Auditoría de Sistemas

Módulo 3: El proceso de auditar

Dra. Marcela Capobianco

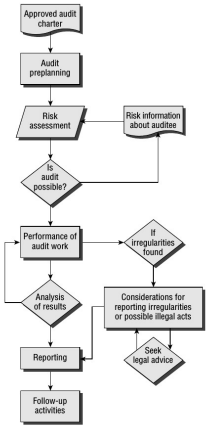
Departamento de Ciencias e Ingeniería de la Computación
Universidad Nacional del Sur

Copyright

Empecemos

- Cómo realizamos la auditoría?

Auditar es un proceso sistemático mediante el cual un profesional competente obtiene y evalúa evidencia sobre hipótesis referidas a un proceso para poder emitir una opinión sobre el mismo



Proceso de auditoría

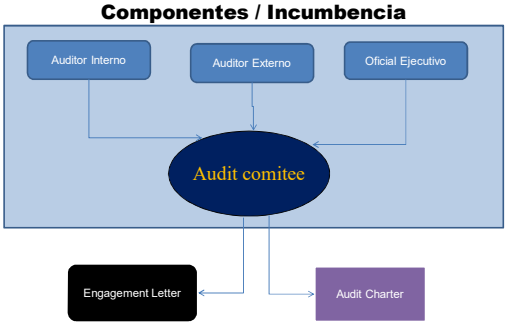
- Vamos a analizar cada uno de estos pasos

RESPONSABLES ➔

Responsable de Auditoria

Comité de auditoría

Componentes / Incumbencia



(…del audit charter hablamos la clase pasada…)

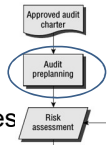
Engagement letter

(Carta de compromiso)

- En el caso que se delegue autoridad a una entidad externa
- Debe incluir:
  - Todos los puntos detallados en la carta de auditoría (audit charter)
  - Independencia del auditor (responsabilidad)
  - Evidencia de un acuerdo con los términos y condiciones (autoridad)
  - Fechas de finalización acordadas (rendición de cuentas)

Pre planificación

- Planificar al menos anualmente el proceso para alcanzar los objetivos de auditoría
- Conocer los objetivos y naturaleza del negocio
- Conocer los objetivos estratégicos
- Conocer los objetivos financieros
- Conocer los objetivos operacionales



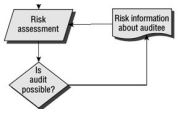
-7-

Pre planificación

-8-

Pre planificación

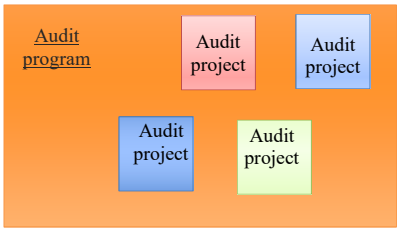
- Identificar restricciones en alcance y recursos
- Se debe revisar los objetivos y la estrategia de riesgo
- Se puede elegir no continuar



-9-

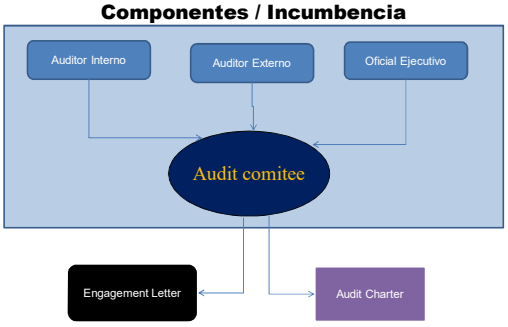
Planificar objetivos detallados

- Un programa de auditoria esta compuesto por varios proyectos de auditoria



-10-

Responsable de Auditoria
Comité de auditoría
Componentes / Incumbencia



-11-

Responsabilidades conjuntas
(comité de auditoria)

- Identificar los factores críticos de éxito y las medidas de rendimiento
- Identificar las funciones y responsabilidades del personal
- Proporcionar acceso a la información, el personal, las ubicaciones y sistemas relevantes para la auditoría
- Cooperar con la práctica de pruebas de auditoría.

-12-

Responsabilidades conjuntas…

- Proporcionar acceso a los resultados de auditorías anteriores o a la comunicación con los auditores anteriores si es necesario
- Especificar las líneas de responsabilidad para la dirección
- Verificar controles independientes y la eficacia del auditor

-13-

Responsabilidades del auditor

- Planificar cada auditoría para lograr objetivos específicos.
- Crear un plan de proyecto por escrito.
- Identificar los recursos necesarios.
- Documentar los procedimientos de auditoría específicos vinculados a los objetivos específicos de auditoría.
- Usar una estrategia de auditoría basado en el riesgo.
- Proporcionar estimaciones de costos de auditoría.

-14-

Algunos tipos de auditorías (SI)

- Producto o servicio: eficiencia, eficacia, controles y los costos del ciclo de vida
- Procesos: métodos o resultados
- Diseño del sistema y/o configuración
- Controles generales: preventivos, de detección y corrección
- Planes de organizacionales: objetivos actuales y futuros

-15-

Programa de auditoría

- El programa de auditoría está basado en el alcance y objetivos de la tarea particular que se esté abordando
- Los auditores de SI evaluan desde diferentes perspectivas
  - Seguridad (confidencialidad, integridad y disponibilidad)
  - Calidad (efectividad y eficiencia)
  - Fiduciario (compliance, confiabilidad)

-16-

Programa de auditoría

- Estrategia y plan de la auditoría
- Identifica alcance objetivos y procedimientos necesarios para obtener la evidencia requerida para luego poder derivar conclusiones fiables de la misma

-17-

Usualmente incluye

- Obtener y registrar un entendimiento del área u objeto a auditar
- Realizar un análisis de riesgo y un plan general y cronograma de actividades
- Planificación más detallada con descomposición de las tareas y referencias temporales concretas

-18-

Usualmente incluye

- Revisión preliminar del área a auditar
- Verificar y evaluar que tan adecuados son los controles existentes para alcanzar los objetivos de control
- Compliance testing (testeo de la implementación de los controles y su aplicación consistente)

-19-

Usualmente incluye

- Testeo sustantivo (confirmar la precisión de la información)
- Realizar un reporte
- Follow-up (seguimiento) en caso de que sea una auditoría interna

-20-

Evaluar los controles

- El auditor de SI debe entender los procedimientos para testear y evaluar los controles
  - Uso de software generalizado de auditoría para resumir los contenidos de archivos de datos (incluyendo logs)
  - Cuestionarios y observación directa

-21-

Análisis de riesgo

- Se debe elegir una metodología de análisis de riesgo
- Y luego identificar riesgos potenciales para esa organización
  - Los activos que deben ser protegidos
  - Las exposiciones de esos activos
  - Las amenazas a los activos
  - Las fuentes internas y externas de las amenazas
  - Los problemas de seguridad que deben abordarse

-22-

Riesgos

"Control" comprende todos los elementos de una organización que, en conjunto, ayudan a las personas a alcanzar los objetivos de la organización. El control es "efectivo" en la medida en que proporcione una seguridad razonable de que la organización alcanzará sus objetivos de manera confiable. El liderazgo implica tomar decisiones frente a la incertidumbre

"Riesgo" es la posibilidad de que uno o más individuos u organizaciones experimenten consecuencias adversas de esas elecciones

-23-

Otra definición

- El riesgo se puede definir como la probabilidad de un evento mezclada con su magnitud (ISO/IEC 73)
- Ejemplo: server goes down (tipo de negocios)
- Ejemplo: ataques de terroristas a un server

-24-

Análisis de riesgos

- Es una parte de la planificación que ayuda a identificar riesgos y vulnerabilidades
- De esta forma los auditores pueden determinar los controles necesarios para mitigar estos riesgos

-25-

Riesgos

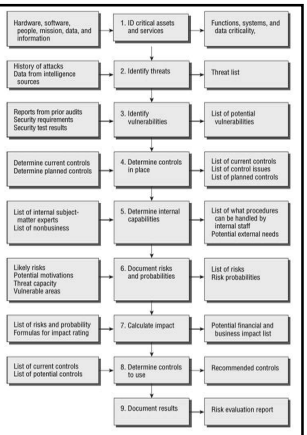
El análisis de riesgos involucra estimar el valor de un producto, proceso o negocio mediante:

- Identificar procesos
- Identificar los tipos de riesgos asociados con cada proceso
- Indentificar los controles asociados con cada proceso
- Evaluar si el control es adecuado
- Determinar los controles claves asociados con cada proceso

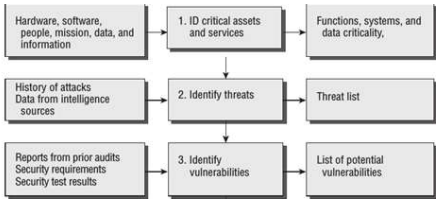
-26-

Análisis de riesgo

- Ejemplo de flowchart de análisis de riesgo

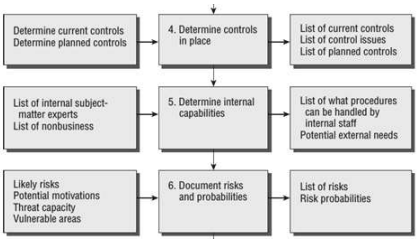


Ejemlo flowchart de análisis de riesgo



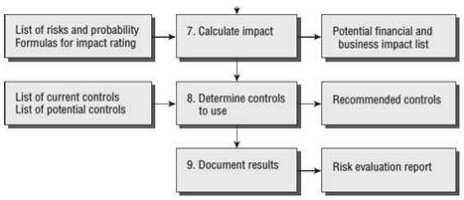
-28-

Ejemlo flowchart de análisis de riesgo (cont.)



-29-

Ejemlo flowchart de análisis de riesgo (cont.)



-30-

Definición de riesgo

- El potencial de que una dada amenaza explotará las vulnerabilidades de un asset o grupo de assets causando daño a la organización (ISO/IEC)

-31-

IT Risk

El riesgo de TI es un **riesgo comercial**, específicamente. el riesgo comercial asociado con el **uso, propiedad, operación, participación, influencia y adopción de TI** dentro de una empresa. Consiste en eventos relacionados con TI que podrían afectar el negocio. Incluye incertidumbre tanto en frecuencia como en magnitud y crea desafíos para cumplir objetivos estratégicos e incertidumbre para la búsqueda de oportunidades.

-32-

IT Risk

- IT risk is a business risk - specifically. the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. It consists of IT-related events that could potentially impact the business. It includes both uncertain frequency and magnitude and it creates chalenges in meeting strategic goals and objectives and uncertainty in the pursuit of opportunities.

-33-

Terminología

-34-

ISACA Risk IT

- El uso de IT trae beneficios y también riesgos asociados
- Los riesgos de IT deben manejarse igual que otros riesgos (de mercado, crediticios, operacionales)
- Muchas veces son relegados por la gerencia
- Risk IT permite integrarlos dentro del enterprise risk management de la organización

-35-

Entender los riesgos de IT

- Para analizar los riesgos de IT el auditor debe tener un entendimiento acabado de:
  - El objeto y la naturaleza del negocio
  - El ambiente en que opera
  - La dependencia de la tecnología
  - Como el riesgo de IT impacta en los riesgos del negocio y en el alcance de los objetivos del negocio

-36-

Entender los riesgos de IT

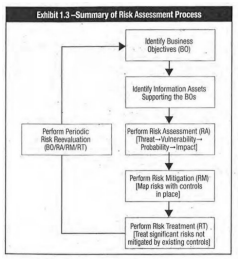
- El auditor en SI se enfoca frecuentemente en riesgos muy serios asociados con:
  - Confidencialidad
  - Disponibilidad de la información
  - Integridad de información crítica y de los procesos que la crean, guardan o manipulan
  - Analizan la efectividad del manejo de riesgos que la organización usa

-37-

Resumen

-38-

Risk assesment



-39-

Risk assesment

- Los riesgos de IT son dinámicos, es estratégico para la gerencia reconocerlo y establecer un proceso de manejo de riesgos de IT
- El proceso debe estar en concordancia con los riesgos de negocio de la organización

-40-

Risk assesment

- Luego se identifican controles para mitigar los riesgos identificados
- Estos contoles deberían prevenir o reducir la probabilidad de que el evento de riesgo ocurra, detectar la ocurrencia, minimizar el impacto o transferir el riesgo

-41-

Risk assesment

- La selección de contramedidas debe realizarse mediante un análisis costo beneficio
  - Costo de control vs beneficio de minimizar el riesgo
  - Cuanto es el riesgo residual que la gerencia está dispuesta a aceptar
  - Métodos preferenciales para lidiar con el riesgo

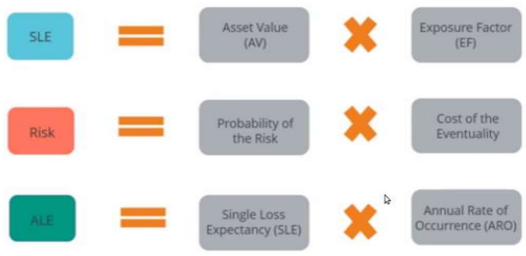
-42-

Ejemplo

- DOS attacks es un riesgo para el servidor
- 10 ocurrencias por año, cada una cuesta 10.000 dolares de pérdida
- 100.000 por año
- Supongamos que podemos implementar un control que reduciría el riesgo a la mitad, lo implementaríamos? (si cuesta 50.000 dolares?, y si cuesta 5.000?)

-43-

Cálculos (a modo informativo …)



SLE = SINGLE LOST EXPECTANCY / ALE = ANUAL LOST EXPECTANCY

-44-

- Ejercicio: Compara los acercamientos para manejar el riesgo de las siguientes normas:
  - Risk IT
  - ISO 27005
  - COSO (Committee of Sponsoring Organizations of the Treadway Commission)

-45-

.Ejemplo

- El activo es información. El valor del activo (AV) se evalúa primero: $ 100,000, por ejemplo.
- La expectativa de pérdida simple (SLE). Contiene información sobre la pérdida potencial cuando ocurre una amenaza (expresada en valores monetarios). Se calcula de la siguiente manera: SLE = AV x EF, donde EF es el factor de exposición. El factor de exposición describe la pérdida que le sucederá al activo como resultado de la amenaza (expresada como valor porcentual). SLE es $ 30,000 en nuestro ejemplo, cuando se estima que EF es 0.3.

-46-

.Ejemplo (cont..)

- Continuemos este caso. La tasa de ocurrencia anualizada (ARO) se describe como una frecuencia estimada de la amenaza que ocurre en un año. ARO se usa para calcular ALE (expectativa de pérdida anualizada). ALE se calcula de la siguiente manera: ALE = SLE x ARO. ALE es $ 15,000 ($ 30,000 x 0.5), cuando se estima que el ARO es de 0.5 (una vez en dos años).

-47-

.Ejemplo (cont..)

Exhibit 2.8—Annual Loss Expectancy Approach

Frequency	Asset Value (US $) 1	100	1,000	10,000	100,000	1 million	10 million	1 billion
1 minute	526	52,560	525,600					
1 hour	9	876	8,760	87,600	876,000			
1 day		37	365	3,650	36,500	36,500		
1 week		5	52	521	5,214	52,143	521,429	
1 month		1	12	120	1,200	12,000	120,000	
3 months			4	40	400	4,000	40,000	
1 year			1	10	100	1,000	10,000	1,000,000
5 years				2	20	200	2,000	200,000
10 years				1	10	100	1,000	100,000
20 years				1	5	50	500	50,000
50 years					2	20	200	20,000
100 years					1	10	100	10,000
300 years						3	33	3,333

(Figures are rounded to US $1,000)

-48-

Respuestas a los riesgos

- Aceparlo: hacer caso omiso de un riesgo. El auditor debe estar preocupado ante la aceptación de situaciones de alto riesgo
- Mitigar (reducir): reducir las probabilidades de un daño. La mayoría de los controles internos son diseñado para mitigar el riesgo

-49-

Respuestas a los riesgos

- Transferir: deje que otro tome el riesgo mediante el uso de un subcontratista o un seguro. Se transfiere el riesgo, pero no la responsabilidad por el fracaso. (ojo, hacer acuerdos de outsourcing y cláusulas con derechos de auditar)
- Evitar: cambiar la situación para evitar la existencia del riesgo (en gral no es posible)

-50-

Procedimiento P1 ISACA

- Ejercicio: leer el procedimiento P1 sobre la metodología de análisis de riesgo, analizarlo y preguntar las dudas sobre como aplicarlo en la clase práctica.
- ISACA P1
- (https://cs.uns.edu.ar/~mc/ADS/downloads/Material%20Complementario/Material%20modulo%203/ISAuditingP1ISRiskAssessmentProcedure-ISACA.pdf)

-51-

Objetivo de la Auditoría

Reducir las pérdidas esperadas por eventos ilegales mediante:

- Controles preventivos: reducen la probabilidad que estos eventos ocurran.
- Controles detectivos y correctivos: reducen la cantidad de pérdidas cuando los eventos ilegales ocurren.

La tarea del auditor es determinar si los controles están ubicados y funcionan para prevenir los eventos ilegales.

-52-

Realizar la auditoría

- Al terminar el análisis de riesgo comenzamos con la auditoría, debemos armar un equipo de trabajo idóneo
- Usar una metodología de auditoría (plan y los procedimientos documentados).
- Comprender las necesidades y expectativas del auditado.
- Respetar los ciclos económicos y los plazos.

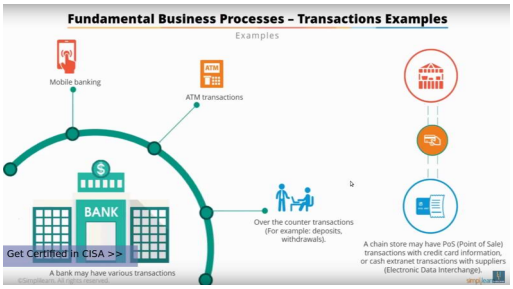
-53-

Realizar la auditoría

- Mantener entrevistas con los clientes y empleados.
- Establecer parámetros de rendimiento de la auditoría.
- Medir el plan de auditoría y como se ajustó al rendimiento real.
- Responder a las quejas de las personas auditadas.

-54-

Entender la empresa



-55-

Investigar

- Zachman framework
- Sherwood applied business Security Architecture
- Service oriented modelling framework

-56-

Recolección de evidencia

- Evidencia: cualquier información usada por el auditor para sustentar las conclusiones de la auditoría
  - Contratos, entrevistas, documentos internos, resultados de los testeos
- La confiabilidad debe ser tenida en cuenta

-57-

Confiabilidad de evidencia

- Independencia del proveedor
- Calificaciones de quien la provee
- Objetividad de la evidencia
- Timing de la evidencia
- La evidencia es competente cuando es válida y relevante
- Ver ITAF. ¿Qué estándares se relacionan con la evidencia?

-58-

Técnicas para recolectar evidencia

- Revisar la estructura organizacional de SI
- Revisar políticas y procedimientos de SI
- Revisar estándares de SI
- Revisar documentación de SI
- Entrevistar al personal apropiado
- Observar performance de procesos y empleados

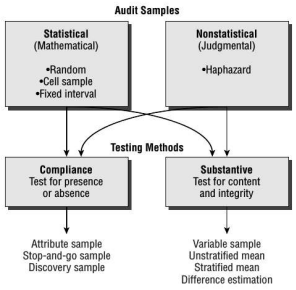
-59-

Sampling

- Se usa cuando tiempo y costo resultan prohibitivos para poder probar todos los eventos o transacciones
- Los dos acercamientos al samping en auditoría son:
  - Sampling estadístico
  - Sampling usando el juicio

-60-

Sampling


Audit Samples
Statistical
(Mathematical)
•Random
•Cell sample
•Fixed interval
Nonstatistical
(Judgmental)
•Haphazard
Testing Methods
Compliance
Test for presence
or absence
Substantive
Test for content
and integrity
Attribute sample
Stop-and-go sample
Discovery sample
Variable sample
Unstratified mean
Stratified mean
Difference estimation

-61-