



Universidade Federal do ABC

INF-108

Segurança da Informação

Aula 02
Gestão de Segurança da Informação

Prof. João Henrique Kleinschmidt
(slides cedidos pelo Prof. Carlos Kamienski - UFABC)



Santo André, fevereiro de 2011



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 refletem 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

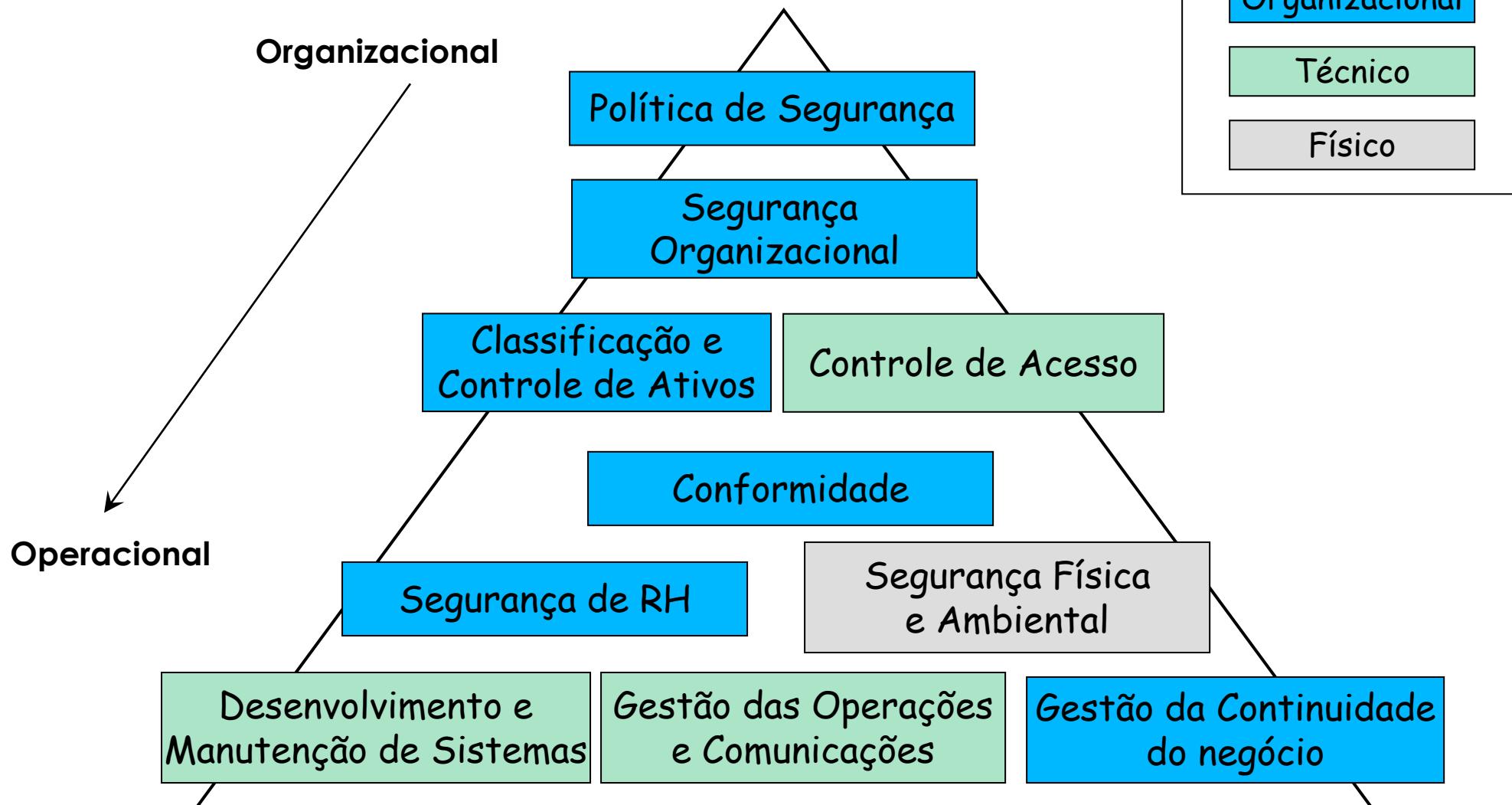


Áreas (cláusulas de controle)





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



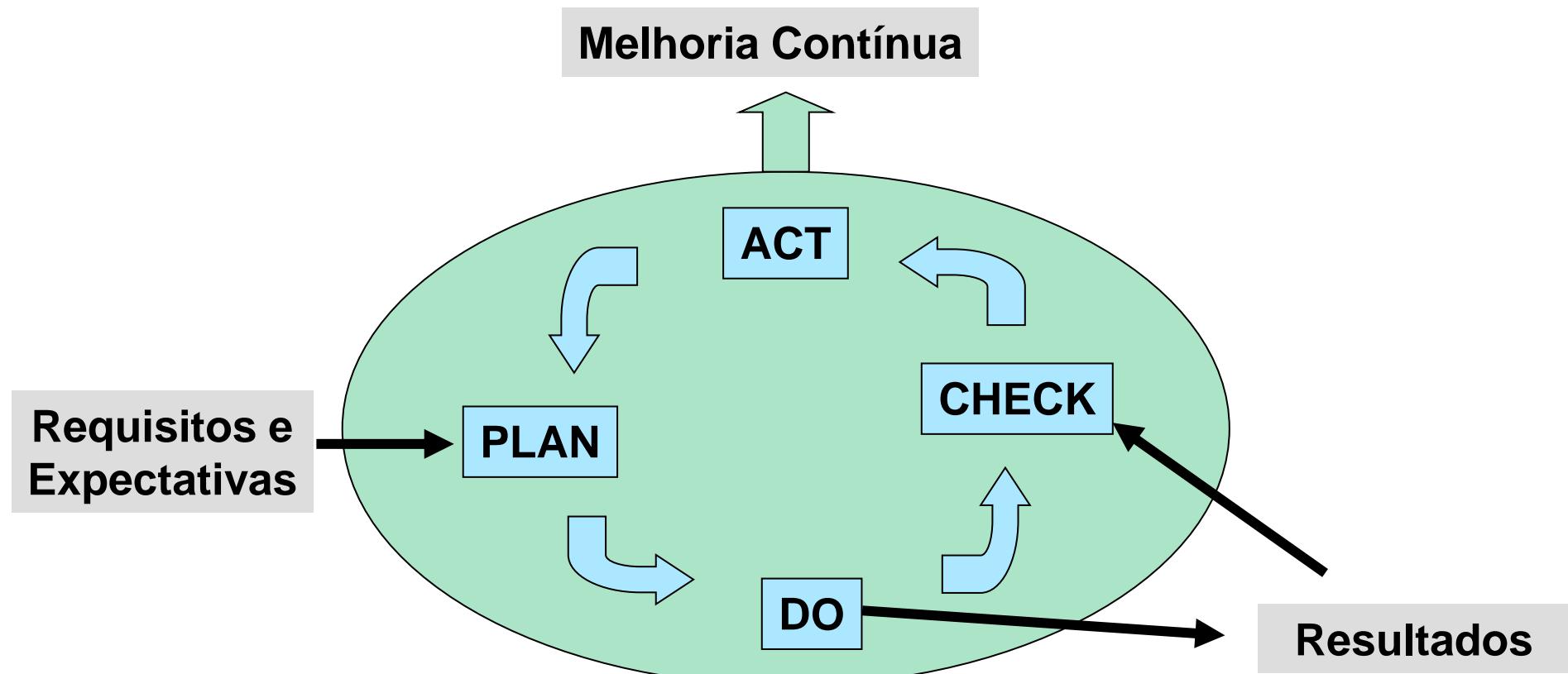
Sistema de Gerenciamento de Segurança da Informação (ISMS)

- 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

- 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
 - Averigar 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)

- Políticas são a base da SI dentro das organizações
- Deve-se responder as perguntas:
 - Elas são abrangentes? Estão atualizadas?
 - Elas estão disponíveis? (por exemplo, nos PCs)
 - Como os usuários obedecem as políticas no dia a dia?
- A RU Secure - Information Security Suite
 - Orientação a todos os colaboradores de uma organização
 - Políticas completas e distribuídas a todos através de um único conjunto de ferramentas
 - Information Security Policies
 - Security Online Support
 - Information Security Officer's (ISO) Manual



Manual do ISO (Gerentão da segurança)

- A indicação de um ISO é uma boa indicação de que uma organização decidiu tornar a IS um processo formal dentro da operação do negócio
 - Se não tiver um ISO, geralmente alguém da TI é o responsável pela SI em tempo parcial
- Estabelecer uma estrutura formal para o processo de SI é uma realização significativa
- O manual oferece conselhos práticos sobre o estabelecimento de um processo de SI
 - Discute as obrigações do ISO
 - Discute aspectos cruciais para um processo efetivo de SI

Un-Registered Evaluation Copy



ISO Manual Navigation and Control

Welcome to the RUSecure™ - Information Security Officer's Manual (ISO Manual). This has been developed using the popular Microsoft 'Help' system and, because of this, the use and navigation of the ISO Manual may already be familiar, especially if you are used to using the Internet Explorer for browsing Internet Web sites.

The viewing area of the ISO Manual is divided into 2 distinct frames with a button bar across the top. The left hand window displays the Contents Tree which shows the layout of the ISO Manual; and the right hand window displays the topic currently selected. As you navigate through the Contents Tree and selecting various topics, the right hand window will also update.

The table below shows the main navigation and location features of the ISO Manual: -

Press the	In order to	Comments
	Retrace your steps. Each time you press the Back button, you will return to the previous topic in order.	Button located on the horizontal tool bar at the top of the ISO Manual window.
	Move to the next topic in the sequence of the Contents pane.	Button located at the top right of each topic page displayed in the right hand pane.
	Move to the previous topic in the sequence of the Contents pane.	Button located at the top right of each topic page displayed in the right hand pane.
	Return to the beginning of the current chapter, or if pressed at the bottom of a page, Return to the top of the current page.	Button located at the top right of each topic page displayed in the right hand pane.



Conteúdo do Manual do ISO

- Estabelecimento de uma estrutura formal de SI
- Obtenção de conselhos e orientação
- Políticas de SI
- Preparação e classificação de Informações e Dados
- Autorização de acesso
- Deveres e responsabilidades do ISO
- Funções administrativas do ISO
- Avaliação de riscos de SI
- Redução de riscos com computadores portáteis
- Gestão segura de correções de dados emergenciais
- Auditoria e conformidade de SI
- Gestão do processo do plano de continuidade de negócios
- Tratamento de questões de SI em recursos humanos
- Tratamento de incidentes de SI



Exemplo: Plano de Continuidade do Negócio (BCP)

- Estágio 1: Iniciar o plano
- Estágio 2: Avaliar riscos e prováveis impactos
- **Estágio 3: Desenvolver o Plano**
- Estágio 4: Testar o plano
- Estágio 5: Treinar e conscientizar as pessoas
- Estágio 6: Manter e atualizar o plano



Un-Registered Evaluation Copy

1304 BCP Stage 3 - Developing the Plan

Once the assessment stage has been completed, the structure of the BCP can be established. The BCP will contain a range of milestones to move the organisation from its disrupted status towards a return to normal operations.

The first important milestone is the Disaster Recovery process which deals with the immediate aftermath of significant events. This may involve the emergency services or other specialists who are trained to deal with extreme situations.

The next stage is to determine the critical business functions which need to be resumed as a priority. Again, the use of a 5 point rating system may be appropriate with '1' representing the most critical business functions to be resumed.

The BCP will of necessity be extremely detailed and will identify key individuals who should be familiar with their duties and activities under the BCP.

Guidelines on Developing the BCP can be found below.

[Guidelines](#)



Use of the guidance contained within RUSecure™ is subject to our
End User Licence Agreement. ©



BUSINESS CONTINUITY PLANNING STAGE 3

DEVELOPING THE PLAN

A Complex and Detailed Process

The Business Continuity Plan is likely to be both a complex and detailed planning exercise. Irrespective of the nature of your organisation's activities, it is likely to contain a range of milestones which will move the organisation from its disrupted status towards a return to normality of operation. Development of a BCP is an important process as it may well enable the organisation to fully recover from the serious disruption it has experienced. If a current BCP fails when activated through lack of testing, the organisation's business may possibly be seriously jeopardised or fail completely.

Dependencies

Before proceeding to develop the BCP, the previous milestone - Assessing the Risk and Likely Impact - should already have been completed.

Dealing with the Actual Emergency

Part of the planning process is to determine and document how the actual potential emergency situation is to be dealt with. Ensure that there are identified person(s) responsible for handling such emergencies and that a suitable plan is available.

Determining the Critical Business Functions

Involving representatives from all business and functional areas, consider and agree upon the critical business processes which must be resumed as a priority. Consider the impact upon, and options regarding, third party contracts and commitments and how to minimise disruption to them. Determine likely impact on customers, particularly customers who depend upon on-line facilities and services.

Fallback Procedures

Develop individual plans and detailed procedures to be followed by the (skeleton) staff, which will be used as the fallback procedures until the return to normal operations. Consider the key elements which need to be in place for a full return to standard business operations; document these as they will represent a basis for return to normality.

Establish Key Events

Develop the Plan and document the precise way in which the organisation will:-

- Trigger the BCP when required
- Receive 'hand over' from those dealing with the actual emergency situation.
- Establish the core business functions in fallback mode
- Resume normal business operations following restitution of key services and infrastructure
- Maintain and update the plan periodically

BCP Sign Off

Have each business unit review, agree and sign off the BCP. Initiate a formal test of the process for the BCP.

Associated guidelines can be viewed in documents [080101G1](#), [080102G1](#), [080104G1](#), [080105G1](#), [080106G1](#).



- Callio Technologies oferece ferramentas para conformidade com ISO 17799 e certificação em BS 7799-2
- Produtos
 - Callio Secura 17799
 - Callio Toolkit 17799
- Os produtos Callio auxiliam as organizações a implementar controles internos para SI, indo além das soluções técnicas tradicionais



Callio Secura 17799



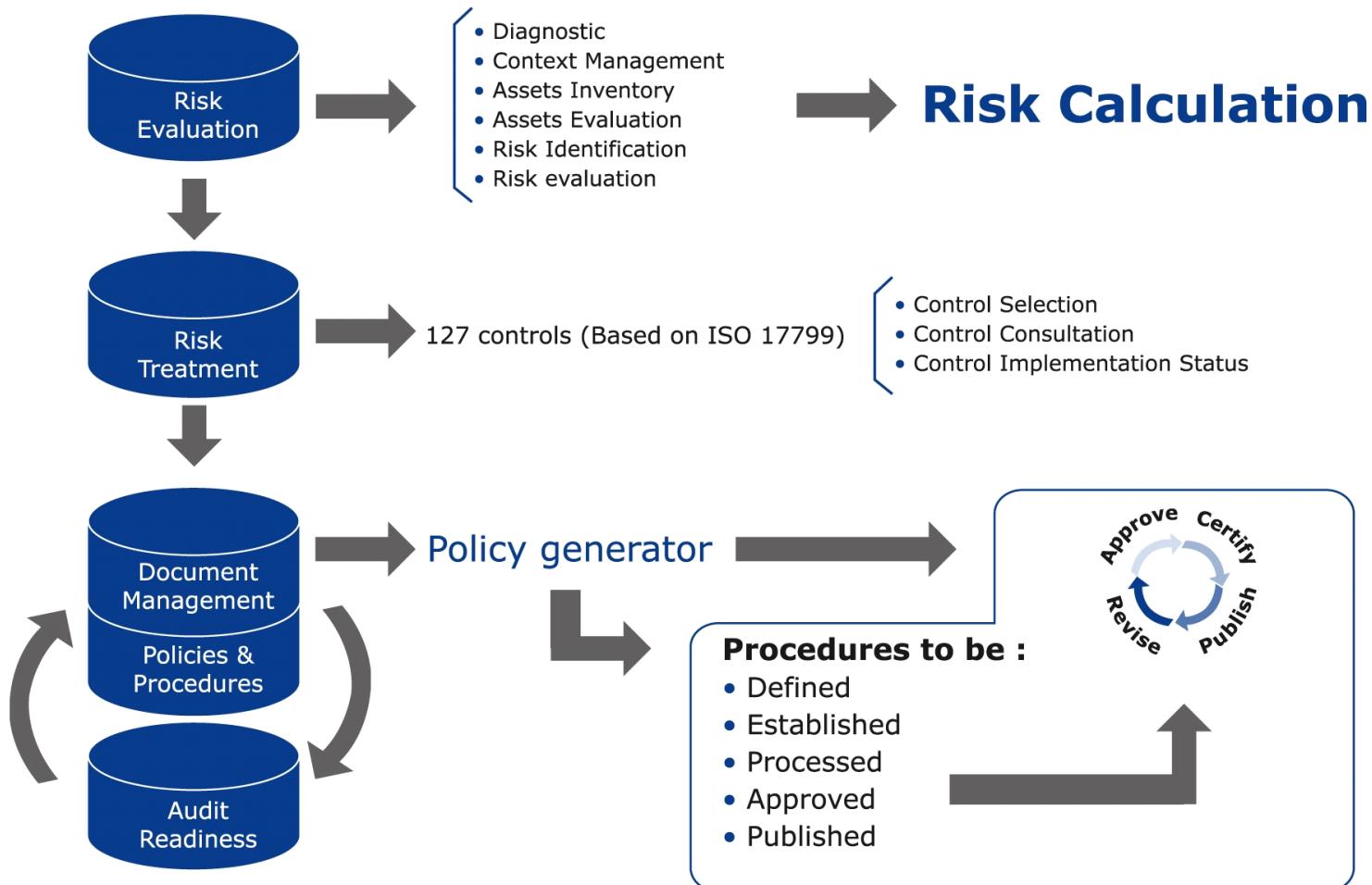
- Baseado na metodologia para ISMS de BS 7799-2, Callio Secura 17799, oferece um conjunto de funcionalidades para ajudar as organizações com gestão e avaliação de riscos e gestão de documentos
- Funcionalidades:
 - Verificação do nível de conformidade com ISO 17799
 - Averiguação do ISMS para certificação BS 7799-2
 - Criação de inventário dos ativos mais importantes
 - Definição das estruturas e processos do ISMS
 - Minimização dos riscos de cada ativo
 - Definição dos cenários de implementação dos controles
 - Esboçar políticas de segurança (mais de 50 exemplos)
 - Gestão do documento de políticas
 - Customização de questionários
 - Metodologias, administração ferramentas, requisitos...



Callio Secura 17799



TOOL



[Home](#)[Home](#)

Methodology



Callio Secura 17799 Methodology

Learn how to implement the ISO 17799 standard and progress toward certification.

Information Security Management



Risk Assessment

Identify and assess the risks associated with the assets you wish to protect.



Risk Treatment

Select and implement the ISO 17799 controls that will reduce risks by order of priority.



Audit Preparation

Validate your information security framework before the external auditor arrives.

Tools



Document Management



Reports



Glossary

Administration



System Management



Project Management

What's New ?



Callio Secura 17799 Online



Callio Toolkit Pro 17799



- Conjunto de ferramentas e documentos para atingir os requisitos de ISO 17799 e BS 7799-2
- Ferramentas:
 - Gerador de políticas
 - Moldes (*templates*) de implementação
 - Módulo de preparação de auditoria (BS 7799-2)
 - Metodologia de implementação
 - Gerador de relatórios
 - Padrões ISO 17799 e BS 7799-2



Callio Toolkit Pro 17799

Main Menu 

www.callio.com

CallioToolkit Demo v1.0.2

ISO Diagnostic	Risk Control	Documentation Center
Compliance Diagnostic	Policies Management	Guide & Documentation
ISMS Diagnostic	Templates	Glossary

Want to buy the full version ?

Need a more powerful tool ?

© All rights reserved. Callio Technologies Inc.



Diagnóstico de conformidade

ISO 17799 Compliance Diagnostic

Summary by Section

In Demo, first few elements are available.

[Summary by Domain](#) [Print Report](#)

No	Section	Answered	%	
3.1	Information security policy	0/2	0%	Details
4.1	Information security infrastructure	0/7	0%	Details
4.2	Security of third party access	0/2	0%	Details
4.3	Outsourcing	0/1	0%	Details
5.1	Accountability for assets	0/1	0%	Details
5.2	Information classification	0/2	0%	Details
6.1	Security in job definition and resourcing	0/4	0%	Details
6.2	User training	0/1	0%	Details
6.3	Responding to security incidents and malfunctions	0/5	0%	Details
7.1	Secure areas	0/5	0%	Details
		0/127	0%	

Documento de Política de SI

ISO 17799 Compliance Diagnostic

Diagnostic Questions

In Demo, first few elements are available.

[Back to Summary](#)

Question : 1 of 2 (Mandatory Control)

3.1 Information security policy

3.1.1 Information security policy document

Question

Is a published policy document, approved by management, published and communicated, as appropriate, to all employees?

Answer

[Guide](#)

Yes
No

Reasons

#1
#2
#3

- Budget
- Culture
- Environnement
- Legislation
- Technology
- Time
- Accepted Risk
- Transferred Risk

[Previous Section](#) [Previous Question](#)



Documento de Política de SI

Guia de Auditoria

Guide

Audit Guide

3.1.1 - Information security policy document

This policy does not need to be extremely extensive, but clearly state senior management's commitment to information security, be under change and version control and be signed by the appropriate senior manager. The policy should at least address the following issues:

- a definition of information security,
- reasons why information security is important to the organization, and its goals and principles,
- a brief explanation of the security policies, principles, standards and compliance requirements,
- definition of all relevant information security responsibilities (see also 4.1.3),
- reference to supporting documentation.

The auditor should ensure that the policy is readily accessible to all employees and that all employees are aware of its existence and understand its contents. The policy may be a stand-alone statement or part of more extensive documentation (e.g. a security policy manual) that defines how the information security policy is



Diagnóstico do ISMS

ISMS Diagnostic X

Summary by Section

In Demo, first few elements are available.

[Print Report](#)

No	ISMS Section	Answered	%	
1	Establishing and managing the ISMS	0/45	0%	Details
2	Documentation requirements	0/14	0%	Details
3	Management responsibility	0/4	0%	Details
4	Management review of the ISMS	0/12	0%	Details
5	ISMS improvement	0/6	0%	Details
		0/81	0%	



Estabelecer/gerenciar o ISMS

 ISMS Diagnostic X

Diagnostic Questions

In Demo, first few elements are available.

[Back to Summary](#)

1 Establishing and managing the ISMS Question : 29 of 45

(PD 3003: 4.2.2.a - Implement and operate the ISMS)

Question

Is there a process in place and being used for formulating a risk treatment plan that identifies the appropriate management action, responsibilities and priorities for managing information security risks?

Justification

Answer

[Guide](#)

Reasons

#1

#2

#3

[Previous Section](#) [Previous Question](#) [Next Question](#) [Next Section](#)



Relatório de diagnóstico

Report : ISMS Diagnostic

ISMS Diagnostic

1 Establishing and managing the ISMS Questions

4.2.2.c - Implement and operate the ISMS

Question: Is there a process in place and being used for implementing the controls selected in order to meet the control objectives?

Justification:

Answer:

Reasons:

#1

#2

#3

4.2.1.a.1 - Establish the ISMS - Scope of the ISMS

Question: Is there a document that describes unambiguously the scope of the ISMS?

Página: 1

Edição de Políticas

Policies Management

Selection of a Policy

In Demo, first few elements are available.

Policy No.	Title
1	Information security policy
2	Information security infrastruc...
3	Security of third party acc...
4	Outsourcing
5	Accountability for assets
6	Information classification
7	Security in job definition a...
8	User training
9	Responding to security inc...
10	Secure areas
11	Equipment security
12	General controls
13	Operational procedures

Policies Management

Edition of a Policy

In Demo, first few elements are available.

General Informations

Policy No. : 1

Title : Information security policy

Objective : The management of Organisation X wishes to set a clear policy direction and demonstrate ongoing support for information security.

Scope : This policy is intended for all of Organisation X's personnel and aims to protect information systems by defining the intentions of senior management.

Responsability :

References :

Related to : 3.1 - Information security policy

Guidelines

Selected	Cust.	No.	Title	Add New Guideline
<input checked="" type="checkbox"/>			Information protection	<button>Details</button> <button>Delete</button>
<input checked="" type="checkbox"/>			Information security standards specific to the field of activit...	<button>Details</button> <button>Delete</button>
<input checked="" type="checkbox"/>			Information use	<button>Details</button> <button>Delete</button>
<input checked="" type="checkbox"/>			Review of security controls	<button>Details</button> <button>Delete</button>

Moldes (*templates*)

Templates Consultation

Selection of a Template

In Demo, first few elements are available.

3.1.1 Information security policy document

[Back ISO Controls](#)

Manual of Security Policies

Document : [7-SecPolManual.doc](#)
Type : Examples

Memorandum

Document : [3-Memorandum.doc](#)
Type : Templates

 callio >
technologies

MANUAL OF INFORMATION SECURITY POLICIES

1. INTRODUCTION

GOAL OF THE SECURITY POLICY

Organization X depends on information and information systems. The goal of the security policy is to set objectives for the organization as regards the protection of its informational assets. The security policy provides the basis for the implementation of security controls that reduce risks and system vulnerabilities. By clarifying the responsibilities of users and the measures they must adopt to protect information and systems, Organization X avoids serious losses or unauthorized disclosure. Moreover, the company's good name is partly dependant on the manner in which it protects its information and information systems. Finally, a security policy can be useful as evidence in litigations, in client contract negotiations, during acquisition bids and for business relations in general. The management of Organization X has initiated and continues to sustain an information security effort thanks to the development of sound policies and procedures.

SECURITY MANAGEMENT FRAMEWORK

All policies and procedures included in this document are approved, supported and defended by the senior management of Organization X. As respect of the security policy is all important to the organization, it is of great interest that the information contained in this document is used and applied in a consistent manner throughout the organization.



Cobra ISO 17799 Consultant

- Baseado em questionários de múltipla escolha:
- Permite:
 - Estabelecer o nível de conformidade para cada uma das 10 áreas cobertas pelo padrão ISO/IEC 17799
 - Identificar quais controles adicionais podem ser aplicados para aumentar a conformidade e aumentar a segurança
 - Produzir relatórios abrangentes e profissionais
- Não fala de ISMS
- COBRA possui também o “Risk Consultant”

Cobra ISO 17799 Consultant

Risk Surveyor

Question Module Selection Menu

Module	Module Description
ASSETCLA	Asset Classification and Control (Sec 5) IT/IT Security Manager
BUSCON	Business Continuity Planning (Sec 11)
COMNETMA	Computer & Operations Management (Sec 8)
COMPLIAN	Compliance (Sec 12)
PERSONNE	Personnel Security (Sec 6)
PHYSEC	Physical and Environmental Sec. (Sec 7)
SECORG	Security Organisation (Sec 4)
SECPOL	Security Policy (Sec 3)
SYSACC	System Access Control (Sec 9)
SYSDEV	System Dev. and Maintenance (Sec 10)

Completer

Risk Surveyor - Question Module SYSACC

Question 3 of 52

MULTIPLE responses are OPTIONAL

Which of the following does the access control policy NOT take into account?

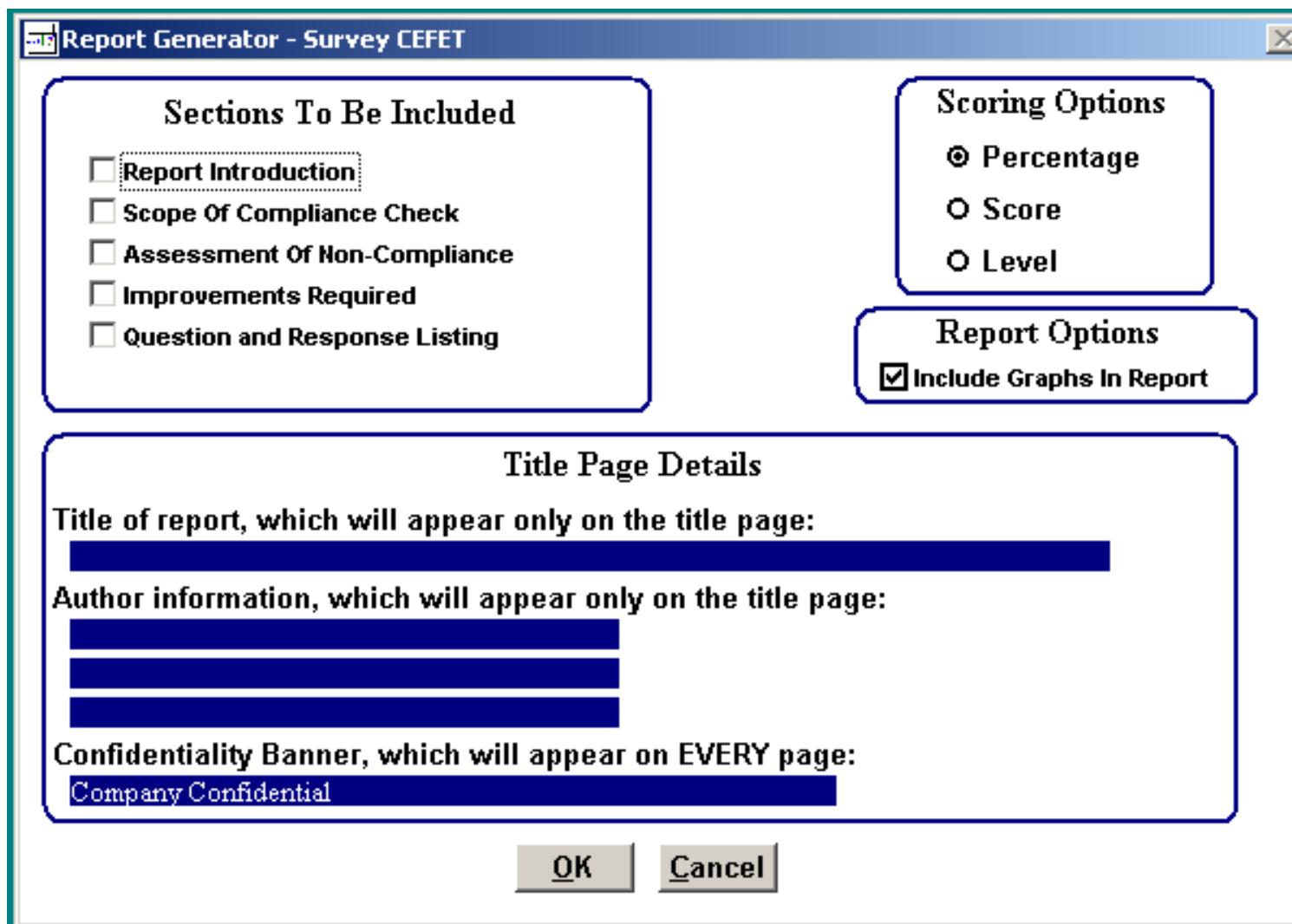
Individual business security
 Information dissemination
 Contractual/Legal Requirements
 Link with Classification Policy
 Networking Considerations

OK

F1=Help F3=Quit F5=Goto F7=Notepad F9=Skip

<< Highlight required response and click left mouse button - press OK when complete >>

Cobra ISO 17799 Consultant Report Generator



Protecting your important information assets

Information Security Management

BS 7799
Information
Security
SME Guide

	Home
	Directory
	EasyGuides
	EasyChecks

your information is@risk



virus and worm attacks, unauthorised access, data theft, system failure, on-line fraud, breach of law, denial of service

protect it with BS 7799 best practice

Welcome to the **SME Guide home page** on BS 7799 Information Security.

The aim of this SME guide is to provide an information resource on a variety of topics related to best practice and BS 7799. It includes a number of short "Easy Guides, Check Lists and Explanatory Notes" which give advice on the things to do, things to remember and things to check in order to implement and comply with the BS 7799 standard.

The guide provides a starting point for SMEs to protect their information and to protect their business.

Here is a "how to use" map of the SME Guide

ROAD MAP

Contacts

Go to the Directory page to check out details of other sources of advice, for a set of FAQs and easy explanations. The Directory also has a link to the **AEB Web Security Guidelines** which is contained in this SME Guide.

Go to the EasyGuide page to check out a number of guidelines on various BS 7799 topics including information security starting point and risk assessment made easy.

Go to the EasyCheck page to check out the check lists including:

- Making backups
- Virus protection
- Information security policy
- Responding to incidents
- Physical security



SME Guide - Easy Check

Protecting your important information assets Information Security Management

EasyCheck

There are seven Easy Check documents available on this SME Guide.

- ◆ [Information Security Policy](#)
- ◆ [Protecting Your Information](#)
- ◆ [Don't Lose It – Back It Up](#)
- ◆ [Protecting Personal Data](#)
- ◆ [Virus and Worm Attacks](#)
- ◆ [Responding to Incidents](#)
- ◆ [Achieving Physical Security](#)

Click on the hyperlinks above to check out the Easy Checks.

The purpose of these Easy Check documents is to provide you with information to enable you to start addressing information security in your company. Together with the Easy Guides contained in this SME Guide they provide a starting point to implement best practice based on the controls featured in ISO/IEC 17799 (BS 7799).

As these Easy Check documents are intended as a starting point they do not cover all the controls in ISO/IEC 17799 (BS 7799) however they cover enough of the key best practice features of the standard to address many of the common threats and risks to your business assets.

If you go down the **Starting Point Route** then maybe you want to do a compliance check

 **Go To Starting Point
Compliance Check**



Bookmarks **Signatures** **Layers** **Pages** **Comments**

Easy Check

Starting Point Compliance Check

As mentioned in the [Doing something to protect your important assets](#) guide, there are some immediate, easy to use best practice security controls that you can put in place to protect yourself and your business. This Starting Point Compliance Check is based on a "gap analysis", which is a simple question & answer process that establishes whether or not a security control has been implemented according to the BS 7799 standard. Several questions per control may be used to arrive at an answer. The more questions that are asked the greater the accuracy of the answers arrived at as to whether or not you are compliant.

You can use the questions in this Starting Point Compliance Check to have a quick check of how much of these starting points you have in place already, and where you easily can improve the security in place.

So answer the following questions for each of the topics, and if your answer is "Not compliant" or "Partially compliant", then you should try to find out why, and to identify where improvements are necessary. The possible answers are:

- **Compliant (C)** – the issue addressed by the question is in place and there is evidence it is being fully implemented and used in compliance with the standard.
- **Partially compliant (PC)** – the issue addressed by the question is partially in place and there is evidence to demonstrate partial compliance with the standard.
- **Not compliant (NC)** – the issue addressed by the question is not in place at all.
- **Not applicable (NA)** – the issue addressed by the question is not applicable to your ISMS and you can justify why this is the case.