Instituto de Auditoría Interna de El Salvador

IV CONAUDI 2016 25 y 26 AGOSTO HOTEL REAL INTERCONTINENTAL

CONGRESO NACIONAL DE AUDITORIA INTERNA

del 25 al 26 de agosto de 2016

Hotel Real Intercontinental, San Salvador

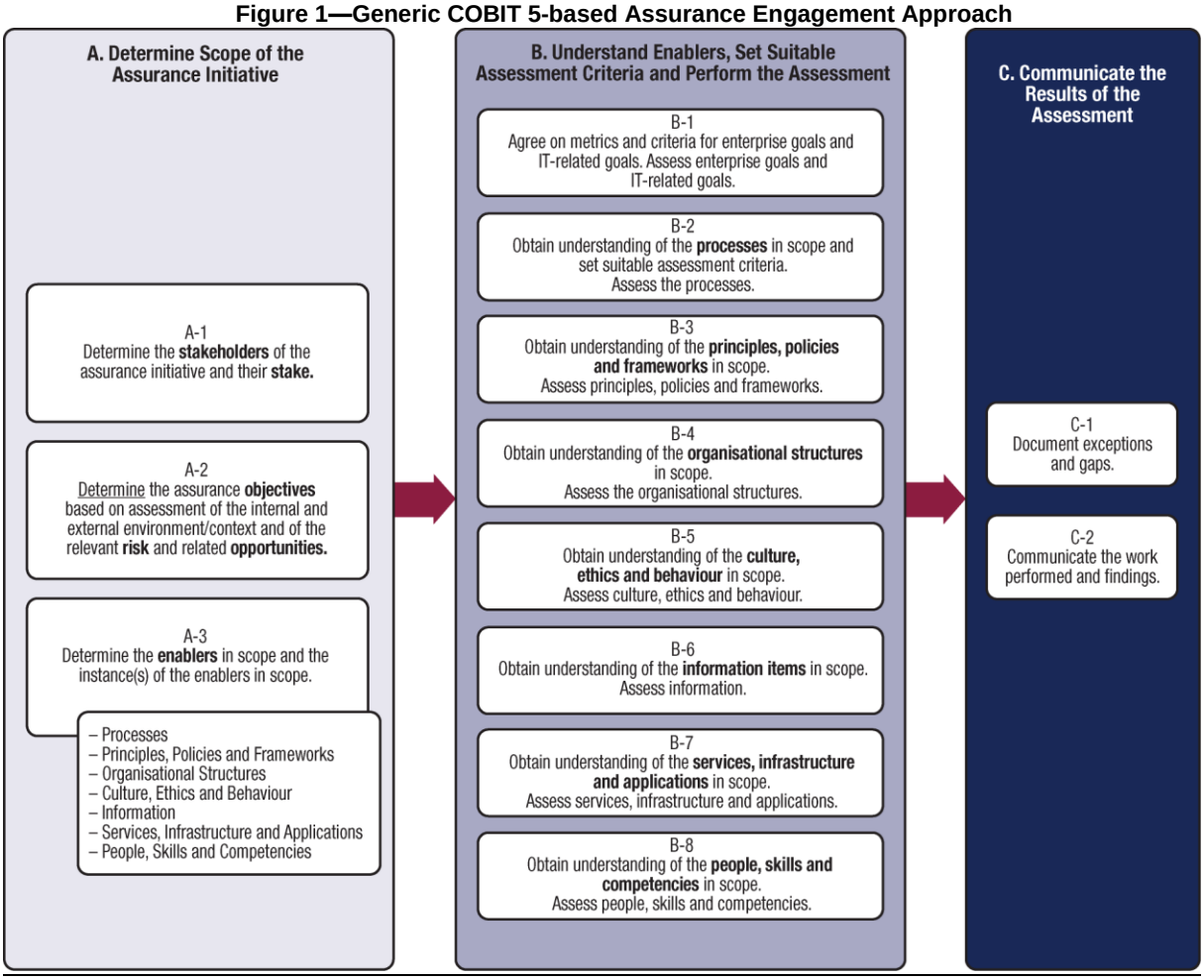
"Programa de Auditoría de la Seguridad de la Información enfocada en la Cyberseguridad"

Hotel Real Intercontinental, San Salvador, El Salvador
Jueves 25 y viernes 26 de agosto de 2016

Introducción

Este programa está basado en el proceso genérico de aseguramiento desarrollado en la sección 2B del libro COBIT 5 para aseguramiento.

Figure 1—Generic COBIT 5-based Assurance Engagement Approach



Notas importantes

La ejecución de este programa requiere que el Auditor de Sistemas cuente con los siguientes conocimientos:

1. Soluciones técnicas de seguridad, tales como Firewalls, dispositivos de análisis de vulnerabilidades, correlacionadores de eventos y similares.
2. Conocimientos de COBIT 5 para aseguramiento.
3. Conocimiento del framework de Cyberseguridad del NIST.
4. El auditor de Sistemas deberá de utilizar su criterio profesional en la definición del alcance de la auditoría y los criterios de evaluación adecuados para el contexto de la organización en la que se aplica.

Auditoría: Gestión de la Seguridad de la Información.

Tema de la Auditoría

El Sistema de gestión de la seguridad implementado para cubrir riesgos de cyberseguridad*.*

Objetivo de la revisión

Proveer aseguramiento de que los controles implementados para mitigar riesgos de cyberseguridad son razonables para contribuir con los objetivos de la organización y que su implementación es eficiente.

Alcance

El alcance está basado en los catalizadores de COBIT 5 que más contribuyen con la Seguridad de la Información: las políticas, la organización, los procesos, la información, la infraestructura y el personal.

El enfoque de aseguramiento basado en COBIT 5

El programa de auditoría está dividido en tres secciones:

- **Fase A—Determinar el alcance de la auditoría**—En esta fase, el auditor define el alcance de la auditoría en función de los catalizadores implementados en la organización. En esta fase el auditor debe de entender los objetivos de la organización y como los catalizadores están contribuyendo con ellos, así como las metas que la función de TI ha definido para la Seguridad de la Información.
- **Fase B—Entender los catalizadores, establecer los criterios de evaluación a utilizar y realizar la evaluación**—En esta fase, el auditor a través de diferentes técnicas de auditoría debe:
  - Entender cómo se han implementado los catalizadores que construyen la Seguridad de la Información.
  - Identificar las métricas definidas para evaluar el funcionamiento de los catalizadores y establecer los criterios aceptables de dichas métricas.
  - Evaluar y obtener evidencia del funcionamiento de todos los catalizadores identificados.
- **Fase C—Comunicar los resultados**—En esta fase el auditor comunica los resultados de su evaluación. Esto incluye la elaboración de informes y la documentacion de toda la evidencia recolectada que permita el futuro análisis de las conclusiones obtenidas en la auditoría. Los informes deberán de llevar también las recomendaciones que permitan superar los hallazgos identificados.

Fase A—Determinar el alcance de la auditoría				
Ref.	**Pasos**	**Referencia**	**Referencia cruzada**	**Comentarios**
A-1	Determinar hacia quienes va dirigido el informe de auditoría y la motivación que tienen para solicitar una auditoría.			
A-1.1	Identificar a los usuarios del informe de auditoría. Establecer con ellos el objetivo de la auditoría.			
A-1.2	Identificar otras partes interesadas y su role en la seguridad de la información.	*Establecer quién es responsable de la Seguridad de la Información, identificar otros roles que son informados, consultados y que rinden cuentas por los resultados de la gestión de la Seguridad de la Información.*		
A-2	Determinar los objetivos de aseguramiento.	Establecer los objetivos que la organización tiene para la Seguridad de la Información y establecer si se validarán **todos o sólo algunos de ellos.**		
A-2.1	Entender la estrategia de la organización y la importancia de la función de la Seguridad de la Información.			
A-2.2	Entender el contexto interno de la organización.			
A-2.3	Entender el contexto externo de la organización.	*Las relaciones con proveedores pueden traer riesgos de seguridad, por lo que es importante identificar entidades externas que tienen conexión con la infraestructura tecnológica de la organización.*		
A-2.4 .	Identificar si es necesario profundizar más en la definición de objetivos de aseguramiento.	En organizaciones grandes, diferentes unidades pueden tener diferentes objetivos principales respecto a la Seguridad de la Información.		
A-2.5	Definir límites organizacionales de la auditoría.			

Fase A—Determinar el alcance de la auditoría				
Ref.	**Pasos**	**Referencia**	**Referencia cruzada**	**Comentarios**
A-3	Determinar los catalizadores que han sido implementados.	El auditor de sistemas debe de considerar de acuerdo con el modelo de catalizadores de COBIT 5, los que han sido implementados para la Seguridad de la Información		
A-3.1	Entender como se ha implementado la función de la Seguridad de la Información para mitigar el riesgo de Cyberseguridad.	Hacer un inventario de las medidas implementadas para mitigar riesgos de cyberseguridad utilizando el anexo 1: Medidas de Cyberseguridad Implementadas.		
A-3.2	Entender como se han implementado catalizadores alrededor del proceso de Seguridad de la Información	**Principios, políticas y marcos de referencia:** Hacer un inventario de las políticas y documentos normativos implementados relativos a la Seguridad de la Información. **Estructuras Organizacionales:** Identificar los roles existentes y hacer un listado del personal involucrado y las funciones asignadas para realizar funciones relacionadas con la Seguridad de la Información. **Cultura, ética y Comportamiento:** Este catalizador es importante para el tema de la Seguridad de la Información debido a que existe el riesgo de que a través de las mismas personas de la organización las amenazas cibernéticas obtengan un medio de ingreso a la organización. Identificar todos los esfuerzos concernientes al entrenamiento recibido por el personal sobre procedimientos de seguridad, cumplimiento de políticas de seguridad y concientización de los riesgos de cyberseguridad. **Información:** Definir los sistemas de información en alcance y la importancia relative de las diferentes bases de datos. Identificar si se han creado políticas y procedimientos específicos para proteger cierta información o si existen requerimientos regulatorios que obliguen a protección especial. (Políticas de privacidad, información financiera sensible, etc.). Identificar si se ha clasificado la información. **Servicios, Infraestructura y aplicaciones.** Establecer un listado de los Servicios, infraestructura y aplicaciones de la organización que son más relevantes para la Seguridad de la Información. Identificar los componentes que son utilizados para implementar medidas de seguridad. (Firewalls, Sistemas de análisis de bitácoras y similares.) **Personas, habilidades y competencias:** Identificar si roles críticos de la función de Seguridad de la Información han sido definidos a través de perfiles de puestos que especifican habilidades requeridas y las competencias. Identificar si se ha determiando el cumplimiento de estos requisitos para las personas involucradas y si planes de desarrollo han sido definidos, implementados o están en planificación.		

Fase B—Entender los catalizadores, establecer los criterios de evaluación a utilizar y realizar la evaluación						
Ref.	**Pasos de auditoría y referencia**				**Referencia Cruzada.**	**Comentarios**
B-1	**Acordar las mejores métricas y criterios de evaluación.**					
B-1.1	Esto es importante. Cualquier medida de seguridad implementada, debe tener establecidas métricas de evaluación con criterios adecuados a las metas de la organización. El éxito del trabajo de auditoría radica en la evaluación del criterio adecuado para determinar el nivel de cumplimiento de una medida de seguridad.					
	Definir las métricas de evaluación y establecer cómo serán auditadas.					
	Objetivo	**Métrica**	**Criterio**	**Procedimiento de Auditoría**		
	EJEMPLO: Proteger los equipos de malware	Porcentaje de Equipos con software antimalware.	*Mayor de 98%*	*Revisar informe de consola central de gestión de antimalware.*		

Fase B—Entender los catalizadores, establecer los criterios de evaluación a utilizar y realizar la evaluación			
Ref.	**Pasos de auditoría y referencia**	**Referencia Cruzada.**	**Comentarios**
B-2	**Entender la implementación de medidas de seguridad y evaluar los criterios de evaluación establecidos.**		
B-2.1	Entender cada medida de seguridad implementada		
	Entender las medidas de seguridad implementadas e identificar la métrica asociada con cada una.		
	Discutir con los responsables las causas e impactos de las desviaciones y discutir planes de acción para corregirlas.		

Fase C—Communicar los resultados de la Auditoría		
Ref.	**Pasos**	**Referencia**
C-1	**Documentar excepciones y brechas.**	
C-1.1	Entender y documentar las debilidades y el impacto en el logro de objetivos.	
C-2	**Comunicar el trabajo realizado y los hallazgos.**	
C-2.1	Preparar un informe que comunique el trabajo realizado y principales hallazgos.	
C-2.2	Detallar los hallazgos, estableciendo planes de acción recomendados y acordados con los responsables.	
C-2.3	Entregar el reporte final de la auditoría conforme los requerimientos de la organización.	