S		✔			
	AI3	Acquire and maintain technology infrastructure	P	P		S						✔		
	AI4	Develop and maintain procedures	P	P		S		S	S	✔	✔	✔	✔	
	AI5	Install and accredit systems	P			S	S			✔	✔	✔	✔	✔
	AI6	Manage changes	P	P		P	P		S	✔	✔	✔	✔	✔
Delivery & Support	DS1	Define and manage service levels	P	P	S	S	S	S	S	✔	✔	✔	✔	✔
	DS2	Manage third-party services	P	P	S	S	S	S	S	✔	✔	✔	✔	✔
	DS3	Manage performance and capacity	P	P			S				✔	✔	✔	
	DS4	Ensure continuous service	P	S			P			✔	✔	✔	✔	✔
	DS5	Ensure systems security			P	P	S	S	S	✔	✔	✔	✔	✔
	DS6	Identify and allocate costs		P					P	✔	✔	✔	✔	✔
	DS7	Educate and train users	P	S						✔				
	DS8	Assist and advise customers	P	P						✔	✔			
	DS9	Manage the configuration	P				S		S		✔	✔	✔	
	DS10	Manage problems and incidents	P	P			S			✔	✔	✔	✔	✔
	DS11	Manage data				P			P					✔
	DS12	Manage facilities				P	P						✔	
	DS13	Manage operations	P	P		S	S			✔	✔		✔	✔
Monitoring	M1	Monitor the processes	P	P	S	S	S	S	S	✔	✔	✔	✔	✔
	M2	Assess internal control adequacy	P	P	S	S	S	P	S	✔	✔	✔	✔	✔
	M3	Obtain independent assurance	P	P	S	S	S	P	S	✔	✔	✔	✔	✔
	M4	Provide for independent audit	P	P	S	S	S	P	S	✔	✔	✔	✔	✔

(**P**) primary (**S**) secondary (✓) applicable to

THE CONTROL OBJECTIVES' PRINCIPLES

COBIT, as embodied in this latest version of its *Control Objectives*, reflects the ongoing commitment of ISACA to enhance and maintain the common body of knowledge required to sustain the information systems audit and control profession.

The COBIT *Framework* has been limited to high-level control objectives in the form of a business need within a particular IT process, the achievement of which is enabled by a control statement, for which consideration should be given to potentially applicable controls.



The control objectives have been organised by process/activity, but navigation aids have been provided not only to facilitate entry from any one vantage point, but also to facilitate combined or global approaches, such as installation/implementation of a process, global management responsibilities for a process and the use of IT resources by a process.

It should also be noted that the control objectives have been defined in a generic way; i.e., not depending on the technical platform, while accepting the fact that some special technology environments may need separate coverage for control objectives. Whereas the COBIT *Framework* focuses on **high-level controls** for each process, *Control Objectives* focuses on **specific, detailed control objectives** associated with each IT process. For each of the 34 IT processes of the *Framework*, there are from three to 30 detailed control objectives, for a total of 318.

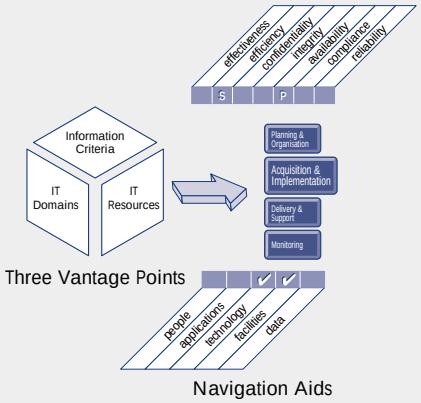
Control Objectives aligns the overall *Framework* with detailed control objectives from 41 primary sources comprising the *de facto* and *de jure* international standards and regulations relating to IT. It contains statements of the desired results or purposes to be achieved by implementing specific control procedures within an IT activity and, thereby, provides a clear policy and good practice for IT control throughout the industry, worldwide.

Control Objectives is directed to the management and staff of the IT, control and audit functions—and, most importantly, to the business process owners. *Control Objectives* provides a working, desktop document for these individuals. Precise and clear definitions of a minimum set of controls to ensure effectiveness, efficiency and economy of resource utilisation are identified. For each process, detailed control objectives are identified as the minimum controls needed to be in place—those controls that will be assessed for sufficiency by the controls professional. *Control Objectives* allows the translation of concepts presented in the *Framework* into specific controls applicable for each IT process.

CONTROL OBJECTIVES NAVIGATION OVERVIEW

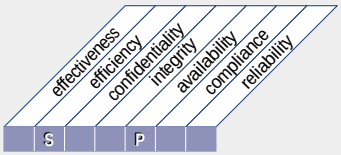
The Control Objectives section contains detailed control objectives for each of the 34 IT processes. On the left page is the high-level control objective. The domain indicator ("PO" for Planning & Organisation, "AI" for Acquisition & Implementation, "DS" for Delivery & Support and "M" for Monitoring) is shown at top left. The applicable information criteria and IT resources managed are shown via mini-matrix, as described below. Beginning on the right page, are the descriptions of the detailed control objectives for the IT process.

To facilitate efficient use of the control objectives in support of the different vantage points, some navigation aids are provided as part of the presentation of the high-level control objectives. For each of the three dimensions along which the COBIT *Framework* can be approached—processes, IT resources and information criteria—a navigation aid is provided.

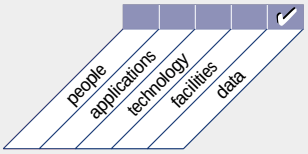


IT domains are identified by this icon in the UPPER RIGHT CORNER of each page in the Control Objectives section, with the domain under review highlighted and enlarged.

The cue to information criteria will be provided in the UPPER LEFT CORNER in the Control Objectives section by means of this mini-matrix, which will identify which criteria are applicable to each high-level control objective and to which degree (primary or secondary).



A second mini-matrix in the LOWER RIGHT CORNER in the Control Objectives section identifies the IT resources that are specifically managed by the process under consideration—not those that merely take part in the process. For example, the "manage data" process concentrates particularly on Integrity and Reliability of the data resource.



CONTROL OBJECTIVE RELATIONSHIPS DOMAINS, PROCESSES AND CONTROL OBJECTIVES

PLANNING & ORGANISATION

1.0 Define a Strategic IT Plan
- 1.1 IT as Part of the Organisation's Long- and Short-Range Plan
- 1.2 IT Long-Range Plan
- 1.3 IT Long-Range Planning—Approach and Structure
- 1.4 IT Long-Range Plan Changes
- 1.5 Short-Range Planning for the IT Function
- 1.6 Communication of IT Plans
- 1.7 Monitoring and Evaluating of IT Plans
- 1.8 Assessment of Existing Systems

2.0 Define the Information Architecture
- 2.1 Information Architecture Model
- 2.2 Corporate Data Dictionary and Data Syntax Rules
- 2.3 Data Classification Scheme
- 2.4 Security Levels

3.0 Determine Technological Direction
- 3.1 Technological Infrastructure Planning
- 3.2 Monitor Future Trends and Regulations
- 3.3 Technological Infrastructure Contingency
- 3.4 Hardware and Software Acquisition Plans
- 3.5 Technology Standards

4.0 Define the IT Organisation and Relationships
- 4.1 IT Planning or Steering Committee
- 4.2 Organisational Placement of the IT Function
- 4.3 Review of Organisational Achievements
- 4.4 Roles and Responsibilities
- 4.5 Responsibility for Quality Assurance
- 4.6 Responsibility for Logical and Physical Security
- 4.7 Ownership and Custodianship
- 4.8 Data and System Ownership
- 4.9 Supervision
- 4.10 Segregation of Duties
- 4.11 IT Staffing
- 4.12 Job or Position Descriptions for IT Staff
- 4.13 Key IT Personnel
- 4.14 Contracted Staff Policies and Procedures
- 4.15 Relationships

5.0 Manage the IT Investment
- 5.1 Annual IT Operating Budget
- 5.2 Cost and Benefit Monitoring
- 5.3 Cost and Benefit Justification

6.0 Communicate Management Aims and Direction
- 6.1 Positive Information Control Environment
- 6.2 Management's Responsibility for Policies
- 6.3 Communication of Organisation Policies
- 6.4 Policy Implementation Resources
- 6.5 Maintenance of Policies
- 6.6 Compliance with Policies, Procedures and Standards
- 6.7 Quality Commitment
- 6.8 Security and Internal Control Framework Policy
- 6.9 Intellectual Property Rights
- 6.10 Issue-Specific Policies
- 6.11 Communication of IT Security Awareness

7.0 Manage Human Resources
- 7.1 Personnel Recruitment and Promotion
- 7.2 Personnel Qualifications
- 7.3 Roles and Responsibilities
- 7.4 Personnel Training
- 7.5 Cross-Training or Staff Back-up
- 7.6 Personnel Clearance Procedures
- 7.7 Employee Job Performance Evaluation
- 7.8 Job Change and Termination

8.0 Ensure Compliance with External Requirements
- 8.1 External Requirements Review
- 8.2 Practices and Procedures for Complying with External Requirements
- 8.3 Safety and Ergonomic Compliance
- 8.4 Privacy, Intellectual Property and Data Flow
- 8.5 Electronic Commerce
- 8.6 Compliance with Insurance Contracts

DOMAINS, PROCESSES AND CONTROL OBJECTIVES

PLANNING & ORGANISATION *continued*

9.0 Assess Risks
- 9.1 Business Risk Assessment
- 9.2 Risk Assessment Approach
- 9.3 Risk Identification
- 9.4 Risk Measurement
- 9.5 Risk Action Plan
- 9.6 Risk Acceptance
- 9.7 Safeguard Selection
- 9.8 Risk Assessment Commitment

10.0 Manage Projects
- 10.1 Project Management Framework
- 10.2 User Department Participation in Project Initiation
- 10.3 Project Team Membership and Responsibilities
- 10.4 Project Definition
- 10.5 Project Approval
- 10.6 Project Phase Approval
- 10.7 Project Master Plan
- 10.8 System Quality Assurance Plan
- 10.9 Planning of Assurance Methods
- 10.10 Formal Project Risk Management
- 10.11 Test Plan
- 10.12 Training Plan
- 10.13 Post-Implementation Review Plan

11.0 Manage Quality
- 11.1 General Quality Plan
- 11.2 Quality Assurance Approach
- 11.3 Quality Assurance Planning
- 11.4 Quality Assurance Review of Adherence to IT Standards and Procedures
- 11.5 System Development Life Cycle Methodology
- 11.6 System Development Life Cycle Methodology for Major Changes to Existing Technology
- 11.7 Updating of the System Development Life Cycle Methodology
- 11.8 Coordination and Communication
- 11.9 Acquisition and Maintenance Framework for the Technology Infrastructure
- 11.10 Third-Party Implementor Relationships
- 11.11 Programme Documentation Standards
- 11.12 Programme Testing Standards
- 11.13 System Testing Standards
- 11.14 Parallel/Pilot Testing
- 11.15 System Testing Documentation
- 11.16 Quality Assurance Evaluation of Adherence to Development Standards
- 11.17 Quality Assurance Review of the Achievement of IT Objectives
- 11.18 Quality Metrics
- 11.19 Reports of Quality Assurance Reviews

ACQUISITION & IMPLEMENTATION

1.0 Identify Automated Solutions
- 1.1 Definition of Information Requirements
- 1.2 Formulation of Alternative Courses of Action
- 1.3 Formulation of Acquisition Strategy
- 1.4 Third-Party Service Requirements
- 1.5 Technological Feasibility Study
- 1.6 Economic Feasibility Study
- 1.7 Information Architecture
- 1.8 Risk Analysis Report
- 1.9 Cost-Effective Security Controls
- 1.10 Audit Trails Design
- 1.11 Ergonomics
- 1.12 Selection of System Software
- 1.13 Procurement Control
- 1.14 Software Product Acquisition
- 1.15 Third-Party Software Maintenance
- 1.16 Contract Application Programming
- 1.17 Acceptance of Facilities
- 1.18 Acceptance of Technology

2.0 Acquire and Maintain Application Software
- 2.1 Design Methods
- 2.2 Major Changes to Existing Systems
- 2.3 Design Approval
- 2.4 File Requirements Definition and Documentation
- 2.5 Programme Specifications
- 2.6 Source Data Collection Design

DOMAINS, PROCESSES AND CONTROL OBJECTIVES

- 2.7 Input Requirements Definition and Documentation
- 2.8 Definition of Interfaces
- 2.9 User-Machine Interface
- 2.10 Processing Requirements Definition and Documentation
- 2.11 Output Requirements Definition and Documentation
- 2.12 Controllability
- 2.13 Availability as a Key Design Factor
- 2.14 IT Integrity Provisions in Application Programme Software
- 2.15 Application Software Testing
- 2.16 User Reference and Support Materials
- 2.17 Reassessment of System Design

3.0 Acquire and Maintain Technology Infrastructure

- 3.1 Assessment of New Hardware and Software
- 3.2 Preventative Maintenance for Hardware
- 3.3 System Software Security
- 3.4 System Software Installation
- 3.5 System Software Maintenance
- 3.6 System Software Change Controls
- 3.7 Use and Monitoring of System Utilities

4.0 Develop and Maintain Procedures

- 4.1 Operational Requirements and Service Levels
- 4.2 User Procedures Manual
- 4.3 Operations Manual
- 4.4 Training Materials

5.0 Install and Accredit Systems

- 5.1 Training
- 5.2 Application Software Performance Sizing
- 5.3 Implementation Plan
- 5.4 System Conversion
- 5.5 Data Conversion
- 5.6 Testing Strategies and Plans
- 5.7 Testing of Changes
- 5.8 Parallel/Pilot Testing Criteria and Performance
- 5.9 Final Acceptance Test
- 5.10 Security Testing and Accreditation
- 5.11 Operational Test
- 5.12 Promotion to Production
- 5.13 Evaluation of Meeting User Requirements
- 5.14 Management's Post-Implementation Review

6.0 Manage Changes

- 6.1 Change Request Initiation and Control
- 6.2 Impact Assessment
- 6.3 Control of Changes
- 6.4 Emergency Changes
- 6.5 Documentation and Procedures
- 6.6 Authorised Maintenance
- 6.7 Software Release Policy
- 6.8 Distribution of Software

DELIVERY & SUPPORT

1.0 Define and Manage Service Levels

- 1.1 Service Level Agreement Framework
- 1.2 Aspects of Service Level Agreements
- 1.3 Performance Procedures
- 1.4 Monitoring and Reporting
- 1.5 Review of Service Level Agreements and Contracts
- 1.6 Chargeable Items
- 1.7 Service Improvement Programme

2.0 Manage Third-Party Services

- 2.1 Supplier Interfaces
- 2.2 Owner Relationships
- 2.3 Third-Party Contracts
- 2.4 Third-Party Qualifications
- 2.5 Outsourcing Contracts
- 2.6 Continuity of Services
- 2.7 Security Relationships
- 2.8 Monitoring

3.0 Manage Performance and Capacity

- 3.1 Availability and Performance Requirements
- 3.2 Availability Plan
- 3.3 Monitoring and Reporting
- 3.4 Modeling Tools
- 3.5 Proactive Performance Management
- 3.6 Workload Forecasting
- 3.7 Capacity Management of Resources

DOMAINS, PROCESSES AND CONTROL OBJECTIVES

DELIVERY & SUPPORT *continued*

- 3.8 Resources Availability
- 3.9 Resources Schedule

4.0 Ensure Continuous Service

- 4.1 IT Continuity Framework
- 4.2 IT Continuity Plan Strategy and Philosophy
- 4.3 IT Continuity Plan Contents
- 4.4 Minimising IT Continuity Requirements
- 4.5 Maintaining the IT Continuity Plan
- 4.6 Testing the IT Continuity Plan
- 4.7 IT Continuity Plan Training
- 4.8 IT Continuity Plan Distribution
- 4.9 User Department Alternative Processing Back-up Procedures
- 4.10 Critical IT Resources
- 4.11 Back-up Site and Hardware
- 4.12 Off-site Back-up Storage
- 4.13 Wrap-up Procedures

5.0 Ensure Systems Security

- 5.1 Manage Security Measures
- 5.2 Identification, Authentication and Access
- 5.3 Security of Online Access to Data
- 5.4 User Account Management
- 5.5 Management Review of User Accounts
- 5.6 User Control of User Accounts
- 5.7 Security Surveillance
- 5.8 Data Classification
- 5.9 Central Identification and Access Rights Management
- 5.10 Violation and Security Activity Reports
- 5.11 Incident Handling
- 5.12 Reaccreditation
- 5.13 Counterparty Trust
- 5.14 Transaction Authorisation
- 5.15 Non-Repudiation
- 5.16 Trusted Path
- 5.17 Protection of Security Functions
- 5.18 Cryptographic Key Management
- 5.19 Malicious Software Prevention, Detection and Correction
- 5.20 Firewall Architectures and Connections with Public Networks
- 5.21 Protection of Electronic Value

6.0 Identify and Allocate Costs

- 6.1 Chargeable Items
- 6.2 Costing Procedures
- 6.3 User Billing and Chargeback Procedures

7.0 Educate and Train Users

- 7.1 Identification of Training Needs
- 7.2 Training Organisation
- 7.3 Security Principles and Awareness Training

8.0 Assist and Advise Customers

- 8.1 Help Desk
- 8.2 Registration of Customer Queries
- 8.3 Customer Query Escalation
- 8.4 Monitoring of Clearance
- 8.5 Trend Analysis and Reporting

9.0 Manage the Configuration

- 9.1 Configuration Recording
- 9.2 Configuration Baseline
- 9.3 Status Accounting
- 9.4 Configuration Control
- 9.5 Unauthorised Software
- 9.6 Software Storage
- 9.7 Configuration Management Procedures
- 9.8 Software Accountability

10.0 Manage Problems and Incidents

- 10.1 Problem Management System
- 10.2 Problem Escalation
- 10.3 Problem Tracking and Audit Trail
- 10.4 Emergency and Temporary Access Authorisations
- 10.5 Emergency Processing Priorities

11.0 Manage Data

- 11.1 Data Preparation Procedures
- 11.2 Source Document Authorisation Procedures
- 11.3 Source Document Data Collection
- 11.4 Source Document Error Handling
- 11.5 Source Document Retention
- 11.6 Data Input Authorisation Procedures
- 11.7 Accuracy, Completeness and Authorisation Checks
- 11.8 Data Input Error Handling
- 11.9 Data Processing Integrity

DOMAINS, PROCESSES AND CONTROL OBJECTIVES

- 11.10 Data Processing Validation and Editing
- 11.11 Data Processing Error Handling
- 11.12 Output Handling and Retention
- 11.13 Output Distribution
- 11.14 Output Balancing and Reconciliation
- 11.15 Output Review and Error Handling
- 11.16 Security Provision for Output Reports
- 11.17 Protection of Sensitive Information During Transmission and Transport
- 11.18 Protection of Disposed Sensitive Information
- 11.19 Storage Management
- 11.20 Retention Periods and Storage Terms
- 11.21 Media Library Management System
- 11.22 Media Library Management Responsibilities
- 11.23 Back-up and Restoration
- 11.24 Back-up Jobs
- 11.25 Back-up Storage
- 11.26 Archiving
- 11.27 Protection of Sensitive Messages
- 11.28 Authentication and Integrity
- 11.29 Electronic Transaction Integrity
- 11.30 Continued Integrity of Stored Data

12.0 Manage Facilities

- 12.1 Physical Security
- 12.2 Low Profile of the IT Site
- 12.3 Visitor Escort
- 12.4 Personnel Health and Safety
- 12.5 Protection Against Environmental Factors
- 12.6 Uninterruptible Power Supply

13.0 Manage Operations

- 13.1 Processing Operations Procedures and Instructions Manual
- 13.2 Start-up Process and Other Operations Documentation
- 13.3 Job Scheduling
- 13.4 Departures from Standard Job Schedules
- 13.5 Processing Continuity
- 13.6 Operations Logs
- 13.7 Safeguard Special Forms and Output Devices
- 13.8 Remote Operations

MONITORING

1.0 Monitor the Processes

- 1.1 Collecting Monitoring Data
- 1.2 Assessing Performance
- 1.3 Assessing Customer Satisfaction
- 1.4 Management Reporting

2.0 Assess Internal Control Adequacy

- 2.1 Internal Control Monitoring
- 2.2 Timely Operation of Internal Controls
- 2.3 Internal Control Level Reporting
- 2.4 Operational Security and Internal Control Assurance

3.0 Obtain Independent Assurance

- 3.1 Independent Security and Internal Control Certification/Accreditation of IT Services
- 3.2 Independent Security and Internal Control Certification/Accreditation of Third-Party Service Providers
- 3.3 Independent Effectiveness Evaluation of IT Services
- 3.4 Independent Effectiveness Evaluation of Third-Party Service Providers
- 3.5 Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments
- 3.6 Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments by Third-Party Service Providers
- 3.7 Competence of Independent Assurance Function
- 3.8 Proactive Audit Involvement

4.0 Provide for Independent Audit

- 4.1 Audit Charter
- 4.2 Independence
- 4.3 Professional Ethics and Standards
- 4.4 Competence
- 4.5 Planning
- 4.6 Performance of Audit Work
- 4.7 Reporting
- 4.8 Follow-up Activities

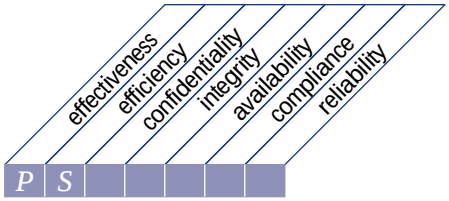
This page intentionally left blank

CONTROL OBJECTIVES

This page intentionally left blank

PLANNING & ORGANISATION

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

defining a strategic IT plan

that satisfies the business requirement

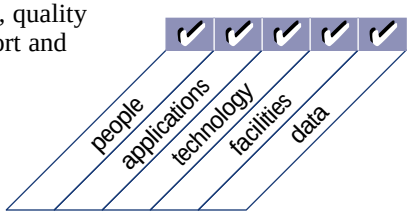
to strike an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment

is enabled by

a strategic planning process undertaken at regular intervals giving rise to long-term plans; the long-term plans should periodically be translated into operational plans setting clear and concrete short-term goals

and takes into consideration

- enterprise business strategy
- definition of how IT supports the business objectives
- inventory of technological solutions and current infrastructure
- monitoring the technology markets
- timely feasibility studies and reality checks
- existing systems assessments
- enterprise position on risk, time-to-market, quality
- need for senior management buy-in, support and critical review



DETAILED CONTROL OBJECTIVES

1 DEFINE A STRATEGIC INFORMATION TECHNOLOGY PLAN

1.1 IT as Part of the Organisation's Long- and Short-Range Plan

CONTROL OBJECTIVE

Senior management is responsible for developing and implementing long- and short-range plans that fulfill the organisation's mission and goals. In this respect, senior management should ensure that IT issues as well as opportunities are adequately assessed and reflected in the organisation's long- and short-range plans. IT long- and short-range plans should be developed to help ensure that the use of IT is aligned with the mission and business strategies of the organisation.

1.2 IT Long-Range Plan

CONTROL OBJECTIVE

IT management and business process owners are responsible for regularly developing IT long-range plans supporting the achievement of the organisation's overall missions and goals. The planning approach should include mechanisms to solicit input from relevant internal and external stakeholders impacted by the IT strategic plans. Accordingly, management should implement a long-range planning process, adopt a structured approach and set up a standard plan structure.

1.3 IT Long-Range Planning — Approach and Structure

CONTROL OBJECTIVE

IT management and business process owners should establish and apply a structured approach regarding the long-range planning process. This should result in a high-quality plan which covers the basic questions of what, who, how, when and why. The IT planning process should take into account risk assessment results, including business, environmental, technology and human resources risks. Aspects which need to be taken into account and adequately addressed during the planning process include the organisational model and changes to it, geographical distribution, technological evolution, costs, legal and regulatory requirements, requirements of third parties or the market, planning horizon, business process re-engineering, staffing, in- or out-sourcing, data, application systems and technology architectures. Benefits of the choices made should be clearly identified. The IT long- and short-range plans should incorporate performance indicators and targets. The plan itself should also refer to other plans such as the organisation quality plan and the information risk management plan.

1.4 IT Long-Range Plan Changes

CONTROL OBJECTIVE

IT management and business process owners should ensure a process is in place to modify the IT long-range plan in a timely and accurate manner to accommodate changes to the organisation's long-range plan and changes in IT conditions. Management should establish a policy requiring that IT long- and short-range plans are developed and maintained.

1.5 Short-Range Planning for the IT Function

CONTROL OBJECTIVE

IT management and business process owners should ensure that the IT long-range plan is regularly translated into IT short-range plans. Such short-range plans should ensure that appropriate IT function resources are allocated on a basis consistent with the IT long-range plan. The short-range plans should be reassessed periodically and amended as necessary in response to changing business and IT conditions. The timely performance of feasibility studies should ensure that the execution of the short-range plans is adequately initiated.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

1.6 **Communication of IT Plans**

CONTROL OBJECTIVE

Management should ensure that IT long- and short-range plans are communicated to business process owners and other relevant parties across the organisation.

1.7 **Monitoring and Evaluating of IT Plans**

CONTROL OBJECTIVE

Management should establish processes to capture and report feedback from business process owners and users regarding the quality and usefulness of long- and short-range plans. The feedback obtained should be evaluated and considered in future IT planning.

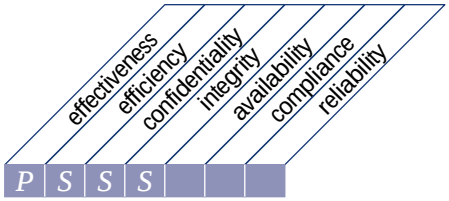
1.8 **Assessment of Existing Systems**

CONTROL OBJECTIVE

Prior to developing or changing the strategic, or long-range, IT plan, IT management should assess the existing information systems in terms of degree of business automation, functionality, stability, complexity, costs, strengths and weaknesses in order to determine the degree to which the existing systems support the organisation's business requirements.

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

defining the information architecture

that satisfies the business requirement

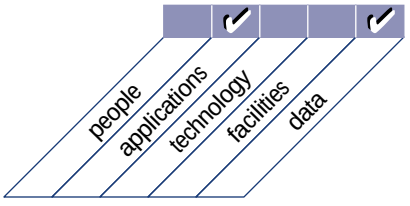
of optimising the organisation of the information systems

is enabled by

creating and maintaining a business information model and ensuring appropriate systems are defined to optimise the use of this information

and takes into consideration

- automated data repository and dictionary
- data syntax rules
- data ownership and criticality/security classification
- an information model representing the business
- enterprise information architectural standards



DETAILED CONTROL OBJECTIVES

2 DEFINE THE INFORMATION ARCHITECTURE

2.1 Information Architecture Model

CONTROL OBJECTIVE

Information should be kept consistent with needs and should be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities effectively and on a timely basis. Accordingly, the IT function should create and regularly update an information architecture model, encompassing the corporate data model and the associated information systems. The information architecture model should be kept consistent with the IT long-range plan.

2.2 Corporate Data Dictionary and Data Syntax Rules

CONTROL OBJECTIVE

The IT function should ensure the creation and continuous updating of a corporate data dictionary which incorporates the organisation's data syntax rules.

2.3 Data Classification Scheme

CONTROL OBJECTIVE

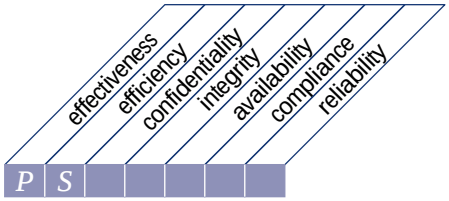
A general classification framework should be established with regard to placement of data in information classes (i.e., security categories) as well as allocation of ownership. The access rules for the classes should be appropriately defined.

2.4 Security Levels

CONTROL OBJECTIVE

Management should define, implement and maintain security levels for each of the data classifications identified above the level of "no protection required." These security levels should represent the appropriate (minimum) set of security and control measures for each of the classifications and should be re-evaluated periodically and modified accordingly. Criteria for supporting different levels of security in the extended enterprise should be established to address the needs of evolving e-commerce, mobile computing and telecommuting environments.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

determining technological direction

that satisfies the business requirement

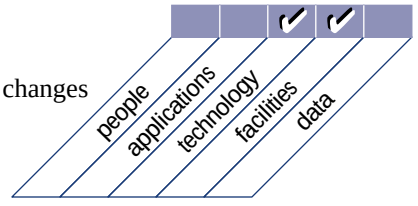
to take advantage of available and emerging technology to drive and make possible the business strategy

is enabled by

creation and maintenance of a technological infrastructure plan that sets and manages clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms

and takes into consideration

- capability of current infrastructure
- monitoring technology developments via reliable sources
- conducting proof-of-concepts
- risk, constraints and opportunities
- acquisition plans
- migration strategy and roadmaps
- vendor relationships
- independent technology reassessment
- hardware and software price/performance changes



DETAILED CONTROL OBJECTIVES

3 DETERMINE TECHNOLOGICAL DIRECTION

3.1 Technological Infrastructure Planning

CONTROL OBJECTIVE

The IT function should create and regularly update a technological infrastructure plan which is in accordance with the IT long- and short-range plans. Such a plan should encompass aspects such as systems architecture, technological direction and migration strategies.

3.2 Monitor Future Trends and Regulations

CONTROL OBJECTIVE

Continuous monitoring of future trends and regulatory conditions should be ensured by the IT function so that these factors can be taken into consideration during the development and maintenance of the technological infrastructure plan.

3.3 Technological Infrastructure Contingency

CONTROL OBJECTIVE

The technological infrastructure plan should be assessed systematically for contingency aspects (i.e., redundancy, resilience, adequacy and evolutionary capability of the infrastructure).

3.4 Hardware and Software Acquisition Plans

CONTROL OBJECTIVE

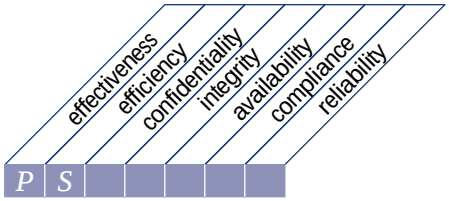
IT management should ensure that hardware and software acquisition plans are established and reflect the needs identified in the technological infrastructure plan.

3.5 Technology Standards

CONTROL OBJECTIVE

Based on the technological infrastructure plan, IT management should define technology norms in order to foster standardisation.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

defining the IT organisation and relationships

that satisfies the business requirement

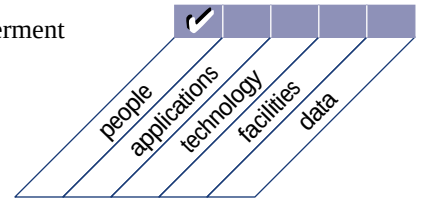
to deliver the right IT services

is enabled by

an organisation suitable in numbers and skills with roles and responsibilities defined and communicated, aligned with the business and that facilitates the strategy and provides for effective direction and adequate control

and takes into consideration

- board level responsibility for IT
- management's direction and supervision of IT
- IT's alignment with the business
- IT's involvement in key decision processes
- organisational flexibility
- clear roles and responsibilities
- balance between supervision and empowerment
- job descriptions
- staffing levels and key personnel
- organisational positioning of security, quality and internal control functions
- segregation of duties



DETAILED CONTROL OBJECTIVES

4 DEFINE THE INFORMATION TECHNOLOGY ORGANISATION AND RELATIONSHIPS

4.1 IT Planning or Steering Committee

CONTROL OBJECTIVE

The organisation's senior management should appoint a planning or steering committee to oversee the IT function and its activities. Committee membership should include representatives from senior management, user management and the IT function. The committee should meet regularly and report to senior management.

4.2 Organisational Placement of the IT Function

CONTROL OBJECTIVE

In placing the IT function in the overall organisation structure, senior management should ensure authority, critical mass and independence from user departments to the degree necessary to guarantee effective IT solutions and sufficient progress in implementing them, and to establish a partnership relation with top management to help increase awareness, understanding and skill in identifying and resolving IT issues.

4.3 Review of Organisational Achievements

CONTROL OBJECTIVE

A framework should be in place for reviewing the organisational structure to continuously meet objectives and changing circumstances.

4.4 Roles and Responsibilities

CONTROL OBJECTIVE

Management should ensure that all personnel in the organisation have and know their roles and responsibilities in relation to information systems. All personnel should have sufficient authority to exercise the role and responsibility assigned to them. Roles should be designed with consideration to appropriate segregation of duties. No one individual should control all key aspects of a transaction or event. Everyone should be made aware that they have some degree of responsibility for internal control and security. Consequently, regular campaigns should be organised and undertaken to increase awareness and discipline.

4.5 Responsibility for Quality Assurance

CONTROL OBJECTIVE

Management should assign the responsibility for the performance of the quality assurance function to staff members of the IT function and ensure that appropriate quality assurance, systems, controls and communications expertise exist in the IT function's quality assurance group. The organisational placement within the IT function and the responsibilities and the size of the quality assurance group should satisfy the requirements of the organisation.

4.6 Responsibility for Logical and Physical Security

CONTROL OBJECTIVE

Management should formally assign the responsibility for assuring both the logical and physical security of the organisation's information assets to an information security manager, reporting to the organisation's senior management. At a minimum, security management responsibility should be established at the organisation-wide level to deal with overall security issues in an organisation. If needed, additional security management responsibilities should be assigned at a system-specific level to cope with the related security issues.

4.7 Ownership and Custodianship

CONTROL OBJECTIVE

Management should create a structure for formally appointing the data owners and custodians. Their roles and responsibilities should be clearly defined.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

4.8 **Data and System Ownership**
CONTROL OBJECTIVE
Management should ensure that all information assets (data and systems) have an appointed owner who makes decisions about classification and access rights. System owners typically delegate day-to-day custodianship to the systems delivery/operations group and delegate security responsibilities to a security administrator. Owners, however, remain accountable for the maintenance of appropriate security measures.

4.9 **Supervision**
CONTROL OBJECTIVE
Senior management should implement adequate supervisory practices in the IT function to ensure that roles and responsibilities are properly exercised, to assess whether all personnel have sufficient authority and resources to execute their roles and responsibilities, and to generally review key performance indicators.

4.10 **Segregation of Duties**
CONTROL OBJECTIVE
Senior management should implement a division of roles and responsibilities which should exclude the possibility for a single individual to subvert a critical process. Management should also make sure that personnel are performing only those duties stipulated for their respective jobs and positions. In particular, a segregation of duties should be maintained between the following functions:
- information systems use
- data entry
- computer operation
- network management
- system administration
- systems development and maintenance
- change management
- security administration
- security audit

4.11 **IT Staffing**
CONTROL OBJECTIVE
Staffing requirements evaluations should be performed regularly to ensure the IT function has a sufficient number of competent IT staff. Staffing requirements should be evaluated at least annually or upon major changes to the business, operational or IT environment. Evaluation results should be acted upon promptly to ensure adequate staffing now and in the future.

4.12 **Job or Position Descriptions for IT Staff**
CONTROL OBJECTIVE
Management should ensure that position descriptions for IT staff are established and updated regularly. These position descriptions should clearly delineate both authority and responsibility, include definitions of skills and experience needed in the relevant position, and be suitable for use in performance evaluation.

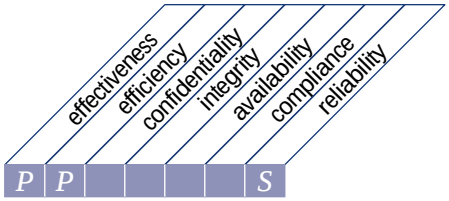
4.13 **Key IT Personnel**
CONTROL OBJECTIVE
IT management should define and identify key IT personnel.

4.14 **Contracted Staff Policies and Procedures**
CONTROL OBJECTIVE
Management should define and implement relevant policies and procedures for controlling the activities of consultants and other contract personnel by the IT function to assure the protection of the organisation's information assets.

4.15 **Relationships**
CONTROL OBJECTIVE
IT management should undertake the necessary actions to establish and maintain an optimal coordination, communication and liaison structure between the IT function and various other interests inside and outside the IT function (i.e., users, suppliers, security officers, risk managers).

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing the IT investment

that satisfies the business requirement

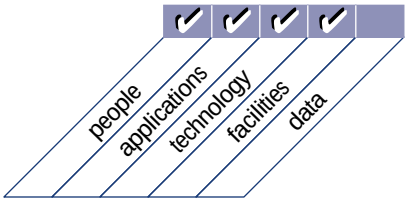
to ensure funding and to control disbursement of financial resources

is enabled by

a periodic investment and operational budget established and approved by the business

and takes into consideration

- funding alternatives
- clear budget ownership
- control of actual spending
- cost justification and awareness of total cost of ownership
- benefit justification and accountability for benefit fulfillment
- technology and application software life cycles
- alignment with enterprise business strategy
- impact assessment
- asset management



DETAILED CONTROL OBJECTIVES

5 MANAGE THE INFORMATION TECHNOLOGY INVESTMENT

5.1 Annual IT Operating Budget

CONTROL OBJECTIVE

Senior management should implement a budgeting process to ensure that an annual IT operating budget is established and approved in line with the organisation's long- and short-range plans as well as with the IT long- and short-range plans. Funding alternatives should be investigated.

5.2 Cost and Benefit Monitoring

CONTROL OBJECTIVE

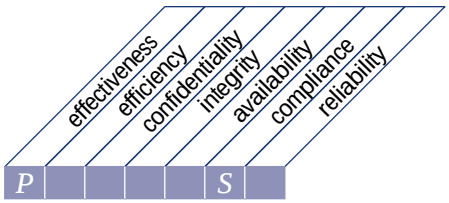
Management should establish a cost monitoring process comparing actuals to budgets. Moreover, the possible benefits derived from the IT activities should be determined and reported. For cost monitoring, the source of the actual figures should be based upon the organisation's accounting system and that system should routinely record, process and report the costs associated with the activities of the IT function. For benefit monitoring, high-level performance indicators should be defined, regularly reported and reviewed for adequacy.

5.3 Cost and Benefit Justification

CONTROL OBJECTIVE

A management control should be in place to guarantee that the delivery of services by the IT function is cost justified and in line with the industry. The benefits derived from IT activities should similarly be analysed.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

communicating management aims and direction

that satisfies the business requirement

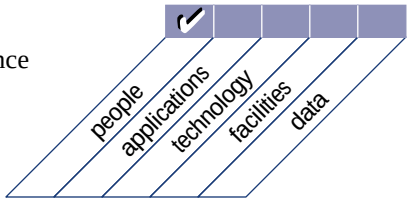
to ensure user awareness and understanding of those aims

is enabled by

policies established and communicated to the user community; furthermore, standards need to be established to translate the strategic options into practical and usable user rules

and takes into consideration

- clearly articulated mission
- technology directives linked to business aims
- code of conduct/ethics
- quality commitment
- security and internal control policies
- security and internal control practices
- lead-by-example
- continuous communications programme
- providing guidance and checking compliance



DETAILED CONTROL OBJECTIVES

6 COMMUNICATE MANAGEMENT AIMS AND DIRECTION

6.1 Positive Information Control Environment

CONTROL OBJECTIVE

In order to provide guidance for proper behaviour, remove temptation for unethical behaviour and provide discipline, where appropriate, management should create a framework and an awareness programme fostering a positive control environment throughout the entire organisation. This should address the integrity, ethical values and competence of the people, management philosophy, operating style and accountability. Specific attention is to be given to IT aspects, including security and business continuity planning.

6.2 Management's Responsibility for Policies

CONTROL OBJECTIVE

Management should assume full responsibility for formulating, developing, documenting, promulgating and controlling policies covering general aims and directives. Regular reviews of policies for appropriateness should be carried out. The complexity of the written policies and procedures should always be commensurate with the organisation size and management style.

6.3 Communication of Organisation Policies

CONTROL OBJECTIVE

Management should ensure that organisational policies are clearly communicated, understood and accepted by all levels in the organisation. The communication process should be supported by an effective plan that uses a diversified set of communication means.

6.4 Policy Implementation Resources

CONTROL OBJECTIVE

Management should plan for appropriate resources for policy implementation and for ensuring compliance, so that they are built into and are an integral part of operations. Management should also monitor the timeliness of the policy implementation.

6.5 Maintenance of Policies

CONTROL OBJECTIVE

Policies should be adjusted regularly to accommodate changing conditions. Policies should be re-evaluated, at least annually or upon significant changes to the operating or business environment, to assess their adequacy and appropriateness, and amended as necessary. Management should provide a framework and process for the periodic review and approval of standards, policies, directives and procedures.

6.6 Compliance with Policies, Procedures and Standards

CONTROL OBJECTIVE

Management should ensure that appropriate procedures are in place to determine whether personnel understand the implemented policies and procedures, and that the polices and procedures are being followed. Compliance procedures for ethical, security and internal control standards should be set by top management and promoted by example.

6.7 Quality Commitment

CONTROL OBJECTIVE

IT management should define, document and maintain a quality philosophy, policies and objectives which are consistent with the corporate philosophies and policies in this regard. The quality philosophy, policies and objectives should be understood, implemented and maintained at all levels of the IT function.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

6.8 **Security and Internal Control Framework Policy**
CONTROL OBJECTIVE
Management should assume full responsibility for developing and maintaining a framework policy which establishes the organisation's overall approach to security and internal control to establish and improve the protection of IT resources and integrity of IT systems. The policy should comply with overall business objectives and be aimed at minimisation of risks through preventive measures, timely identification of irregularities, limitation of losses and timely restoration. Measures should be based on cost/benefit analyses and should be prioritised. In addition, management should ensure that this high-level security and internal control policy specifies the purpose and objectives, the management structure, the scope within the organisation, the definition and assignment of responsibilities for implementation at all levels, and the definition of penalties and disciplinary actions associated with failing to comply with security and internal control policies. Criteria for periodic re-evaluation of the framework should be defined to support responsiveness to changing organisational, environmental and technical requirements.

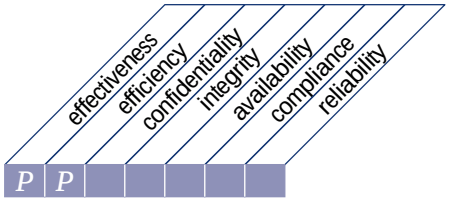
6.9 **Intellectual Property Rights**
CONTROL OBJECTIVE
Management should provide and implement a written policy on intellectual property rights covering in-house as well as contract-developed software.

6.10 **Issue-Specific Policies**
CONTROL OBJECTIVE
Measures should be put in place to ensure that issue-specific policies are established to document management decisions in addressing particular activities, applications, systems or technologies.

6.11 **Communication of IT Security Awareness**
CONTROL OBJECTIVE
An IT security awareness programme should communicate the IT security policy to each IT user and assure a complete understanding of the importance of IT security. It should convey the message that IT security is to the benefit of the organisation, all its employees, and that everybody is responsible for it. The IT security awareness programme should be supported by, and represent, the view of management.

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing human resources

that satisfies the business requirement

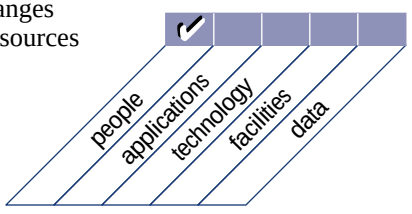
to acquire and maintain a motivated and competent workforce and maximise personnel contributions to the IT processes

is enabled by

sound, fair and transparent personnel management practices to recruit, line, vet, compensate, train, appraise, promote and dismiss

and takes into consideration

- recruitment and promotion
- training and qualification requirements
- awareness building
- cross-training and job rotation
- hiring, vetting and dismissal procedures
- objective and measurable performance evaluation
- responsiveness to technical and market changes
- properly balancing internal and external resources
- succession plan for key positions



DETAILED CONTROL OBJECTIVES

7 MANAGE HUMAN RESOURCES

7.1 Personnel Recruitment and Promotion

CONTROL OBJECTIVE

Management should implement and regularly assess the needed processes to ensure that personnel recruiting and promotion practices are based on objective criteria and consider education, experience and responsibility. These processes should be in line with the overall organisation's policies and procedures in this regard, such as hiring, orienting, training, evaluating, counselling, promoting, compensating and disciplining. Management should ensure that knowledge and skill needs are continually assessed and that the organisation is able to obtain a workforce that has the skills which match those necessary to achieve organisational goals.

7.2 Personnel Qualifications

CONTROL OBJECTIVE

IT management should regularly verify that personnel performing specific tasks are qualified on the basis of appropriate education, training and/or experience, as required. Management should encourage personnel to obtain membership in professional organisations.

7.3 Roles and Responsibilities

CONTROL OBJECTIVE

Management should clearly define roles and responsibilities for personnel, including the requirement to adhere to management policies and procedures, the code of ethics and professional practices. The terms and conditions of employment should stress the employee's responsibility for information security and internal control.

7.4 Personnel Training

CONTROL OBJECTIVE

Management should ensure that employees are provided with orientation upon hiring and with on-going training to maintain their knowledge, skills, abilities and security awareness to the level required to perform effectively. Education and training programmes conducted to effectively raise the technical and management skill levels of personnel should be reviewed regularly.

7.5 Cross-Training or Staff Back-up

CONTROL OBJECTIVE

Management should provide for sufficient cross-training or back-up of identified key personnel to address unavailabilities. Management should establish succession plans for all key functions and positions. Personnel in sensitive positions should be required to take uninterrupted holidays of sufficient length to exercise the organisation's ability to cope with unavailabilities and to prevent and detect fraudulent activity.

7.6 Personnel Clearance Procedures

CONTROL OBJECTIVE

IT management should ensure that their personnel are subjected to security clearance before they are hired, transferred or promoted, depending on the sensitivity of the position. An employee who was not subjected to such a clearance when first hired, should not be placed in a sensitive position until a security clearance has been obtained.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

7.7 **Employee Job Performance Evaluation**

CONTROL OBJECTIVE

Management should implement an employee performance evaluation process, reinforced by an effective reward system, that is designed to help employees understand the connection between their performance and the organisation's success. Evaluation should be performed against established standards and specific job responsibilities on a regular basis. Employees should receive counselling on performance or conduct whenever appropriate.

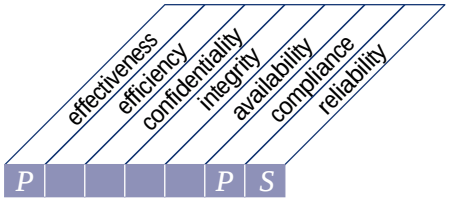
7.8 **Job Change and Termination**

CONTROL OBJECTIVE

Management should ensure that appropriate and timely actions are taken regarding job changes and job terminations so that internal controls and security are not impaired by such occurrences.

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

ensuring compliance with external requirements

that satisfies the business requirement

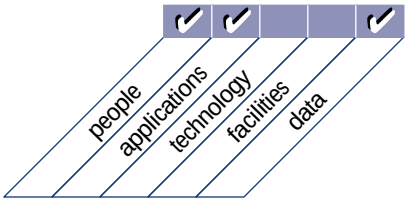
to meet legal, regulatory and contractual obligations

is enabled by

identifying and analysing external requirements for their IT impact, and taking appropriate measures to comply with them

and takes into consideration

- laws, regulations and contracts
- monitoring legal and regulatory developments
- regular monitoring for compliance
- safety and ergonomics
- privacy
- intellectual property



DETAILED CONTROL OBJECTIVES

8 ENSURE COMPLIANCE WITH EXTERNAL REQUIREMENTS

8.1 External Requirements Review

CONTROL OBJECTIVE

The organisation should establish and maintain procedures for external requirements review and for the coordination of these activities. Continuous research should determine the applicable external requirements for the organisation. Legal, government or other external requirements related to IT practices and controls should be reviewed. Management should also assess the impact of any external relationships on the organisation's overall information needs, including determination of the extent to which IT strategies need to conform with or support the requirements of any related third-parties.

8.2 Practices and Procedures for Complying with External Requirements

CONTROL OBJECTIVE

Organisational practices should ensure that appropriate corrective actions are taken on a timely basis to guarantee compliance with external requirements. In addition, adequate procedures assuring continuous compliance should be established and maintained. In this regard, management should seek legal advice if required.

8.3 Safety and Ergonomic Compliance

CONTROL OBJECTIVE

Management should ensure compliance with safety and ergonomic standards in the working environment of IT users and personnel.

8.4 Privacy, Intellectual Property and Data Flow

CONTROL OBJECTIVE

Management should ensure compliance with privacy, intellectual property, transborder data flow and cryptographic regulations applicable to the IT practices of the organisation.

8.5 Electronic Commerce

CONTROL OBJECTIVE

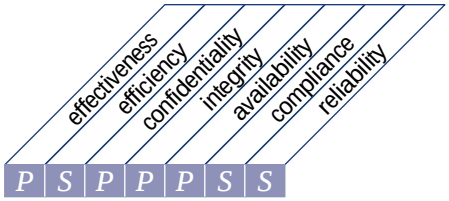
Management should ensure that formal contracts are in place establishing agreement between trading partners on communication processes and on standards for transaction message security and data storage. When trading on the Internet, management should enforce adequate controls to ensure compliance with local laws and customs on a world-wide basis.

8.6 Compliance with Insurance Contracts

CONTROL OBJECTIVE

Management should ensure that insurance contract requirements are properly identified and continuously met.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

assessing risks

that satisfies the business requirement

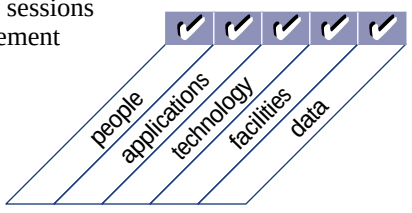
of supporting management decisions through achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors

is enabled by

the organisation engaging itself in IT risk-identification and impact analysis, involving multi-disciplinary functions and taking cost-effective measures to mitigate risks

and takes into consideration

- risk management ownership and accountability
- different kinds of IT risks (technology, security, continuity, regulatory, etc.)
- defined and communicated risk tolerance profile
- root cause analyses and risk brainstorming sessions
- quantitative and/or qualitative risk measurement
- risk assessment methodology
- risk action plan
- timely reassessment



DETAILED CONTROL OBJECTIVES

9 ASSESS RISKS

9.1 Business Risk Assessment

CONTROL OBJECTIVE

Management should establish a systematic risk assessment framework. Such a framework should incorporate a regular assessment of the relevant information risks to the achievement of the business objectives, forming a basis for determining how the risks should be managed to an acceptable level. The process should provide for risk assessments at both the global level and system specific level, for new projects as well as on a recurring basis, and with cross-disciplinary participation. Management should ensure that reassessments occur and that risk assessment information is updated with results of audits, inspections and identified incidents.

9.2 Risk Assessment Approach

CONTROL OBJECTIVE

Management should establish a general risk assessment approach which defines the scope and boundaries, the methodology to be adopted for risk assessments, the responsibilities and the required skills. Management should lead the identification of the risk mitigation solution and be involved in identifying vulnerabilities. Security specialists should lead threat identification and IT specialists should drive the control selection. The quality of the risk assessments should be ensured by a structured method and skilled risk assessors.

9.3 Risk Identification

CONTROL OBJECTIVE

The risk assessment approach should focus on the examination of the essential elements of risk and the cause/effect relationship between them. The essential elements of risk include tangible and intangible assets, asset value, threats, vulnerabilities, safeguards, consequences and likelihood of threat. The risk identification process should include qualitative and, where appropriate, quantitative risk ranking and should obtain input from management brainstorming, strategic planning, past audits and other assessments. The risk assessment should consider business, regulatory, legal, technology, trading partner and human resources risks.

9.4 Risk Measurement

CONTROL OBJECTIVE

The risk assessment approach should ensure that the analysis of risk identification information results in a quantitative and/or qualitative measurement of risk to which the examined area is exposed. The risk acceptance capacity of the organisation should also be assessed.

9.5 Risk Action Plan

CONTROL OBJECTIVE

The risk assessment approach should provide for the definition of a risk action plan to ensure that cost-effective controls and security measures mitigate exposure to risks on a continuing basis. The risk action plan should identify the risk strategy in terms of risk avoidance, mitigation or acceptance.

9.6 Risk Acceptance

CONTROL OBJECTIVE

The risk assessment approach should ensure the formal acceptance of the residual risk, depending on risk identification and measurement, organisational policy, uncertainty incorporated in the risk assessment approach itself and the cost effectiveness of implementing safeguards and controls. The residual risk should be offset with adequate insurance coverage, contractually negotiated liabilities and self-insurance.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

9.7 **Safeguard Selection**

CONTROL OBJECTIVE

While aiming for a reasonable, appropriate and proportional system of controls and safeguards, controls with the highest return on investment (ROI) and those that provide quick wins should receive first priority. The control system also needs to balance prevention, detection, correction and recovery measures. Furthermore, management needs to communicate the purpose of the control measures, manage conflicting measures and monitor the continuing effectiveness of all control measures.

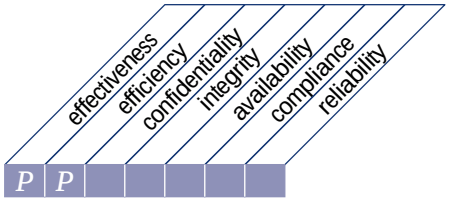
9.8 **Risk Assessment Commitment**

CONTROL OBJECTIVE

Management should encourage risk assessment as an important tool in providing information in the design and implementation of internal controls, in the definition of the IT strategic plan and in the monitoring and evaluation mechanisms.

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing projects

that satisfies the business requirement

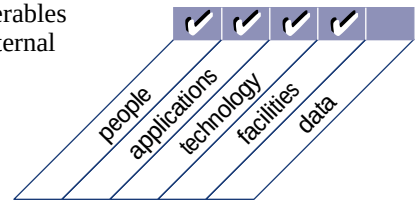
to set priorities and to deliver on time and within budget

is enabled by

the organisation identifying and prioritising projects in line with the operational plan and the adoption and application of sound project management techniques for each project undertaken

and takes into consideration

- business management sponsorship for projects
- program management
- project management capabilities
- user involvement
- task breakdown, milestone definition and phase approvals
- allocation of responsibilities
- rigorous tracking of milestones and deliverables
- cost and manpower budgets, balancing internal and external resources
- quality assurance plans and methods
- program and project risk assessments
- transition from development to operations



DETAILED CONTROL OBJECTIVES

10 MANAGE PROJECTS

10.1 Project Management Framework

CONTROL OBJECTIVE

Management should establish a general project management framework which defines the scope and boundaries of managing projects, as well as the project management methodology to be adopted and applied to each project undertaken. The methodology should cover, at a minimum, the allocation of responsibilities, task breakdown, budgeting of time and resources, milestones, check points and approvals.

10.2 User Department Participation in Project Initiation

CONTROL OBJECTIVE

The organisation's project management framework should provide for participation by the affected user department management in the definition and authorisation of a development, implementation or modification project.

10.3 Project Team Membership and Responsibilities

CONTROL OBJECTIVE

The organisation's project management framework should specify the basis for assigning staff members to the project and define the responsibilities and authorities of the project team members.

10.4 Project Definition

CONTROL OBJECTIVE

The organisation's project management framework should provide for the creation of a clear written statement defining the nature and scope of every implementation project before work on the project begins.

10.5 Project Approval

CONTROL OBJECTIVE

The organisation's project management framework should ensure that for each proposed project, the organisation's senior management reviews the reports of the relevant feasibility studies as a basis for its decision on whether to proceed with the project.

10.6 Project Phase Approval

CONTROL OBJECTIVE

The organisation's project management framework should provide for designated managers of the user and IT functions to approve the work accomplished in each phase of the cycle before work on the next phase begins.

10.7 Project Master Plan

CONTROL OBJECTIVE

Management should ensure that for each approved project a project master plan is created which is adequate for maintaining control over the project throughout its life and which includes a method of monitoring the time and costs incurred throughout the life of the project. The content of the project plan should include statements of scope, objectives, required resources and responsibilities and should provide information to permit management to measure progress.

10.8 System Quality Assurance Plan

CONTROL OBJECTIVE

Management should ensure that the implementation of a new or modified system includes the preparation of a quality plan which is then integrated with the project master plan and formally reviewed and agreed to by all parties concerned.

10.9 Planning of Assurance Methods

CONTROL OBJECTIVE

Assurance tasks are to be identified during the planning phase of the project management

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

framework. Assurance tasks should support the accreditation of new or modified systems and should assure that internal controls and security features meet the related requirements.

10.10 **Formal Project Risk Management**

CONTROL OBJECTIVE

Management should implement a formal project risk management programme for eliminating or minimising risks associated with individual projects (i.e., identifying and controlling the areas or events that have the potential to cause unwanted change).

10.11 **Test Plan**

CONTROL OBJECTIVE

The organisation's project management framework should require that a test plan be created for every development, implementation and modification project.

10.12 **Training Plan**

CONTROL OBJECTIVE

The organisation's project management framework should require that a training plan be created for every development, implementation and modification project.

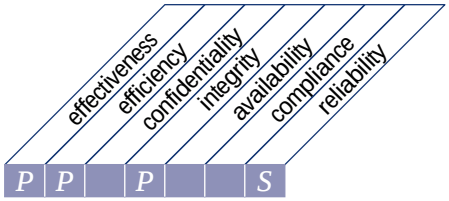
10.13 **Post-Implementation Review Plan**

CONTROL OBJECTIVE

The organisation's project management framework should provide, as an integral part of the project team's activities, for the development of a plan for a post-implementation review of every new or modified information system to ascertain whether the project has delivered the planned benefits.

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing quality

that satisfies the business requirement

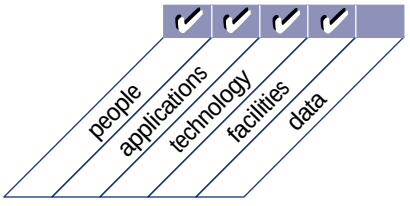
to meet the IT customer requirements

is enabled by

the planning, implementing and maintaining of quality management standards and systems providing for distinct development phases, clear deliverables and explicit responsibilities

and takes into consideration

- establishment of a quality culture
- quality plans
- quality assurance responsibilities
- quality control practices
- system development life cycle methodology
- programme and system testing and documentation
- quality assurance reviews and reporting
- training and involvement of end user and quality assurance personnel
- development of a quality assurance knowledge base
- benchmarking against industry norms



DETAILED CONTROL OBJECTIVE

11 MANAGE QUALITY

11.1 General Quality Plan

CONTROL OBJECTIVE

Management should develop and regularly maintain an overall quality plan based on the organisational and IT long-range plans. The plan should promote the continuous improvement philosophy and answer the basic questions of what, who and how.

11.2 Quality Assurance Approach

CONTROL OBJECTIVE

Management should establish a standard approach regarding quality assurance which covers both general and project specific quality assurance activities. The approach should prescribe the type(s) of quality assurance activities (such as reviews, audits, inspections, etc.) to be performed to achieve the objectives of the general quality plan. It should also require specific quality assurance reviews.

11.3 Quality Assurance Planning

CONTROL OBJECTIVE

Management should implement a quality assurance planning process to determine the scope and timing of the quality assurance activities.

11.4 Quality Assurance Review of Adherence to IT Standards and Procedures

CONTROL OBJECTIVE

Management should ensure that the responsibilities assigned to the quality assurance personnel include a review of general adherence to IT standards and procedures.

11.5 System Development Life Cycle Methodology

CONTROL OBJECTIVE

The organisation's management should define and implement IT standards and adopt a system development life cycle methodology governing the process of developing, acquiring, implementing and maintaining computerised information systems and related technology. The chosen system development life cycle methodology should be appropriate for the systems to be developed, acquired, implemented and maintained.

11.6 System Development Life Cycle Methodology for Major Changes to Existing Technology

CONTROL OBJECTIVE

In the event of major changes to existing technology, management should ensure that a system development life cycle methodology is observed, as in the case of the acquisition or development of new technology.

11.7 Updating of the System Development Life Cycle Methodology

CONTROL OBJECTIVE

Management should implement a periodic review of its system development life cycle methodology to ensure that its provisions reflect current generally accepted techniques and procedures.

11.8 Coordination and Communication

CONTROL OBJECTIVE

Management should establish a process for ensuring close coordination and communication between customers of the IT function and system implementors. This process should entail structured methods using the system development life cycle methodology to ensure the provision of quality IT solutions which meet the business demands. Management should promote an organisation which is characterised by close cooperation and communication throughout the system development life cycle.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

11.9 **Acquisition and Maintenance Framework for the Technology Infrastructure**
CONTROL OBJECTIVE
A general framework should be in place regarding the acquisition and maintenance of the technology infrastructure. The different steps to be followed regarding the technology infrastructure (such as acquiring; programming, documenting, and testing; parameter setting; maintaining and applying fixes) should be governed by, and in line with, the acquisition and maintenance framework for the technology infrastructure.

11.10 **Third-Party Implementor Relationships**
CONTROL OBJECTIVE
Management should implement a process to ensure good working relationships with third-party implementors. Such a process should provide that the user and implementor agree to acceptance criteria, handling of changes, problems during development, user roles, facilities, tools, software, standards and procedures.

11.11 **Programme Documentation Standards**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should incorporate standards for programme documentation which have been communicated to the concerned staff and enforced. The methodology should ensure that the documentation created during information system development or modification projects conforms to these standards.

11.12 **Programme Testing Standards**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should provide standards covering test requirements, verification, documentation and retention for testing individual software units and aggregated programmes created as part of every information system development or modification project.

11.13 **System Testing Standards**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should provide standards covering test requirements, verification, documentation, and retention for the testing of the total system as a part of every information system development or modification project.

11.14 **Parallel/Pilot Testing**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should define the circumstances under which parallel or pilot testing of new and/or existing systems will be conducted.

11.15 **System Testing Documentation**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should provide, as part of every information system development, implementation, or modification project, that the documented results of testing the system are retained.

11.16 **Quality Assurance Evaluation of Adherence to Development Standards**

CONTROL OBJECTIVE

The organisation's quality assurance approach should require that a post-implementation review of an operational information system assess whether the project team adhered to the provisions of the system development life cycle methodology.

11.17 **Quality Assurance Review of the Achievement of IT Objectives**

CONTROL OBJECTIVE

The quality assurance approach should include a review of the extent to which particular systems and application development activities have achieved the objectives of the information services function.

11.18 **Quality Metrics**

CONTROL OBJECTIVE

Management should define and use metrics to measure the results of activities, thus assessing whether quality goals have been achieved.

11.19 **Reports of Quality Assurance Reviews**

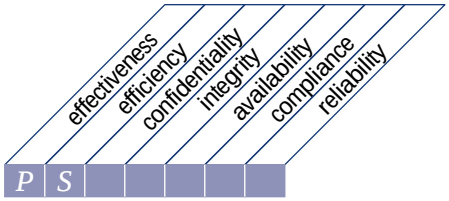
CONTROL OBJECTIVE

Reports of quality assurance reviews should be prepared and submitted to management of user departments and the IT function.

This page intentionally left blank

ACQUISITION & IMPLEMENTATION

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

identifying automated solutions

that satisfies the business requirement

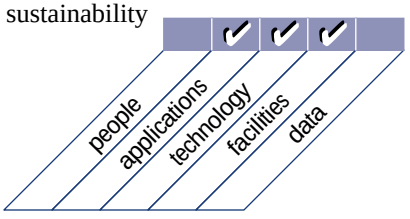
of ensuring an effective and efficient approach to satisfy the user requirements

is enabled by

an objective and clear identification and analysis of the alternative opportunities measured against user requirements

and takes into consideration

- knowledge of solutions available in the market
- acquisition and implementation methodologies
- user involvement and buy in
- alignment with enterprise and IT strategies
- information requirements definition
- feasibility studies (costs, benefits, alternatives, etc.)
- functionality, operability, acceptability and sustainability requirements
- compliance with information architecture
- cost-effective security and control
- supplier responsibilities



DETAILED CONTROL OBJECTIVES

1 IDENTIFY AUTOMATED SOLUTIONS

1.1 Definition of Information Requirements

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should provide that the business requirements satisfied by the existing system and to be satisfied by the proposed new or modified system (software, data and infrastructure) be clearly defined before a development, implementation or modification project is approved. The system development life cycle methodology should require that the solution's functional and operational requirements be specified including performance, safety, reliability, compatibility, security and legislation.

1.2 Formulation of Alternative Courses of Action

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should provide for the analysis of the alternative courses of action that will satisfy the business requirements established for a proposed new or modified system.

1.3 Formulation of Acquisition Strategy

CONTROL OBJECTIVE

Information systems acquisition, development and maintenance should be considered in the context of the organisation's IT long- and short-range plans. The organisation's system development life cycle methodology should provide for a software acquisition strategy plan defining whether the software will be acquired off-the-shelf, developed internally, through contract or by enhancing the existing software, or a combination of all these.

1.4 Third-Party Service Requirements

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should provide for the evaluation of the requirements and the specifications for an RFP (request for proposal) when dealing with a third-party service vendor.

1.5 Technological Feasibility Study

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should provide for an examination of the technological feasibility of each alternative for satisfying the business requirements established for the development of a proposed new or modified information system project.

1.6 Economic Feasibility Study

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should provide, in each proposed information systems development, implementation and modification project, for an analysis of the costs and benefits associated with each alternative being considered for satisfying the established business requirements.

1.7 Information Architecture

CONTROL OBJECTIVE

Management should ensure that attention is paid to the enterprise data model while solutions are being identified and analysed for feasibility.

1.8 Risk Analysis Report

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should provide, in each proposed information system development, implementation or modification project, for an analysis and documentation of the security threats, potential vulnerabilities and impacts, and the feasible security and internal control safeguards for reducing or eliminating the identified risk. This should be realised in line with the overall risk assessment framework.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

1.9 **Cost-Effective Security Controls**
CONTROL OBJECTIVE
Management should ensure that the costs and benefits of security are carefully examined in monetary and non-monetary terms to guarantee that the costs of controls do not exceed benefits. The decision requires formal management sign-off. All security requirements should be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for an information system. Security requirements for business continuity management should be defined to ensure that the planned activation, fallback and resumption processes are supported by the proposed solution.

1.10 **Audit Trails Design**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should require that adequate mechanisms for audit trails are available or can be developed for the solution identified and selected. The mechanisms should provide the ability to protect sensitive data (e.g., user ID's) against discovery and misuse.

1.11 **Ergonomics**
CONTROL OBJECTIVE
Management should ensure that the information system development, implementation and change projects undertaken by the IT function pay attention to ergonomic issues associated with the introduction of automated solutions.

1.12 **Selection of System Software**
CONTROL OBJECTIVE
Management should ensure that a standard procedure is adhered to by the IT function to identify all potential system software programmes that will satisfy its operational requirements.

1.13 **Procurement Control**
CONTROL OBJECTIVE
Management should develop and implement a central procurement approach describing a common set of procedures and standards to be followed in the procurement of information technology related hardware, software and services. Products should be reviewed and tested prior to their use and the financial settlement.

1.14 **Software Product Acquisition**
CONTROL OBJECTIVE
Software product acquisition should follow the organisation's procurement policies.

1.15 **Third-Party Software Maintenance**
CONTROL OBJECTIVE
Management should require that for licensed software acquired from third-party providers, the providers have appropriate procedures to validate, protect and maintain the software product's integrity rights. Consideration should be given to the support of the product in any maintenance agreement related to the delivered product.

1.16 **Contract Application Programming**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should provide that the procurement of contract programming services be justified with a written request for services from a designated member of the IT function. The contract should stipulate that the software, documentation and other deliverables are subject to testing and review prior to acceptance. In addition, it should require that the end products of completed contract programming services be tested and reviewed according to the related standards by the IT function's quality assurance group and other concerned parties (such as users, project managers, etc.) before payment for the work and approval of the end product. Testing to be includ-

ed in contract specifications should consist of system testing, integration testing, hardware and component testing, procedure testing, load and stress testing, tuning and performance testing, regression testing, user acceptance testing and, finally, pilot testing of the total system to avoid any unexpected system failure.

1.17 **Acceptance of Facilities**

CONTROL OBJECTIVE

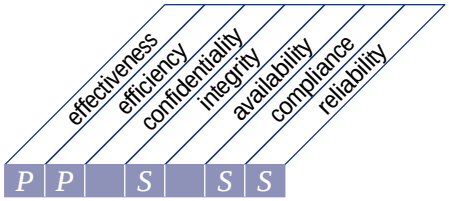
Management should ensure that an acceptance plan for facilities to be provided is agreed upon with the supplier in the contract and this plan defines the acceptance procedures and criteria. In addition, acceptance tests should be performed to guarantee that the accommodation and environment meet the requirements specified in the contract.

1.18 **Acceptance of Technology**

CONTROL OBJECTIVE

Management should ensure that an acceptance plan for specific technology to be provided is agreed upon with the supplier in the contract and this plan defines the acceptance procedures and criteria. In addition, acceptance tests provided for in the plan should include inspection, functionality tests and workload trials.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

acquiring and maintaining application software

that satisfies the business requirement

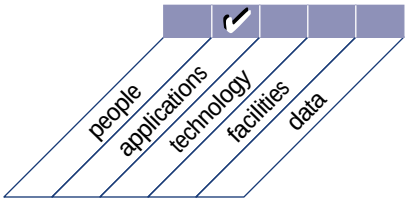
to provide automated functions which effectively support the business process

is enabled by

the definition of specific statements of functional and operational requirements, and a phased implementation with clear deliverables

and takes into consideration

- functional testing and acceptance
- application controls and security requirements
- documentation requirements
- application software life cycle
- enterprise information architecture
- system development life cycle methodology
- user-machine interface
- package customisation



DETAILED CONTROL OBJECTIVES

2 ACQUIRE AND MAINTAIN APPLICATION SOFTWARE

2.1 Design Methods

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should provide that appropriate procedures and techniques, involving close liaison with system users, are applied to create the design specifications for each new information system development project and to verify the design specifications against the user requirements.

2.2 Major Changes to Existing Systems

CONTROL OBJECTIVE

Management should ensure, that in the event of major changes to existing systems, a similar development process is observed as in the case of the development of new systems.

2.3 Design Approval

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should require that the design specifications for all information system development and modification projects be reviewed and approved by management, the affected user departments and the organisation's senior management, when appropriate.

2.4 File Requirements Definition and Documentation

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should provide that an appropriate procedure be applied for defining and documenting the file format for each information system development or modification project. Such a procedure should ensure that the data dictionary rules are respected.

2.5 Programme Specifications

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should require that detailed written programme specifications be prepared for each information system development or modification project. The methodology should further ensure that programme specifications agree with system design specifications.

2.6 Source Data Collection Design

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should require that adequate mechanisms for the collection and entry of data be specified for each information system development or modification project.

2.7 Input Requirements Definition and Documentation

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should require that adequate mechanisms exist for defining and documenting the input requirements for each information system development or modification project.

2.8 Definition of Interfaces

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should provide that all external and internal interfaces are properly specified, designed and documented.

2.9 User-Machine Interface

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should provide for the development of an interface between the user and machine which is easy to use and self-documenting (by means of online help functions).

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

2.10 **Processing Requirements Definition and Documentation**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should require that adequate mechanisms exist for defining and documenting the processing requirements for each information system development or modification project.

2.11 **Output Requirements Definition and Documentation**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should require that adequate mechanisms exist for defining and documenting the output requirements for each information system development or modification project.

2.12 **Controllability**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should require that adequate mechanisms for assuring the internal control and security requirements be specified for each information system development or modification project. The methodology should further ensure that information systems are designed to include application controls which guarantee the accuracy, completeness, timeliness and authorisation of inputs, processing and outputs. Sensitivity assessment should be performed during initiation of system development or modification. The basic security and internal control aspects of a system to be developed or modified should be assessed along with the conceptual design of the system in order to integrate security concepts in the design as early as possible.

2.13 **Availability as a Key Design Factor**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should provide that availability is considered in the design process for new or modified information systems at the earliest possible stage. Availability should be analysed and, if necessary, increased through maintainability and reliability improvements.

2.14 **IT Integrity Provisions in Application Programme Software**
CONTROL OBJECTIVE
The organisation should establish procedures to assure, where applicable, that application programmes contain provisions which routinely verify the tasks performed by the software to help assure data integrity, and which provide the restoration of the integrity through rollback or other means.

2.15 **Application Software Testing**
CONTROL OBJECTIVE
Unit testing, application testing, integration testing, system testing, and load and stress testing should be performed according to the project test plan and established testing standards before it is approved by the user. Adequate measures should be conducted to prevent disclosure of sensitive information used during testing.

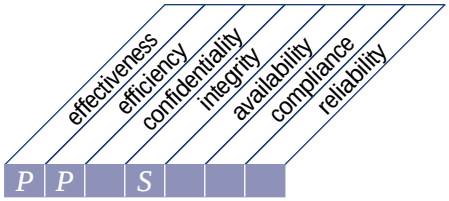
2.16 **User Reference and Support Materials**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should provide that adequate user reference and support manuals be prepared (preferably in electronic format) as part of every information system development or modification project.

2.17 **Reassessment of System Design**

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should ensure that the system design is reassessed whenever significant technical and/or logical discrepancies occur during system development or maintenance.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

acquiring and maintaining technology infrastructure

that satisfies the business requirement

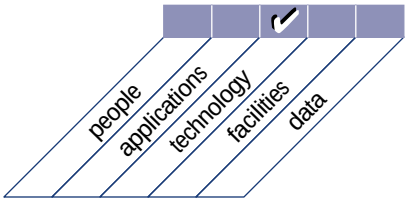
to provide the appropriate platforms for supporting business applications

is enabled by

judicious hardware and software acquisition, standardising of software, assessment of hardware and software performance, and consistent system administration

and takes into consideration

- compliance with technology infrastructure directions and standards
- technology assessment
- installation, maintenance and change controls
- upgrade, conversion and migration plans
- use of internal and external infrastructures and/or resources
- supplier responsibilities and relationships
- change management
- total cost of ownership
- system software security



DETAILED CONTROL OBJECTIVES

3 ACQUIRE AND MAINTAIN TECHNOLOGY INFRASTRUCTURE

3.1 Assessment of New Hardware and Software

CONTROL OBJECTIVE

Hardware and software selection criteria should be based on the functional specifications for the new or modified system and should identify mandatory and optional requirements. Procedures should be in place to assess new hardware and software for any impact on the performance of the overall system.

3.2 Preventative Maintenance for Hardware

CONTROL OBJECTIVE

IT management should schedule routine and periodic hardware maintenance to reduce the frequency and impact of performance failures.

3.3 System Software Security

CONTROL OBJECTIVE

IT management should ensure that the set-up of system software to be installed does not jeopardise the security of the data and programmes being stored on the system. Attention should be paid to set-up and maintenance of system software parameters.

3.4 System Software Installation

CONTROL OBJECTIVE

Procedures should be implemented to ensure that system software is installed in accordance with the acquisition and maintenance framework for the technology infrastructure. Testing should be performed before use in the production environment is authorised. A group independent of the users and developers should control the movement of programmes and data among libraries.

3.5 System Software Maintenance

CONTROL OBJECTIVE

Procedures should be implemented to ensure that system software is maintained in accordance with the acquisition and maintenance framework for the technology infrastructure.

3.6 System Software Change Controls

CONTROL OBJECTIVE

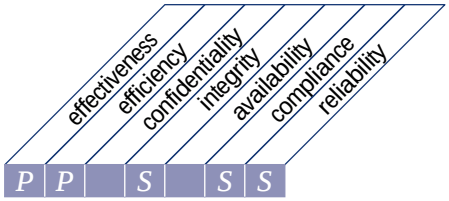
Procedures should be implemented to ensure that system software changes are controlled in line with the organisation's change management procedures.

3.7 Use and Monitoring of System Utilities

CONTROL OBJECTIVE

Policies and techniques should be implemented for using, monitoring and evaluating the use of system utilities. Responsibilities for using sensitive software utilities should be clearly defined and understood by developers, and the use of the utilities should be monitored and logged.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

developing and maintaining procedures

that satisfies the business requirement

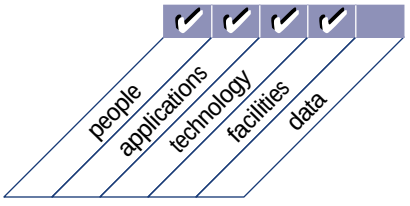
to ensure the proper use of the applications and the technological solutions put in place

is enabled by

a structured approach to the development of user and operations procedure manuals, service requirements and training materials

and takes into consideration

- business process re-design
- treating procedures as any other technology deliverable
- timely development
- user procedures and controls
- operational procedures and controls
- training materials
- managing change



DETAILED CONTROL OBJECTIVES

4 DEVELOP AND MAINTAIN PROCEDURES

4.1 Operational Requirements and Service Levels

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should ensure the timely definition of operational requirements and service levels.

4.2 User Procedures Manual

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should provide that adequate user procedures manuals be prepared and refreshed as part of every information system development, implementation or modification project.

4.3 Operations Manual

CONTROL OBJECTIVE

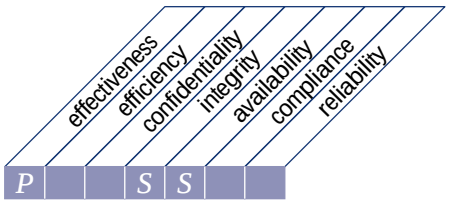
The organisation's system development life cycle methodology should provide that an adequate operations manual be prepared and kept up-to-date as part of every information system development, implementation or modification project.

4.4 Training Materials

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should ensure that adequate training materials are developed as part of every information system development, implementation or modification project. These materials should be focused on the system's use in daily practice.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

installing and accrediting systems

that satisfies the business requirement

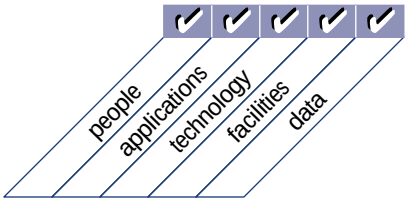
to verify and confirm that the solution is fit for the intended purpose

is enabled by

the realisation of a well-formalised installation migration, conversion and acceptance plan

and takes into consideration

- training of user and IT operations personnel
- data conversion
- a test environment reflecting the live environment
- accreditation
- post-implementation reviews and feedback
- end user involvement in testing
- continuous quality improvement plans
- business continuity requirements
- capacity and throughput measurement
- agreed upon acceptance criteria



DETAILED CONTROL OBJECTIVES

5 INSTALL AND ACCREDIT SYSTEMS

5.1 Training

CONTROL OBJECTIVE

Staff of the affected user departments and the operations group of the IT function should be trained in accordance with the defined training plan and associated materials, as part of every information systems development, implementation or modification project.

5.2 Application Software Performance Sizing

CONTROL OBJECTIVE

Application software performance sizing (optimisation) should be established as an integral part of the organisation's system development life cycle methodology to forecast the resources required for operating new and significantly changed software.

5.3 Implementation Plan

CONTROL OBJECTIVE

An implementation plan should be prepared, reviewed and approved by relevant parties and be used to measure progress. The implementation plan should address site preparation, equipment acquisition and installation, user training, installation of operating software changes, implementation of operating procedures and conversion.

5.4 System Conversion

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should provide, as part of every information system development, implementation or modification project, that the necessary elements from the old system are converted to the new one according to a pre-established plan.

5.5 Data Conversion

CONTROL OBJECTIVE

Management should require that a data conversion plan is prepared, defining the methods of collecting and verifying the data to be converted and identifying and resolving any errors found during conversion. Tests to be performed include comparing the original and converted files, checking the compatibility of the converted data with the new system, checking master files after conversion to ensure the accuracy of master file data and ensuring that transactions affecting master files update both the old and the new master files during the period between initial conversion and final implementation. A detailed verification of the initial processing of the new system should be performed to confirm successful implementation. Management should ensure that the responsibility for successful conversion of data lies with the system owners.

5.6 Testing Strategies and Plans

CONTROL OBJECTIVE

Testing strategies and plans should be prepared and signed off by the system owner and IT management.

5.7 Testing of Changes

CONTROL OBJECTIVE

Management should ensure that changes are tested in accordance with the impact and resource assessment in a separate test environment by an independent (from builders) test group before use in the regular operational environment begins. Back-out plans should also be developed. Acceptance testing should be carried out in an environment representative of the future operational environment (e.g., similar security, internal controls, workloads, etc.).

5.8 Parallel/Pilot Testing Criteria and Performance

CONTROL OBJECTIVE

Procedures should be in place to ensure that parallel or pilot testing is performed in accordance with a pre-established plan and that the criteria for terminating the testing process are specified in advance.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

5.9 **Final Acceptance Test**
CONTROL OBJECTIVE
Procedures should provide, as part of the final acceptance or quality assurance testing of new or modified information systems, for a formal evaluation and approval of the test results by management of the affected user department(s) and the IT function. The tests should cover all components of the information system (e.g., application software, facilities, technology, user procedures).

5.10 **Security Testing and Accreditation**
CONTROL OBJECTIVE
Management should define and implement procedures to ensure that operations and user management formally accept the test results and the level of security for the systems, along with the remaining residual risk. These procedures should reflect the agreed upon roles and responsibilities of end user, system development, network management and system operations personnel, taking into account segregation, supervision and control issues.

5.11 **Operational Test**
CONTROL OBJECTIVE
Management should ensure that before moving the system into operation, the user or designated custodian (the party designated to run the system on behalf of the user) validates its operation as a complete product, under conditions similar to the application environment and in the manner in which the system will be run in a production environment.

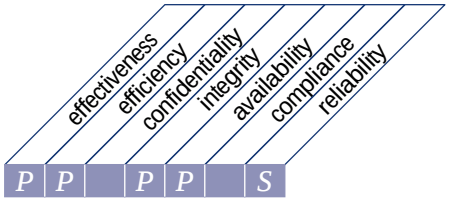
5.12 **Promotion to Production**
CONTROL OBJECTIVE
Management should define and implement formal procedures to control the handover of the system from development to testing to operations. Management should require that system owner authorisation is obtained before a new system is moved into production and that, before the old system is discontinued, the new system will have successfully operated through all daily, monthly and quarterly production cycles. The respective environments should be segregated and properly protected.

5.13 **Evaluation of Meeting User Requirements**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should require that a post-implementation review of operational information system requirements (e.g., capacity, throughput, etc.) be conducted to assess whether the users' needs are being met by the system.

5.14 **Management's Post-Implementation Review**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should require that a post-implementation review of an operational information system assess and report on whether the system delivered the benefits envisioned in the most cost effective manner.

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing changes

that satisfies the business requirement

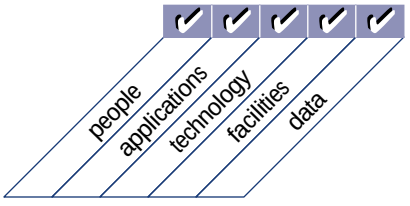
to minimise the likelihood of disruption, unauthorised alterations and errors

is enabled by

a management system which provides for the analysis, implementation and follow-up of all changes requested and made to the existing IT infrastructure

and takes into consideration

- identification of changes
- categorisation, prioritisation and emergency procedures
- impact assessment
- change authorisation
- release management
- software distribution
- use of automated tools
- configuration management
- business process re-design



DETAILED CONTROL OBJECTIVES

6 MANAGE CHANGES

6.1 Change Request Initiation and Control

CONTROL OBJECTIVE

IT management should ensure that all requests for changes, system maintenance and supplier maintenance are standardised and are subject to formal change management procedures. Changes should be categorised and prioritised and specific procedures should be in place to handle urgent matters. Change requestors should be kept informed about the status of their request.

6.2 Impact Assessment

CONTROL OBJECTIVE

A procedure should be in place to ensure that all requests for change are assessed in a structured way for all possible impacts on the operational system and its functionality.

6.3 Control of Changes

CONTROL OBJECTIVE

IT management should ensure that change management and software control and distribution are properly integrated with a comprehensive configuration management system. The system used to monitor changes to application systems should be automated to support the recording and tracking of changes made to large, complex information systems.

6.4 Emergency Changes

CONTROL OBJECTIVE

IT management should establish parameters defining emergency changes and procedures to control these changes when they circumvent the normal process of technical, operational and management assessment prior to implementation. The emergency changes should be recorded and authorised by IT management prior to implementation.

6.5 Documentation and Procedures

CONTROL OBJECTIVE

The change process should ensure that whenever system changes are implemented, the associated documentation and procedures are updated accordingly.

6.6 Authorised Maintenance

CONTROL OBJECTIVE

IT management should ensure maintenance personnel have specific assignments and that their work is properly monitored. In addition, their system access rights should be controlled to avoid risks of unauthorised access to automated systems.

6.7 Software Release Policy

CONTROL OBJECTIVE

IT management should ensure that the release of software is governed by formal procedures ensuring sign-off, packaging, regression testing, handover, etc.

6.8 Distribution of Software

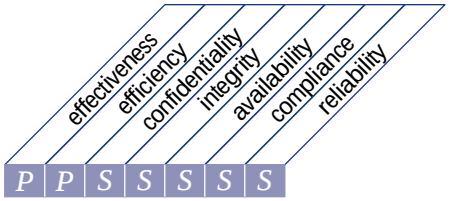
CONTROL OBJECTIVE

Specific internal control measures should be established to ensure distribution of the correct software element to the right place, with integrity, and in a timely manner with adequate audit trails.

This page intentionally left blank

DELIVERY & SUPPORT

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

defining and managing service levels

that satisfies the business requirement

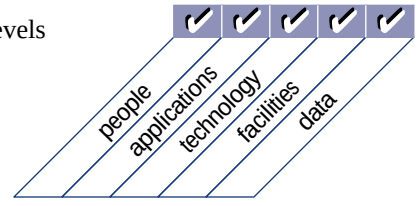
to establish a common understanding of the level of service required

is enabled by

the establishment of service-level agreements which formalise the performance criteria against which the quantity and quality of service will be measured

and takes into consideration

- formal agreements
- definition of responsibilities
- response times and volumes
- charging
- integrity guarantees
- non-disclosure agreements
- customer satisfaction criteria
- cost/benefit analysis of required service levels
- monitoring and reporting



DETAILED CONTROL OBJECTIVES

1 DEFINE AND MANAGE SERVICE LEVELS

1.1 Service Level Agreement Framework

CONTROL OBJECTIVE

Management should define a framework wherein it promotes the definition of formal service level agreements and defines the minimal contents: availability, reliability, performance, capacity for growth, levels of support provided to users, continuity planning, security, minimum acceptable level of satisfactorily delivered system functionality, restrictions (limits on the amount of work), service charges, central print facilities (availability), central print distribution and change procedures. Users and the IT function should have a written agreement which describes the service level in qualitative and quantitative terms. The agreement defines the responsibilities of both parties. The IT function must offer the agreed quality and quantity of service and the users must constrain the demands they place upon the service within the agreed limits.

1.2 Aspects of Service Level Agreements

CONTROL OBJECTIVE

Explicit agreement should be reached on the aspects that a service level agreement should have. The service level agreement should cover at least the following aspects: availability, reliability, performance, capacity for growth, levels of support provided to users, continuity planning, security, minimum acceptable level of satisfactorily delivered system functionality, restrictions (limits on the amount of work), service charges, central print facilities (availability), central print distribution and change procedures.

1.3 Performance Procedures

CONTROL OBJECTIVE

Procedures should be put in place to ensure that the manner of and responsibilities for performance governing relations (e.g., non-disclosure agreements) between all the involved parties are established, coordinated, maintained and communicated to all affected departments.

1.4 Monitoring and Reporting

CONTROL OBJECTIVE

Management should appoint a service level manager who is responsible for monitoring and reporting on the achievement of the specified service performance criteria and all problems encountered during processing. The monitoring statistics should be analysed on a timely basis. Appropriate corrective action should be taken and failures should be investigated.

1.5 Review of Service Level Agreements and Contracts

CONTROL OBJECTIVE

Management should implement a regular review process for service level agreements and underpinning contracts with third-party service providers.

1.6 Chargeable Items

CONTROL OBJECTIVE

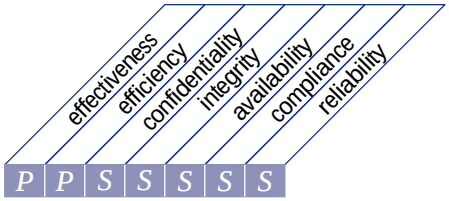
Provisions for chargeable items should be included in the service level agreements to make trade-offs possible on service levels versus costs.

1.7 Service Improvement Programme

CONTROL OBJECTIVE

Management should implement a process to ensure that users and service level managers regularly agree on a service improvement programme for pursuing cost-justified improvements to the service level.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing third-party services

that satisfies the business requirement

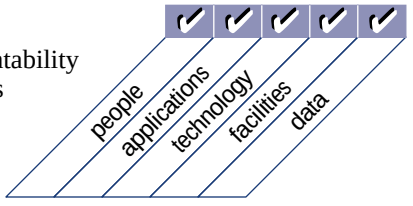
to ensure that roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy requirements

is enabled by

control measures aimed at the review and monitoring of existing agreements and procedures for their effectiveness and compliance with organisation policy

and takes into consideration

- third-party service agreements
- contract management
- non-disclosure agreements
- legal and regulatory requirements
- service delivery monitoring and reporting
- enterprise and IT risk assessments
- performance rewards and penalties
- internal and external organisational accountability
- analysis of cost and service level variances



DETAILED CONTROL OBJECTIVES

2 MANAGE THIRD-PARTY SERVICES

2.1 Supplier Interfaces

CONTROL OBJECTIVE

Management should ensure that all third-party providers' services are properly identified and that the technical and organisational interfaces with suppliers are documented.

2.2 Owner Relationships

CONTROL OBJECTIVE

The customer organisation management should appoint a relationship owner who is responsible for ensuring the quality of the relationships with third-parties.

2.3 Third-Party Contracts

CONTROL OBJECTIVE

Management should define specific procedures to ensure that for each relationship with a third-party service provider a formal contract is defined and agreed upon before work starts.

2.4 Third-Party Qualifications

CONTROL OBJECTIVE

Management should ensure that, before selection, potential third-parties are properly qualified through an assessment of their capability to deliver the required service (due diligence).

2.5 Outsourcing Contracts

CONTROL OBJECTIVE

Specific organisational procedures should be defined to ensure that the contract between the facilities management provider and the organisation is based on required processing levels, security, monitoring and contingency requirements, and other stipulations as appropriate.

2.6 Continuity of Services

CONTROL OBJECTIVE

With respect to ensuring continuity of services, management should consider business risk related to the third-party in terms of legal uncertainties and the going concern concept, and negotiate escrow contracts where appropriate.

2.7 Security Relationships

CONTROL OBJECTIVE

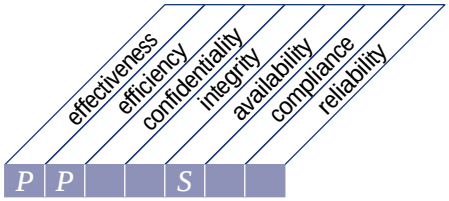
With regard to relationships with third-party service providers, management should ensure that security agreements (e.g., non-disclosure agreements) are identified and explicitly stated and agreed to, and conform to universal business standards in accordance with legal and regulatory requirements, including liabilities.

2.8 Monitoring

CONTROL OBJECTIVE

A process for monitoring of the service delivery of the third-party should be set up by management to ensure the continuing adherence to the contract agreements.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing performance and capacity

that satisfies the business requirement

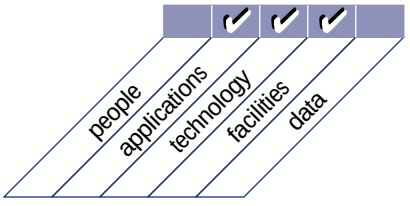
to ensure that adequate capacity is available and that best and optimal use is made of it to meet required performance needs

is enabled by

data collection, analysis and reporting on resource performance, application sizing and workload demand

and takes into consideration

- availability and performance requirements
- automated monitoring and reporting
- modeling tools
- capacity management
- resource availability
- hardware and software price/performance changes



DETAILED CONTROL OBJECTIVES

3 MANAGE PERFORMANCE AND CAPACITY

3.1 Availability and Performance Requirements

CONTROL OBJECTIVE

The management process should ensure that business needs are identified regarding availability and performance of information services and converted into availability terms and requirements.

3.2 Availability Plan

CONTROL OBJECTIVE

Management should ensure the establishment of an availability plan to achieve, monitor and control the availability of information services.

3.3 Monitoring and Reporting

CONTROL OBJECTIVE

Management should implement a process to ensure that the performance of IT resources is continuously monitored and exceptions are reported in a timely and comprehensive manner.

3.4 Modeling Tools

CONTROL OBJECTIVE

IT management should ensure that appropriate modeling tools are used to produce a model of the current system which has been calibrated and adjusted against actual workload and is accurate within recommended load levels. Modeling tools should be used to assist with the prediction of capacity, configuration reliability, performance and availability requirements. In-depth technical investigations should be conducted on systems hardware and should include forecasts concerning future technologies.

3.5 Proactive Performance Management

CONTROL OBJECTIVE

The performance management process should include forecasting capability to enable problems to be corrected before they affect system performance. Analysis should be conducted on system failures and irregularities pertaining to frequency, degree of impact and amount of damage.

3.6 Workload Forecasting

CONTROL OBJECTIVE

Controls are to be in place to ensure that workload forecasts are prepared to identify trends and to provide information needed for the capacity plan.

3.7 Capacity Management of Resources

CONTROL OBJECTIVE

IT management should establish a planning process for the review of hardware performance and capacity to ensure that cost-justifiable capacity always exists to process the agreed workloads and to provide the required performance quality and quantity prescribed in service level agreements. The capacity plan should cover multiple scenarios.

3.8 Resources Availability

CONTROL OBJECTIVE

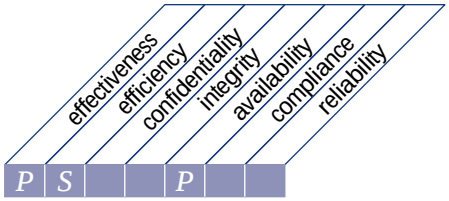
When identified as availability requirements, management should prevent resources from being unavailable by implementing fault tolerance mechanisms, prioritising tasks and equitable resource allocation mechanisms.

3.9 Resources Schedule

CONTROL OBJECTIVE

Management should ensure the timely acquisition of required capacity, taking into account aspects such as resilience, contingency, workloads and storage plans.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

ensuring continuous service

that satisfies the business requirement

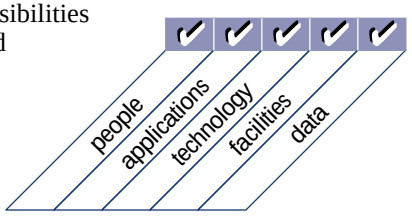
to make sure IT services are available as required and to ensure a minimum business impact in the event of a major disruption

is enabled by

having an operational and tested IT continuity plan which is in line with the overall business continuity plan and its related business requirements

and takes into consideration

- criticality classification
- alternative procedures
- back-up and recovery
- systematic and regular testing and training
- monitoring and escalation processes
- internal and external organisational responsibilities
- business continuity activation, fallback and resumption plans
- risk management activities
- assessment of single points of failure
- problem management



DETAILED CONTROL OBJECTIVES

4 ENSURE CONTINUOUS SERVICE

4.1 IT Continuity Framework

CONTROL OBJECTIVE

IT management, in cooperation with business process owners, should establish a continuity framework which defines the roles, responsibilities and the risk-based approach/methodology to be adopted, and the rules and structures to document the continuity plan as well as the approval procedures.

4.2 IT Continuity Plan Strategy and Philosophy

CONTROL OBJECTIVE

Management should ensure that the IT continuity plan is in line with the overall business continuity plan to ensure consistency. Furthermore, the IT continuity plan should take into account the IT long- and short-range plans to ensure consistency.

4.3 IT Continuity Plan Contents

CONTROL OBJECTIVE

IT management should ensure that a written plan is developed containing the following:

- Guidelines on how to use the continuity plan
- Emergency procedures to ensure the safety of all affected staff members
- Response procedures meant to bring the business back to the state it was in before the incident or disaster
- Recovery procedures meant to bring the business back to the state it was in before the incident or disaster
- Procedures to safeguard and reconstruct the home site
- Co-ordination procedures with public authorities
- Communication procedures with stakeholders, employees, key customers, critical suppliers, stockholders and management
- Critical information on continuity teams, affected staff, customers, suppliers, public authorities and media

4.4 Minimising IT Continuity Requirements

CONTROL OBJECTIVE

IT management should establish procedures and guidelines for minimising the continuity requirements with regard to personnel, facilities, hardware, software, equipment, forms, supplies and furniture.

4.5 Maintaining the IT Continuity Plan

CONTROL OBJECTIVE

IT management should provide for change control procedures in order to ensure that the continuity plan is up-to-date and reflects actual business requirements. This requires continuity plan maintenance procedures aligned with change and management and human resources procedures.

4.6 Testing the IT Continuity Plan

CONTROL OBJECTIVE

To have an effective continuity plan, management needs to assess its adequacy on a regular basis or upon major changes to the business or IT infrastructure; this requires careful preparation, documentation, reporting test results and, according to the results, implementing an action plan.

4.7 IT Continuity Plan Training

CONTROL OBJECTIVE

The disaster continuity methodology should ensure that all concerned parties receive regular training sessions regarding the procedures to be followed in case of an incident or disaster.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

4.8 **IT Continuity Plan Distribution**
CONTROL OBJECTIVE
Given the sensitive nature of information in the continuity plan, the latter should be distributed only to authorised personnel and should be safeguarded against unauthorised disclosure. Consequently, sections of the plan need to be distributed on a need-to-know basis.

4.9 **User Department Alternative Processing Back-up Procedures**
CONTROL OBJECTIVE
The continuity methodology should ensure that the user departments establish alternative processing procedures that may be used until the IT function is able to fully restore its services after a disaster or an event.

4.10 **Critical IT Resources**
CONTROL OBJECTIVE
The continuity plan should identify the critical application programmes, third-party services, operating systems, personnel and supplies, data files and time frames needed for recovery after a disaster occurs. Critical data and operations should be identified, documented, prioritised and approved by the business process owners, in cooperation with IT management.

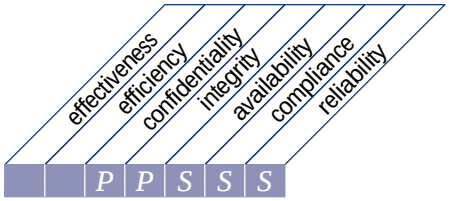
4.11 **Back-up Site and Hardware**
CONTROL OBJECTIVE
Management should ensure that the continuity methodology incorporates an identification of alternatives regarding the back-up site and hardware as well as a final alternative selection. If applicable, a formal contract for these type of services should be concluded.

4.12 **Off-site Back-up Storage**
CONTROL OBJECTIVE
Off-site storage of critical back-up media, documentation and other IT resources should be established to support recovery and business continuity plans. Business process owners and IT function personnel should be involved in determining what back-up resources need to be stored off-site. The off-site storage facility should be environmentally appropriate to the media and other resources stored and should have a level of security commensurate with that needed to protect the back-up resources from unauthorised access, theft or damage. IT management should ensure that off-site arrangements are periodically assessed, at least annually, for content, environmental protection and security.

4.13 **Wrap-up Procedures**
CONTROL OBJECTIVE
On successful resumption of the IT function after a disaster, IT management should establish procedures for assessing the adequacy of the plan and update the plan accordingly.

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

ensuring systems security

that satisfies the business requirement

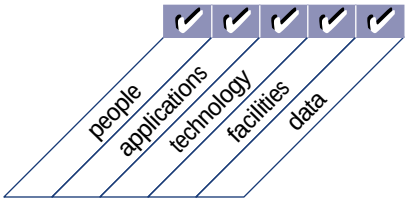
to safeguard information against unauthorised use, disclosure or modification, damage or loss

is enabled by

logical access controls which ensure that access to systems, data and programmes is restricted to authorised users

and takes into consideration

- confidentiality and privacy requirements
- authorisation, authentication and access control
- user identification and authorisation profiles
- need-to-have and need-to-know
- cryptographic key management
- incident handling, reporting and follow-up
- virus prevention and detection
- firewalls
- centralised security administration
- user training
- tools for monitoring compliance, intrusion testing and reporting



DETAILED CONTROL OBJECTIVES

5 ENSURE SYSTEMS SECURITY

5.1 Manage Security Measures

CONTROL OBJECTIVE

IT security should be managed such that security measures are in line with business requirements. This includes:

- Translating risk assessment information to the IT security plans
- Implementing the IT security plan
- Updating the IT security plan to reflect changes in the IT configuration
- Assessing the impact of change requests on IT security
- Monitoring the implementation of the IT security plan
- Aligning IT security procedures to other policies and procedures

5.2 Identification, Authentication and Access

CONTROL OBJECTIVE

The logical access to and use of IT computing resources should be restricted by the implementation of adequate identification, authentication and authorisation mechanisms, linking users and resources with access rules. Such mechanisms should prevent unauthorised personnel, dial-up connections and other system (network) entry ports from accessing computer resources and minimise the need for authorised users to use multiple sign-ons. Procedures should also be in place to keep authentication and access mechanisms effective (e.g., regular password changes).

5.3 Security of Online Access to Data

CONTROL OBJECTIVE

In an online IT environment, IT management should implement procedures in line with the security policy that provides access security control based on the individual's demonstrated need to view, add, change or delete data.

5.4 User Account Management

CONTROL OBJECTIVE

Management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing of user accounts. A formal approval procedure outlining the data or system owner granting the access privileges should be included. The security of third-party access should be defined contractually and address administration and non-disclosure requirements. Outsourcing arrangements should address the risks, security controls and procedures for information systems and networks in the contract between the parties.

5.5 Management Review of User Accounts

CONTROL OBJECTIVE

Management should have a control process in place to review and confirm access rights periodically. Periodic comparison of resources with recorded accountability should be made to help reduce the risk of errors, fraud, misuse or unauthorised alteration.

5.6 User Control of User Accounts

CONTROL OBJECTIVE

Users should systematically control the activity of their proper account(s). Also information mechanisms should be in place to allow them to oversee normal activity as well as to be alerted to unusual activity in a timely manner.

5.7 Security Surveillance

CONTROL OBJECTIVE

IT security administration should ensure that security activity is logged and any indication of imminent security violation is reported immediately to all who may be concerned, internally and externally, and is acted upon in a timely manner.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

5.8 **Data Classification**
CONTROL OBJECTIVE
Management should implement procedures to ensure that all data are classified in terms of sensitivity by a formal and explicit decision by the data owner according to the data classification scheme. Even data needing "no protection" should require a formal decision to be so designated. Owners should determine disposition and sharing of data, as well as whether and when programs and files are to be maintained, archived or deleted. Evidence of owner approval and data disposition should be maintained. Policies should be defined to support reclassification of information, based on changing sensitivities. The classification scheme should include criteria for managing exchanges of information between organisations, addressing both security and compliance with relevant legislation.

5.9 **Central Identification and Access Rights Management**
CONTROL OBJECTIVE
Controls are in place to ensure that the identification and access rights of users as well as the identity of system and data ownership are established and managed in a unique and central manner to obtain consistency and efficiency of global access control.

5.10 **Violation and Security Activity Reports**
CONTROL OBJECTIVE
IT security administration should ensure that violation and security activity is logged, reported, reviewed and appropriately escalated on a regular basis to identify and resolve incidents involving unauthorised activity. The logical access to the computer resources accountability information (security and other logs) should be granted based upon the principle of least privilege, or need-to-know.

5.11 **Incident Handling**
CONTROL OBJECTIVE
Management should establish a computer security incident handling capability to address security incidents by providing a centralised platform with sufficient expertise and equipped with rapid and secure communication facilities. Incident management responsibilities and procedures should be established to ensure an appropriate, effective and timely response to security incidents.

5.12 **Reaccreditation**
CONTROL OBJECTIVE
Management should ensure that reaccreditation of security (e.g., through "tiger teams") is periodically performed to keep up-to-date the formally approved security level and the acceptance of residual risk.

5.13 **Counterparty Trust**
CONTROL OBJECTIVE
Organisational policy should ensure that control practices are implemented to verify the authenticity of the counterparty providing electronic instructions or transactions. This can be implemented through trusted exchange of passwords, tokens or cryptographic keys.

5.14 **Transaction Authorisation**
CONTROL OBJECTIVE
Organisational policy should ensure that, where appropriate, controls are implemented to provide authenticity of transactions and establish the validity of a user's claimed identity to the system. This requires use of cryptographic techniques for signing and verifying transactions.

5.15 **Non-Repudiation**

CONTROL OBJECTIVE

Organisational policy should ensure that, where appropriate, transactions cannot be denied by either party, and controls are implemented to provide non-repudiation of origin or receipt, proof of submission, and receipt of transactions. This can be implemented through digital signatures, time stamping and trusted third-parties, with appropriate policies that take into account relevant regulatory requirements.

5.16 **Trusted Path**

CONTROL OBJECTIVE

Organisational policy should ensure that sensitive transaction data is only exchanged over a trusted path. Sensitive information includes security management information, sensitive transaction data, passwords and cryptographic keys. To achieve this, trusted channels may need to be established using encryption between users, between users and systems, and between systems.

5.17 **Protection of Security Functions**

CONTROL OBJECTIVE

All security related hardware and software should at all times be protected against tampering to maintain their integrity and against disclosure of secret keys. In addition, organisations should keep a low profile about their security design, but should not base their security on the design being secret.

5.18 **Cryptographic Key Management**

CONTROL OBJECTIVE

Management should define and implement procedures and protocols to be used for generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorised disclosure. If a key is compromised, management should ensure this information is propagated to any interested party through the use of Certificate Revocation Lists or similar mechanisms.

5.19 **Malicious Software Prevention, Detection and Correction**

CONTROL OBJECTIVE

Regarding malicious software, such as computer viruses or trojan horses, management should establish a framework of adequate preventative, detective and corrective control measures, and occurrence response and reporting. Business and IT management should ensure that procedures are established across the organisation to protect information systems and technology from computer viruses. Procedures should incorporate virus protection, detection, occurrence response and reporting.

5.20 **Firewall Architectures and Connections with Public Networks**

CONTROL OBJECTIVE

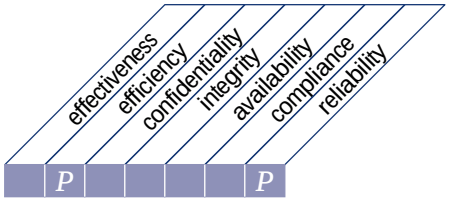
If connection to the Internet or other public networks exists, adequate firewalls should be operative to protect against denial of services and any unauthorised access to the internal resources; should control any application and infrastructure management flows in both directions; and should protect against denial of service attacks.

5.21 **Protection of Electronic Value**

CONTROL OBJECTIVE

Management should protect the continued integrity of all cards or similar physical mechanisms used for authentication or storage of financial or other sensitive information, taking into consideration the related facilities, devices, employees and validation methods used.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

identifying and allocating costs

that satisfies the business requirement

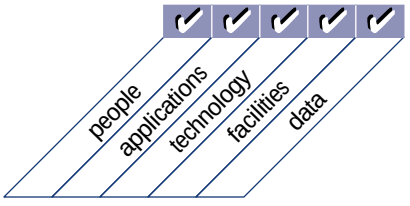
to ensure a correct awareness of the costs attributable to IT services

is enabled by

a cost accounting system which ensures that costs are recorded, calculated and allocated to the required level of detail and to the appropriate service offering

and takes into consideration

- resources identifiable and measurable
- charging policies and procedures
- charge rates and charge-back process
- linkage to service level agreement
- automated reporting
- verification of benefit realisation
- external benchmarking



DETAILED CONTROL OBJECTIVES

6 IDENTIFY AND ALLOCATE COSTS

6.1 Chargeable Items

CONTROL OBJECTIVE

IT management, with guidance from senior management, should ensure that chargeable items are identifiable, measurable and predictable by users. Users should be able to control the use of information services and associated billing levels.

6.2 Costing Procedures

CONTROL OBJECTIVE

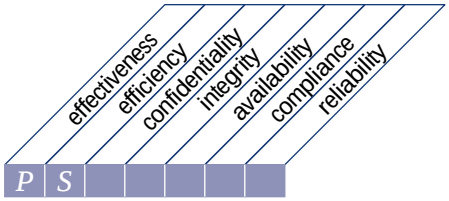
IT management should define and implement costing procedures to provide management information on the costs of delivering information services while ensuring cost effectiveness. Variances between forecasts and actual costs are to be adequately analysed and reported on to facilitate the cost monitoring. In addition, management should periodically evaluate the results of the IT function's job cost accounting procedures, in light of the organisation's other financial measurement systems.

6.3 User Billing and Chargeback Procedures

CONTROL OBJECTIVE

IT management should define and use billing and chargeback procedures. It should maintain user billing and chargeback procedures that encourage the proper usage of computer resources and assure the fair treatment of user departments and their needs. The rate charged should reflect the associated costs of providing services.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

educating and training users

that satisfies the business requirement

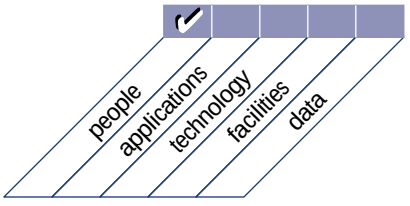
to ensure that users are making effective use of technology and are aware of the risks and responsibilities involved

is enabled by

a comprehensive training and development plan

and takes into consideration

- training curriculum
- skills inventory
- awareness campaigns
- awareness techniques
- use of new training technologies and methods
- personnel productivity
- development of knowledge base



DETAILED CONTROL OBJECTIVES

7 EDUCATE AND TRAIN USERS

7.1 Identification of Training Needs

CONTROL OBJECTIVE

In line with the long-range plan, management should establish and maintain procedures for identifying and documenting the training needs of all personnel using information services. A training curriculum for each group of employees should be established.

7.2 Training Organisation

CONTROL OBJECTIVE

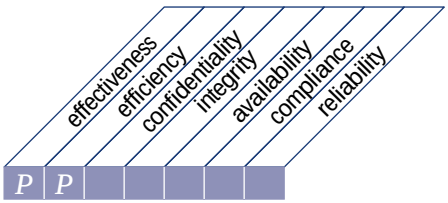
Based on the identified needs, management should define the target groups, identify and appoint trainers, and organise timely training sessions. Training alternatives should also be investigated (internal or external location, in-house trainers or third-party trainers, etc.).

7.3 Security Principles and Awareness Training

CONTROL OBJECTIVE

All personnel must be trained and educated in system security principles, including periodic updates with special focus on security awareness and incident handling. Management should provide an education and training programme that includes: ethical conduct of the IT function, security practices to protect against harm from failures affecting availability, confidentiality, integrity and performance of duties in a secure manner.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

assisting and advising customers

that satisfies the business requirement

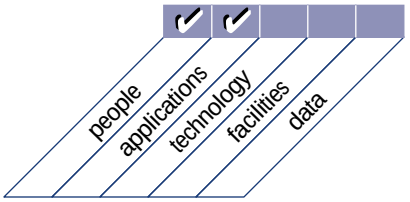
to ensure that any problem experienced by the user is appropriately resolved

is enabled by

a help desk facility which provides first-line support and advice

and takes into consideration

- customer query and problem response
- query monitoring and clearance
- trend analysis and reporting
- development of knowledge base
- root cause analysis
- problem tracking and escalation



DETAILED CONTROL OBJECTIVES

8 ASSIST AND ADVISE CUSTOMERS

8.1 Help Desk

CONTROL OBJECTIVE

User support should be established within a "help desk" function. Individuals responsible for performing this function should closely interact with problem management personnel.

8.2 Registration of Customer Queries

CONTROL OBJECTIVE

Procedures should be in place to ensure that all customer queries are adequately registered by the help desk.

8.3 Customer Query Escalation

CONTROL OBJECTIVE

Help desk procedures should ensure that customer queries which cannot immediately be resolved are appropriately escalated within the IT function.

8.4 Monitoring of Clearance

CONTROL OBJECTIVE

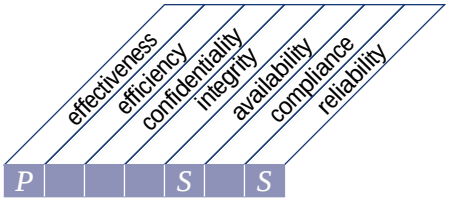
Management should establish procedures for timely monitoring of the clearance of customer queries. Long outstanding queries should be investigated and acted upon.

8.5 Trend Analysis and Reporting

CONTROL OBJECTIVE

Procedures should be in place which assure adequate reporting with regard to customer queries and resolution, response times and trend identification. The reports should be adequately analysed and acted upon.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing the configuration

that satisfies the business requirement

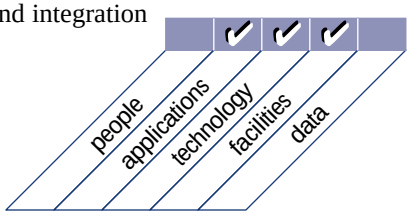
to account for all IT components, prevent unauthorised alterations, verify physical existence and provide a basis for sound change management

is enabled by

controls which identify and record all IT assets and their physical location, and a regular verification programme which confirms their existence

and takes into consideration

- asset tracking
- configuration change management
- checking for unauthorised software
- software storage controls
- software and hardware interrelationships and integration
- use of automated tools



DETAILED CONTROL OBJECTIVES

9 MANAGE THE CONFIGURATION

9.1 Configuration Recording

CONTROL OBJECTIVE

Procedures should be in place to ensure that only authorised and identifiable configuration items are recorded in inventory upon acquisition. These procedures should also provide for the authorised disposal and consequential sale of configuration items. Moreover, procedures should be in place to keep track of changes to the configuration (e.g., new item, status change from development to prototype). Logging and control should be an integrated part of the configuration recording system including reviews of changed records.

9.2 Configuration Baseline

CONTROL OBJECTIVE

IT management should be ensured that a baseline of configuration items is kept as a checkpoint to return to after changes.

9.3 Status Accounting

CONTROL OBJECTIVE

IT management should ensure that the configuration records reflect the actual status of all configuration items including the history of changes.

9.4 Configuration Control

CONTROL OBJECTIVE

Procedures should ensure that the existence and consistency of recording of the IT configuration is periodically checked.

9.5 Unauthorised Software

CONTROL OBJECTIVE

Clear policies restricting the use of personal and unlicensed software should be developed and enforced. The organisation should use virus detection and remedy software. Business and IT management should periodically check the organisation's personal computers for unauthorised software. Compliance with the requirements of software and hardware license agreements should be reviewed on a periodic basis.

9.6 Software Storage

CONTROL OBJECTIVE

A file storage area (library) should be defined for all valid software items in appropriate phases of the system development life cycle. These areas should be separated from each other and from development, testing and production file storage areas.

9.7 Configuration Management Procedures

CONTROL OBJECTIVE

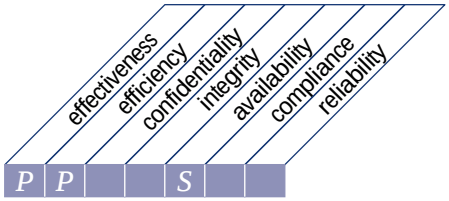
Configuration management procedures should be established to ensure that critical components of the organisation's IT resources have been appropriately identified and are maintained. There should be an integrated process whereby current and future processing demands are measured and provide input to the IT resource acquisitions process.

9.8 Software Accountability

CONTROL OBJECTIVE

Software should be labeled, inventoried and properly licensed. Library management software should be used to produce audit trails of program changes and to maintain program version numbers, creation-date information and copies of previous versions.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing problems and incidents

that satisfies the business requirement

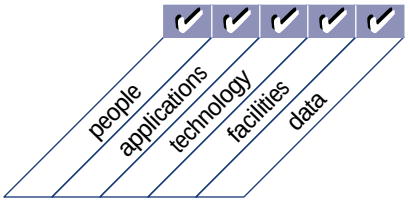
to ensure that problems and incidents are resolved, and the cause investigated to prevent any recurrence

is enabled by

a problem management system which records and progresses all incidents

and takes into consideration

- audit trails of problems and solutions
- timely resolution of reported problems
- escalation procedures
- incident reports
- accessibility of configuration information
- supplier responsibilities
- coordination with change management



DETAILED CONTROL OBJECTIVES

10 MANAGE PROBLEMS AND INCIDENTS

10.1 Problem Management System

CONTROL OBJECTIVE

IT management should define and implement a problem management system to ensure that all operational events which are not part of the standard operation (incidents, problems and errors) are recorded, analysed and resolved in a timely manner. Emergency programme change procedures should be promptly tested, documented, approved and reported. Incident reports should be established in the case of significant problems.

10.2 Problem Escalation

CONTROL OBJECTIVE

IT management should define and implement problem escalation procedures to ensure that identified problems are solved in the most efficient way on a timely basis. These procedures should ensure that these priorities are appropriately set. The procedures should also document the escalation process for the activation of the IT continuity plan.

10.3 Problem Tracking and Audit Trail

CONTROL OBJECTIVE

The problem management system should provide for adequate audit trail facilities which allow tracing from incident to underlying cause (e.g., package release or urgent change implementation) and back. It should closely interwork with change management, availability management and configuration management.

10.4 Emergency and Temporary Access Authorisations

CONTROL OBJECTIVE

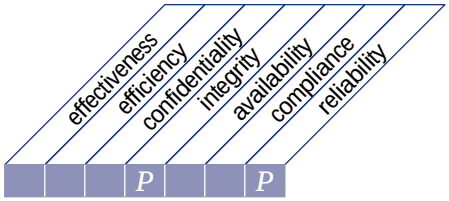
Emergency and temporary access authorisations should be documented on standard forms and maintained on file, approved by appropriate managers, securely communicated to the security function and automatically terminated after a predetermined period.

10.5 Emergency Processing Priorities

CONTROL OBJECTIVE

Emergency processing priorities should be established, documented and approved by appropriate program and IT management.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing data

that satisfies the business requirement

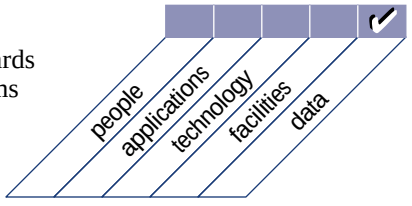
to ensure that data remains complete, accurate and valid during its input, update and storage

is enabled by

an effective combination of application and general controls over the IT operations

and takes into consideration

- form design
- source document controls
- input, processing and output controls
- media identification, movement and library management
- data back-up and recovery
- authentication and integrity
- data ownership
- data administration policies
- data models and data representation standards
- integration and consistency across platforms
- legal and regulatory requirements



DETAILED CONTROL OBJECTIVES

11 MANAGE DATA

11.1 Data Preparation Procedures
CONTROL OBJECTIVE
Management should establish data preparation procedures to be followed by user departments. In this context, input form design should help to assure that errors and omissions are minimised. Error handling procedures during data origination should reasonably ensure that errors and irregularities are detected, reported and corrected.

11.2 Source Document Authorisation Procedures
CONTROL OBJECTIVE
Management should ensure that source documents are properly prepared by authorised personnel who are acting within their authority and that an adequate segregation of duties is in place regarding the origination and approval of source documents.

11.3 Source Document Data Collection
CONTROL OBJECTIVE
The organisation's procedures should ensure that all authorised source documents are complete and accurate, properly accounted for and transmitted in a timely manner for entry.

11.4 Source Document Error Handling
CONTROL OBJECTIVE
Error handling procedures during data origination should reasonably ensure that errors and irregularities are detected, reported and corrected.

11.5 Source Document Retention
CONTROL OBJECTIVE
Procedures should be in place to ensure original source documents are retained or are reproducible by the organisation for an adequate amount of time to facilitate retrieval or reconstruction of data as well as to satisfy legal requirements.

11.6 Data Input Authorisation Procedures
CONTROL OBJECTIVE
The organisation should establish appropriate procedures to ensure that data input is performed only by authorised staff.

11.7 Accuracy, Completeness and Authorisation Checks
CONTROL OBJECTIVE
Transaction data entered for processing (people-generated, system-generated or interfaced inputs) should be subject to a variety of controls to check for accuracy, completeness and validity. Procedures should also be established to assure that input data is validated and edited as close to the point of origination as possible.

11.8 Data Input Error Handling
CONTROL OBJECTIVE
The organisation should establish procedures for the correction and resubmission of data which was erroneously input.

11.9 Data Processing Integrity
CONTROL OBJECTIVE
The organisation should establish procedures for the processing of data that ensure separation of duties is maintained and that work performed is routinely verified. The procedures should ensure adequate update controls such as run-to-run control totals and master file update controls are in place.

11.10 Data Processing Validation and Editing
CONTROL OBJECTIVE
The organisation should establish procedures to ensure that data processing validation, authentication and editing are performed as close to the point of origination as possible. When using Artificial Intelligence systems, these systems should be placed in an interactive control framework with human operators to ensure that vital decisions are approved.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

11.11 **Data Processing Error Handling**
CONTROL OBJECTIVE
The organisation should establish data processing error handling procedures that enable erroneous transactions to be identified without being processed and without undue disruption of the processing of other valid transactions.

11.12 **Output Handling and Retention**
CONTROL OBJECTIVE
The organisation should establish procedures for the handling and retention of output from its IT application programs. In case negotiable instruments (e.g., value cards) are the output recipients, special care should be taken to prevent misuse.

11.13 **Output Distribution**
CONTROL OBJECTIVE
The organisation should establish and communicate written procedures for the distribution of IT output.

11.14 **Output Balancing and Reconciliation**
CONTROL OBJECTIVE
The organisation should establish procedures for assuring that output routinely is balanced to the relevant control totals. Audit trails should be provided to facilitate the tracing of transaction processing and the reconciliation of disrupted data.

11.15 **Output Review and Error Handling**
CONTROL OBJECTIVE
The organisation's management should establish procedures for assuring that the accuracy of output reports is reviewed by the provider and the relevant users. Procedures should also be in place for controlling errors contained in the output.

11.16 **Security Provision for Output Reports**
CONTROL OBJECTIVE
The organisation should establish procedures for assuring that the security of output reports is maintained for those awaiting distribution, as well as those already distributed to users.

11.17 **Protection of Sensitive Information During Transmission and Transport**
CONTROL OBJECTIVE
Management should ensure that adequate protection of sensitive information is provided during transmission and transport against unauthorised access, modification and misaddressing.

11.18 **Protection of Disposed Sensitive Information**
CONTROL OBJECTIVE
Management should define and implement procedures to prevent access to sensitive information and software from computers, disks and other equipment or media when they are disposed of or transferred to another use. Such procedures should guarantee that data marked as deleted or to be disposed cannot be retrieved by any internal or third party.

11.19 **Storage Management**
CONTROL OBJECTIVE
Procedures should be developed for data storage which consider retrieval requirements, and cost effectiveness and security policy.

11.20 **Retention Periods and Storage Terms**
CONTROL OBJECTIVE
Retention periods and storage terms should be defined for documents, data, programmes and reports and messages (incoming and outgoing) as well as the data (keys, certificates) used for their encryption and authentication.

11.21 **Media Library Management System**
CONTROL OBJECTIVE
The IT function should establish procedures to assure that contents of its media library containing data are inventoried systematically, that any discrepancies disclosed by a physical inventory are remedied in a timely fashion and that measures are taken to maintain the integrity of magnetic media stored in the library.

11.22 **Media Library Management Responsibilities**
CONTROL OBJECTIVE
Housekeeping procedures designed to protect media library contents should be established by IT management. Standards should be defined for the external identification of magnetic media and the control of their physical movement and storage to support accountability. Responsibilities for media (magnetic tape, cartridge, disks and diskettes) library management should be assigned to specific members of the IT function.

11.23 **Back-up and Restoration**
CONTROL OBJECTIVE
Management should implement a proper strategy for back-up and restoration to ensure that it includes a review of business requirements, as well as the development, implementation, testing and documentation of the recovery plan. Procedures should be set up to ensure that back-ups are satisfying the above-mentioned requirements.

11.24 **Back-up Jobs**
CONTROL OBJECTIVE
Procedures should be in place to ensure back-ups are taken in accordance with the defined back-up strategy and the usability of back-ups is regularly verified.

11.25 **Back-up Storage**
CONTROL OBJECTIVE
Back-up procedures for IT-related media should include the proper storage of the data files, software and related documentation, both on-site and off-site. Back-ups should be stored securely and the storage sites periodically reviewed regarding physical access security and security of data files and other items.

11.26 **Archiving**
CONTROL OBJECTIVE
Management should implement a policy and procedures for ensuring that archival meets legal and business requirements, and is properly safeguarded and accounted for.

11.27 **Protection of Sensitive Messages**
CONTROL OBJECTIVE
Regarding data transmission over the Internet or any other public network, management should define and implement procedures and protocols to be used to ensure integrity, confidentiality and non-repudiation of sensitive messages.

11.28 **Authentication and Integrity**
CONTROL OBJECTIVE
The authentication and integrity of information originated outside the organisation, whether received by telephone, voicemail, paper document, fax or e-mail, should be appropriately checked before potentially critical action is taken.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

11.29 **Electronic Transaction Integrity**

CONTROL OBJECTIVE

Taking into consideration that the traditional boundaries of time and geography are less reliant, management should define and implement appropriate procedures and practices for sensitive and critical electronic transactions ensuring integrity and authenticity of:

- atomicity (indivisible unit of work, all of its actions succeed or they all fail)
- consistency (if the transaction cannot achieve a stable end state, it must return the system to its initial state)
- isolation (a transaction's behavior is not affected by other transactions that execute concurrently)
- durability (transaction's effects are permanent after it commits, its changes should survive system failures)

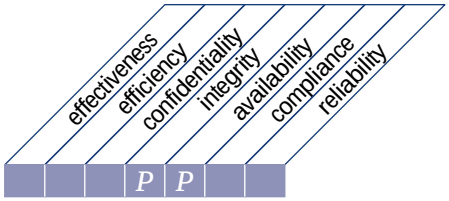
11.30 **Continued Integrity of Stored Data**

CONTROL OBJECTIVE

Management should ensure that the integrity and correctness of the data kept on files and other media (e.g., electronic cards) is checked periodically. Specific attention should be paid to value tokens, reference files and files containing privacy information.

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing facilities

that satisfies the business requirement

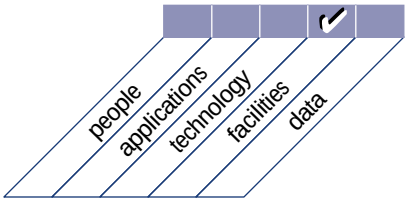
to provide a suitable physical surrounding which protects the IT equipment and people against man-made and natural hazards

is enabled by

the installation of suitable environmental and physical controls which are regularly reviewed for their proper functioning

and takes into consideration

- access to facilities
- site identification
- physical security
- inspection and escalation policies
- business continuity planning and crisis management
- personnel health and safety
- preventive maintenance policies
- environmental threat protection
- automated monitoring



DETAILED CONTROL OBJECTIVES

12 MANAGE FACILITIES

12.1 Physical Security

CONTROL OBJECTIVE

Appropriate physical security and access control measures should be established for IT facilities, including off-site use of information devices in conformance with the general security policy. Physical security and access controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media and any other elements required for the system's operation. Access should be restricted to individuals who have been authorised to gain such access. Where IT resources are located in public areas, they should be appropriately protected to prevent or deter loss or damage from theft or vandalism.

12.2 Low Profile of the IT Site

CONTROL OBJECTIVE

IT management should ensure a low profile is kept and the physical identification of the site of the IT operations is limited.

12.3 Visitor Escort

CONTROL OBJECTIVE

Appropriate procedures are to be in place ensuring that individuals who are not members of the IT function's operations group are escorted by a member of that group when they must enter the computer facilities. A visitor's log should be kept and reviewed regularly.

12.4 Personnel Health and Safety

CONTROL OBJECTIVE

Health and safety practices should be put in place and maintained in conformance with applicable international, national, regional, state and local laws and regulations.

12.5 Protection Against Environmental Factors

CONTROL OBJECTIVE

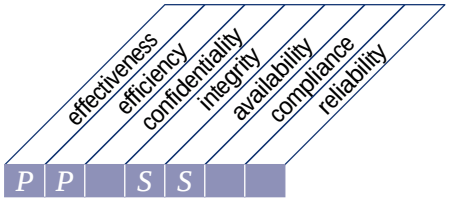
IT management should assure that sufficient measures are put in place and maintained for protection against environmental factors (e.g., fire, dust, power, excessive heat and humidity). Specialised equipment and devices to monitor and control the environment should be installed.

12.6 Uninterruptible Power Supply

CONTROL OBJECTIVE

Management should assess regularly the need for uninterruptable power supply batteries and generators for critical IT applications to secure against power failures and fluctuations. When justified, the most appropriate equipment should be installed.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing operations

that satisfies the business requirement

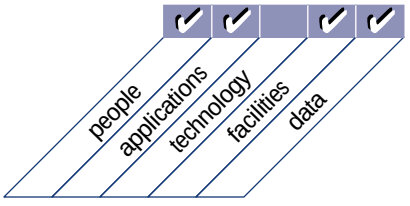
to ensure that important IT support functions are performed regularly and in an orderly fashion

is enabled by

a schedule of support activities which is recorded and cleared for the accomplishment of all activities

and takes into consideration

- operations procedure manual
- start-up process documentation
- network services management
- workload and personnel scheduling
- shift hand-over process
- system event logging
- coordination with change, availability and business continuity management
- preventive maintenance
- service level agreements
- automated operations
- incident logging, tracking and escalation



DETAILED CONTROL OBJECTIVES

13 MANAGE OPERATIONS

13.1 Processing Operations Procedures and Instructions Manual

CONTROL OBJECTIVE

IT management should establish and document standard procedures for IT operations (including network operations). All IT solutions and platforms in place should be operated using these procedures, which should be reviewed periodically to ensure effectiveness and adherence.

13.2 Start-up Process and Other Operations Documentation

CONTROL OBJECTIVE

IT management should ensure that the operations staff is adequately familiar and confident with the start-up process and other operations tasks by having them documented, periodically tested and adjusted when required.

13.3 Job Scheduling

CONTROL OBJECTIVE

IT management should ensure that the continuous scheduling of jobs, processes and tasks is organised into the most efficient sequence, maximising throughput and utilisation, to meet the objectives set in service level agreements. The initial schedules as well as changes to these schedules should be appropriately authorised.

13.4 Departures from Standard Job Schedules

CONTROL OBJECTIVE

Procedures should be in place to identify, investigate and approve departures from standard job schedules.

13.5 Processing Continuity

CONTROL OBJECTIVE

Procedures should require processing continuity during operator shift changes by providing for formal handover of activity, status updates and reports on current responsibilities.

13.6 Operations Logs

CONTROL OBJECTIVE

Management controls should guarantee that sufficient chronological information is being stored in operations logs to enable the reconstruction, review and examination of the time sequences of processing and the other activities surrounding or supporting processing.

13.7 Safeguard Special Forms and Output Devices

CONTROL OBJECTIVE

Management should establish appropriate physical safeguards over special forms, such as negotiable instruments, and over sensitive output devices, such as signature cartridges, taking into consideration proper accounting of IT resources, forms or items requiring additional protection and inventory management.

13.8 Remote Operations

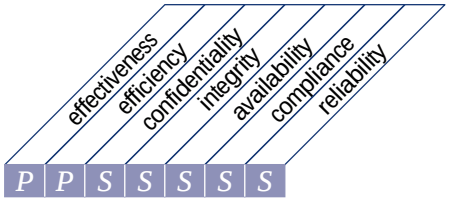
CONTROL OBJECTIVE

For remote operations, specific procedures should ensure that the connection and disconnection of the links to the remote site(s) are defined and implemented.

This page intentionally left blank

MONITORING

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

monitoring the processes

that satisfies the business requirement

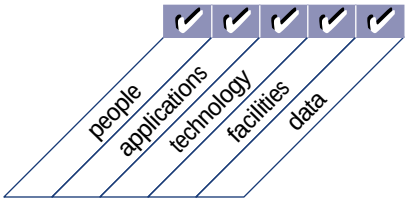
to ensure the achievement of the performance objectives set for the IT processes

is enabled by

the definition of relevant performance indicators, the systematic and timely reporting of performance and prompt acting upon deviations

and takes into consideration

- scorecards with performance drivers and outcome measures
- customer satisfaction assessments
- management reporting
- knowledge base of historical performance
- external benchmarking



DETAILED CONTROL OBJECTIVES

1 MONITOR THE PROCESSES

1.1 Collecting Monitoring Data

CONTROL OBJECTIVE

For the IT and internal control processes, management should ensure relevant performance indicators (e.g., benchmarks) from both internal and external sources are being defined, and that data is being collected for the creation of management information reports and exception reports regarding these indicators. Controls should also be aimed at validating the propriety and integrity of both organisational and individual performance measures and indicators.

1.2 Assessing Performance

CONTROL OBJECTIVE

Services to be delivered by the IT function should be measured (key performance indicators and/or critical success factors) by management and be compared with target levels. Assessments of the IT function should be performed on a continuous basis.

1.3 Assessing Customer Satisfaction

CONTROL OBJECTIVE

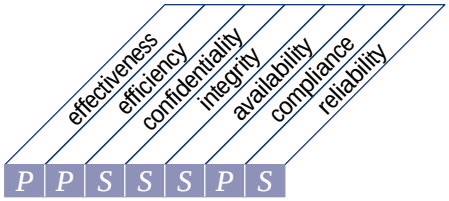
At regular intervals management should measure customer satisfaction regarding the services delivered by the IT function to identify shortfalls in service levels and establish improvement objectives.

1.4 Management Reporting

CONTROL OBJECTIVE

Management reports should be provided for senior management's review of the organisation's progress toward identified goals. Status reports should include the extent to which planned objectives have been achieved, deliverables obtained, performance targets met and risks mitigated. Upon review, appropriate management action should be initiated and controlled.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

assessing internal control adequacy

that satisfies the business requirement

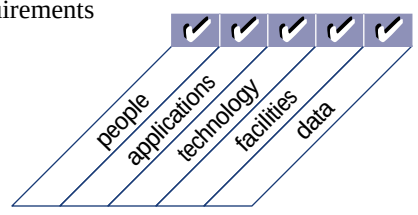
to ensure the achievement of the internal control objectives set for the IT processes

is enabled by

the commitment to monitoring internal controls, assessing their effectiveness, and reporting on them on a regular basis

and takes into consideration

- responsibilities for internal control
- ongoing internal control monitoring
- benchmarks
- error and exception reporting
- self-assessments
- management reporting
- compliance with legal and regulatory requirements



DETAILED CONTROL OBJECTIVES

2 ASSESS INTERNAL CONTROL ADEQUACY

2.1 Internal Control Monitoring

CONTROL OBJECTIVE

Management should monitor the effectiveness of internal controls in the normal course of operations through management and supervisory activities, comparisons, reconciliations and other routine actions. Deviations should evoke analysis and corrective action. In addition, deviations should be communicated to the individual responsible for the function and also at least one level of management above that individual. Serious deviations should be reported to senior management.

2.2 Timely Operation of Internal Controls

CONTROL OBJECTIVE

Reliance on internal controls requires that controls operate promptly to highlight errors and inconsistencies, and that these are corrected before they impact production and delivery. Information regarding errors, inconsistencies and exceptions should be kept and systematically reported to management.

2.3 Internal Control Level Reporting

CONTROL OBJECTIVE

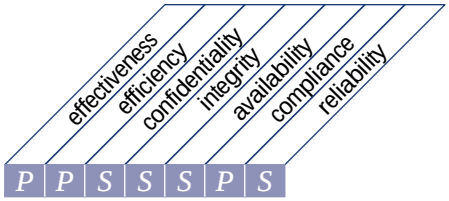
Management should report information on internal control levels and exceptions to the affected parties to ensure the continued effectiveness of its internal control system. Actions should be taken to identify what information is needed at a particular level of decision making.

2.4 Operational Security and Internal Control Assurance

CONTROL OBJECTIVE

Operational security and internal control assurance should be established and periodically repeated, with self-assessment or independent audit to examine whether or not the security and internal controls are operating according to the stated or implied security and internal control requirements. Ongoing monitoring activities by management should look for vulnerabilities and security problems.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

obtaining independent assurance

that satisfies the business requirement

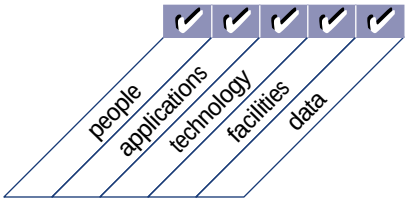
to increase confidence and trust among the organisation, customers, and third-party providers

is enabled by

independent assurance reviews carried out at regular intervals

and takes into consideration

- independent certifications and accreditation
- independent effectiveness evaluations
- independent assurance of compliance with laws and regulatory requirements
- independent assurance of compliance with contractual commitments
- third-party service provider reviews and benchmarking
- performance of assurance reviews by qualified personnel
- proactive audit involvement



DETAILED CONTROL OBJECTIVES

3 OBTAIN INDEPENDENT ASSURANCE

3.1 Independent Security and Internal Control Certification/Accreditation of IT Services

CONTROL OBJECTIVE

Management should obtain independent certification/accreditation of security and internal controls prior to implementing critical new IT services and re-certification/ re-accreditation of these services on a routine cycle after implementation.

3.2 Independent Security and Internal Control Certification/Accreditation of Third-Party Service Providers

CONTROL OBJECTIVE

Management should obtain independent certification/accreditation of security and internal controls prior to using IT service providers and re-certification/re-accreditation on a routine cycle.

3.3 Independent Effectiveness Evaluation of IT Services

CONTROL OBJECTIVE

Management should obtain independent evaluation of the effectiveness of IT services on a routine cycle.

3.4 Independent Effectiveness Evaluation of Third-Party Service Providers

CONTROL OBJECTIVE

Management should obtain independent evaluation of the effectiveness of IT service providers on a routine cycle.

3.5 Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments

CONTROL OBJECTIVE

Management should obtain independent assurance of the IT function's compliance with legal and regulatory requirements, and contractual commitments on a routine cycle.

3.6 Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments by Third-Party Service Providers

CONTROL OBJECTIVE

Management should obtain independent assurance of third-party service providers' compliance with legal and regulatory requirements and contractual commitments on a routine cycle.

3.7 Competence of Independent Assurance Function

CONTROL OBJECTIVE

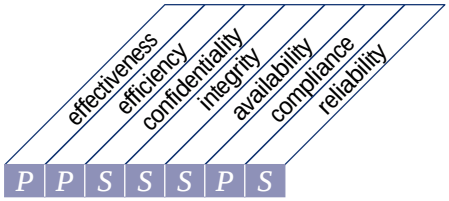
Management should ensure that the independent assurance function possesses the technical competence, and skills and knowledge necessary to perform such reviews in an effective, efficient and economical manner.

3.8 Proactive Audit Involvement

CONTROL OBJECTIVE

IT management should seek audit involvement in a proactive manner before finalising IT service solutions.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

providing for independent audit

that satisfies the business requirement

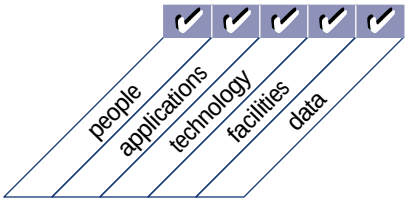
to increase confidence levels and benefit from best practice advice

is enabled by

independent audits carried out at regular intervals

and takes into consideration

- audit independence
- proactive audit involvement
- performance of audits by qualified personnel
- clearance of findings and recommendations
- follow-up activities
- impact assessments of audit recommendations (costs, benefits and risks)



DETAILED CONTROL OBJECTIVES

4 PROVIDE FOR INDEPENDENT AUDIT

4.1 Audit Charter

CONTROL OBJECTIVE

A charter for the audit function should be established by the organisation's senior management. This document should outline the responsibility, authority and accountability of the audit function. The charter should be reviewed periodically to assure that the independence, authority and accountability of the audit function are maintained.

4.2 Independence

CONTROL OBJECTIVE

The auditor should be independent from the auditee in attitude and appearance (actual and perceived). Auditors should not be affiliated with the section or department being audited, and, to the extent possible, should also be independent of the subject organisation itself. Thus, the audit function is to be sufficiently independent of the area being audited to permit objective completion of the audit.

4.3 Professional Ethics and Standards

CONTROL OBJECTIVE

The audit function should ensure adherence to applicable codes of professional ethics (e.g., Code of Professional Ethics of the Information Systems Audit and Control Association) and auditing standards (e.g., Standards for Information Systems Auditing of the Information Systems Audit and Control Association) in all that they do. Due professional care should be exercised in all aspects of the audit work, including the observance of applicable audit and IT standards.

4.4 Competence

CONTROL OBJECTIVE

Management should ensure that the auditors responsible for the review of the organisation's IT activities are technically competent and collectively possess the skills and knowledge (i.e., CISA domains) necessary to perform such reviews in an effective, efficient and economical manner. Management should ensure that audit staff assigned to information systems auditing tasks maintain their technical competence through appropriate continuing professional education.

4.5 Planning

CONTROL OBJECTIVE

Senior management should establish a plan to ensure that regular and independent audits are obtained regarding the effectiveness, efficiency and economy of security and internal control procedures, and management's ability to control IT function activities. Senior management should determine priorities with regard to obtaining independent audits within this plan. Auditors should plan the information systems audit work to address the audit objectives and to comply with applicable professional auditing standards.

4.6 Performance of Audit Work

CONTROL OBJECTIVE

Audits should be appropriately supervised to provide assurances that audit objectives are achieved and applicable professional auditing standards are met. Auditors should ensure that they obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

4.7 **Reporting**

CONTROL OBJECTIVE

The organisation's audit function should provide a report, in an appropriate form, to intended recipients upon the completion of audit work. The audit report should state the scope and objectives of the audit, the period of coverage, and the nature and extent of the audit work performed. The report should identify the organisation, the intended recipients and any restrictions on circulation. The audit report should also state the findings, conclusions and recommendations concerning the audit work performed, and any reservations or qualifications that the auditor has with respect to the audit.

4.8 **Follow-up Activities**

CONTROL OBJECTIVE

Resolution of audit comments rests with management. Auditors should request and evaluate appropriate information on previous findings, conclusions and recommendations to determine whether appropriate actions have been implemented in a timely manner.

APPENDICES

This page intentionally left blank

IT GOVERNANCE MANAGEMENT GUIDELINE

The following Management Guideline and Maturity Model identify the Critical Success Factors (CSFs), Key Goal Indicators (KGIs), Key Performance Indicators (KPIs) and Maturity Model for **IT governance.** First, IT governance is defined, articulating the business need. Next, the information criteria related to IT governance are identified. The business need is measured by the KGIs and enabled by a control statement, leveraged by all the IT resources. The achievement of the enabling control statement is measured by the KPIs, which consider the CSFs. The Maturity Model is used to evaluate an organisation's level of achievement of IT governance—from Non-existent (the lowest level) to Initial/Ad Hoc, to Repeatable but Intuitive, to Defined Process, to Managed and Measurable, to Optimised (the highest level). To achieve the Optimised maturity level for IT governance, an organisation must be at least at the Optimised level for the Monitoring domain and at least at the Managed and Measurable level for all other domains.

(See the COBIT *Management Guidelines* for a thorough discussion of the use of these tools.)

IT GOVERNANCE MANAGEMENT GUIDELINE

Governance over information technology and its processes with the business goal of adding value, while balancing risk versus return

ensures delivery of information to the business that addresses the required Information Criteria and is measured by Key Goal Indicators

is enabled by *creating and maintaining a system of process and control excellence appropriate for the business that directs and monitors the business value delivery of IT*

considers Critical Success Factors that leverage all IT Resources and is measured by Key Performance Indicators

Information Criteria
effectiveness
efficiency
confidentiality
integrity
availability
compliance
reliability

IT Resources
people
applications
technology
facilities
data

Critical Success Factors

- IT governance activities are integrated into the enterprise governance process and leadership behaviours
- IT governance focuses on the enterprise goals, strategic initiatives, the use of technology to enhance the business and on the availability of sufficient resources and capabilities to keep up with the business demands
- IT governance activities are defined with a clear purpose, documented and implemented, based on enterprise needs and with unambiguous accountabilities
- Management practices are implemented to increase efficient and optimal use of resources and increase the effectiveness of IT processes
- Organisational practices are established to enable: sound oversight; a control environment/culture; risk assessment as standard practice; degree of adherence to established standards; monitoring and follow up of control deficiencies and risks
- Control practices are defined to avoid breakdowns in internal control and oversight
- There is integration and smooth interoperability of the more complex IT processes such as problem, change and configuration management
- An audit committee is established to appoint and oversee an independent auditor, focusing on IT when driving audit plans, and review the results of audits and third-party reviews.

Key Goal Indicators

- Enhanced performance and cost management
- Improved return on major IT investments
- Improved time to market
- Increased quality, innovation and risk management
- Appropriately integrated and standardised business processes
- Reaching new and satisfying existing customers
- Availability of appropriate bandwidth, computing power and IT delivery mechanisms
- Meeting requirements and expectations of the customer of the process on budget and on time
- Adherence to laws, regulations, industry standards and contractual commitments
- Transparency on risk taking and adherence to the agreed organisational risk profile
- Benchmarking comparisons of IT governance maturity
- Creation of new service delivery channels

Key Performance Indicators

- Improved cost-efficiency of IT processes (costs vs. deliverables)
- Increased number of IT action plans for process improvement initiatives
- Increased utilisation of IT infrastructure
- Increased satisfaction of stakeholders (survey and number of complaints)
- Improved staff productivity (number of deliverables) and morale (survey)
- Increased availability of knowledge and information for managing the enterprise
- Increased linkage between IT and enterprise governance
- Improved performance as measured by IT balanced scorecards

IT Governance Maturity Model

Governance over information technology and its processes with the business goal of adding value, while balancing risk versus return

0 Non-existent There is a complete lack of any recognisable IT governance process. The organisation has not even recognised that there is an issue to be addressed and hence there is no communication about the issue.

1 Initial / Ad Hoc There is evidence that the organisation has recognised that IT governance issues exist and need to be addressed. There are, however, no standardised processes, but instead there are ad hoc approaches applied on an individual or case-by-case basis. Management's approach is chaotic and there is only sporadic, non-consistent communication on issues and approaches to address them. There may be some acknowledgement of capturing the value of IT in outcome-oriented performance of related enterprise processes. There is no standard assessment process. IT monitoring is only implemented reactively to an incident that has caused some loss or embarrassment to the organisation.

2 Repeatable but Intuitive There is global awareness of IT governance issues. IT governance activities and performance indicators are under development, which include IT planning, delivery and monitoring processes. As part of this effort, IT governance activities are formally established into the organisation's change management process, with active senior management involvement and oversight. Selected IT processes are identified for improving and/or controlling core enterprise processes and are effectively planned and monitored as investments, and are derived within the context of a defined IT architectural framework. Management has identified basic IT governance measurements and assessment methods and techniques, however, the process has not been adopted across the organisation. There is no formal training and communication on governance standards and responsibilities are left to the individual. Individuals drive the governance processes within various IT projects and processes. Limited governance tools are chosen and implemented for gathering governance metrics, but may not be used to their full capacity due to a lack of expertise in their functionality.

3 Defined Process The need to act with respect to IT governance is understood and accepted. A baseline set of IT governance indicators is developed, where linkages between outcome measures and performance drivers are defined, documented and integrated into strategic and operational planning and monitoring processes. Procedures have been standardised, documented and implemented. Management has communicated standardised procedures and informal training is established. Performance indicators over all IT governance activities are being recorded and tracked, leading to enterprise-wide improvements. Although measurable, procedures are not sophisticated, but are the formalisation of existing practices. Tools are standardised, using currently available techniques. IT Balanced Business Scorecard ideas are being adopted by the organization. It is, however, left to the individual to get training, to follow the standards and to apply them. Root cause analysis is only occasionally applied. Most processes are monitored against some (baseline) metrics, but any deviation, while mostly being acted upon by individual initiative, would unlikely be detected by management. Nevertheless, overall accountability of key process performance is clear and management is rewarded based on key performance measures.

4 Managed and Measurable There is full understanding of IT governance issues at all levels, supported by formal training. There is a clear understanding of who the customer is and responsibilities are defined and monitored through service level agreements. Responsibilities are clear and process ownership is established. IT processes are aligned with the business and with the IT strategy. Improvement in IT processes is based primarily upon a quantitative understanding and it is possible to monitor and measure compliance with procedures and process metrics. All process stakeholders are aware of risks, the importance of IT and the opportunities it can offer. Management has defined tolerances under which processes must operate. Action is taken in many, but not all cases where processes appear not to be working effectively or

efficiently. Processes are occasionally improved and best internal practices are enforced. Root cause analysis is being standardised. Continuous improvement is beginning to be addressed. There is limited, primarily tactical, use of technology, based on mature techniques and enforced standard tools. There is involvement of all required internal domain experts. IT governance evolves into an enterprise-wide process. IT governance activities are becoming integrated with the enterprise governance process.

5 Optimised There is advanced and forward-looking understanding of IT governance issues and solutions. Training and communication is supported by leading-edge concepts and techniques. Processes have been refined to a level of external best practice, based on results of continuous improvement and maturity modeling with other organisations. The implementation of these policies has led to an organisation, people and processes that are quick to adapt and fully support IT governance requirements. All problems and deviations are root cause analysed and efficient action is expediently identified and initiated. IT is used in an extensive, integrated and optimised manner to automate the workflow and provide tools to improve quality and effectiveness. The risks and returns of the IT processes are defined, balanced and communicated across the enterprise. External experts are leveraged and benchmarks are used for guidance. Monitoring, self-assessment and communication about governance expectations are pervasive within the organisation and there is optimal use of technology to support measurement, analysis, communication and training. Enterprise governance and IT governance are strategically linked, leveraging technology and human and financial resources to increase the competitive advantage of the enterprise.

COBIT PROJECT DESCRIPTION

The COBIT project continues to be supervised by a Project Steering Committee formed by international representatives from industry, academia, government and the security and control profession. The Project Steering Committee has been instrumental in the development of the COBIT *Framework* and in the application of the research results. International working groups were established for the purpose of quality assurance and expert review of the project's interim research and development deliverables. Overall project guidance is provided by the IT Governance Institute.

RESEARCH AND APPROACH FOR EARLIER DEVELOPMENT

Starting with the COBIT *Framework* defined in the 1st edition, the application of international standards and guidelines and research into best practices have led to the development of the control objectives. Audit guidelines were next developed to assess whether these control objectives are appropriately implemented.

Research for the 1st and 2nd editions included the collection and analysis of identified international sources and was carried out by teams in Europe (Free University of Amsterdam), the US (California Polytechnic University) and Australia (University of New South Wales). The researchers were charged with the compilation, review, assessment and appropriate incorporation of international technical standards, codes of conduct, quality standards, professional standards in auditing and industry practices and requirements, as they relate to the *Framework* and to individual control objectives. After collection and analysis, the researchers were challenged to examine each domain and process in depth and suggest new or modified control objectives applicable to that particular IT process. Consolidation of the results was performed by the COBIT Steering Committee and the Director of Research of ISACF.

RESEARCH AND APPROACH FOR THE 3RD EDITION

The COBIT 3rd Edition project consisted of developing the *Management Guidelines* and updating COBIT 2nd Edition based on new and revised international references.

Furthermore, the COBIT *Framework* was revised and enhanced to support increased management control, to introduce performance management and to further develop IT governance. In order to provide management with an application of the *Framework* so that it can assess and make choices for control implementation and improvements over its information and related technology, as well as measure performance, the *Management Guidelines* include Maturity Models, Critical Success Factors, Key Goal Indicators and Key Performance Indicators related to the *Control Objectives*.

Management Guidelines was developed by using a worldwide panel of 40 experts from industry, academia, government and the IT security and control profession. These experts participated in a residential workshop guided by professional facilitators and using development guidelines defined by the COBIT Steering Committee. The workshop was strongly supported by the Gartner Group and PricewaterhouseCoopers, who not only provided thought leadership but also sent several of their experts on control, performance management and information security. The results of the workshop were draft Maturity Models, Critical Success Factors, Key Goal Indicators and Key Performance Indicators for each of COBIT's 34 high-level control objectives. Quality assurance of the initial deliverables was conducted by the COBIT Steering Committee and the results were posted for exposure on the ISACA web site. The *Management Guidelines* document was finally prepared to offer a new management-oriented set of tools, while providing integration and consistency with the COBIT *Framework*.

The update to the *Control Objectives*, based on new and revised international references, was conducted by members of ISACA chapters, under the guidance of COBIT Steering Committee members. The intention was not to perform a global analysis of all material or a redevelopment of the *Control Objectives*, but to provide an incremental update process.

The results of the development of the *Management Guidelines* were then used to revise the COBIT *Framework*, especially the considerations, goals and enabler statements of the high-level control objectives.

COBIT PRIMARY REFERENCE MATERIAL

COSO: Committee of Sponsoring Organisations of the Treadway Commission. *Internal Control — Integrated Framework.* 2 Vols. American Institute of Certified Accountants, New Jersey, 1994.

OECD Guidelines: Organisation for Economic Co-operation and Development. *Guidelines for the Security of Information,* Paris, 1992.

DTI Code of Practice for Information Security Management: Department of Trade and Industry and British Standard Institute. *A Code of Practice for Information Security Management,* London, 1993, 1995.

ISO 9000-3: International Organisation for Standardisation. *Quality Management and Quality Assurance Standards — Part 3: Guidelines for the Application of ISO 9001 to the development, supply and maintenance of software,* Switzerland, 1991.

An Introduction to Computer Security: The NIST Handbook: NIST Special Publication 800-12, National Institute of Standards and Technology, U.S. Department of Commerce, Washington, DC, 1995.

ITIL IT Management Practices: Information Technology Infrastructure Library. Practices and guidelines developed by the Central Computer and Telecommunications Agency (CCTA), London, 1989.

IBAG Framework: Draft Framework from the Infosec Business Advisory Group to SOGIS (Senior Officials Group on Information Security, advising the European Commission), Brussels, 1994.

NSW Premier's Office Statements of Best Practices and Planning Information Management and Techniques: *Statements of Best Practice #1 through #6.* Premier's Department New South Wales, Government of New South Wales, Australia, 1990 through 1994.

Memorandum Dutch Central Bank: *Memorandum on the Reliability and Continuity of Electronic Data Processing in Banking.* De Nederlandsche Bank, Reprint from Quarterly Bulletin #3, Netherlands, 1998.

EDPAF Monograph #7, EDI: An Audit Approach: Jamison, Rodger. *EDI: An Audit Approach,* Monograph Series #7, Information Systems Audit and Control Foundation, Inc., Rolling Meadows, IL, April 1994.

PCIE (President's Council on Integrity and Efficiency) Model Framework: *A Model Framework for Management Over Automated Information Systems.* Prepared jointly by the President's Council on Management Improvement and the President's Council on Integrity and Efficiency, Washington, DC, 1987.

Japan Information Systems Auditing Standards: *Information System Auditing Standard of Japan.* Provided by the Chuo Audit Corporation, Tokyo, August 1994.

CONTROL OBJECTIVES Controls in an Information Systems Environment: Control Guidelines and Audit Procedures: EDP Auditors Foundation (now the Information Systems Audit and Control Foundation), Fourth Edition, Rolling Meadows, IL, 1992.

CISA Job Analysis: Information Systems Audit and Control Association Certification Board. "Certified Information Systems Auditor Job Analysis Study," Rolling Meadows, IL, 1994.

IFAC International Information Technology Guidelines—Managing Security of Information: International Federation of Accountants, New York, 1998.

IFAC International Guidelines on Information Technology Management—Managing Information Technology Planning for Business Impact: International Federation of Accountants, New York, 1999.

Guide for Auditing for Controls and Security, A System Development Life Cycle Approach: *NIST Special Publication 500-153:* National Institute of Standards and Technology, U.S. Department of Commerce, Washington, DC, 1988.

Government Auditing Standards: US General Accounting Office, Washington, DC, 1999.

SPICE: Software Process Improvement and Capability Determination. A standard on software process improvement, British Standards Institution, London, 1995.

Denmark Generally Accepted IT Management Practices: The Institute of State Authorized Accountants, Denmark, 1994.

DRI International, Professional Practices for Business Continuity Planners: Disaster Recovery Institute International. *Guideline for Business Continuity Planners*, St. Louis, MO, 1997.

IIA, SAC Systems Audibility and Control: Institute of Internal Auditors Research Foundation, *Systems Audibility and Control Report*, Altamonte Springs, FL, 1991, 1994.

IIA, Professional Practices Pamphlet 97-1, Electronic Commerce: Institute of Internal Auditors Research Foundation, Altamonte Springs, FL, 1997.

E & Y Technical Reference Series: Ernst & Young, *SAP R/3 Audit Guide*, Cleveland, OH, 1996.

C & L Audit Guide SAP R/3: Coopers & Lybrand, *SAP R/3: Its Use, Control and Audit*, New York, 1997.

ISO IEC JTC1/SC27 Information Technology — Security: International Organisation for Standardisation (ISO) Technical Committee on Information Technology Security, Switzerland, 1998.

ISO IEC JTC1/SC7 Software Engineering: International Organisation for Standardisation (ISO) Technical Committee on Software Process Assessment. *An Assessment Model and Guidance Indicator,* Switzerland, 1992.

ISO TC68/SC2/WG4, Information Security Guidelines for Banking and Related Financial Services: International Organisation for Standardisation (ISO) Technical Committee on Banking and Financial Services, Draft, Switzerland, 1997.

Common Criteria and Methodology for Information Technology Security Evaluation: CSE (Canada), SCSSI (France), BSI (Germany), NLNCSA (Netherlands), CESG (United Kingdom), NIST (USA) and NSA (USA), 1999.

Recommended Practice for EDI: EDIFACT (EDI for Administration Commerce and Trade), Paris, 1987.

TickIT: *Guide to Software Quality Management System Construction and Certification*. British Department of Trade and Industry (DTI), London, 1994

ESF Baseline Control—Communications: European Security Forum, London. *Communications Network Security*, September 1991; *Baseline Controls for Local Area Networks*, September, 1994.

ESF Baseline Control—Microcomputers: European Security Forum, London. *Baseline Controls Microcomputers Attached to Network*, June 1990.

Computerized Information Systems (CIS) Audit Manual: EDP Auditors Foundation (now the Information Systems Audit and Control Foundation), Rolling Meadows, IL, 1992.

Standards for Internal Control in the Federal Government (GAO/AIMD-00-21.3.1): US General Accounting Office, Washington, DC 1999.

Guide for Developing Security Plans for Information Technology: NIST Special Publication 800-18, National Institute for Standards and Technology, US Department of Commerce, Washington, DC, 1998.

Financial Information Systems Control Audit Manual (FISCAM): US General Accounting Office, Washington, DC, 1999.

BS7799-Information Security Management: British Standards Institute, London, 1999.

CICA Information Technology Control Guidelines, 3rd Edition: Canadian Institute of Chartered Accountants, Toronto, 1998.

ISO/IEC TR 1335-n Guidelines for the Management of IT Security (GMITS), Parts 1-5: International Organisation for Standardisation, Switzerland, 1998.

AICPA/CICA SysTrust™ Principles and Criteria for Systems Reliability, Version 1.0: American Institute of Certified Public Accountants, New York, and Canadian Institute of Chartered Accountants, Toronto, 1999.

Glossary of Terms

AICPA	American Institute of Certified Public Accountants
CICA	Canadian Institute of Chartered Accountants
CISA	Certified Information Systems Auditor
CCEB	Common Criteria for Information Technology Security
Control	The policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected
COSO	Committee of Sponsoring Organisations of the Treadway Commission
DRI	Disaster Recovery Institute International
DTI	Department of Trade and Industry of the United Kingdom
EDIFACT	Electronic Data Interchange for Administration, Commerce and Trade
EDPAF	Electronic Data Processing Auditors Foundation (now ISACF)
ESF	European Security Forum, a cooperation of 70+ primarily European multi-nationals with the goal of researching common security and control issues in IT
GAO	US General Accounting Office
I4	International Information Integrity Institute, similar association as the ESF, with similar goals but primarily US-based and run by Stanford Research Institute
IBAG	Infosec Business Advisory Group, industry representatives who advise the Infosec Committee. This Committee is composed of government officials of the European Community and itself advises the European Commission on IT security matters.
IFAC	International Federation of Accountants
IIA	Institute of Internal Auditors
INFOSEC	Advisory Committee for IT Security Matters to the European Commission
ISACA	Information Systems Audit and Control Association
ISACF	Information Systems Audit and Control Foundation
ISO	International Organisation for Standardisation (with offices in Geneva, Switzerland)
ISO9000	Quality management and quality assurance standards as defined by ISO
IT Control Objective	A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity
ITIL	Information Technology Infrastructure Library
ITSEC	Information Technology Security Evaluation Criteria. The harmonised criteria of France, Germany, the Netherlands and the United Kingdom, since then also supported by the European Commission (see also TCSEC, the US equivalent).
NBS	National Bureau of Standards of the US
NIST (formerly NBS)	National Institute of Standards and Technology, based in Washington, DC
NSW	New South Wales, Australia
OECD	Organisation for Economic Cooperation and Development
OSF	Open Software Foundation
PCIE	President's Council on Integrity and Efficiency
SPICE	Software Process Improvement and Capability Determination—a standard on software process improvement
TCSEC	Trusted Computer System Evaluation Criteria, also known as The Orange Book: security evaluation criteria for computer systems as originally defined by the US Department of Defense. See also ITSEC, the European equivalent.
TickIT	Guide to Software Quality Management System Construction and Certification

INDEX

INDEX

INDEX

INDEX

GOVERNANCE INSTITUTE™

3701 ALGONQUIN ROAD, SUITE 1010
ROLLING MEADOWS, ILLINOIS 60008, USA

TELEPHONE: +1.847.253.1545
FACSIMILE: +1.847.253.1443
E-MAIL: research@isaca.org
WEB SITES: *www.ITgovernance.org*
www.isaca.org

TELL US WHAT YOU THINK ABOUT COBIT

We are interested in knowing your reaction to *COBIT: Control Objectives for Information and related Technology*. Please provide your comments below.

_____

_____

_____

_____

_____

_____

_____

_____

Name _____

Company _____

Address _____

City _____ State/Province _____

Country _____ ZIP/Postal Code _____

FAX Number _____

E-mail Address _____

☐ I am interested in learning more about how COBIT can be used in my organisation. Please ask a representative to contact me.

☐ Please send me more information about:

- ☐ Purchasing other COBIT products
- ☐ COBIT Training Courses (in-house or general session)
- ☐ Certified Information Systems Auditor™ (CISA®) Certification
- ☐ *Information Systems Control Journal*
- ☐ Information Systems Audit and Control Association (ISACA)

Thank you!

All respondents will be acknowledged.

Elixender Lamprea León.
Ing. de Sistemas, C.I.V. No. 93.724
Tel.: 0276-3431268, 0414-7077227
San Cristóbal, Edo. Táchira, Venezuela (2004)

OBJETIVO: Análisis, Desarrollo, Aplicación, Consultoría y Auditoria de la Función Informática y las Tecnologías de Información en las Organizaciones. Docencia relacionada con las áreas del conocimiento relacionadas con las Tecnologías de Información y Comunicaciones.

Educación:	
Superior:	Postgrado: Especialización en Sistemas de Información, UCAB / UCAT, 2004
	Pregrado: Ingeniería de Sistemas U.N.A., Táchira 1994
	Técnica: Análisis y Programación de Sistemas Instituto Francisco J. Caldas, Bogotá, 1980
Docente:	Enfoque Didáctico en Educación Superior UCAT, Táchira, 2001
	Planificación de la Enseñanza Instituto Politécnico Santiago Mariño, Táchira, 1999
	Evaluación de los Aprendizajes UCAT, Táchira, 2000
Técnica:	Aplicaciones Microsoft Office ASTECC, Táchira, 1999
	Instalación de Redes Instituto Universitario de Tecnología, Táchira, 1996
	Diseño Grafico Computarizado Corel Draw Universidad de los Andes, Táchira, 1997
	Evaluación del Desempeño Centro de Altos Estudios, Táchira, 1997
	Sistema Operativo UNIX, Administración UNIX, Lenguaje "C", System Administrador, Base de Datos Informix-SQL, Lenguaje Informix-4GL Centro de Estudios NCR SUMMA SISTEMAS Maracaibo, 1987
	Programación R.P.G II ESPRINCA, Táchira, 1981

Varios:	
	Organizador I Jornadas de Informática Instituto Universitario de Tecnología IUTAI, San Cristóbal Junio, 2001
	Participante Congreso Iberoamericano de Educación e Informática UNESCO, OCEI, CREI, Caracas 1992
	Participante, Congreso Nacional sobre Informática Educativa ULA, Merida, 1994
	Autor de la Columna: "Informática PRO2000", Diario La Nación Tachira, 1998, 1999
	Coautor del Proyecto "Metodología para el Desarrollo de Sistemas de Información" en la Administración Pública Nacional. Representante por Foncafé ante la O.C.E.I, Caracas. 1991
	Tesis de Pregrado Ingeniería de Sistemas: "Sistema Integrado Contable-Presupuestario para el Plan Único de Cuentas Públicas, SICOP-FONCAFE, Puntuación: 10/10, U.N.A. Táchira, 1994

Experiencia Profesional y Docente	
Profesional:	Carlos García & Asociados, Consultor, Auditor de Sistemas, Instructor de Aplicaciones y Bases de Datos, 1990 - Actual
	Compañía Anónima de Electricidad de Los Andes CADELA Instructor de Curso sobre Auditoria Informática. Gerencia de Contraloría, 2003.
	Asistencia Técnica en Computación y Comunicaciones, ASTECC C.A Consultor, Coordinador de Proyectos, Táchira, 1993 - Actual
	INDRA Sistemas, Coordinador de Soporte Técnico del Estado Táchira, 2000
	Fondo Nacional del Café, FONCAFE, Gerente de Sistemas, Jefe de Informática III (1986-1999) Gerente de Planificación y Evaluación (Encargado eventual)
	MORCA Computación, Integrador de Sistemas e Instructor Informático, Auditor de Sistemas, Táchira, 1999
	Fundación CIARA, Instructor de Base de Datos y Aplicaciones Informix SQL – 4GL, Caracas, 1998
	Lafarge, Cementos Táchira, Instructor y Consultor en el área de Aplicaciones Informáticas, Táchira, 1996
	Contraloría General del Estado Táchira, Instructor y Consultor en Sistema Operativo UNIX, Táchira, 1996
	Administración y Organización Técnica, AOTEC, Coordinador Educativo en el Area de Sistemas, Táchira, 1987
	Estudios y Proyectos en Informática ESPRINCA Analista de Sistemas, Táchira, 1986
	ProInformática Analista de Sistemas, Táchira 1984
	Turismo de Montaña, Turymsa. Analista de Sistemas, Táchira 1984
Docente:	Universidad Católica del Táchira, Escuela de Administración Docente, Area de Informática, 1999 - Actual
	Instituto Universitario de Tecnología Agroindustrial IUTAI San Cristóbal, Docente, Departamento de Informática, 2000 - Actual
	Instituto Politécnico Santiago Mariño, Docente, Departamento de Ingeniería de Sistemas, Táchira, 1998-2000
	Escuela Superior de Educación Continua ESEC – IUFRONT Instructor, Area Informática, Táchira, 2000

Datos Personales:	
	Fecha de Nacimiento: 01-01-1960
	Nacionalidad: Venezolana
	Estado Civil: Casado
	Residencia: Urb. Monterrey, Edif. 10, Apto. No. 27, San Cristóbal, Edo. Táchira, Venezuela. Tel.: 0276-3431268
	Contactos: 0414-7077227, elixender@cantv.net
	Identificación: Cedula Id. No. V-13.793.899
	Gremios: Colegio de Ingenieros de Venezuela, CIV No. 93724
	Asociación de Profesores IUT-AI San Cristóbal