EXIN Information Security Management ISO/IEC 27001 PROFESSIONAL

Guia de preparação

Edição 201811

Conteúdo

1. Visão Geral

EXIN Information Security Management Professional based on ISO/IEC 27001 (ISMP.PR)

Escopo

O módulo EXIN Information Security Management Professional baseado na ISO/IEC 27001 (ISMP.PR) testa seus conhecimentos sobre os aspectos organizacionais e gerenciais da segurança da informação.

Os tópicos para este módulo são:

- Perspectivas em segurança da informação: negócio, cliente, provedor de serviços/fornecedor
- Gerenciamento de Risco: análise, controles, riscos residuais
- Controles de segurança da informação: organizacionais, técnicos, físicos.

Resumo

A segurança da informação é a preservação da confidencialidade, integridade e disponibilidade de informações (definição da norma ISO/IEC 27000).

A segurança da informação vem ganhando importância no mundo da Tecnologia de Informação (TI). A globalização da economia conduz a um crescente intercâmbio de informações entre as organizações (seus funcionários, clientes e fornecedores) e uma explosão no uso de computadores e dispositivos de informática em rede.

Na atualidade, as atividades centrais de muitas empresas dependem completamente da TI. Sistemas de gerenciamento para planejamento de recursos empresariais (ERP), os sistemas de controle que governam o funcionamento de um edifício ou as funções de um equipamento de fabricação, as comunicações no dia-a-dia — tudo — é executado em computadores. A vasta maioria das informações — o bem de consumo mais valioso do mundo — passa pela TI. As informações são cruciais para a continuidade e o funcionamento adequado tanto de organizações individuais quanto das economias que elas alimentam; estas informações devem ser protegidas contra o acesso por pessoas não autorizadas, protegidas contra a modificação ou destruição acidental ou mal-intencionada e devem estar disponíveis quando necessárias. As empresas e os usuários individuais da tecnologia também estão começando a entender a importância da segurança e estão começando a fazer escolhas baseadas na segurança da tecnologia ou do serviço.

Existem outras tendências importantes que estão aumentando a importância da disciplina de Segurança da Informação:

- As exigências de conformidade estão aumentando: A maioria dos países conta com múltiplas leis ou regulamentos que controlam o uso e exigem a proteção de vários tipos de dados. Estas leis são cada vez mais numerosas e suas exigências estão crescendo.
- Muitas indústrias, particularmente o mundo financeiro, têm regulamentos além daqueles impostos por um governo. Estes também estão crescendo em número e complexidade.
- Normas de segurança estão sendo desenvolvidas e refinadas nos níveis industrial, nacional e internacional.
- Certificações de segurança e uma prova auditável de que uma organização está seguindo as normas e/ou melhores práticas de segurança algumas vezes são exigidas como uma condição para a realização de negócios com uma determinada organização ou em uma região ou país específico.

A norma internacional para Segurança da Informação ISO/IEC 27001:2013, é uma norma amplamente respeitada e citada e fornece uma estrutura para a organização e o gerenciamento de um programa de segurança da informação. A implementação de um programa baseado nesta norma será bastante útil para uma organização em sua meta de atender às diversas exigências encontradas no complexo ambiente operacional da atualidade. Um conhecimento robusto desta norma é importante para o desenvolvimento pessoal de todos os profissionais da área de segurança da informação.

A seguinte definição é usada nos módulos de Segurança da Informação do EXIN: A Segurança da Informação lida com a definição, a implementação, a manutenção, a conformidade e a avaliação de um conjunto coerente de controles que protegem a disponibilidade, a integridade e a confidencialidade do suprimento (manual e automatizado) de informações.

Contexto

O certificado EXIN Information Security Management Professional é baseado no certificado de EXIN Information Security Foundation, onde os conceitos básicos de segurança da informação são testados.

Grupo alvo

Profissionais de segurança. Este módulo é voltado para qualquer pessoa que esteja envolvida na implementação, avaliação e reporte de segurança da informação, tais como um Gerente de Segurança da Informação (ISM), Executivo de Segurança da Informação (ISO) ou um Gerente de Linha, Gerente de Processo ou Gerente de Projeto com responsabilidades relevantes.

Conhecimento básico em Segurança da Informação é recomendado como por exemplo, através da certificação do ISFS (EXIN Information Security Foundation based on ISO/IEC 27001).

Requisitos para a certificação

- Curso de treinamento Information Security Management Professional com um provedor de treinamento credenciado pelo EXIN (ATO), incluindo a realização efetiva dos dois exercícios práticos como parte do curso.
- Realização e aprovação no exame EXIN Information Security Management Professional based on ISO/IEC 27001.

Detalhes do exame

Tipo de exame:	Perguntas de múltipla escolha
Número de perguntas:	30
Nota de aprovação:	65%
Com consulta/observações:	Não
Equipamentos eletrônicos permitidos:	Não
Tempo designado para o exame:	90 minutos

O As Regras e Regulamentos dos exames EXIN aplicam-se a este exame.

Nível Bloom

A certificação EXIN Information Security Management Professional based on ISO/IEC 27001 testa os candidatos nos Níveis Bloom 3 e 4 de acordo com a Taxonomia Revisada de Bloom:

- Nível Bloom 3: Aplicação – mostra que os candidatos têm a capacidade de utilizar as informações em um contexto diferente daquele em que elas foram aprendidas.
  Este tipo de pergunta pretende demonstrar que o candidato é capaz de resolver problemas em novas situações, aplicando o conhecimento adquirido, fatos, técnicas e regras de um modo novo ou diferente. A pergunta geralmente contém um breve cenário.
- Nível Bloom 4: Análise – mostra que os candidatos têm a capacidade de decompor as informações aprendidas em suas partes para compreendê-las. Este nível Bloom é testado principalmente nos exercícios práticos. Os exercícios práticos têm o objetivo de demonstrar que o candidato é capaz de examinar e decompor a informação em partes, identificando motivos ou causas, fazer inferências e encontrar evidências para respaldo de generalizações.

Treinamento

Horas de contato

O número mínimo de horas presenciais para esse treinamento é de 20 horas. Isso inclui atribuições práticas, preparação para o exame e paradas curtas (breaks). Este número de horas não inclui tarefas para casa, a logística (preparação) relacionada à sessão do exame, a sessão do exame e intervalos de almoço.

Carga de estudos indicade

120 horas, dependendo do conhecimento existente.

Provedores de treinamento

Você pode encontrar a lista dos nossos provedores de treinamento: www.exin.com.

2. Requisitos do exame

Os requisitos do exame estão listados nas especificações do exame. A tabela a seguir lista os tópicos (requisitos do exame) e os subtópicos do módulo (especificações do exame).

Requisito do exame	Especificação do exame	Peso
1. Perspectivas em segurança da informação		**10%**
	1.1 O candidato compreende o interesse para o negócio da segurança da informação.	3.3%
	1.2 O candidato compreende o ponto de vista do cliente sobre o controle da informação.	3.3%
	1.3 O candidato compreende as responsabilidades do fornecedor em garantir a segurança.	3.3%
2. Gerenciamento de Risco		**30%**
	2.1 O candidato compreende os princípios de gerenciamento de risco.	10%
	2.2 O candidato sabe como controlar os riscos.	10%
	2.3 O candidato sabe como lidar com os riscos residuais.	10%
3. Controles de segurança da informação		**60%**
	3.1 O candidato tem conhecimento sobre controles organizacionais.	20%
	3.2 O candidato tem conhecimento sobre controles técnicos.	20%
	3.3 O candidato tem conhecimento sobre controles físicos, relacionados a recursos humanos e de continuidade de negócios.	20%
	Total	100%

Especificações do exame

1. Perspectivas em segurança da informação

1.1 O candidato compreende o interesse para o negócio da segurança da informação.

O candidato pode...

1.1.1 distinguir os tipos de informação com base em seu valor para o negócio.

1.1.2 explicar as características de um sistema de gerenciamento para segurança da informação.

1.2 O candidato compreende o ponto de vista do cliente sobre o controle da informação.

O candidato pode...

1.2.1 explicar a importância do controle da informação ao terceirizar.

1.2.2 recomendar um fornecedor com base na garantia dos controles de segurança.

1.3 O candidato compreende as responsabilidades do fornecedor em garantir a segurança.

O candidato pode...

1.3.1 distinguir aspectos da segurança em processos de gerenciamento de serviços.

1.3.2 apoiar atividades para conformidade.

2. Gerenciamento de Risco

2.1 O candidato compreende os princípios de gerenciamento de risco.

O candidato pode...

2.1.1 explicar os princípios da análise de riscos.

2.1.2 identificar riscos baseados na classificação dos ativos.

2.1.3 calcular os riscos baseados na classificação dos ativos.

2.2 O candidato sabe como controlar os riscos.

O candidato pode...

2.2.1 classificar os controles com base na Confidencialidade, Integridade e Disponibilidade (CIA).

2.2.2 escolher controles com base nos estágios do ciclo de vida do incidente.

2.2.3 escolher diretrizes relevantes para a aplicação dos controles.

2.3 O candidato sabe como lidar com os riscos residuais.

O candidato pode...

2.3.1 distinguir estratégias de risco.

2.3.2 produzir casos de negócios para controles.

2.3.3 produzir relatórios sobre as análises de risco.

3. Controles de segurança da informação

3.1 O candidato tem conhecimento sobre controles organizacionais.

O candidato pode...

3.1.1 redigir políticas e procedimentos de segurança da informação.

3.1.2 implementar estratégias para gerenciamento de incidentes de segurança da informação.

3.1.3 realizar uma campanha de conscientização na organização.

3.1.4 implementar papéis e responsabilidades para segurança da informação.

3.2 O candidato tem conhecimento sobre controles técnicos.

O candidato pode...

3.2.1 explicar a finalidade das arquiteturas de segurança.

3.2.2 explicar a finalidade dos serviços de segurança.

3.2.3 explicar a importância dos elementos de segurança na infraestrutura de TI.

3.3 O candidato tem conhecimento sobre controles físicos, relacionados a recursos humanos e de continuidade de negócios.
O candidato pode...

3.3.1 recomendar controles para acesso físico.

3.3.2 recomendar controles de segurança para o ciclo de vida do emprego.

3.3.3 favorecer o desenvolvimento e o teste de um plano de continuidade de negócios.

3. Lista de conceitos básicos

Este capítulo contém os termos com que os candidatos devem se familiarizar.

Por favor, note que o conhecimento destes termos de maneira independente não é suficiente para o exame; O candidato deve compreender os conceitos e estar apto a fornecer exemplos.

Inglês	Português
acceptance	aceitar
access management	gerenciamento de acesso
asset	ativo
attack	ataque
audit	auditoria
authentication	autenticar
authorization	autorização
availability	disponibilidade
avoidance	evitar
awareness (campaigns)	(campanhas de) conscientização
business continuity (plan)	(plano de) continuidade de negócios
Business Impact Analysis (BIA)	Análise de Impacto no Negócio (BIA - Business Impact Analysis)
Certificate Authority (CA)	Autoridade de Certificação (CA)
Cloud computing	Computação em nuvem
code of practice for information security	código de práticas de segurança da informação
compliance	conformidade
confidentiality	confidencialidade
controls	controles
cryptography	criptografia
defense	evitar
Delphi	Delphi
disaster recovery plan	plano de recuperação de desastres
encryption	encriptação
escrow agreement	acordo judicia
event management	gerenciamento de eventos
FAIR	FAIR
firewall	firewall
Host-Based Intrusion Detection and Protection System (Host-Based IDPS)	Sistema de Detecção de Intrusão e Proteção Baseado no Host (IDPS)
incident management	gerenciamento de incidentes
incident response plan	plano de resposta a incidentes
Information Security Management System (ISMS)	Sistema de Gerenciamento de Segurança de Informação (ISMS)
information security perspectives	perspectivas em segurança da informação
information security program	programa de segurança da informação
integrity	integridade

Intrusion Detection System	Sistema de Detecção de Intrusão
ISO/IEC 27001	ISO/IEC 27001
ISO/IEC 27002	ISO/IEC 27002
IT strategy	Estratégia de TI
legislation	legislação
logical access control	controle de acesso lógico
Microsoft Risk Management Approach	Abordagem de Gestão de Riscos da Microsoft
mitigation	mitigar
mitigation plan	plano de mitigação
network content filter	filtro de conteúdo de rede
Network-Based Intrusion Detection and Protection System (Network-Based IDPS)	Sistema de Detecção de Intrusão e Proteção Baseado na Rede (IDPS)
open design	designs abertos
perimeter	perímetro
physical access control	controle de acesso físico
Plan-Do-Check-Act (PDCA) cycle	Ciclo Planejar-Fazer-Verificar-Agir (Plan, Do, Check, Act - PDCA)
policy	política
private key	chave particular
problem management	gerenciamento de problemas
procedure	procedimento
protocol	protocolo
public key	chave pública
Public Key Infrastructure (PKI)	Infraestrutura de Chave Pública (PKI)
Recovery Point Objective (RPO)	Objetive de Ponto de Recuperação (RPO)
Recovery Time Objective (RTO)	Objetivo de Tempo de Recuperação (RTO)
residual risk	risco resídua
retention policy	política de retenção
risk	risco
risk analysis	análise de riscos
risk appetite	apetite de riscos
risk assessment	avaliação dos riscos
risk management framework	estrutura de gerenciamento de riscos
risk manager	gerente do risco
risk strategy	estratégia de risco
risk treatment (plan)	(plano de) tratamento de riscos
security architecture	arquitetura de segurança
security governance	governança de segurança
security services	serviços de segurança
Service Oriented Architecture (SOA)	Arquitetura Orientada para Serviços
Statement of Applicability	Declaração de Aplicabilidade
third party	terceira parte
threats	ameaças
topic-specific policy	política específica de tópicos
Total Cost of Ownership (TCO)	Custo total da Posse (TCO)

transference	transferir
Virtual Private Network (VPN)	VPN
vulnerability	vulnerabilidade
zoning	zoneamento

4. Literatura

Literatura do exame

O conhecimento necessário para o exame EXIN Information Security Management Professional based on ISO/IEC 27001 é abordado na seguinte literatura:

A. Cazemier, J.A., Overbeek, P. e Peters, L.
Information Security Management with ITIL V3
Van Haren Publishing: 2010
ISBN: 978 90 8753 552 0

B. Whitman, M.E., Mattord, H.J.
Management of Information Security
Cengage learning: 2018 (sexto edição)
ISBN: 978 1 337 40571 3
https://www.cengagebrain.co.uk/shop/isbn/9780357192795

C. ISO/IEC 27001:2017 (EN)
Information technology – Security techniques – Information security management systems – Requirements
Suíça, ISO/IEC, 27001

Literatura adicional

D. BSI-standard 100-2
IT-Grundschutz Methodology
Bundesamt für Sicherheit in der Informationstechnik
A versão em inglês está disponível para download no Partnernet ou http://bit.ly/bsi-standard_100-2

E. ISO/IEC 27005:2018 (EN)
Information technology -- Security techniques -- Information security risk management
Suíça, ISO/IEC, 2018
www.iso.org

F. Pfleeger, Charles P. and Pfleeger, Shari Lawrence
Security in Computing, quarto edição
Upper Saddle River NJ, Prentice Hall, 2006
ISBN 978 0132390774

G. ISO/IEC 27000:2018 (EN)
Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
Suíça, ISO/IEC, 2018
www.iso.org

H. ISO/IEC 27002:2017 (EN)
Information technology -- Security techniques – Code of practice for information security controls
Suíça, ISO/IEC, 2017
www.iso.org

Comentários

- A literatura adicional destina-se apenas a referência e aprofundamento do conhecimento.
- A Literatura **B** fornece um **Glossário** de termos que, se relacionados aos capítulos mencionados na visão geral da literatura a seguir, constituem conceitos básicos para os exames.
- Na Literatura **B,** Capítulo 6, os modelos citados na página 222 não precisam ser conhecidos.
- Na Literatura **B**, Capítulo 6, figura 6-3 na página 230; a seta deveria estar virada para a direita e não para a esquerda (Planejar – Fazer – Verificar – Agir)

Referência da literatura

Requisito do exame	Especificação do exame	Literatura
1. Perspectivas em segurança da informação		
	1.1 O candidato compreende o interesse para o negócio da segurança da informação.	A: §1.1.1-1.1.4, §2.1, Cap. 3, §5.6 B: §1.1, §6.2
	1.2 O candidato compreende o ponto de vista do cliente sobre o controle da informação.	A: §5.3.4, §5.7, Annexo A C: Annexo A 15
	1.3 O candidato compreende as responsabilidades do fornecedor em garantir a segurança.	A: Cap. 4, Annexo A B: §1.1, §9.2, §9.4 C: Annexo A 12.7, 15, 18
2. Gerenciamento de Risco		
	2.1 O candidato compreende os princípios de gerenciamento de risco.	A: §4.3 B: Cap. 6 C: Annexo A 8
	2.2 O candidato sabe como controlar os riscos.	A: §2.1, §3.2 B: Cap. 5, §6.2, Cap. 7, §8.3 C: Annexo A 6, 14
	2.3 O candidato sabe como lidar com os riscos residuais.	A: §2.1, §4.5 B: Cap. 7, §12.2 C: §7.5, Annexo A 16
3. Controles de segurança da informação		
	3.1 O candidato tem conhecimento sobre controles organizacionais.	A: §2.1, §3.2, §4.5, §5.2, 5.3, §5.5, Annexo A B: Cap. 10, §2.4, §3.3, Cap. 4, Cap. 5, §7.1, Cap. 8 C: Cap. 5, Annexo A 5, 6.1, 7, 9, 16
	3.2 O candidato tem conhecimento sobre controles técnicos.	A: Cap. 2 B: Cap. 8, Cap. 12 C: Annexo A 9, §12.1-12.4, §13.1-13.2
	3.3 O candidato tem conhecimento sobre controles físicos, relacionados a recursos humanos e de continuidade de negócios.	A: §2.2, §5.3 B: Cap. 10, Cap. 11, §12.1 C: Annexo A 7, 11, 17

Contato EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER