CONTROLES

Revisar los controles existentes

- Revisar políticas y procedimientos
- Entrevistar personal clave
- Se debe estar atento a las respuestas y a los errores cometidos por los entrevistados
- Hemos mencionado la palabra controles, como clave para la tarea del auditor
- En qué consiste un control?

-63-

Un Control es un sistema

Un mecanismo de usuario/contraseña, ¿es un control? Sólo en el contexto de un sistema que asegure:

- seguridad para elegir passwords,
- correcta validación de passwords,
- almacenamiento seguro de las passwords,
- seguimiento en el uso indebido de passwords

-64-

Se Controlan Eventos Ilegales

¿Cómo puede surgir un evento ilegal?

- si se ingresan al sistema inputs no autorizados, inexactos, incompletos, redundantes, ineficaces o ineficientes,
- si el sistema transforma el input de una manera no autorizada, inexacta, incompleta, ineficiente o ineficaz

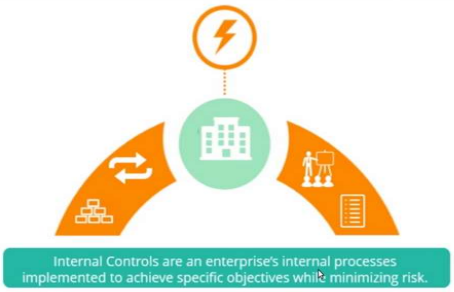
-65-

Controles internos

- Comprenden políticas, procedimientos y estructuras organizacionales que se implementan para reducir los riesgos de la organización
- Proveen seguridad a la gerencia de que los objetivos de negocio serán alcanzados
- Y de que los eventos de riesgo serán prevenidos, detectados o corregidos
- Pueden ser manuales o automatizados

-66-

Controles internos



CONTROLES – PROCESOS – OBJETIVOS – RIESGOS

-67-

Controles internos

Una Clasificación....

- **Controles generales**
  - information system control procedures (ej: como asegurar un servidor o base de datos)
- **Controles de aplicaciones**,
  - (ej: sólo el encargado puede autorizar una devolución)

-68-

Tipos de Controles

Control Preventivo: instrucciones de cómo completar un formulario. (Nota: las instrucciones solas no son el control, son parte.)

Control Detectivo: un programa que valida datos de input, rechazando los erróneos.

Control Correctivo: un programa que detecta el ruido en comunicaciones y permite corregir datos corruptos.

-69-

Aspectos clave en los controles

- Qué se debería **alcanzar**
- Qué se debería **evitar**
- No sólo deben ayudar a alcanzar los objetivos operacionales y de negocio sino que deben abordar los eventos no deseados mediante **prevención, detección y corrección**

-70-

Exhibit 1.4—Control Classifications

Class	Function	Examples
Preventive	• Detect problems before they arise. • Monitor both operation and inputs. • Attempt to predict potential problems before they occur and make adjustments. • Prevent an error, omission or malicious act from occurring.	• Employ only qualified personnel. • Segregate duties (deterrent factor). • Control access to physical facilities. • Use well-designed documents (prevent errors). • Establish suitable procedures for authorization of transactions. • Complete programmed edit checks. • Use access control software that allows only authorized personnel to access sensitive files. • Use encryption software to prevent unauthorized disclosure of data.
Detective	• Use controls that detect and report the occurrence of an error, omission or malicious act.	• Hash totals • Check points in production jobs • Echo controls in telecommunications • Error messages over tape labels • Duplicate checking of calculations • Periodic performance reporting with variances • Past-due account reports • Internal audit functions • Review of activity logs to detect unauthorized access attempts
Corrective	• Minimize the impact of a threat. • Remedy problems discovered by detective controls. • Identify the cause of a problem. • Correct errors arising from a problem. • Modify the processing system(s) to minimize future occurrences of the problem.	• Contingency planning • Backup procedures • Rerun procedures

Métodos de implementación

- Administrativo: uso de políticas y procedimientos.
- Técnicos: involucran un proceso por software o hardware
- Físico: implementación de barreras físicas o disuasivos visuales.

-72-

Preventivos

Preventative "stops"	Administrative	Hiring procedures, background checks, segregation of duties, training, change control process, acceptable use policy (AUP), organizational charts, job descriptions, written procedures, business contracts, laws and regulations, risk management, project management, service-level agreements (SLAs), system documentation
	Technical	Data backups, virus scanners, designated redundant system for high availability system ready for failover (HA standby), encryption, access control lists (ACLs), system certification process
	Physical	Access control, locked doors, fences, property tags, security guards, live monitoring of CCTV, human-readable labels, warning signs

-73-

Detectivos

Detective "finds"	Administrative	Auditing, system logs, mandatory vacation periods, exception reporting, run-to-run totals, check numbers, control self-assessment (CSA), risk assessment, oral testimony
	Technical	Intrusion detection system (IDS), High availability systems detecting or signaling system failover condition(HA failure detection), automated log readers (CAATs), checksum, verifying digital signatures, biometrics for identification (many search), CCTV used for logging, network scanners, computer forensics, diagnostic utilities
	Physical	Broken glass, physical inventory count, alarm system (burglar, smoke, water, temperature, fire), tamper seals, fingerprints, receipts and invoices

-74-

Correctivos

Corrective "fixes"	Administrative	Termination procedures (friendly/unfriendly), business continuity and disaster recovery plans, outsourcing, insourcing, implementing recommendations of prior audit, lessons learned, property and casualty insurance
	Technical	Data restoration from backup, High availability system failover to redundant system (HA failover occurs), redundant network routing, file repair utilities
	Physical	Hot-warm-cold sites for disaster recovery, fire-control sprinklers, heating and AC, humidity control

-75-

Objetivos de control interno

- Controles internos de accounting: confiabilidad de registros y reportes financieros
- Controles de operaciones
- Controles administrativos: tienen que ver con la eficiencia operacional y como adhieren a las políticas de la gerencia

-76-

Ejemplos

- Safeguarding de IT assests
- Concordancia con las leyes
- Concordancia con las políticas de la empresa
- Confidencialidad
- Efficiencia de las operaciones
- Disponibilidad de los servicios de IT

-77-

Objetivos de control de los SI

- Los objetivos son los mismos ya sean los sistemas manuales o automáticos
- Pero la forma en que se los implementa es diferente
- Los objetivos se deben por tanto abordar de una forma que sea relevante a los procesos relacionados con los SI

-78-

Objetivos de control de los SI

- Salvaguarda de los activos
- Asegurar la integridad de sistemas operativos incluyendo el manejo de redes
- Asegurar la integridad de sistemas de aplicaciones críticos como sistemas financieros y que manejen datos sensibles

-79-

Objetivos de control de los SI

- Autorización de la entrada
- Validación de la entrada
- Correctitud del procesamientos de transacciones
- Precisión, completitud y seguridad de la salida
- Integridad, disponibilidad y confidencialidad de las BD

-80-

Objetivos de control de los SI

- Asegurar una apropiada identificación y autenticación de los usuarios

(La ***identificación*** es la capacidad de identificar de forma exclusiva a un usuario de un sistema o una aplicación que se está ejecutando en el sistema. La ***autenticación*** es la capacidad de demostrar que un usuario o una aplicación es realmente quién dicha persona o aplicación asegura ser.)

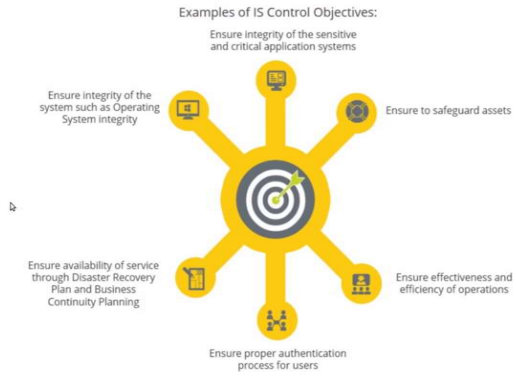
- Asegurar la eficiencia y efectividad de las operaciones
- Cumplir con normas, políticas, regulaciones
- Asegurar disponibilidad de los servicios de IT desarrollando BCP y DRP

-81-

Ejemplos

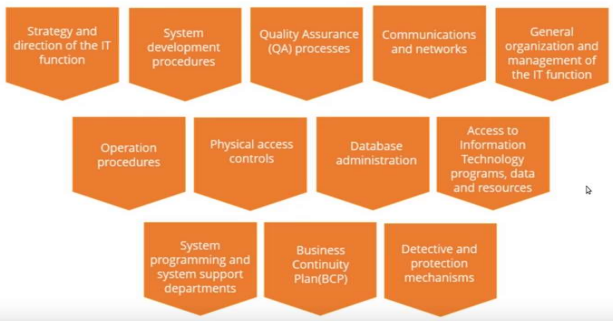
- Identification – controles que aseguran que todos los usuarios son univocamente e irrefutablemente identificados
- Authentication - controles que proveen un mecanismo de autenticación en el sistema de aplicación
- Authorization - controles que aseguran que solo los usuarios apropiados tienen acceso a determinados sistemas de aplicación
- Input controls - controles que aseguran que la integridad de los datos que llegan desde fuentes de más arriba al sistema de aplicación

-82-



-83-

IS control procedures (resumen)

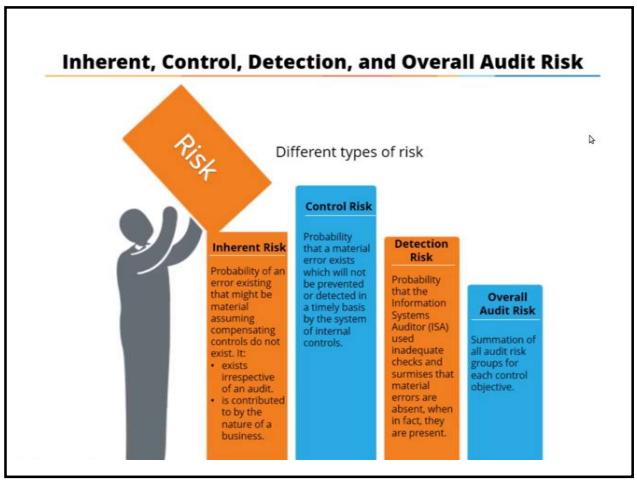


-84-

Auditoría basada en riesgo

- Entender la organización y sus transacciones
- Los riesgos de SI asociados
- Como se procesan esas transacciones en los SI
- Los siguientes riesgos preocupan al auditor

-85-



Auditoría basada en riesgo (resumen)

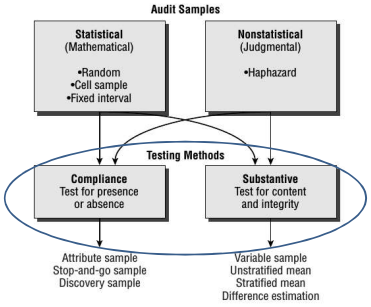
Leyes y regulaciones aplicables a una auditoría

Técnicas de recolección evidencia

Reviewing IS organizational structures	Reviewing IS documentation	Reviewing IS Standards	Reviewing IS Policies and Procedures
Interviewing appropriate personnel	Observing processes and employee performance	Re-performance	Walkthroughs

-89-

Evidencia: audit samples



-90-

Compliance testing

- Las pruebas de conformidad pruebas detectan la presencia o existencia de un control
- Incluyen:
  - la verificación de que las políticas y los procedimientos se han puesto en marcha,
  - procedimientos de control de cambios
  - Uso de los registros de auditoría del sistema

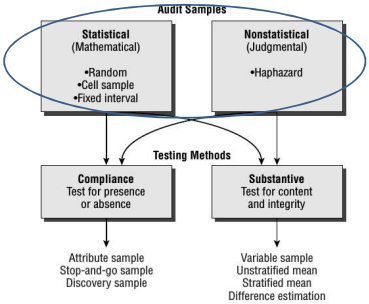
-91-

Substantive testing

- Las pruebas de confirmación se trata de verificar el contenido y la integridad de la evidencia
- Incluyen:
  - la realización de recuentos de inventario físico,
  - ejecutar exploraciones detalladas para detectar la eficacia de una configuración específica del sistema.

-92-

Evidencia: audit samples



-93-

Sampling estadístico

- Usa métodos estadísticos para determinar el tamaño, precisión, el criterio de selección y el nivel de confianza de la muestra
- Este método puede ser usado para inferir características de la población a partir de la muestra
- Ejemplo: altura promedio de una población

Para trabajar como auditor es muy importante tener conocimientos sólidos de estadística

-94-

Sampling no estadístico

- Usa la subjetividad del auditor para determinar el método de sampling, el tamaño de la muestra y su selección
- No es el método preferido
- No puede ser usado para inferir características poblacionales

-95-

Attribute sampling

- Concerniente a la presencia o ausencia de un atributo
- Ej: operaciones de venta en las que se pagó un determinado impuesto
- Usado en compliance testing
- Las conclusiones son porcentajes de incidencia

-96-

Tipos de attribute sampling

- Tamaño fijo muestra
- Estimación por frecuencia
- Stop-or-go
- Discovery sampling

-97-

Variable sampling

- Usando para estimar valor o alguna otra medida cuantitativa
- Se suele aplicar en testing sustantivo
- Nos da conclusiones sobre desviaciones de la norma
- Dos tipos: estratifica o no estratificado

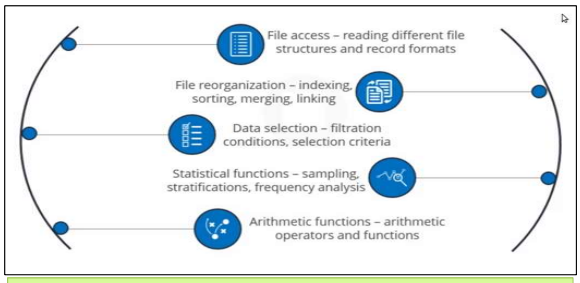
-98-

Usando CAATs

- Pueden realizar una serie de testeos de compliance y sustantivos imposible de hacer en forma manual
- Son invaluables para compilar evidencia durante el proceso de auditoría
- Suelen tener escritores de reportes automatizados

-99-

Software de auditoría de proposito gral



- Audit Control Language (ACL)
- Interactive Data Extraction and Analysis (IDEA).

-100-

Ejemplos de uso de CAATs

- Herramientas para evaluar un host y evaluar vulnerabilidades conocidas en su configuración
- Análisis del tráfico de la red usando un sniffer
- Herramientas de trazabilidad que siguen procesos a través de un SW de aplicación usando datos de testeo

-101-

Ejemplos de uso de CAATs

- Herramientas para testear la configuración de SW específico, como una base de datos SQL
- Testear la fortaleza de los passwords con respecto a una política

-102-

CAATs para auditoría continua

- Online event monitor: herramientas para leer y correlacionar logs del sistema o transacciones. Generan reportes automáticos con alarmar para eventos determinados.
  - Software that reads event logs
  - Intrusion detection systems
  - Virus scanners
  - Software that detects configuration changes

-103-

CAATs para auditoría continua

- Embedded program audit hooks: programadas por el desarrollador para generar banderas de alerta para el auditor, antes de que los problemas se haga más serio
- Seleccionará transacciones para que sean examinadas

-104-

CAATs para auditoría continua

- Embedded audit module (EAM) – Integrated test facility: permite al auditor crear transacciones dummy, que serán procesadas
- Luego se compara la salida con sus propios cálculos
- Permite realizar testeo sustantivo sin interrumpir las operaciones

-105-

CAATs para auditoría continua

- Snapshots: tomar "instantáneas" de una transacción, que se procesa a través de un sistema de aplicación
- Versión automatizada de un tutorial de transacciones manuales
- Las instantáneas se toman en puntos de procesamiento de materiales en el sistema de aplicación

-106-

CAATs para auditoría continua

- Ejemplo: una orden se introduce en el sistema de entrada de pedidos del fabricante. Pasa por una serie de puntos de procesamiento
  - el cliente tiene que ser un cliente autorizado;
  - el importe de la compra debe estar dentro de ciertos límites de crédito;
  - un descuento podría darse dependiendo de la situación del cliente y el tipo de producto que el cliente quiere comprar;
  - la orden podría ser "explotada" para determinar las piezas necesarias para hacer que el producto solicitado;

-107-

CAATs para auditoría continua

- En algunos o todos de estos puntos, se tomarían instantáneas para examinar la correctitud del procesamiento en cada punto.

-108-

CAATs para auditoría continua

- System control audit review file with embedded audit modules (SCARF/EAM): los auditores incrustan rutinas de auditoria en una aplicación a nivel sistema
- Así recolectan datos sobre eventos de interés

-109-

CAATs para auditoría continua

- Ejemplo: en una cia de seguros detectar cambios de nombre del titular de la poliza seguidos de retiros de fondos.
- Cuando se cambia el nombre, se registra el cambios via SCARF. Cualquier retiro de fondos material en una de estas cuentas será reportado para ser analizado.
- Un empleado podría cambiar el nombre, poner el propio y pedir dinero prestado contra la poliza! (se detectaría mediante SCARF)

-110-

Objetivos de la auditoría

- No confundir con los objetivos de control (como debería funcionar un sist de control interno)
- Se suele focalizar en que existan controles internos que minimicen los riesgos de negocio y que estén funcionando
- La gerencia puede darle al auditor un objetivo de control interno para evaluar

-111-

Objetivos de auditoría

- Un elemento clave es trasladar objetivos generales en objetivos de control específicos de SI
- Luego identificamos también controles generales y de aplicación clave para el objetivo y se testea por compliance
- O se decide usar un testeo sustantivo
- Si se confia en los controles existentes se minimiza el testeo sustantivo

-112-

Comunicando los resultados

- La entrevista final da una oportunidad al auditor de discutir los resultados. El auditor debe:
  - Asegurar que los hechos presentados en el reporte con correctos
  - Asegurar que las soluciones son realistas
  - Recomendar fechas de implementación

-113-

Comunicando los resultados

- Primero se debe hablar con quien fue auditado (departamento, persona, etc)
- Luego se comunican los resultados a la gerencia
- Si piden ayuda para implementar lo que se recomendó recordar que un auditor no es un consultor

-114-

Comunicación

- Facilitación: ponerse en el lugar del otro
- Buenas habilidades para escuchar
- Negociación
- Resolución de conflictos
- Escribir / describir claramente los problemas

-115-

Reporte de resultados
Usualmente contiene

- Una intro al reporte, objetivos,cuenta el alcance, lo que se hizo, fechas, restricciones
- Audit findings: en secciones separadas
- Conclusión general del auditor y opinion sobre los controles y los riesgos encontrados
- Recomendaciones y que se encontró en forma más detallada

-116-

Reporte

- No hay un formato específico cada organización tendrá el suyo
- Es el producto final y comunica lo que se encontró a la gerencia
- El auditor entrenado sabe como es más efectivo comunicar los resultados
- Ver ITAF

-117-

Reporte

- Al hablar sobre el reporte se deben discutir fechas para implementar las medidas correctivas
- Saber negociar, entender que puede haber otras prioridades pero ser firmes
- Ejercicio: encontrar que guías y estándares se relacionan con el reporte

-118-

Documentos a generar en una auditoría

-119-

Documentos a generar en una auditoría

- Planificación y preparación del alcance y los objetivos
- Descripción del área de alcance
- Programa de auditoría
- Pasos realizados y evidencia recolectada
- Uso de servicios de auditores externos
- Reporte

-120-

Opiniones de Auditoría: estándares

.Opinión excusada: en base al trabajo realizado no se puede emitir opinión

.Opinión adversa: el auditor determina que han ocurrido pérdidas sustanciales

.Opinión calificada: el auditor determina que han ocurrido pérdidas no sustanciales

.Opinión no calificada: no han ocurrido pérdidas

-121-

Resumiendo, un informe de Auditoría…

- Un informe típico debería incluir:
  - una introducción que describa los objetivos de la auditoría,
  - el enfoque general utilizado,
  - un resumen de las conclusiones críticas,
  - recomendaciones para abordar las conclusiones críticas,
  - datos que respalden las conclusiones críticas.

-122-

Bibliografía

- CISA Study guide, Cannon, Bergman y Pamplin, Wiley, 2013.
- Auditors guide to information systems auditing, R. Cascarino, Willey, 2007. Capítulo 3-6.
- CISA Manual 2013. ISACA.

-123-

Preguntas…

- The concept of due care is best defined as which of the following?
  - A. Proportional to the level of risk or loss that could occur
  - B. Basic care providing a minimal level
  - C. Ordinary care providing an average level
  - D. Extraordinary care above and beyond average

-124-

Preguntas…

- Which of the following describes the relationship between compliance testing and substantive testing?
  - A. Compliance testing checks for the presence of controls; substantive testing checks the integrity of internal contents.
  - B. Substantive testing tests for presence; compliance testing tests actual contents.
  - C. The tests are identical in nature; the difference is whether the audit subject is under the Sarbanes-Oxley regulation.
  - D. Compliance testing tests individual account balances; substantive testing checks for written corporate policies.

-125-