Auditoria de Sistemas Computacionais

Aula 01

Conceitos Gerais de Auditoria de Sistemas

Conteúdo

- Fundamentos de Auditoria de Sistemas de Informações (ASI)
- Padrões e Código de Ética para ASI
- Desenvolvimento da equipe de ASI
- Controles Internos e Avaliação
- Ferramentas e Técnicas de Auditoria de Tecnologia de Informação
- Auditoria de Controles Organizacionais e Operacionais
- Aquisição, Desenvolvimento, Manutenção e Documentação de Sist.
- Auditoria de Controles de Hardware
- Auditoria de Controles de Acesso
- Auditoria de Operação de Computador
- Auditoria de Controles de Suporte Técnico
- Procedimento de Auditoria de Sistemas Aplicativos
- Avaliação de Software de ASI
- Auditoria de Plano de Contingência
- Emissão de Relatórios

Programa

Fundamentos de Auditoria de SI

- Conceito, Contexto, Problemas, Forma de Atuação
- Controles Internos
- Pontos de Controle

Parâmetros de Controles Internos

O Planejamento da Auditoria

O Conceito da Auditoria de Sistemas

1) "A auditoria é uma atividade que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais de uma determinada entidade, com o intuito de verificar sua conformidade com certos objetivos e políticas institucionais, orçamentos, regras, normas e padrões."
DIAS, Cláudia *Segurança e Auditoria da Tecnologia da Informação*. Axcel Books do Brasil, Rio de Janeiro, 2000.

2) A auditoria de sistemas é o ramo da auditoria que revisa e avalia os controles internos informatizados, visando:
   - proteger os ativos da organização;
   - manter a integridade e autenticidade dos dados;
   - atingir eficaz e eficientemente os objetivos da organização.

O Contexto da Auditoria de Sistemas

Auditoria de SI é instrumento da direção, dos acionistas, do ambiente externo, do usuário para:

- opinar, avaliar, validar a qualidade dos dados e da informação e dos sistemas que a geram e mantêm, em termos de segurança, confiabilidade e eficiência.

Interna ou Externa

Exige conhecimentos de TI

Problemas da Auditoria de Sistemas

Auditores tendem a ficar defasados tecnologicamente em relação ao ambiente computacional da organização.

Falta de bons profissionais em auditoria, combinando experiência e conhecimento em TI e auditoria.

Executivos precisam ser educados para obter proveito da auditoria.

Problemas da Auditoria de Sistemas 2

Complexidade crescente do ambiente computacional

- sistemas centrais (mainframes, sistemas multi-usuários)
- microcomputadores independentes
- redes de computadores
- ambiente cliente/servidor
- internet e intranet
- *web services* e organizações interconectadas

Ambiente atual

Complexidade Crescente da TI

Novos modelos de desenvolvimento de software – CMM/CMMI

Gerência de projetos – PMI/PMBOK

Novos aspectos da segurança e avaliação de riscos

O futuro da auditoria de sistemas

Novas funções no ambiente:

- Analista de Segurança (*security officer*)
- Analista de Qualidade
- Analista de Conformidade (*compliance officer*)

Auditoria de segurança e qualidade

Maior automação do processo de auditoria, através de suporte intrínseco dos sistemas

Análise de custo/benefício da auditoria

Gestão e qualidade da auditoria

Controle Interno

Controle interno é função administrativa, exercida pelo auditor de sistemas, que valida as demais funções administrativas - planejamento, execução e controle ou seja, todos os procedimentos internos instituídos pela empresa com o objetivo de evitar a ocorrência de falhas, involuntárias ou dolosas.

Ênfase da auditoria nos processos computacionais e na administração de tecnologia da informação.

Certificar a qualidade intrínseca dos sistemas e dos processos.

Controle Interno e Auditoria

Administração por confronto
- Ambiente de contestação, buscando otimização, eficiência, eficácia e segurança

Administração por exceção
- onde atuar?
- que subconjunto avaliar e validar?
- otimização da análise de risco

Ponto de Controle
- subconjunto submetido à auditoria
- alto risco

Controle Interno e Auditoria

Frameworks de Controles Internos:
- CoCo (CICA - Canadá)
- COSO - Comittee of Sponsoring Organizations of the Threadway (USA)
- Cadbury - The Cadbury Commision (UK)
- BIS (Comitê da Basiléia): A Framework for Internal Control for Banking Organizations

Autoavaliação
- Utiliza o framework para determinar o grau de risco

Parâmetros de Controle Interno

Controle Interno Sistemas
- Fidelidade da informação em relação ao dado
- Segurança física
- Segurança lógica
- Confidencialidade
- Segurança ambiental
- Obediência à legislação

Controle Interno Administrativo
- Eficiência
- Eficácia
- Obediência às políticas da administração

Pontos de Controle

Abordagem do parâmetro de controle interno

Abordagem da fraqueza buscada
- erro, omissão, falha de procedimentos
- falta, erro, correção de resultados

Formado por rotinas e informações operacionais e de controle.

Recursos humanos, materiais, tecnológicos

Forma de Atuação

Através dos sistemas de informações
Através do centro de computação
Através dos processos ou resultados

analisando

Rotinas operacionais
Informações operacionais
Rotinas de controle
Informações de controle

Ponto de Controle

É a situação do ambiente computacional caracterizada como de interesse para validação e avaliação:

- sistema
- módulo de um sistema
- banco de dados
- tabela de um banco de dados (arquivo)
- coluna de uma tabela (campo)
- linhas na tabela (registros)

Auditoria do Ponto de Controle

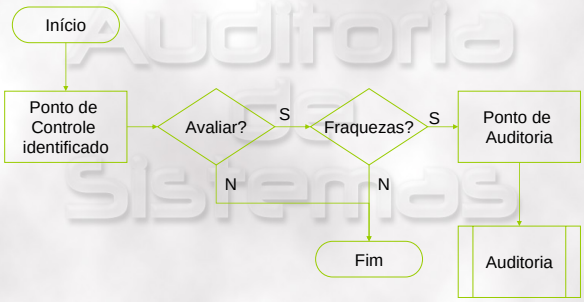
Identificação dentro do ambiente

Caracterização em termos de recursos, processos e resultados.

Análise de risco

- parâmetros do controle interno
- fraquezas passíveis de ocorrer

Ciclo de Vida do Ponto de Controle



Análise de Risco

Conhecer o ambiente a ser auditado

- levantamento de dados
  - fluxo do processamento
  - inventário de recursos humanos e materiais
  - arquivos processados (bancos de dados)
  - relatórios e consultas produzidos
- estudo da documentação do ambiente
- complementação de informações
- visita ao ambiente computacional
- entrevistas com os profissionais do ambiente

Análise de Risco 2

Planejamento da auditoria

- conhecimento do ambiente computacional
- determinação dos Pontos de Controle
- estabelecimento dos objetivos de validação e avaliação dos Pontos de Controle
  - técnicas de auditoria
  - prazos de execução da validação
  - custos incorridos com a validação
  - nível de tecnologia exigida do auditor
  - natureza da fraqueza do controle internos passível de ser alcançada

Análise de Risco 3

Planejamento da auditoria (cont)

- análise da sensibilidade de cada Ponto de Controle
  - matriz Ponto de Controle, Parâmetro, Voto, Fraqueza do Controle, Voto, Técnica de Auditoria a aplicar, Voto, Voto Médio
- hierarquização dos Pontos de Controle
- documentação do processo de planejamento da auditoria

Produtos Gerados

Relatórios de Fraquezas de Controle Interno
- Objetivos do projeto de auditoria
- pontos de controle auditados
- conclusão sobre cada ponto de controle
- alternativas de solução propostas (pontos de recomendação)

Certificado de Controle Interno

Técnicas de Auditoria de Sistemas

Questionário
Simulação de dados (test-deck)
Visita in loco
Mapeamento estatístico
Rastreamento
Entrevista
Análise relatório / tela
Simulação paralela
Análise de log
Análise de programa fonte
Snapshot

Auditoria do Ambiente Computacional

Sistemas em operação
Desenvolvimento de sistemas
Centro de computação
- Gestão
- Segurança

Dúvidas

Auditoria de Sistemas

Término
da
Aula 01