Aula 5

Auditoria de Sistemas

Prof. André Roberto Guerra

Organização da aula

- *Compliance*
- Normas, guias e procedimentos de auditoria
- CobiT
- ITIL
- Norma ISO 17799

Conversa Inicial

- Como sensibilizar e difundir na organização questões de ética e práticas administrativas, financeiras e de relacionamento politicamente corretas?
- Com a correta implantação de um programa de *compliance* e a seleção de um profissional preparado para ocupar a função de CO (*Compliance Officer* = Profissional de *Compliance*)

- A utilização de normas/controles para os sistemas de informação é facilitada pela existência de normas e padrões (*standards*) internacionais de SI que incorporam modelos estruturados (*frameworks*) e que são referenciais para a gestão e auditoria de sistemas de informação

Compliance

- Estar em conformidade (*to comply*, em inglês) interna e externamente traz uma série de benefícios imediatos para uma organização
- Implantar um programa de *compliance* é investimento

Procedimentos para implantação do programa de *compliance*

- Fixação de padrões de conduta, código de ética e políticas internas e externas de relacionamentos críticos

- Gestão de riscos, paralelamente à auditoria, e acompanhamentos gerenciais, com transparência e respostas ágeis e efetivas em desvios de padrões
- Melhoria contínua de processos, monitoria do programa e treinamentos frequentes

ISO 37001: norma certificável de programas de *compliance*

- Independentemente do tipo, tamanho e natureza da atividade, seja do setor público, privado ou sem fins lucrativos, os requisitos da ISO 37001 podem ser aplicáveis a qualquer organização
- O que antes era um diferencial agora é requisito competitivo essencial para empresas sensíveis ou que operam com o sistema público através de licitações ou agências reguladoras

Normas, guias e procedimentos

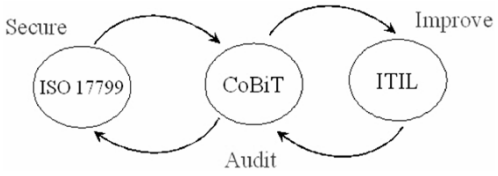
- Organizações podem exercer a Governança dos SI (*IT Governance*) em abordagem local (ad-hoc), criando seus referenciais baseados na experiência, ou utilizar normas internacionais desenvolvidas e aperfeiçoadas, recorrendo à experiência acumulada de um grupo de organizações e de profissionais da vanguarda de SI

- A utilização dessas normas internacionais é defendida como a mais adequada, devido às características e benefícios:
  - já existem
  - são estruturadas
  - incorporam as melhores práticas
  - permitem o compartilhamento de conhecimento
  - são auditáveis

- Para a correta adaptação das normas deve-se garantir que elas incorporem um conjunto mínimo de princípios de Governança de SI:
  - alinhamento estratégico
  - acréscimo de valor
  - gestão do risco
  - gestão dos recursos
  - medição do desempenho

- Para uma possível utilização dos referenciais, é sugerido o uso do método Six Sigma, que prevê 5 principais fases:
  - definição (*define*)
  - medição (*measure*)
  - análise (*analyse*)
  - melhoria (*improve*)
  - controle (*control*)

- O referencial mais adequado para as medidas de segurança (*secure*) é a ISO 17799; para a auditoria (*audit*) é o CobiT; e para a melhoria (*improve*) é o ITIL



Fonte: LeBlanc, 2004.

CobiT

- Pela análise dos 3 referenciais apresentados, o CobiT será aplicado na auditoria de SI pelas seguintes razões
  - Desde a criação, o CobiT tem foco na criação de um referencial para auditar os processos de SI

- A entidade responsável pela elaboração do CobiT é uma Associação de Auditores de SI (ISACA – Information Systems Audit and Control Association), o que não acontece com os outros dois referenciais
- O CobiT possui uma visão de gestão dos processos de SI e privilegia o alinhamento com o negócio

- O CobiT é útil para as organizações enquanto instrumento orientador e integrador de controles de SI em todos os níveis de governança
- Como consequência, os destinatários privilegiados do CobiT são os auditores de SI, sendo também utilizado pelos gestores de topo e gestores de SI

- Considera 5 recursos de SI:
  - pessoas
  - aplicativos
  - tecnologia
  - instalações
  - dados

- Considera 7 princípios:
  - eficácia
  - eficiência
  - confidencialidade
  - integridade
  - disponibilidade
  - conformidade
  - confiabilidade

- CobiT considera os controles de SI em 4 domínios
  - Planejar e organizar (PO – Plan and Organize)
  - Adquirir e implementar (AI – Acquire and Implement)
  - Produzir e suportar (DS – Deliver and Support)
  - Monitorar e avaliar (M – Monitor and Evaluate)

- Cada um dos 4 domínios é constituído por 34 processos (controles de alto nível), constituídos por 318 atividades (controles detalhados)

ITIL

- ITIL® (Information Technology Infrastructure Library) é o *framework* para gerenciamento de serviços de TI mais adotado mundialmente – V3 (versão atual)
- Foi desenvolvida no final dos anos 1980 pelo governo britânico, primeiramente como CCTA (Central Computer and Telecommunications Agency) e futuramente pela OGC (Office of Government Commerce)

- Conjunto de melhores práticas para a gestão de serviços de SI, abordando:
  - promoção da qualidade dos serviços de SI
  - visão holística da gestão dos serviços de SI
  - orientação para o negócio (cliente/usuário)
  - uso eficaz/eficiente dos SI

- Os dois módulos centrais (*core*) do modelo estruturado e seus respectivos processos são:
- Suporte aos serviços
  - Gestão de incidentes
  - Gestão de problemas
  - Gestão de configurações
  - Gestão de alterações
  - Gestão de versões
  - Apoio aos serviços

- Produção dos serviços (*service delivery*)
  - Gestão de capacidade
  - Gestão de disponibilidade
  - Gestão de níveis de serviço
  - Gestão de continuidade de serviços
  - Gestão financeira dos serviços

- 5 módulos complementares ITIL
  - Gestão da infraestrutura de TIC
  - Gestão de aplicações
  - Gestão da segurança
  - Planejamento da implementação da gestão dos serviços
  - Perspectiva de negócio

Norma ISO 17799

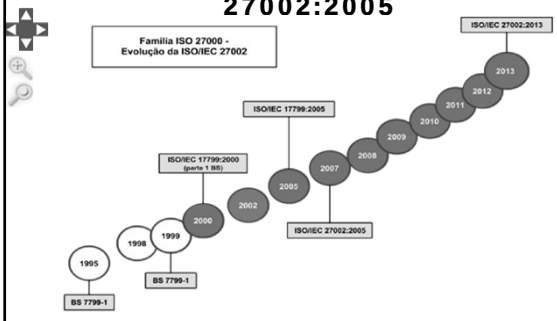
- Conforme definido pela Associação Brasileira de Normas Técnicas (ABNT, 2005), os objetivos da normalização são:
  - comunicação
  - segurança
  - proteção do consumidor
  - eliminação de barreiras técnicas e comerciais

- A norma brasileira NBR ISO/IEC 17799:2005 é um guia prático que estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização

- Nesse sentido, a norma se subdivide em 16 capítulos
  1. Introdução
  2. Objetivo
  3. Termos e definições
  4. Estrutura da norma
  5. Análise/avaliação e tratamento de riscos
  6. Política de segurança da informação
  7. Organizando a segurança da informação
  8. Gestão de ativos

9. Segurança em Recursos Humanos
10. Segurança física e do ambiente
11. Gerenciamento das operações e comunicações,
12. Controle de acessos
13. Aquisição, desenvolvimento e manutenção de sistemas de informação
14. Gestão de incidentes de segurança da informação
15. Gestão da continuidade do negócio
16. Conformidade

Evolução da norma ISO/IEC 27002:2005



Fonte: FRIEDRICK, 2014.

A norma ABNT NBR ISO/IEC 27002

- **A norma contem 11 controles de segurança da informação, e, juntos, totalizam 39 categorias principais**

Capítulo	Título	Números subcapítulos
5	Política de segurança da informação	1
6	Organizando a segurança da informação	2
7	Gestão de ativos	2
8	Segurança em Recursos Humanos	3
9	Segurança física e do ambiente	2
10	Gestão de operações e comunicações	10
11	Controle de acesso	7
12	Aquisição, desenvolvimento e manutenção de SI	6
13	Gestão de incidentes de segurança informação	2
14	Gestão da continuidade do negócio	1
15	Conformidade	3

Fonte: ABNT, 2005.

Finalizando

- **A maioria das organizações direciona as atenções e investimentos em segurança apenas nos seus ativos tangíveis físicos e financeiros, mas dedicam pouca atenção e investimentos aos ativos de informação, considerados vitais na sociedade do conhecimento**