COBIT: MODELO PARA AUDITORIA Y CONTROL DE SISTEMAS DE INFORMACIÓN

10 DE MAYO 2007 BOLETIN 54

La evaluación de los requerimientos del negocio, los recursos y procesos IT, son puntos bastante importantes para el buen funcionamiento de una compañía y para el aseguramiento de su supervivencia en el mercado.

El COBIT es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso.

El COBIT es un modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad IT y que abarca controles específicos de IT desde una perspectiva de negocios.

Las siglas COBIT significan Objetivos de Control para Tecnología de Información y Tecnologías relacionadas (Control Objectives for Information Systems and related Technology). El modelo es el resultado de una investigación con expertos de varios países, desarrollado por ISACA (Information Systems Audit and Control Association).

COBIT, lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de tecnología. Vinculando tecnología informática y prácticas de control, el modelo 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 los computadores personales y las redes. Está basado en la filosofía de que los recursos 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.

La estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.

"La adecuada implementación de un modelo COBIT en una organización, provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que aseguran que los procesos y recursos de información y tecnología contribuyen al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado.

UNIVERSIDAD EAFIT
Consultorio Contable
Proyección Empresarial

Área de Auditoria y Control

UNIVERSIDAD EAFIT
Abierta al mundo
Acreditada Institucionalmente por el Ministerio de Educación Nacional

El conjunto de lineamientos y estándares internacionales conocidos como COBIT, define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro "dominios" principales, a saber:

PLANIFICACION Y ORGANIZACION:

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.

- ADQUISION E IMPLANTACION:

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.

- SOPORTE Y SERVICIOS:

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.

- MONITOREO:

Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

Estos dominios agrupan objetivos de control de alto nivel, que cubren tanto los aspectos de información, como de la tecnología que la respalda. Estos dominios y objetivos de control facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

USUARIOS:

• La Gerencia: para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.

• Los Usuarios Finales: quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.

• 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.

• 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.

CARACTERISTICAS:

• Orientado al negocio
• Alineado con estándares y regulaciones "de facto"
• Basado en una revisión crítica y analítica de las tareas y actividades en TI
• Alineado con estándares de control y auditoria (COSO, IFAC, IIA, ISACA, AICPA)

PRINCIPIOS

El enfoque del control en TI 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.

Requerimientos de la información del negocio:
Para alcanzar los requerimientos de negocio, la información necesita satisfacer ciertos criterios:

Requerimientos de Calidad: Calidad, Costo y Entrega.
Requerimientos Fiduciarios: Efectividad y Eficiencia operacional, Confiabilidad de los reportes financieros y Cumplimiento le leyes y regulaciones.

EFECTIVIDAD

La información debe ser relevante y pertinente para los procesos del negocio y debe ser proporcionada en forma oportuna, correcta, consistente y utilizable.

EFICIENCIA

Se debe proveer información mediante el empleo óptimo de los recursos (la forma más productiva y económica).

CONFIABILIDAD

proveer la información apropiada para que la administración tome las decisiones adecuadas para manejar la empresa y cumplir con sus responsabilidades.

CUMPLIMIENTO

de las leyes, regulaciones y compromisos contractuales con los cuales está comprometida la empresa.

Requerimientos de Seguridad: Confidencialidad, Integridad y Disponibilidad

CONFIDENCIALIDAD

Protección de la información sensible contra divulgación no autorizada.

INTEGRIDAD

Refiere a lo exacto y completo de la información así como a su validez de acuerdo con las expectativas de la empresa.

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.

En COBIT se establecen los siguientes recursos en TI necesarios para alcanzar los objetivos de negocio:

DATOS

Todos los objetos de información. Considera información interna y externa, estructurada o no, gráficas, sonidos, etc.

APLICACIONES

Entendidas como sistemas de información, que integran procedimientos manuales y sistematizados.

TECNOLOGÍA

incluye hardware y software básico, sistemas operativos, sistemas de administración de bases de datos, de redes, telecomunicaciones, multimedia, etc.

INSTALACIONES

Incluye los recursos necesarios para alojar y dar soporte a los sistemas de información.

RECURSO HUMANO

Por la habilidad, conciencia y productividad del personal para planear, adquirir, prestar servicios, dar soporte y monitorear los sistemas de Información, o de procesos de TI.

TECNOLOGIAS DE INFORMACIÓN

Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de la Tecnología de Información (TI) relacionada. En esta sociedad global (donde la información viaja a través del "ciberespacio" sin las restricciones de tiempo, distancia y velocidad) esta criticidad emerge de:

> La creciente dependencia en información y en los sistemas que proporcionan dicha información
> La creciente vulnerabilidad y un amplio espectro de amenazas, tales como las "ciber amenazas" y la guerra de información
> El costo de las inversiones actuales y futuras en información y en tecnología de información; y
> El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos.

Para muchas organizaciones, la información y la tecnología que la respalda, representan los activos más valiosos de la empresa, por lo que la gestión de los riesgos asociados de la Tecnología de Información, o Gobernabilidad de TI (IT Governance), ha ganado notoriedad en tiempos recientes como un aspecto clave de la gobernabilidad corporativa, dada su capacidad de proporcionar valor agregado al negocio, balanceando la relación entre el riesgo y el retorno de la inversión sobre TI y sus procesos. Estos aspectos se enfatizan en el Marco de referencia COBIT, el cual se define como conjunto de Objetivos de Control para la Información y Tecnologías Relacionadas.

Bajo este escenario, una adecuada administración de los recursos de TI es fundamental para mejorar la calidad de los productos y servicios brindados por el área, lo que se reflejará en mejoras en los procesos que respalda, y en el nivel de seguridad y control con el cual se trabaja, elevando su capacidad para satisfacer los objetivos de cumplimiento definidos en la estructura d e control interno de la organización, reduciendo además los costos administrativos asociados al entorno informático.

(COBIT), define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro (4) "dominios" principales, a saber:
- Planificación y organización
- Adquisición e implantación
- Soporte y Servicios
- Monitoreo

Estos dominios agrupan objetivos de control de alto nivel, que cubren tanto los aspectos de información, como de la tecnología que la respalda. En conjunto, estos dominios y los objetivos de control, facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. Asimismo, se deben tomar en cuenta los recursos que proporciona la Tecnología de Información, tales como: datos, sistemas de aplicación, tecnología (plataformas), instalaciones y el recurso humano.