Guia de preparação

Edição 202509

Conteúdo

1. Visão geral

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

Escopo

A certificação EXIN Information Security Management Professional based on ISO/IEC 27001 confirma que o profissional pode gerenciar os riscos de segurança da informação organizacionais, de pessoas, físicos e tecnológicos, respeitando as preferências das partes interessadas.

Esta certificação inclui os seguintes tópicos:

- perspectivas em segurança da informação
- gerenciamento de riscos
- controles de segurança da informação

Resumo

A globalização da economia conduz a uma crescente troca de informações. As informações cruzam não apenas as fronteiras dos países, mas também a linha tênue entre a vida privada e a área de negócios. O âmbito da responsabilização cresce juntamente com a informação que é gerenciada. Essa informação deve ser protegida contra o acesso por pessoas não autorizadas e contra modificação ou destruição acidental ou mal-intencionada e deve estar disponível quando necessário.

Existem outras tendências 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. Essas 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 esteja seguindo as normas e/ou melhores práticas de segurança algumas vezes são exigidas como uma condição para a realização de negócios.

A ISO/IEC 27001, norma internacional para gestão de segurança da informação, é amplamente respeitada e referenciada, fornecendo uma estrutura para a organização e gerenciamento de um programa de segurança da informação. A implementação de um programa baseado nessa 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 dessa norma é importante para o desenvolvimento pessoal de todos os profissionais da área de segurança da informação.

No programa EXIN Information Security Management based on ISO/IEC 27001, a seguinte definição é usada: a segurança da informação é a preservação da confidencialidade, integridade e disponibilidade da informação.

Contexto

A certificação EXIN Information Security Management Professional based on ISO/IEC 27001 faz parte do programa de qualificação EXIN Information Security Management based on ISO/IEC 27001.

Público-alvo

Esta certificação se destina a todos os profissionais de segurança envolvidos na implementação, avaliação e reporte de um programa de segurança da informação, incluindo as seguintes funções:

- information security manager (ISM)
- information security officer (ISO)
- gerente de linha
- gerente de processo
- gerente de projeto com responsabilidades de segurança

Requisitos para a certificação

- Conclusão bem-sucedida do exame EXIN Information Security Management Professional based on ISO/IEC 27001.
- Treinamento credenciado de EXIN Information Security Management Professional based on ISO/IEC 27001, incluindo exercícios práticos.

Detalhes do exame

Tipo do exame:	Questões de múltipla escolha
Número de questões:	30
Mínimo para aprovação:	65% (20/30 questões)
Com consulta:	Não
Anotações:	Não
Equipamentos eletrônicos permitidos:	Não
Tempo designado para o exame:	90 minutos

As Regras e Regulamentos dos exames EXIN aplicam-se a esse 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. Esse 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. Esse 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

A carga horária recomendada para este treinamento é de 21 horas. Isso inclui exercícios práticos, preparação para o exame e pausas curtas. Essa carga horária não inclui pausas para almoço, trabalhos extra aula e o exame.

Indicação de tempo de estudo

112 horas (4 ECTS), dependendo do conhecimento pré-existente.

Provedor de treinamento

Você encontrará uma lista de nossos provedores de treinamento credenciados em www.exin.com.

2. Requisitos do exame

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

Requisitos do exame	Especificações do exame	Peso
1. Perspectivas em segurança da informação		**10%**
	1.1 Interesse do negócio pela segurança da informação	3,3%
	1.2 Perspectiva do cliente sobre governança	3,3%
	1.3 Responsabilidades do fornecedor na garantia de segurança	3,3%
2. Gerenciamento de riscos		**30%**
	2.1 Princípios de gerenciamento de riscos	10%
	2.2 Controlar os riscos	10%
	2.3 Lidar com os riscos residuais	10%
3. Controles de segurança da informação		**60%**
	3.1 Controles organizacionais	20%
	3.2 Controles tecnológicos	20%
	3.3 Controles físicos e controles de pessoas	20%
	Total	**100%**

Especificações do exame

1 Perspectivas em segurança da informação

1.1 Interesse do negócio pela segurança da informação

O candidato é capaz de...

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 gestão para a segurança da informação.

1.2 Perspectiva do cliente sobre governança

O candidato é capaz de...

1.2.1 explicar a importância da governança da informação ao terceirizar.

1.2.2 recomendar um fornecedor com base nos controles de segurança.

1.3 Responsabilidades do fornecedor na garantia de segurança

O candidato é capaz de...

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

1.3.2 apoiar atividades para conformidade.

2 Gerenciamento de riscos

2.1 Princípios de gerenciamento de riscos

O candidato é capaz de...

2.1.1 explicar os princípios da análise de riscos.

2.1.2 identificar os riscos para a classificação dos ativos.

2.1.3 calcular os riscos para a classificação dos ativos.

2.2 Controlar os riscos

O candidato é capaz de...

2.2.1 classificar os controles com base na confidencialidade, integridade e disponibilidade.

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

2.2.3 escolher diretrizes relevantes para a aplicação de controles.

2.3 Lidar com os riscos residuais

O candidato é capaz de...

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 riscos.

3 Controles de segurança da informação

3.1 Controles organizacionais

O candidato é capaz de...

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.

3.1.5 apoiar o desenvolvimento e o teste de um plano de continuidade de negócios.

3.2 Controles tecnológicos

O candidato é capaz de...

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 Controles físicos e controles de pessoas

O candidato é capaz de...

3.3.1 recomendar controles para acesso físico.

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

3. Lista de conceitos básicos

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

Por favor, note que o conhecimento desses 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	autenticação
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)
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	defesa
disaster recovery plan	plano de recuperação de desastres
encryption	encriptação
escrow agreement	acordo judicial
event management	gerenciamento de eventos
firewall	firewall
host-based intrusion detection and prevention system (host-based IDPS)	sistema de detecção e prevenção de intrusão baseado no host (IDPS de host)
incident management	gerenciamento de incidentes
incident response plan	plano de resposta a incidentes
information security management system (ISMS)	sistema de gestão de segurança da informação (SGSI)
information security perspectives	perspectivas em segurança da informação
information security program	programa de segurança da informação
integrity	integridade
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
mitigation	mitigação
mitigation plan	plano de mitigação
network content filter	filtro de conteúdo de rede

network-based intrusion detection and prevention system (network-based IDPS)	sistema de detecção e prevenção de intrusão baseado na rede (IDPS de rede)
open design	designs abertos
perimeter	perímetro
physical access control	controle de acesso físico
Plan, Do, Check, Act (PDCA) cycle	Ciclo Planejar, Fazer, Checar, Agir (Plan, Do, Check, Act; PDCA)
policy	política
private key	chave privada
problem management	gerenciamento de problemas
procedure	procedimento
protocol	protocolo
public key	chave pública
public key infrastructure (PKI)	infraestrutura de chave pública (ICP)
Recovery Point Objective (RPO)	objetivo de ponto de recuperação (RPO)
Recovery Time Objective (RTO)	objetivo de tempo de recuperação (RTO)
residual risk	risco residual
retention policy	política de retenção
risk	risco
risk analysis	análise de riscos
risk appetite	apetite de riscos
risk assessment	avaliação de riscos
risk management framework	estrutura de gerenciamento de riscos
risk manager	gerente de riscos
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 (SOA)
Statement of Applicability (SoA)	Declaração de Aplicabilidade (SoA)
third party	terceiro
threat	ameaça
topic-specific policy	política específica de tópicos
Total Cost of Ownership (TCO)	Custo total da Posse (TCO)
transference	transferência
virtual private network (VPN)	rede privada virtual (VPN)
vulnerability	vulnerabilidade
zoning	zoneamento

4. Literatura

Literatura do exame

O conhecimento necessário para o exame é coberto na seguinte literatura:

A. EXIN
EXIN Information Security Management Professional based on ISO/IEC 27001 Body of Knowledge
EXIN (2025)
Acesse www.exin.com. Clique em 'Profissionais' e, em seguida, em 'Certificações' para encontrar a certificação. O download gratuito pode ser encontrado sob 'Leitura obrigatória'.

Literatura adicional

B. ISO/IEC 27000:2018
Information technology – Security techniques – Information security management systems – Overview and vocabulary
Suíça, ISO/IEC, 2018
www.iso.org

C. ISO/IEC 27001:2022
Information security, cybersecurity and privacy protection – Information security management systems – Requirements
Suíça, ISO/IEC, 2022
www.iso.org

D. ISO/IEC 27002:2022
Information security, cybersecurity and privacy protection – Information security controls
Suíça, ISO/IEC, 2022
www.iso.org

E. ISO/IEC 27005:2022
Information security, cybersecurity and privacy protection – Guidance on managing information security risks
Suíça, ISO/IEC, 2022
www.iso.org

Comentário

A literatura adicional destina-se exclusivamente à referência e ao aprofundamento do conhecimento.

Matriz da literatura

Requisitos do exame	Especificações do exame	Referência
1. Perspectivas em segurança da informação		
	1.1 Interesse do negócio pela segurança da informação	A, Slides 010 – 019
	1.2 Perspectiva do cliente sobre governança	A, Slides 020 – 022
	1.3 Responsabilidades do fornecedor na garantia de segurança	A, Slides 023 – 035, 111 – 113
2. Gerenciamento de riscos		
	2.1 Princípios de gerenciamento de riscos	A, Slides 026 – 057
	2.2 Controlar os riscos	A, Slides 009 – 011, 028 – 068, 115
	2.3 Lidar com os riscos residuais	A, Slides 028 – 035, 049 – 052
3. Controles de segurança da informação		
	3.1 Controles organizacionais	A, Slides 023 – 025, 031 – 034, 052 – 053, 058 – 085, 091 – 095
	3.2 Controles tecnológicos	A, Slides 058 – 068, 098 – 115
	3.3 Controles físicos e controles de pessoas	A, Slides 058 – 068, 086 – 097

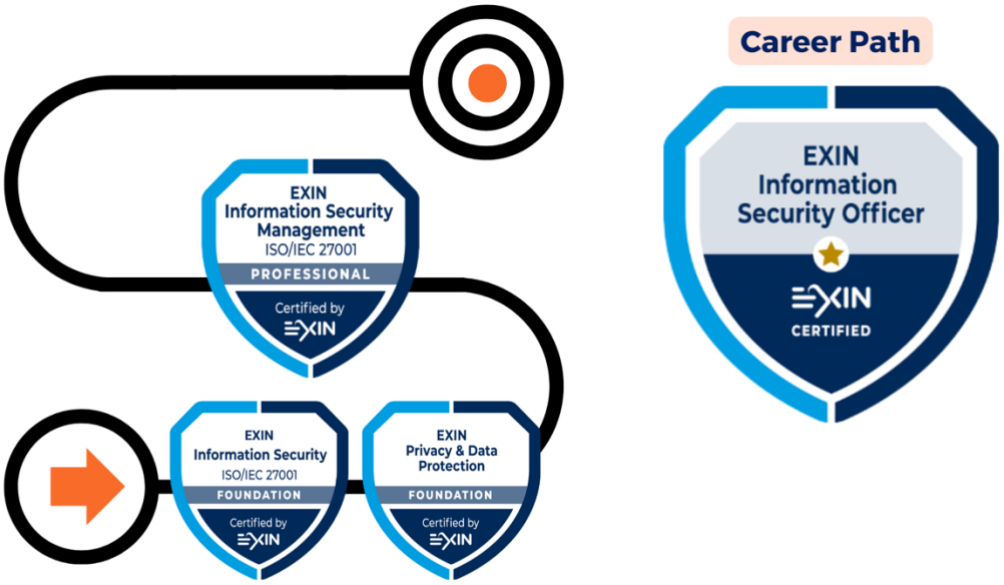
5. Career Path

O EXIN acredita no valor do aprendizado contínuo e na importância de combinar diversas habilidades para prosperar no atual mundo dinâmico e em evolução. Com os EXIN Career Paths, os candidatos podem se preparar para funções específicas e continuar crescendo e avançando em sua jornada profissional. Para obter mais informações sobre os EXIN Career Paths, consulte https://www.exin.com/career-paths/.

A certificação EXIN Information Security Management Professional based on ISO/IEC 27001 faz parte dos seguintes EXIN Career Paths.

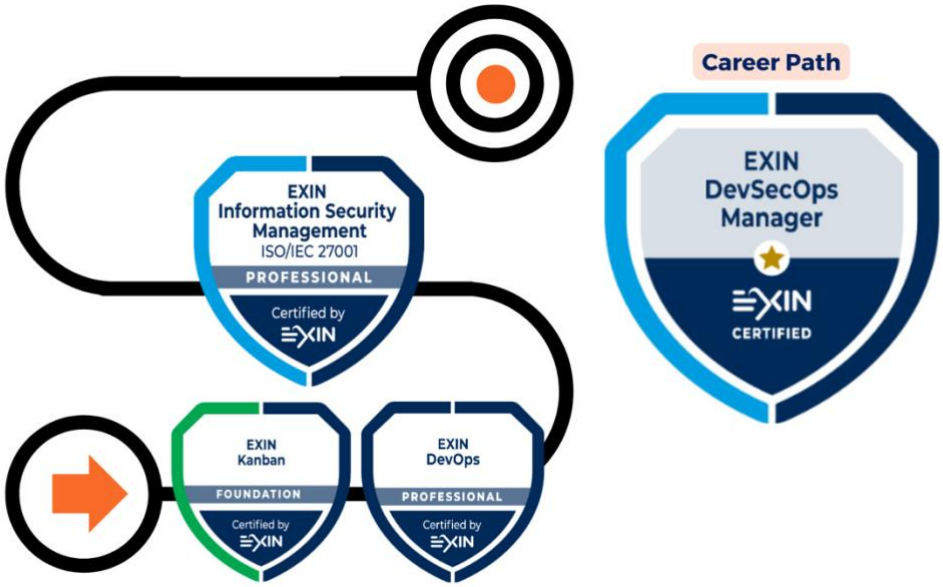
EXIN Information Security Officer

EXIN Information Security Officer equipa os profissionais com conhecimento e habilidades para implementar medidas eficazes de segurança da informação e gerenciamento de riscos, mantendo o foco na privacidade e proteção dos dados.



EXIN DevSecOps Manager

EXIN DevSecOps Manager equipa os profissionais com conhecimento e habilidades para implementar e otimizar o DevOps e, ao mesmo tempo, melhorar as práticas de segurança.



Contato EXIN

www.exin.com