EXIN Information Security Management ISO/IEC 27001 FOUNDATION

Certified by EXIN

Guia de preparação

Edição 202305

Conteúdo

1. Visão geral

EXIN Information Security Foundation based on ISO/IEC 27001 (ISFS.PR)

Escopo

A certificação EXIN Information Security Foundation based on ISO/IEC 27001 confirma que o profissional compreende os princípios e conceitos da segurança da informação aplicados ao ambiente de trabalho e sabe como mitigar riscos.

A certificação abrange:
- informação e segurança
- ameaças e riscos
- controles de segurança
- legislação, regulamentações e normas

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. 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.

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

O EXIN Information Security Foundation based on ISO/IEC 27001 testa os conceitos básicos da segurança da informação e suas relações. Os objetivos desse módulo são aumentar a conscientização de que a informação é valiosa e vulnerável e aprender quais são os controles necessários para proteger a informação.

Contexto

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

Público-alvo

A certificação EXIN Information Security Foundation based on ISO/IEC 27001 se destina a todos que processam informação em uma organização. Ela também é indicada para donos de pequenas empresas independentes para os quais é necessário ter algum conhecimento básico sobre segurança da informação. Essa certificação é um bom ponto de partida para novos profissionais de segurança da informação.

Requisitos para a certificação

- Conclusão bem-sucedida do exame EXIN Information Security Foundation based on ISO/IEC 27001.

Detalhes do exame

Tipo do exame:	Questões de múltipla escolha
Número de questões:	40
Mínimo para aprovação:	65% (26/40 questões)
Com consulta:	Não
Anotações:	Não
Equipamentos eletrônicos permitidos:	Não
Tempo designado para o exame:	60 minutos

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

Nível Bloom

A certificação EXIN Information Security Foundation based on ISO/IEC 27001 testa os candidatos nos Níveis Bloom 1 e 2 de acordo com a Taxonomia Revisada de Bloom:

- Nível Bloom 1: Lembrança – depende da recuperação de informações. Os candidatos precisarão absorver, lembrar, reconhecer e recordar.
- Nível Bloom 2: Compreensão – um passo além da lembrança. O entendimento mostra que os candidatos compreendem o que é apresentado e podem avaliar como o material de aprendizagem pode ser aplicado em seu próprio ambiente. Esse tipo de pergunta pretende demonstrar que o candidato é capaz de organizar, comparar, interpretar e escolher a descrição correta de fatos e ideias.

Treinamento

Horas de contato

A carga horária recomendada para este treinamento é de 14 horas. Isso inclui trabalhos em grupo, 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

56 horas (2 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. Informação e segurança		**27,5%**
	1.1 Conceitos relativos à informação	10%
	1.2 Aspectos de confiabilidade	7,5%
	1.3 Proteção da informação na organização	10%
2. Ameaças e riscos		**12,5%**
	2.1 Ameaças e riscos	12,5%
3. Controles de segurança		**52,5%**
	3.1 Descrição de controles de segurança	2,5%
	3.2 Controles organizacionais	15%
	3.3 Controles de pessoas	7,5%
	3.4 Controles físicos	10%
	3.5 Controles técnicos	17,5%
4. Legislação, regulamentações e normas		**7,5%**
	4.1 Legislação e regulamentações	2,5%
	4.2 Normas	5%
	Total	**100%**

Especificações do exame

1 Informação e segurança
- 1.1 Conceitos relativos à informação
  O candidato é capaz de...
  - 1.1.1 explicar a diferença entre dados e informação.
  - 1.1.2 explicar os conceitos de gestão de segurança da informação.
- 1.2 Aspectos de confiabilidade
  O candidato é capaz de...
  - 1.2.1 explicar o valor da tríade da CIA.
  - 1.2.2 descrever os conceitos de responsabilização e auditabilidade.
- 1.3 Proteção da informação na organização
  O candidato é capaz de...
  - 1.3.1 descrever os objetivos e o conteúdo de uma política de segurança da informação.
  - 1.3.2 explicar como garantir segurança da informação quando se trabalha com fornecedores.
  - 1.3.3 descrever papéis e responsabilidades relacionados à segurança da informação.

2 Ameaças e riscos
- 2.1 Ameaças e riscos
  O candidato é capaz de...
  - 2.1.1 explicar ameaça, risco e gerenciamento de riscos.
  - 2.1.2 descrever os tipos de danos.
  - 2.1.3 descrever estratégias de risco.
  - 2.1.4 descrever uma análise de risco.

3 Controles de segurança
- 3.1 Descrição de controles de segurança
  O candidato é capaz de...
  - 3.1.1 dar exemplos de cada tipo de controle de segurança.
- 3.2 Controles organizacionais
  O candidato é capaz de...
  - 3.2.1 explicar como classificar ativos de informação.
  - 3.2.2 descrever controles para gerenciar o acesso à informação.
  - 3.2.3 explicar gerenciamento de ameaças e vulnerabilidades, gerenciamento de projetos e gerenciamento de incidentes em segurança da informação.
  - 3.2.4 explicar o valor da continuidade de negócios.
  - 3.2.5 descrever o valor de auditorias e avaliações.
- 3.3 Controles de pessoas
  O candidato é capaz de...
  - 3.3.1 explicar como reforçar a segurança da informação por meio de contratos e acordos.
  - 3.3.2 explicar como alcançar conscientização sobre a segurança da informação.
- 3.4 Controles físicos
  O candidato é capaz de...
  - 3.4.1 descrever controles físicos de entrada.
  - 3.4.2 descrever como proteger a informação no interior de áreas seguras.
  - 3.4.3 descrever como funcionam os anéis de proteção.

3.5 Controles técnicos

O candidato é capaz de...

3.5.1 descrever como gerenciar ativos de informação.

3.5.2 descrever como desenvolver sistemas levando em consideração a segurança da informação.

3.5.3 citar controles que garantem segurança de rede.

3.5.4 descrever controles técnicos para gerenciar o acesso.

3.5.5 descrever como proteger sistemas de informação contra malware, phishing e spam.

3.5.6 explicar como registro e monitoramento contribuem para a segurança da informação.

4 Legislação, regulamentações e normas

4.1 Legislação e regulamentações

O candidato é capaz de...

4.1.1 dar exemplos de legislação e regulamentações relacionadas à segurança da informação.

4.2 Normas

O candidato é capaz de...

4.2.1 descrever as normas ISO/IEC 27000, ISO/IEC 27001 e ISO/IEC 27002.

4.2.2 descrever outras normas relacionadas à segurança da informação.

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
access control	controle de acesso
accountability	responsabilização
annualized loss expectancy (ALE)	expectativa de perda anual (ALE)
annualized rate of occurrence (ARO)	taxa de ocorrência anual (ARO)
asset	ativo
auditability	auditabilidade
authentication	autenticação
authorization	autorização
availability	disponibilidade
backup	backup (cópia de segurança)
biometrics	biometria
business continuity management (BCM)	gerenciamento da continuidade de negócios (GCN)
certificate	certificado
change management	gerenciamento da mudança
chief information security officer (CISO)	chief information security officer (CISO)
classification	classificação
code of conduct	código de conduta
compliance	conformidade
confidentiality	confidencialidade
controls • corrective • detective • insurance • preventive • reductive • repressive (suppressive)	controles • corretivo • detectivo • seguro cyber • preventivo • redutivo • repressivo (supressivo)
cryptography	criptografia
cyber crime	crime cibernético
damage • direct damage • indirect damage	danos • danos diretos • danos indiretos
data	dados
digital signature	assinatura digital
due care	due care
due diligence	due diligence
escalation	escalação
exposure	exposição
(business) impact	impacto no negócio
incident cycle	ciclo de vida de um incidente
information	informação
information analysis	análise da informação
information management	gerenciamento da informação

information security management system (ISMS)	sistema de gestão de segurança da informação (SGSI)
information security manager (ISM)	information security manager (ISM)
information security officer (ISO)	information security officer (ISO)
information security policy	política de segurança da informação
information security strategy	estratégia de segurança da informação
information system	sistema de informação
integrity	integridade
likelihood	probabilidade
non-disclosure agreement (NDA)	acordo de não divulgação (NDA)
Plan, Do, Check, Act (PDCA)	Plan, Do, Check, Act (PDCA)
personally identifiable information (PII)	personally identifiable information (PII)
phishing	phishing
privacy	privacidade
protection ring	anel de proteção
public key infrastructure (PKI)	infraestrutura de chave pública (ICP)
reliability	confiabilidade
risk	risco
risk analysis • qualitative risk analysis • quantitative risk analysis	análise de risco • análise qualitativa de risco • análise quantitativa de risco
risk assessment	avaliação de riscos
risk management	gerenciamento de riscos
risk strategy • risk avoiding • risk bearing (risk acceptance) • risk neutral	estratégia de risco • evitar o risco • aceitar o risco • reduzir o risco
risk treatment	tratamento de risco
security incident	incidente de segurança
segregation of duties	segregação de funções
single loss expectancy (SLE)	expectativa de perda por incidente (SLE)
stand-by arrangement	stand-by arrangement
threat • human threat • non-human threat	ameaça • ameaça humana • ameaça não humana
threat agent	agente de ameaça
validation	validação
verification	verificação
virtual private network (VPN)	rede privada virtual (VPN)
vulnerability	vulnerabilidade

4. Literatura

Literatura do exame

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

A. Baars, H., Hintzbergen, J., and Hintzbergen, K.
Foundations of Information Security – Based on ISO 27001 and ISO 27002
Van Haren Publishing: 4ª edição totalmente revisada, 2023
ISBN: 978 94 018 0958 0 (cópia física)
ISBN: 978 94 018 0959 7 (eBook)
ISBN: 978 94 018 0960 3 (ePub)

Matriz da literatura

Requisitos do exame	Especificações do exame	Referência
1. Informação e segurança		
	1.1 Conceitos relativos à informação	Capítulos 3.1 - 3.3, 4.7 - 4.9
	1.2 Aspectos de confiabilidade	Capítulos 3.4, 4.4 - 4.6
	1.3 Proteção da informação na organização	Capítulos 4.2, 4.3, 4.11 - 4.14, 5.1 - 5.6, 5.14, 5.19 - 5.23, 5.35, 7.7, 7.9, 7.10, 8.30
2. Ameaças e riscos		
	2.1 Ameaças e riscos	Capítulos 3.5, 3.7, 3.9 - 3.11
3. Controles de segurança		
	3.1 Descrição de controles de segurança	Capítulo 3.8
	3.2 Controles organizacionais	Capítulos 3.6.2, 5.3, 5.7 - 5.18, 5.24 – 5.30, 5.35, 5.36, 6.8
	3.3 Controles de pessoas	Capítulo 6
	3.4 Controles físicos	Capítulo 7
	3.5 Controles técnicos	Capítulos 4.10, 8
4. Legislação, regulamentações e normas		
	4.1 Legislação e regulamentações	Capítulos 5.31 - 5.34
	4.2 Normas	Capítulos 1, 3.6, 3.12, 4.1, 4.12, 5.36

Contato EXIN

www.exin.com