


# Preparation guide

Editie 202509

Copyright © EXIN Holding B.V. 2025. All rights reserved.
EXIN® is a registered trademark.

No part of this publication may be reproduced, stored, utilized or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written permission from EXIN.

# Inhoud


1. Overzicht 4
2. Exameneisen 7
3. Begrippenlijst 10
4. Literatuur 12
5. Career Path 13

# 1. Overzicht

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

### Scope

Met de certificering EXIN Information Security Foundation based on ISO/IEC 27001 wordt bevestigd dat professionals de principes en concepten van informatiebeveiliging, zoals toegepast in de werkomgeving, begrijpen en weten hoe risico's kunnen worden beperkt.

De certificering omvat:
- informatie en beveiliging
- dreigingen en risico's
- beheersmaatregelen
- wet- en regelgeving en normen

### Samenvatting

De globalisering van de economie leidt tot steeds meer informatie-uitwisseling. Informatie overschrijdt daarbij niet alleen landsgrenzen, maar ook de dunne scheidslijn tussen het private en het zakelijke domein. Naarmate er meer informatie wordt beheerd, neemt ook de eindverantwoordelijkheid verder toe. ISO/IEC 27001, de internationale norm voor informatiebeveiligingsmanagement, is een alom gerespecteerde norm waar veelvuldig naar wordt verwezen en die een kader biedt voor de opzet en het management van een informatiebeveiligingsprogramma.

Binnen het programma EXIN Information Security Management based on ISO/IEC 27001 wordt de volgende definitie gebruikt: informatiebeveiliging is de bescherming van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie.

EXIN Information Security Foundation based on ISO/IEC 27001 toetst het begrip van de basisconcepten van informatiebeveiliging en het onderlinge verband hiertussen. Deze module is erop gericht het bewustzijn te vergroten dat informatie waardevol en kwetsbaar is, en te leren welke beheersmaatregelen nodig zijn om informatie veilig te houden.

## Context

De certificering EXIN Information Security Foundation based on ISO/IEC 27001 is onderdeel van het certificeringsprogramma EXIN Information Security Management based on ISO/IEC 27001.




## Doelgroep

EXIN Information Security Foundation based on ISO/IEC 27001 is bestemd voor iedereen in een organisatie die informatie verwerkt. Verder is de certificering geschikt voor ondernemers met een klein, onafhankelijk bedrijf die enige basiskennis van informatiebeveiliging dienen te hebben. Deze certificering vormt ook een goede basis voor nieuwe professionals op het gebied van informatiebeveiliging.

## Certificeringseisen

- Met goed gevolg afleggen van het examen EXIN Information Security Foundation based on ISO/IEC 27001.

### Examendetails

| | |
|---|---|
| Examenvorm: | Multiple-choicevragen |
| Aantal vragen: | 40 |
| Cesuur: | 65% (26/40 vragen) |
| Open boek: | Nee |
| Notities: | Nee |
| Elektronische hulpmiddelen toegestaan: | Nee |
| Examenduur: | 60 minuten |

Op dit examen is het Reglement voor de examens van EXIN van toepassing.

### Bloom level

De certificering EXIN Information Security Foundation based on ISO/IEC 27001 toetst kandidaten op Bloom levels 1 en 2 volgens Bloom's Revised Taxonomy:

- Bloom level 1: Onthouden – op dit niveau kunnen kandidaten zich de geleerde stof herinneren. Ze kunnen herkennen, beschrijven en benoemen.
- Bloom level 2: Begrijpen – een stap hoger dan onthouden. Op dit niveau begrijpen kandidaten de aangeboden materialen en kunnen ze aangeven hoe ze deze in hun eigen omgeving kunnen toepassen. Met dit type vragen wordt bepaald of de kandidaat in staat is om feiten en ideeën te ordenen, te vergelijken, te interpreteren en correct te beschrijven.

## Training

### Contacturen

Het aangeraden aantal contacturen tijdens de training is 14. Dit omvat groepsopdrachten, voorbereiding op het examen en korte pauzes. Dit aantal uren is exclusief lunchpauzes, huiswerk en het examen.

### Indicatie studielast

56 uur (2 ECTS), afhankelijk van bestaande kennis.

### Trainingsorganisatie

Een lijst van geaccrediteerde trainingsorganisaties kunt u vinden op de website van EXIN www.exin.com.

# 2. Exameneisen

De exameneisen staan vermeld in de examenspecificaties. De volgende tabel bevat de onderwerpen (exameneisen) en deelonderwerpen (examenspecificaties) van de module.

| Exameneisen | Examenspecificaties | Gewicht |
|---|---|---|
| **1. Informatie en beveiliging** | | **27,5%** |
| | 1.1 Concepten met betrekking tot informatie | 10% |
| | 1.2 Betrouwbaarheidsaspecten | 7,5% |
| | 1.3 Informatie beveiligen in de organisatie | 10% |
| **2. Dreigingen en risico's** | | **12,5%** |
| | 2.1 Dreigingen en risico's | 12,5% |
| **3. Beheersmaatregelen** | | **52,5%** |
| | 3.1 Schetsen van beheersmaatregelen | 2,5% |
| | 3.2 Organisatorische beheersmaatregelen | 15% |
| | 3.3 Menselijke beheersmaatregelen | 7,5% |
| | 3.4 Fysieke beheersmaatregelen | 10% |
| | 3.5 Technische beheersmaatregelen | 17,5% |
| **4. Wet- en regelgeving en normen** | | **7,5%** |
| | 4.1 Wet- en regelgeving | 2,5% |
| | 4.2 Normen | 5% |
| | **Totaal** | **100%** |

## Examenspecificaties

**1 Informatie en beveiliging**

1.1 Concepten met betrekking tot informatie
De kandidaat kan…
- 1.1.1 het verschil tussen data en informatie uitleggen.
- 1.1.2 concepten met betrekking tot informatiebeveiligingsmanagement uitleggen.

1.2 Betrouwbaarheidsaspecten
De kandidaat kan…
- 1.2.1 de waarde van de BIV-driehoek uitleggen.
- 1.2.2 de concepten eindverantwoordelijkheid en controleerbaarheid beschrijven.

1.3 Informatie beveiligen in de organisatie
De kandidaat kan…
- 1.3.1 de doelstellingen en inhoud van een informatiebeveiligingsbeleid schetsen.
- 1.3.2 uitleggen hoe informatiebeveiliging kan worden gewaarborgd wanneer er met leveranciers wordt gewerkt.
- 1.3.3 rollen en verantwoordelijkheden schetsen die verband houden met informatiebeveiliging.

**2 Dreigingen en risico's**

2.1 Dreigingen en risico's
De kandidaat kan…
- 2.1.1 dreigingen, risico's en risicomanagement uitleggen.
- 2.1.2 soorten schade beschrijven.
- 2.1.3 risicostrategieën beschrijven.
- 2.1.4 risicoanalyse beschrijven.

**3 Beheersmaatregelen**

3.1 Schetsen van beheersmaatregelen
De kandidaat kan…
- 3.1.1 voorbeelden geven van elke soort beheersmaatregelen.

3.2 Organisatorische beheersmaatregelen
De kandidaat kan…
- 3.2.1 uitleggen hoe informatiemiddelen worden geclassificeerd.
- 3.2.2 beheersmaatregelen voor de toegang tot informatie beschrijven.
- 3.2.3 dreigings- en kwetsbaarhedenmanagement, projectmanagement en incidentmanagement uitleggen in de context van informatiebeveiliging.
- 3.2.4 de waarde van bedrijfscontinuïteit uitleggen.
- 3.2.5 de waarde van audits en controles beschrijven.

3.3 Menselijke beheersmaatregelen
De kandidaat kan…
- 3.3.1 uitleggen hoe informatiebeveiliging wordt verbeterd met contracten en overeenkomsten.
- 3.3.2 uitleggen hoe bewustwording met betrekking tot informatiebeveiliging wordt verhoogd.

3.4 Fysieke beheersmaatregelen
De kandidaat kan…
- 3.4.1 beheersmaatregelen voor fysieke toegang beschrijven.
- 3.4.2 beschrijven hoe informatie binnen beveiligde gebieden wordt beschermd.
- 3.4.3 uitleggen hoe beschermingsringen werken.

3.5 Technische beheersmaatregelen
De kandidaat kan…
3.5.1 schetsen hoe informatiemiddelen worden beheerd.
3.5.2 beschrijven hoe systemen worden ontwikkeld met aandacht voor informatiebeveiliging.
3.5.3 beheersmaatregelen noemen die de netwerkbeveiliging waarborgen.
3.5.4 technische beheersmaatregelen voor toegangsbeheer (access control) beschrijven.
3.5.5 beschrijven hoe informatiesystemen worden beschermd tegen malware, phishing en spam.
3.5.6 uitleggen hoe logging en monitoring bijdragen aan informatiebeveiliging.

## 4 Wet- en regelgeving en normen

4.1 Wet- en regelgeving
De kandidaat kan…
4.1.1 voorbeelden geven van wet- en regelgeving met betrekking tot informatiebeveiliging.

4.2 Normen
De kandidaat kan…
4.2.1 de inhoud van de normen ISO/IEC 27000, ISO/IEC 27001 en ISO/IEC 27002 schetsen.
4.2.2 de inhoud van andere normen met betrekking tot informatiebeveiliging schetsen.

# 3. Begrippenlijst

Dit hoofdstuk bevat de begrippen en afkortingen die kandidaten moeten kennen.

Let op! Uitsluitend kennis van deze termen is niet voldoende voorbereiding voor het examen; de kandidaten moeten de begrippen begrijpen en in staat zijn om voorbeelden te geven.

| **Engels** | **Nederlands** |
|---|---|
| access control | toegangsbeheer (access control) |
| accountability | eindverantwoordelijkheid |
| annualized loss expectancy (ALE) | annualized loss expectancy (ALE) |
| annualized rate of occurrence (ARO) | annualized rate of occurrence (ARO) |
| asset | middel |
| auditability | controleerbaarheid |
| authentication | authenticatie |
| authorization | autorisatie |
| availability | beschikbaarheid |
| backup | back-up |
| biometrics | biometrie |
| business continuity management (BCM) | bedrijfscontinuïteitsbeheer (business continuity management, BCM) |
| certificate | certificaat |
| change management | wijzigingsbeheer (change management) |
| chief information security officer (CISO) | chief information security officer (CISO) |
| classification | classificatie |
| code of conduct | gedragscode |
| compliance | naleving (compliance) |
| confidentiality | vertrouwelijkheid |
| controls<br>• corrective<br>• detective<br>• insurance<br>• preventive<br>• reductive<br>• repressive (suppressive) | beheersmaatregelen<br>• correctief<br>• detectief<br>• verzekering<br>• preventief<br>• reductief<br>• repressief |
| cryptography | cryptografie |
| cyber crime | cybercrime |
| damage<br>• direct damage<br>• indirect damage | schade<br>• directe schade<br>• indirecte schade |
| data | data |
| digital signature | digitale handtekening |
| due care | due care |
| due diligence | due dilligence |
| escalation | escalatie |
| exposure | blootstelling |
| (business) impact | (bedrijfs)impact |
| incident cycle | incidentcyclus |
| information | informatie |
| information analysis | informatieanalyse |
| information management | informatiemanagement |

| | |
|---|---|
| information security management system (ISMS) | managementsysteem voor informatiebeveiliging (ISMS) |
| information security manager (ISM) | information security manager (ISM) |
| information security officer (ISO) | information security officer (ISO) |
| information security policy | informatiebeveiligingsbeleid |
| information security strategy | informatiebeveiligingsstrategie |
| information system | informatiesysteem |
| integrity | integriteit |
| likelihood | waarschijnlijkheid |
| non-disclosure agreement (NDA) | geheimhoudingsverklaring (NDA) |
| Plan, Do, Check, Act (PDCA) | Plan, Do, Check, Act (PDCA) |
| personally identifiable information (PII) | persoonlijk identificeerbare informatie (PII) |
| phishing | phishing |
| privacy | privacy |
| protection ring | beschermingsringen |
| public key infrastructure (PKI) | Public Key Infrastructure (PKI) |
| reliability | betrouwbaarheid |
| risk | risico |
| risk analysis<br>• qualitative risk analysis<br>• quantitative risk analysis | risicoanalyse<br>• kwalitatieve risicoanalyse<br>• kwantitatieve risicoanalyse |
| risk assessment | risicobeoordeling |
| risk management | risicomanagement |
| risk strategy<br>• risk avoiding<br>• risk bearing (risk acceptance)<br>• risk neutral | risicostrategie<br>• risicomijdend<br>• risicodragend (risicoacceptatie)<br>• risiconeutraal |
| risk treatment | risicobehandeling |
| security incident | beveiligingsincident |
| segregation of duties | functiescheiding |
| single loss expectancy (SLE) | single loss expectancy (SLE) |
| stand-by arrangement | hot site op afroep |
| threat<br>• human threat<br>• non-human threat | dreiging<br>• menselijke dreiging<br>• niet-menselijke dreiging |
| threat agent | aanvaller |
| validation | validatie |
| verification | verificatie |
| virtual private network (VPN) | virtual private network (VPN) |
| vulnerability | kwetsbaarheid |

# 4. Literatuur

## Examenliteratuur

De benodigde kennis voor het examen wordt in de volgende literatuur beschreven:

**A.** Hintzbergen, J., Hintzbergen, K. en Baars, H.
**Basiskennis informatiebeveiliging op basis van 27001 en ISO 27002**
Van Haren Publishing: 4e herziene versie, 2023
ISBN: 978 94 018 0991 7 (papieren versie)
ISBN: 978 94 018 0993 4 (eBoek)
ISBN: 978 94 018 0993 1 (ePub)

## Literatuurmatrix

| Exameneisen | Examenspecificaties | Referentie |
|---|---|---|
| **1. Informatie en beveiliging** | | |
| | 1.1 Concepten met betrekking tot informatie | Hoofdstuk 3.1 - 3.3, 4.7 - 4.9 |
| | 1.2 Betrouwbaarheidsaspecten | Hoofdstuk 3.4, 4.4 - 4.6 |
| | 1.3 Informatie beveiligen in de organisatie | Hoofdstuk 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. Dreigingen en risico's** | | |
| | 2.1 Dreigingen en risico's | Hoofdstuk 3.5, 3.7, 3.9 – 3.11 |
| **3. Beheersmaatregelen** | | |
| | 3.1 Schetsen van beheersmaatregelen | Hoofdstuk 3.8 |
| | 3.2 Organisatorische beheersmaatregelen | Hoofdstuk 3.6.2, 5.3, 5.7 – 5.18, 5.24 – 5.30, 5.35, 5.36, 6.8 |
| | 3.3 Menselijke beheersmaatregelen | Hoofdstuk 6 |
| | 3.4 Fysieke beheersmaatregelen | Hoofdstuk 7 |
| | 3.5 Technische beheersmaatregelen | Hoofdstuk 4.10, 8 |
| **4. Wet- en regelgeving en normen** | | |
| | 4.1 Wet- en regelgeving | Hoofdstuk 5.31 – 5.34 |
| | 4.2 Normen | Hoofdstuk 1, 3.6, 3.12, 4.1, 4.12, 5.36 |
| | | |

# 5. Career Path

EXIN gelooft in de waarde van levenslang leren en het belang van het combineren van diverse vaardigheden om te kunnen floreren in de dynamische en steeds veranderende wereld van vandaag. Met onze EXIN Career Paths kunnen kandidaten zich voorbereiden op specifieke functies en blijven groeien en vooruitgang boeken in hun professionele carrière. Ga voor meer informatie over de EXIN Career Paths naar https://www.exin.com/career-paths/.

De certificering EXIN Information Security Foundation based on ISO/IEC 27001 is onderdeel van de volgende EXIN Career Paths.

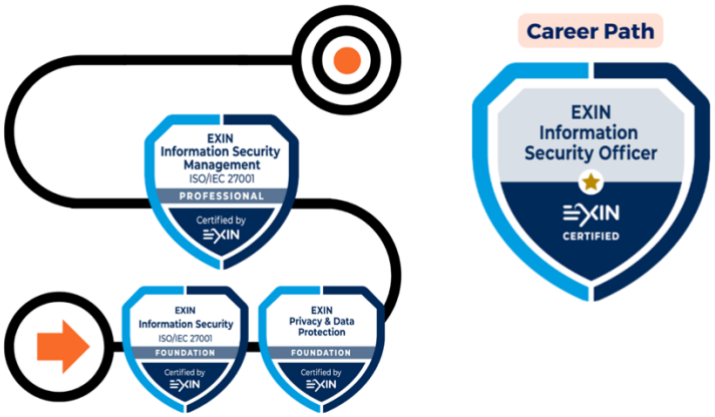
## EXIN Data Protection Officer

EXIN Data Protection Officer stelt professionals in staat om maatregelen voor informatiebeveiliging te implementeren die zijn gericht op het naleven van regelgeving op het gebied van gegevensbescherming.




## EXIN Information Security Officer

EXIN Information Security Officer biedt professionals de kennis en vaardigheden om effectieve maatregelen voor informatiebeveiliging en effectief risicomanagement te implementeren terwijl ze focus houden op gegevensbescherming en privacy.



## EXIN Artificial Intelligence Compliance Officer

EXIN Artificial Intelligence Compliance Officer bereidt professionals voor op het naleven van de meest relevante regelgeving op het gebied van kunstmatige intelligentie (AI) en gegevensbescherming en van robuuste normen voor informatiebeveiliging om een ethisch en verantwoord gebruik van AI te waarborgen.






## Contact EXIN

www.exin.com