Segurança de Redes

Gestão de Segurança da Informação

Prof. João Henrique Kleinschmidt

Segurança da Informação

- Preservação de:

Confidencialidade

Integridade

Disponibilidade

Como a SI pode ser obtida?

- Implementando **CONTROLES**, para garantir que os objetivos de segurança sejam alcançados

Políticas

Práticas

Procedimentos

Estruturas organizacionais

Funções de softwares

Fatores Críticos de Sucesso

- Política de segurança, objetivos e atividades que reflitam os **objetivos do negócio**
- Implementação da segurança consistente com a **cultura organizacional**
- Comprometimento e **apoio da direção**
- Compreensão dos **requisitos** de segurança, **avaliação** de riscos e **gerenciamento** de riscos

Fatores Críticos de Sucesso

- **Divulgação** (propaganda) sobre segurança para todos os gestores e funcionários
- **Distribuição** das diretrizes sobre normas e política de segurança para todos os funcionários e fornecedores
- **Educação e treinamento** para todos os envolvidos
- **Sistema de medição** abrangente para avaliar o desempenho da gestão de SI e obtenção de sugestões de melhoria

Normas para Segurança da Informação

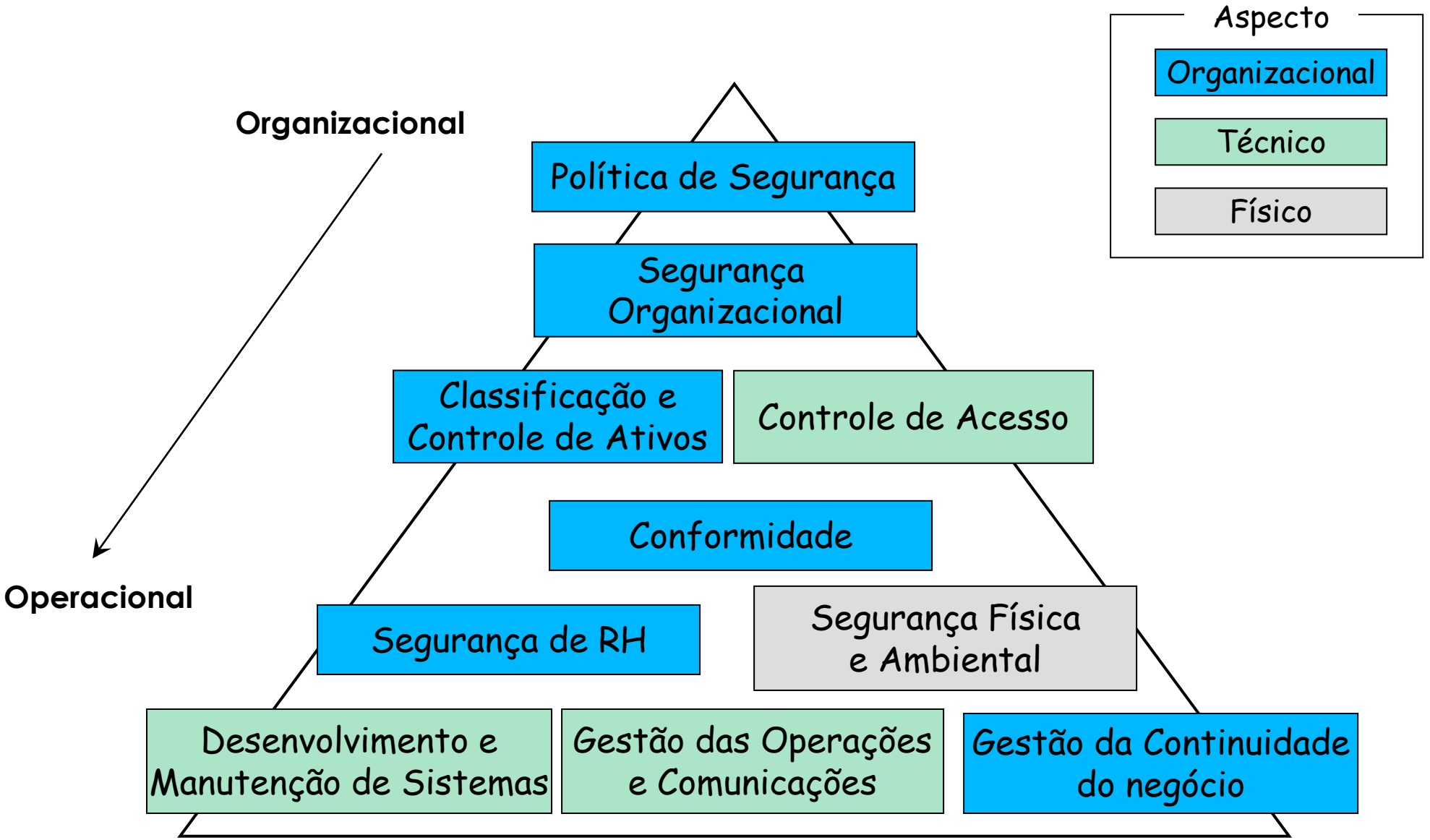
- ISO/IEC 27001
- ISO/IEC 27002
- NBR ABNT 27001 e 27002 (traduções)

Normas ISO/IEC

- ISO/IEC 27001
  - Origem norma britânica BS-7799-2
  - Sistemas de Gestão de SI (ISMS – information security management system)
  - Objetivo da organização: certificação
- ISO/IEC 27002
  - Conhecida anteriormente como ISO/IEC 17799
  - Origem na norma britânica BS-7799-1
  - Código de prática para a gestão da SI
  - Objetivo da organização: conformidade

Áreas (cláusulas de controle)

Áreas (cláusulas de controle)



Seções da ISO 27002

- Norma organizada em 11 seções
- Cada seção cobre um tópico ou área diferente
  - objetivos específicos

Seções da ISO 27001

1. Política de Segurança
   - Determina expectativas para SI
   - Fornece direção/suporte ao gerenciamento
   - Base para revisões e avaliações regulares
2. Organizando a Segurança da Informação
   - Infraestrutura de SI
   - Coordenação da SI

Seções da ISO 27001

3. Gestão de Ativos
   - Inventário dos ativos, normas de uso, etc
4. Segurança de RH
   - Educação e informação dos funcionários atuais ou potenciais sobre a expectativa da empresa quanto a assuntos confidenciais e de segurança, e como sua função na segurança se enquadra na operação geral da empresa

Seções da ISO 27001

5. Segurança Física e do Ambiente
   - Trata de proteger áreas seguras, equipamentos de segurança e controles gerais
6. Gerenciamento de Operações e Comunicações
   - garantir instalações para a operação correta e segura do processamento de informações
   - minimizar o risco de falhas dos sistemas
   - proteger a integridade do software e/ou das informações
   - manter a integridade e disponibilidade do processamento de informações e comunicações
   - garantir a proteção das informações em redes e da infraestrutura de suporte
   - evitar danos ao patrimônio e interrupções nas atividades da empresa
   - prevenir perdas, modificações ou uso inadequado das informações trocadas entre empresas

Seções da ISO 27001

7. Controle de Acesso
   - Monitoração e controle do acesso a recursos da rede e de aplicativos, para proteger contra abusos internos e intrusões externas
8. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação
   - Recomenda implementar e manter recursos de TI visando segurança em mente, usando os controles de segurança em todas as etapas do processo

Seções da ISO 27001

9. Gestão de Incidentes de SI
   - Gestão e tratamento de incidentes
10. Gestão da Continuidade dos Negócios
   - Maneiras para neutralizar interrupções às atividades comerciais e proteger processos de negócio cruciais, no evento de uma falha ou desastre

Seções da ISO 27001

11. Compatibilidade

- análise da integração da implementação da norma com requisitos legais revisão da política de segurança e compatibilidade técnica
- considerações sobre o sistema do processo de auditoria

Vantagens das Normas

- Conformidade com regras dos governos para o gerenciamento de riscos
- Maior proteção das informações confidenciais da organização
- Redução no risco de ataques de hackers
- Recuperação de ataques mais fácil e rápidas

Vantagens das Normas

- Metodologia estruturada de segurança que está alcançando reconhecimento internacional
- Maior confiança mútua entre parceiros comerciais
- Custos possivelmente menores para seguros de riscos computacionais
- Melhores práticas de privacidade e conformidade com leis de privacidade

Sistema de Gerenciamento de Segurança da Informação (ISMS)

Sistema de Gerenciamento de Segurança da Informação (ISMS)

Um ISMS tem o objetivo de instituir a política e objetivos de segurança de informação da organização

...

E cumprir esses objetivos

Sistema de Gerenciamento de Segurança da Informação (ISMS)

Um ISMS provê uma abordagem sistemática para gerenciar informações sensíveis e protegê-las

O ISMS envolve pessoas, processos e sistemas de informação

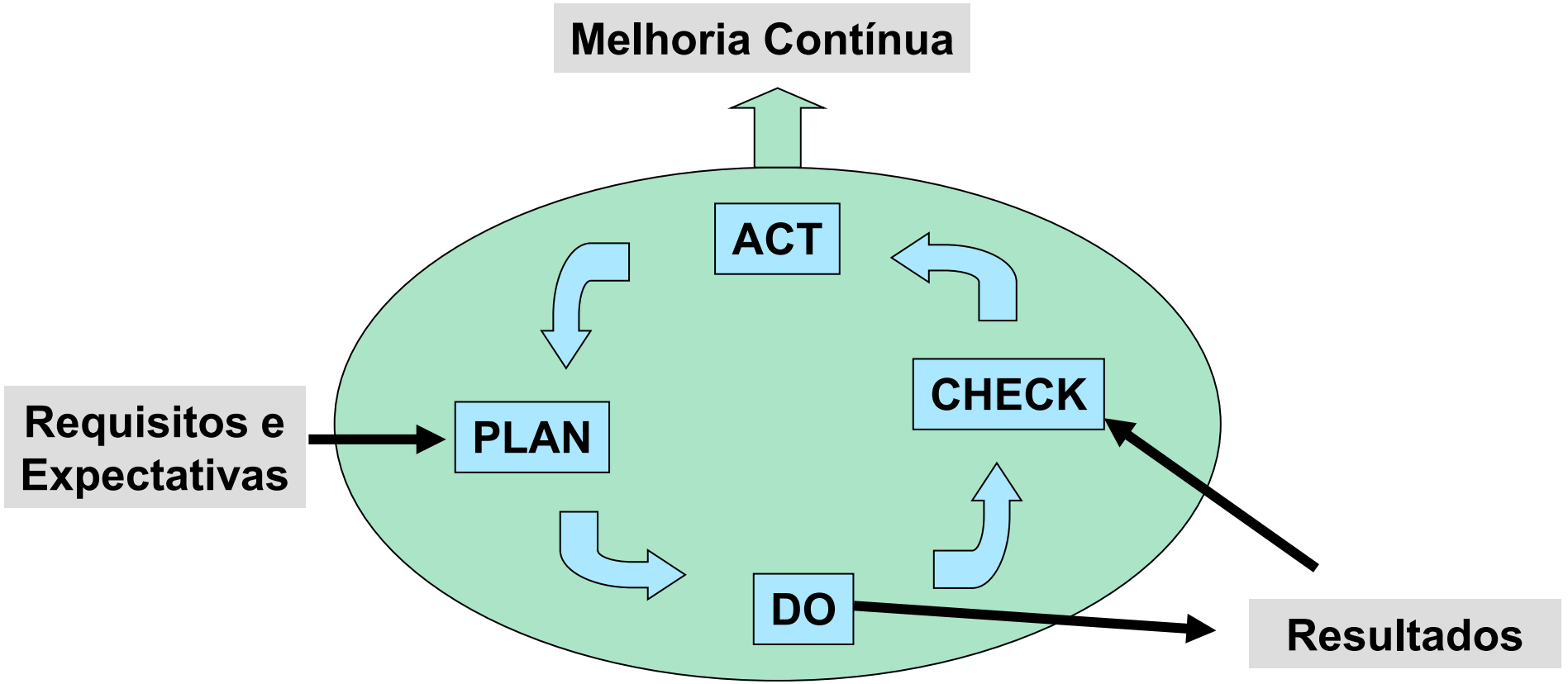
Sistema de Gerenciamento de Segurança da Informação (ISMS)

- O ISMS faz parte do sistema de gerenciamento global de uma organização
- Baseado em uma abordagem de riscos
- Com o objetivo de
  - Estabelecer
  - Implementar, operar
  - Monitorar, revisar
  - Manter, melhorar
- A segurança da informação

ISMS

- A norma ISO 27001:2005 especifica o ISMS e oferece diretrizes para a sua aplicação
- Proporciona controles de segurança para proteger os ativos e garantir confiança
- Baseado no modelo Plan-Do-Check-Act (PDCA)
  - **Plan**: estabelecimento do ISMS
  - **Do**: implementação e operação do ISMS
  - **Check**: monitoração e revisão do ISMS
  - **Act**: manutenção e melhoria do ISMS

ISMS: Modelo PDCA



ISMS – Motivação

- Questões - Organização
  - Por que uma organização deveria implantar um ISMS?
  - Por que uma organização deveria ser certificada na norma ISO 27001?

- Questões - Profissional
  - O que um profissional de SI ganha se especializando na área de gestão de SI?
  - Não seria mais vantajoso se especializar em assuntos (produtos, mecanismos) técnicos?

ISMS – Motivação

- Possível Resposta - Organização
  - **"A segurança que pode ser alcançada por meios técnicos é limitada"**
    - (Norma ISO/IEC 27002:2005)

- Possíveis Respostas - Profissional
  - Depende dos interesses, dos objetivos de carreira e da fase profissional de cada um
  - Certamente, profissionais que almejam progressão profissional devem se preocupar mais com questões gerenciais (em detrimento das questões técnicas ☹)

ISMS - Motivação

- O ISMS é um sistema de gestão
- Portanto, deve obrigatoriamente seguir uma metodologia específica para assegurar o sucesso da sua implantação na organização
- Em princípio, o estudo de metodologias é algo que tem um grande potencial para se tornar enfadonho e desinteressante
- No entanto, ninguém consegue uma certificação (ISO 9000, CMMI, etc), sem o estudo e compreensão da metodologia projetada
  - Com a norma ISO 27001 ocorre o mesmo
- Para alguns, estudar assuntos técnicos é algo mais prazeroso e estimulante
  - Inclusive para certificações técnicas (Microsoft, CISCO, etc)

ISMS - Motivação

Programas de gestão abrangem toda (ou grande parte de) uma organização e em geral tem grande notoriedade

Assuntos técnicos, em geral, ficam limitados a locais específicos da empresa e em geral somente são conhecidos por pessoas da área

ISMS - Motivação

- Exemplo de ação governamental contra a fome
- Suponha que um governo queira implantar um programa para erradicar a fome de uma determinada cidade, estado, região ou país
- Qual abordagem seguir?
  - Criar um slogan bonito? ("No Starvation" ☺)
  - Fazer incontáveis reuniões e tentar coletar o maior número possível de opiniões e informações?
  - Debater amplamente com a sociedade?
  - Sair implantando programas pontuais (como as ONGs) pra ver se a soma dos resultados individuais alcança o objetivo final?
  - **Ou, criar um programa de gestão sério, baseado em alguma metodologia e colocá-lo em funcionamento?**

ISMS - Motivação

- O que é necessário para que a ação governamental funcione de acordo com os objetivos?
- **Planejamento**
  - (competente, eficaz e sério)
- **Implementação**
  - (competente, eficaz e séria)
- **Monitoramento**
  - (competente, eficaz e séria)
- **Aprimoramento**
  - (competente, eficaz e sério)
- Enfim: Plan-Do-Check-Act = PDCA

Requisitos e Expectativas

- Requisito: Exemplo
  - Brechas na segurança da informação não causarão prejuízo financeiro sérios e/ou constrangimento para a organização
- Expectativa: Exemplo
  - Se um incidente sério ocorrer (digamos, o portal de comércio eletrônico é "hackeado") deve haver pessoas com treinamento suficiente para adotar os procedimentos adequados para minimizar os impactos

Seções do ISMS

- Estabelecer e gerenciar o ISMS
  - PDCA
- Requisitos de documentação
- Responsabilidade da Gestão
- Análise/revisão de gestão do ISMS
- Aprimoramento do ISMS

Plan: Estabelecer

- Definir o escopo do ISMS
- Definir as políticas da organização
- Definir abordagem sistemática de gestão de riscos
- Identificar os riscos
- Avaliar os risco
- Identificar/avaliar opções de tratamento de riscos
- Selecionar os objetivos de controle e controles
- Preparar uma declaração de aplicação

Do: Implementar e operar

- Formular um plano de tratamento de riscos
- Implementar o plano de tratamento de riscos
- Implementar os controles selecionados (plan)
- Implementar programas de conscientização e treinamento
- Gerenciar as operações
- Gerenciar os recursos
- Implementar procedimentos para detecção rápida e resposta a incidentes de segurança

Check:Monitorar e revisar

- Executar procedimentos para
  - detectar erros, identificar brechas de segurança, descobrir se as tarefas de segurança estão sendo desempenhos de acordo com o planejado, etc.
- Executar verificações periódicas da efetividade do ISMS, considerando as questões anteriores
- Verificar o nível de risco residual e aceitável, levando em consideração mudanças
- Executar auditorias internas periódicas do ISMS
- Averiguar a efetividade do gerenciamento do ISMS
- Registrar ações e eventos que podem ter impacto na efetividade e desempenho do ISMS

Act:Manter e aprimorar

- Implementar e identificar melhorias no ISMS
- Tomar medidas corretivas e preventivas
  - Corretivas: tomar ações para eliminar as causas das não conformidades de implementação e operação do ISMS
  - Preventivas: determinar possíveis não conformidades futuras para prevenir sua ocorrência
- Comunicar resultados e ações e ter a concordância de todas as partes interessadas
- Assegurar que os aprimoramentos atingem os seus objetivos

Requisitos de documentação

- Requisitos gerais
  - Política de segurança e objetivos de controle, escopo, relatório de avaliação de riscos, plano de tratamento de riscos, documentação de procedimentos, declaração de aplicação
- Controle de documentos
  - O uso/acesso/revisão/alteração/distribuição dos documentos deve ser protegido e controlado
- Controle de registros
  - Documentar controles para identificação, armazenamento, recuperação, tempo de retenção e distribuição

Responsabilidade da Gestão

- Compromisso da gestão: mostrar evidências
  - Estabelecer uma política e objetivos de SI
  - Estabelecer papéis e responsabilidades
  - Comunicar a importância do ISMS na organização
  - Decidir níveis aceitáveis de riscos
  - Executar revisão da gestão
- Gerenciamento de recursos
  - Provisão de recursos
  - Treinamento, conscientização, capacitação

Revisão de gestão do ISMS

- Estabelecer revisões periódicas
  - Documentar e disseminar informações sobre elas
- Informações de entrada
  - Auditorias, feedbacks, vulnerabilidades não consideradas anteriormente, etc.
- Informações de saída
  - Aprimoramentos ao ISMS, modificação de procedimentos, necessidades de recursos
- Autorias internas do ISMS

Aprimoramento do ISMS

- Aprimoramento contínuo
- Ações corretivas
- Ações preventivas

Ferramentas para trabalhar com normas e ISMS

Ferramentas para normas

- Ferramentas que auxiliam:
  - Implantação
  - Verificação de conformidade
  - Averiguação para certificação
- São ferramentas baseadas em bases de conhecimento, que oferecem questionários para
  - Guiar o processo de implantação
  - Averiguar o nível de conformidade
  - Sugerir aprimoramentos

Ferramentas para Normas

- RUSecure (www.rusecure.co.uk)
  - Information Security Officer´s Manual (demo)
- Callio (www.callio.com)
  - Callio Secura 17799
  - Callio Toolkit Pro 17799 (demo)
- Risk World (www.riskworld.com)
  - COBRA ISO 17799 Consultant (demo)
- ISM SME Guide
  - Information Security Management SME Guide (demo)