

Nederlandse norm

NEN-EN-ISO/IEC 27001 (nl)

Informatiebeveiliging, cybersecurity en
bescherming van de privacy -
Managementsysteem voor informatiebeveiliging -
Eisen

Information security, cybersecurity and privacy
protection - Information security management
systems - Requirements

Vervangt NEN-EN-ISO/IEC 27001:2017+A11:2020

ICS 03.100.70; 35.030
augustus 2023

Dit document bevat de vertaling in het Nederlands van de Europese norm EN ISO/IEC 27001:2023.
De Europese norm EN-ISO/IEC 27001:2023 heeft de status van Nederlandse norm.

Normcommissie 381027 'Cybersecurity & Privacy'



THIS PUBLICATION IS COPYRIGHT PROTECTED

DEZE PUBLICATIE IS AUTEURSRECHTELIJK BESCHERMD

Apart from exceptions provided by the law, nothing from this publication may be duplicated and/or published by means of photocopy, microfilm, storage in computer files or otherwise, which also applies to full or partial processing, without the written consent of Stichting Koninklijk Nederlands Normalisatie Instituut.

Stichting Koninklijk Nederlands Normalisatie Instituut shall, with the exclusion of any other beneficiary, collect payments owed by third parties for duplication and/or act in and out of law, where this authority is not transferred or falls by right to Stichting Reprerecht.

Auteursrecht voorbehouden. Behoudens uitzondering door de wet gesteld mag zonder schriftelijke toestemming van Stichting Koninklijk Nederlands Normalisatie Instituut niets uit deze uitgave worden verveelvoudigd en/of openbaar gemaakt door middel van fotokopie, microfilm, opslag in computerbestanden of anderszins, hetgeen ook van toepassing is op gehele of gedeeltelijke bewerking.

Stichting Koninklijk Nederlands Normalisatie Instituut is met uitsluiting van ieder ander gerechtigd de door derden verschuldigde vergoedingen voor verveelvoudiging te innen en/of daartoe in en buiten rechte op te treden, voor zover deze bevoegdheid niet is overgedragen c.q. rechtens toekomt aan Stichting Reprerecht.

Although the utmost care has been taken with this publication, errors and omissions cannot be entirely excluded. Stichting Koninklijk Nederlands Normalisatie Instituut and/or the members of the committees therefore accept no liability, not even for direct or indirect damage, occurring due to or in relation with the application of publications issued by Stichting Koninklijk Nederlands Normalisatie Instituut.

Hoewel bij deze uitgave de uiterste zorg is nagestreefd, kunnen fouten en onvolledigheden niet geheel worden uitgesloten. Stichting Koninklijk Nederlands Normalisatie Instituut en/of de leden van de commissies aanvaarden derhalve geen enkele aansprakelijkheid, ook niet voor directe of indirecte schade, ontstaan door of verband houdend met toepassing van door Stichting Koninklijk Nederlands Normalisatie Instituut gepubliceerde uitgaven.



© 2023 Stichting Koninklijk Nederlands Normalisatie Instituut
www.nen.nl

EUROPESE NORM

EN ISO/IEC 27001

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

juli 2023

ICS 03.100.70; 35030

EN ISO/IEC 27001:2017

— Nederlandstalige versie

Informatietechnologie – Beveiligingstechnieken – Managementsystemen voor informatiebeveiliging – Eisen

Informationstechnik -
Sicherheitsverfahren -
Informationssicherheits-
Managementsysteme - Anforderungen

Information technology – Security
techniques – Information security
management systems -
Requirements

Technologies de l'information -
Techniques de sécurité - Systèmes
de management de la sécurité de
l'information - Exigences

Deze norm is de Nederlandstalige versie van de Europese norm EN ISO/IEC 27001:2023. Hij is vertaald door NEN. Hij heeft dezelfde status als de officiële versies.

Deze Europese norm is door CEN aangenomen op 23 juli 2023.

CEN- en CENELEC-leden zijn verplicht zich te houden aan het huishoudelijk reglement van CEN-CENELEC, waarin is vastgelegd onder welke voorwaarden aan deze Europese norm, zonder veranderingen, de status van nationale norm moet worden gegeven. Bijgewerkte lijsten van en bibliografische gegevens betreffende zulke nationale normen kunnen op aanvraag worden verkregen bij het managementcentrum van CEN-CENELEC en bij elk CEN- en CENELEC-lid.

Deze Europese norm bestaat in drie officiële versies (Duits, Engels en Frans). Een versie in een andere taal die onder verantwoordelijkheid van een CEN- en CENELEC-lid in de eigen landstaal is gemaakt en die is aangemeld bij het managementcentrum van CEN-CENELEC, heeft dezelfde status als de officiële versies.

CEN- en CENELEC-leden zijn de nationale normalisatie-instanties van België, Bulgarije, Cyprus, Denemarken, Duitsland, Estland, Finland, Frankrijk, Griekenland, Hongarije, Ierland, IJsland, Italië, Kroatië, Letland, Litouwen, Luxemburg, Malta, Nederland, Noord-Macedonië, Noorwegen, Oostenrijk, Polen, Portugal, Roemenië, Servië, Slovenië, Slowakije, Spanje, Tsjechië, Turkije, het Verenigd Koninkrijk, Zweden en Zwitserland.

CEN

Europees Comité voor Normalisatie

Europäisches Komitee für Normung

European Committee for Standardization

Comité Européen de Normalisation

Managementcentrum van CEN-CENELEC: Wetenschapsstraat 23, B-1040 Brussel

© 2023 CEN/CENELEC

Alle rechten van gebruik, in welke vorm en op welke wijze
dan ook, zijn voorbehouden aan CEN- en CENELEC-leden.

Ref. nr. EN ISO/IEC 27001:2023 nl

(blanco)

Inhoud

Europees voorwoord.....	6
ISO/IEC-voorwoord.....	6
0 Inleiding.....	8
1 Onderwerp en toepassingsgebied.....	9
2 Normatieve verwijzingen	9
3 Termen en definities.....	9
4 Context van de organisatie.....	9
4.1 Inzicht in de organisatie en haar context.....	9
4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden.....	10
4.3 Het toepassingsgebied van het managementsysteem voor informatiebeveiliging vaststellen	10
4.4 Managementsysteem voor informatiebeveiliging.....	10
5 Leiderschap	10
5.1 Leiderschap en betrokkenheid.....	10
5.2 Beleid.....	11
5.3 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie.....	11
6 Planning.....	12
6.1 Acties om risico's en kansen op te pakken	12
6.2 Informatiebeveiligingsdoelstellingen en de planning om ze te bereiken.....	14
6.3 Planning van wijzigingen.....	14
7 Ondersteuning.....	15
7.1 Middelen.....	15
7.2 Competentie.....	15
7.3 Bewustzijn.....	15
7.4 Communicatie.....	15
7.5 Gedocumenteerde informatie.....	16
8 Uitvoering.....	17
8.1 Operationele planning en beheersing.....	17
8.2 Risicobeoordeling van informatiebeveiliging	17
8.3 Informatiebeveiligingsrisico's behandelen.....	17
9 Evaluatie van de prestaties.....	17
9.1 Monitoren, meten, analyseren en evalueren.....	17
9.2 Interne audit.....	18
9.3 Management review	19
10 Verbetering.....	19
10.1 Continue verbetering.....	19
10.2 Afwijkingen en corrigerende maatregelen.....	20
Bijlage A (normatief) Referentie voor beheersmaatregelen voor informatiebeveiliging	21
Bibliografie	31

Europees voorwoord

De tekst van ISO/IEC 27001:2022) is opgesteld door Technische Commissie ISO/IEC JTC 1 'Information technology' van de Internationale Organisatie voor Standaardisatie (ISO) en is overgenomen als EN ISO/IEC 27001:2023 door Technische Commissie CEN-CENELEC JTC 13 'Cybersecurity and Data Protection', waarvan DIN het secretariaat voert.

Aan deze Europese norm moet uiterlijk in januari 2024 de status van nationale norm worden gegeven, door publicatie van een identieke tekst of door bekrachtiging, en strijdige nationale normen moeten uiterlijk in januari 2024 worden ingetrokken.

Er wordt gewezen op de mogelijkheid dat sommige elementen van dit document onderwerp zijn van patentrechten. CEN is niet verantwoordelijk voor identificatie van dergelijke patentrechten.

Dit document vervangt NEN EN ISO 27001:2017.

Eventuele feedback en vragen over dit document behoren te worden gericht aan de nationale normalisatie-instantie of de nationale commissie van de gebruiker. Een volledige lijst van deze instanties is te vinden op de CEN-website.

Volgens het huishoudelijk reglement van CEN-CENELEC zijn de normalisatieorganisaties van de volgende landen verplicht deze Europese norm in te voeren: België, Bulgarije, Cyprus, Denemarken, Duitsland, Estland, Finland, Frankrijk, Griekenland, Hongarije, Ierland, IJsland, Italië, Kroatië, Letland, Litouwen, Luxemburg, Malta, Nederland, Noord-Macedonië, Noorwegen, Oostenrijk, Polen, Portugal, Roemenië, Servië, Slovenië, Slowakije, Spanje, Tsjechië, Turkije, het Verenigd Koninkrijk, Zweden en Zwitserland.

[Verklaring van bekrachtiging]

De tekst van ISO/IEC 27001:2022 is zonder wijzigingen door CEN als EN ISO/IEC 27001:2023 aanvaard.

ISO/IEC-voorwoord

ISO (International Organization for Standardization) en IEC (International Electrotechnical Commission) vormen tezamen een stelsel dat gespecialiseerd is in wereldwijde normalisatie. Nationale organisaties die lid zijn van ISO of IEC participeren in het ontwikkelen van internationale normen via technische commissies die door de desbetreffende organisatie zijn ingesteld ten behoeve van de normalisatie in specifieke technische werkelden. Technische commissies van ISO en IEC werken samen bij onderwerpen waarin zij een gemeenschappelijk belang hebben. Andere internationale organisaties, zowel overheidsinstanties als ngo's, nemen, in samenwerking met ISO en IEC, ook deel aan deze werkzaamheden.

De procedures die zijn gebruikt voor het ontwikkelen van dit document en de procedures die zijn bedoeld voor het verdere onderhoud ervan, worden beschreven in de ISO/IEC-richtlijnen, deel 1. Hierbij wordt met name gewezen op de verschillende goedkeuringscriteria die nodig zijn voor de verschillende soorten documenten. Dit document is opgesteld volgens de redactionele regels die in de ISO/IEC-richtlijnen, deel 2 zijn opgenomen (zie www.iso.org/directives of www.iec.ch/members_experts/refdocs).

Er wordt gewezen op de mogelijkheid dat sommige elementen van dit document onderwerp zijn van patentrechten. ISO en IEC zijn niet verantwoordelijk voor identificatie van dergelijke patentrechten. Nadere informatie over eventuele patentrechten die zijn geïdentificeerd tijdens het ontwikkelen van

het document, is te vinden in de inleiding en/of de ISO-lijst met ontvangen patentverklaringen (zie www.iso.org/patents) of de IEC-lijst met ontvangen patentverklaringen (zie <http://patents.iec.ch>).

Eventuele handelsnamen die in dit document worden gebruikt, zijn verstrekt ter informatie voor het gemak van de gebruiker en houden geen aanbeveling in.

Uitleg over de vrijwillige aard van normen, de betekenis van ISO-specifieke termen en uitdrukkingen met betrekking tot conformiteitsbeoordeling, alsmede informatie over hoe ISO voldoet aan de beginselen van de Wereldhandelsorganisatie (WTO) in de Technical Barriers to Trade (TBT), wordt gegeven op: www.iso.org/iso/foreword.html. Voor IEC, zie www.iec.ch/understanding-standards.

Dit document is opgesteld door ISO/IEC JTC 1, *Information Technology*, SC 27, *Information security, cybersecurity and privacy protection*.

Deze derde editie herroept en vervangt de tweede editie (ISO/IEC 27001:2013), die is herzien en is afgestemd op ISO/IEC 27002:2022. Ook de Technische Corrigenda ISO/IEC 27001:2013/COR 1:2014 en ISO/IEC 27001:2013/COR 2:2015 zijn hierin opgenomen.

De belangrijkste wijzigingen zijn als volgt:

— de tekst is in overeenstemming gebracht met de geharmoniseerde structuur voor managementsysteemnormen.

Eventuele feedback of vragen over dit document behoren te worden gericht aan het nationale normalisatie-instituut van de gebruiker. Een volledig overzicht van deze instituten is te vinden op www.iso.org/members.html en www.iec.ch/national-committees.

0 Inleiding

0.1 Algemeen

Dit document is opgesteld om te voorzien in eisen voor het inrichten, implementeren, in stand houden en continu verbeteren van een managementsysteem voor informatiebeveiliging. De invoering van een managementsysteem voor informatiebeveiliging is een strategische beslissing van de organisatie. Het inrichten en implementeren van het managementsysteem voor informatiebeveiliging van een organisatie wordt beïnvloed door de behoeften en doelstellingen van de organisatie, beveiligingseisen, de organisatieprocessen die worden toegepast en de omvang en structuur van de organisatie. Naar verwachting veranderen al deze factoren die van invloed zijn, in de loop van de tijd.

Het managementsysteem voor informatiebeveiliging zorgt ervoor dat de vertrouwelijkheid, integriteit en beschikbaarheid van informatie worden behouden door een risicomanagementproces toe te passen en geeft belanghebbenden het vertrouwen dat risico's afdoende worden beheerst.

Het is belangrijk dat het managementsysteem voor informatiebeveiliging deel uitmaakt van en geïntegreerd is in de processen en algehele managementstructuur van de organisatie en dat informatiebeveiliging in aanmerking wordt genomen tijdens het ontwerpen van processen, informatiesystemen en beheersmaatregelen. Er wordt van uitgegaan dat de schaalgrootte van een managementsysteem voor informatiebeveiliging wordt afgestemd op de behoeften van de organisatie.

Zowel interne als externe partijen kunnen dit document gebruiken om te beoordelen in welke mate de organisatie in staat is aan haar eigen informatiebeveiligingseisen te voldoen.

De volgorde waarin eisen in dit document worden gepresenteerd, zegt niets over het belang ervan of over de volgorde waarin ze moeten worden geïmplementeerd. De nummering van punten in lijsten is alleen voor referentiedoeleinden.

ISO/IEC 27000 beschrijft het overzicht en het vocabulaire van managementsystemen voor informatiebeveiliging, waarbij wordt verwezen naar de normenfamilie voor managementsystemen voor informatiebeveiliging (waaronder ISO/IEC 27003 [2], ISO/IEC 27004 [3] en ISO/IEC 27005 [4]), met de desbetreffende termen en definities.

0.2 Compatibiliteit met andere managementsysteemnormen

Dit document past de in bijlage SL bij ISO/IEC Directives, Part 1, Consolidated ISO Supplement gedefinieerde hoofdstructuur, identieke paragraaftitels, identieke tekst, gemeenschappelijke termen en kerndefinities toe en behoudt daardoor compatibiliteit met andere managementsysteemnormen waarop bijlage SL is toegepast.

Deze in bijlage SL gedefinieerde gemeenschappelijke benadering is nuttig voor organisaties die ervoor kiezen één managementsysteem uit te voeren dat aan de eisen van twee of meer managementsysteemnormen voldoet. ¹⁾

1) Nederlandse voetnoot: Om de gebruikers van meerdere managementsysteemnormen van dienst te zijn, is in deze norm de identieke kerntekst door een (kleur)markering onderscheiden van de aanvullende voor informatiebeveiliging specifieke tekst. De gele markering betreft de identieke kerntekst.

Informatiebeveiliging, cybersecurity en bescherming van de privacy — Managementsysteem voor informatiebeveiliging — Eisen

1 Onderwerp en toepassingsgebied

Dit document specificeert de eisen voor het binnen de context van de organisatie inrichten, implementeren, in stand houden en continu verbeteren van een managementsysteem voor informatiebeveiliging. Dit document bevat ook eisen voor het beoordelen en behandelen van informatiebeveiligingsrisico's afgestemd op de behoeften van de organisatie. De eisen in dit document zijn algemeen en bedoeld om van toepassing te zijn voor alle organisaties, ongeacht type, omvang of aard. Het uitsluiten van een of meer eisen van hoofdstuk 4 t/m 10 is niet aanvaardbaar als een organisatie naleving van dit document wil claimen.

2 Normatieve verwijzingen

Naar de volgende documenten wordt in de tekst zo verwezen dat de bepalingen ervan geheel of gedeeltelijk ook voor dit document gelden. Bij gedateerde verwijzingen is alleen de aangehaalde versie van toepassing. Voor ongedateerde verwijzingen geldt de laatste versie van het desbetreffende document (met inbegrip van eventuele wijzigings- en correctiebladen).

ISO/IEC 27000, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

3 Termen en definities

Voor de toepassing van dit document gelden de termen en definities zoals opgenomen in ISO/IEC 27000.

ISO en IEC onderhouden op de volgende adressen terminologiedatabases voor gebruik in het kader van normalisatie:

— ISO Online browsing platform: te bereiken op <http://www.iso.org/obp>

— IEC Electropedia: te bereiken op <https://www.electropedia.org/>

4 Context van de organisatie

4.1 Inzicht in de organisatie en haar context

De organisatie moet externe en interne (belangrijke) punten vaststellen die relevant zijn voor haar doelstelling en die haar vermogen beïnvloeden om het (de) beoogde resulta(a)t(en) van haar managementsysteem voor informatiebeveiliging te behalen.

OPMERKING Het vaststellen van deze (belangrijke) punten verwijst naar het vaststellen van de externe en interne context van de organisatie zoals bedoeld in hoofdstuk 5.4.1 van ISO 31000:2018 [5].

4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden

De organisatie moet vaststellen:

- a) welke belanghebbenden relevant zijn voor het managementsysteem voor informatiebeveiliging;
- b) welke eisen van deze belanghebbenden relevant zijn;
- c) welke van deze eisen zullen worden geadresseerd in het managementsysteem voor informatiebeveiliging.

OPMERKING De eisen van belanghebbenden kunnen wettelijke en regelgevende eisen en contractuele verplichtingen omvatten.

4.3 Het toepassingsgebied van het managementsysteem voor informatiebeveiliging vaststellen

De organisatie moet de grenzen en toepasselijkheid van het managementsysteem voor informatiebeveiliging bepalen om het toepassingsgebied ervan vast te stellen.

Bij het vaststellen van dit toepassingsgebied moet de organisatie het volgende overwegen:

- a) de in 4.1 genoemde externe en interne belangrijke punten (issues);
- b) de in 4.2 genoemde eisen;
- c) raakvlakken en afhankelijkheden tussen activiteiten die door de organisatie worden uitgevoerd en activiteiten die door andere organisaties worden uitgevoerd.

Het toepassingsgebied moet beschikbaar zijn als gedocumenteerde informatie.

4.4 Managementsysteem voor informatiebeveiliging

De organisatie moet een managementsysteem voor informatiebeveiliging inrichten, implementeren, onderhouden en continu verbeteren, met inbegrip van de benodigde processen en hun interacties, in overeenstemming met de eisen van dit document.

5 Leiderschap

5.1 Leiderschap en betrokkenheid

Het topmanagement moet leiderschap en betrokkenheid tonen met betrekking tot het managementsysteem voor informatiebeveiliging door:

- a) te bewerkstelligen dat het informatiebeveiligingsbeleid en de informatiebeveiligingsdoelstellingen worden vastgesteld en compatibel zijn met de strategische richting van de organisatie;
- b) te bewerkstelligen dat de eisen van het managementsysteem voor informatiebeveiliging in de processen van de organisatie worden geïntegreerd;
- c) te bewerkstelligen dat de voor het managementsysteem voor informatiebeveiliging benodigde middelen beschikbaar zijn;

- d) het belang van doeltreffend informatiebeveiligingsmanagement en van het voldoen aan de eisen van het managementsysteem voor informatiebeveiliging te communiceren;
- e) te bewerkstelligen dat het managementsysteem voor informatiebeveiliging zijn beoogde resulta(a)t(en) behaalt;
- f) mensen aan te sturen en te ondersteunen om een bijdrage te leveren aan de doeltreffendheid van het managementsysteem voor informatiebeveiliging;
- g) continue verbetering te bevorderen; en
- h) andere relevante managementrollen te ondersteunen om hun leiderschap te tonen binnen hun verantwoordelijkheidsgebieden.

OPMERKING Verwijzing naar 'bedrijfs' in dit document kan ruim worden geïnterpreteerd als een verwijzing naar de activiteiten die wezenlijk zijn gezien de doelen waarvoor de organisatie bestaat.

5.2 Beleid

Het topmanagement moet een informatiebeveiligingsbeleid vaststellen dat:

- a) passend is voor het doel van de organisatie;
- b) informatiebeveiligingsdoelstellingen (zie 6.2) bevat of het kader biedt voor het vaststellen van informatiebeveiligingsdoelstellingen;
- c) een verbintenis bevat om te voldoen aan van toepassing zijnde eisen in verband met informatiebeveiliging;
- d) een verbintenis bevat tot continue verbetering van het managementsysteem voor informatiebeveiliging.

Het informatiebeveiligingsbeleid moet:

- e) beschikbaar zijn als gedocumenteerde informatie;
- f) worden gecommuniceerd binnen de organisatie;
- g) beschikbaar zijn voor belanghebbenden voor zover van toepassing.

5.3 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie

Het topmanagement moet bewerkstelligen dat de verantwoordelijkheden en bevoegdheden voor rollen die relevant zijn voor informatiebeveiliging worden toegekend en gecommuniceerd binnen de organisatie.

Het topmanagement moet de verantwoordelijkheid en bevoegdheid toekennen met betrekking tot:

- a) het bewerkstelligen dat het managementsysteem voor informatiebeveiliging voldoet aan de eisen van dit document;
- b) het rapporteren over de prestaties van het managementsysteem voor informatiebeveiliging aan het topmanagement.

OPMERKING Het topmanagement kan ook verantwoordelijkheden en bevoegdheden toewijzen voor het binnen de organisatie rapporteren van de prestaties van het managementsysteem voor informatiebeveiliging.

6 Planning

6.1 Acties om risico's en kansen op te pakken

6.1.1 Algemeen

Bij het plannen voor het managementsysteem voor informatiebeveiliging moet de organisatie de in 4.1 genoemde belangrijke punten (issues) en de in 4.2 genoemde eisen overwegen, en de risico's en kansen vaststellen die moeten worden opgepakt om:

- a) te waarborgen dat het managementsysteem voor informatiebeveiliging zijn beoogde resulta(a)t(en) kan behalen;
- b) ongewenste effecten te voorkomen of te verminderen;
- c) continue verbetering te bereiken.

De organisatie moet:

- d) acties plannen om deze risico's en kansen op te pakken; en
- e) plannen op welke manier:
 - 1) de acties in de processen van haar managementsysteem voor informatiebeveiliging worden geïntegreerd en geïmplementeerd; en
 - 2) de doeltreffendheid van deze acties wordt geëvalueerd.

6.1.2 Risicobeoordeling van informatiebeveiliging

De organisatie moet een risicobeoordelingsprocedure voor informatiebeveiliging definiëren en toepassen die:

- a) risicocriteria voor informatiebeveiliging vaststelt en onderhoudt, waaronder:
 - 1) de risicoacceptatiecriteria; en
 - 2) criteria voor het uitvoeren van risicobeoordelingen van informatiebeveiliging;
- b) waarborgt dat herhaalde risicobeoordelingen van informatiebeveiliging consistente, valide en vergelijkbare resultaten opleveren;
- c) de informatiebeveiligingsrisico's identificeert:
 - 1) pas de risicobeoordelingsprocedure voor informatiebeveiliging toe om de risico's in verband met het verlies van vertrouwelijkheid, integriteit en beschikbaarheid van informatie binnen het toepassingsgebied van het managementsysteem voor informatiebeveiliging te identificeren; en
 - 2) identificeer de risico-eigenaren;

d) de informatiebeveiligingsrisico's analyseert:

- 1) beoordeel de potentiële gevolgen indien de risico's die in 6.1.2 c) 1) zijn vastgesteld, zich zouden voordoen;
- 2) beoordeel de realistische waarschijnlijkheid dat de risico's die zijn vastgesteld in 6.1.2 c) 1) zich voordoen; en
- 3) stel de risiconiveaus vast;

e) de informatiebeveiligingsrisico's evalueert:

- 1) vergelijk de resultaten van de risicoanalyse met de risicocriteria die zijn vastgesteld in 6.1.2 a); en
- 2) prioriteer de geanalyseerde risico's voor risicobehandeling.

De organisatie moet gedocumenteerde informatie bewaren over de risicobedoordelingsprocedure voor informatiebeveiliging.

6.1.3 Behandeling van informatiebeveiligingsrisico's

De organisatie moet een procedure voor de behandeling van informatiebeveiligingsrisico's definiëren en toepassen om:

- a) passende opties voor de behandeling van informatiebeveiligingsrisico's te selecteren, rekening houdend met de resultaten van de risicobedoordeling;
- b) alle beheersmaatregelen vast te stellen die nodig zijn om de gekozen optie(s) voor de behandeling van informatiebeveiligingsrisico's te implementeren;

OPMERKING 1 Organisaties kunnen beheersmaatregelen naar behoefte ontwerpen of ze uit een bepaalde bron halen.

- c) de in 6.1.3 b) hierboven vastgestelde beheersmaatregelen te vergelijken met de beheersmaatregelen in bijlage A en te verifiëren of er geen noodzakelijke beheersmaatregelen zijn weggelaten;

OPMERKING 2 Bijlage A bevat een lijst van mogelijke beheersmaatregelen voor informatiebeveiliging. Gebruikers van dit document worden op bijlage A gewezen om ervoor te zorgen dat er geen noodzakelijke beheersmaatregelen voor informatiebeveiliging over het hoofd worden gezien.

OPMERKING 3 De lijst van beheersmaatregelen voor informatiebeveiliging in bijlage A is niet volledig en zo nodig kunnen er aanvullende beheersmaatregelen voor informatiebeveiliging in worden opgenomen.

- d) een verklaring van toepasselijkheid op te stellen die het volgende bevat:

- de noodzakelijke beheersmaatregelen (zie 6.1.3 b) en c));
- een rechtvaardiging voor het opnemen ervan;
- de informatie of de benodigde beheersmaatregelen zijn geïmplementeerd of niet; en
- de rechtvaardiging voor het uitsluiten van beheersmaatregelen uit bijlage A.

- e) een plan voor de behandeling van informatiebeveiligingsrisico's te formuleren; en

- f) de goedkeuring van risico-eigenaren voor het plan voor de behandeling van informatiebeveiligingsrisico's en hun acceptatie van de resterende informatiebeveiligingsrisico's te verkrijgen.

De organisatie moet gedocumenteerde informatie bewaren over de risicobehandelingsprocedure voor informatiebeveiliging.

OPMERKING 4 Het proces voor risicobehoordeling en -behandeling in het kader van informatiebeveiliging in dit document komt overeen met de beginselen en algemene richtlijnen van ISO 31000 [5].

6.2 Informatiebeveiligingsdoelstellingen en de planning om ze te bereiken

De organisatie moet voor relevante functies en op relevante niveaus informatiebeveiligingsdoelstellingen vaststellen.

De informatiebeveiligingsdoelstellingen moeten:

- a) consistent zijn met het informatiebeveiligingsbeleid;
- b) meetbaar zijn (indien praktisch uitvoerbaar);
- c) rekening houden met van toepassing zijnde informatiebeveiligingseisen en de resultaten van risicobehoordeling en -behandeling;
- d) worden gemonitord;
- e) worden gecommuniceerd;
- f) passend bij de situatie worden geactualiseerd;
- g) beschikbaar zijn als gedocumenteerde informatie.

[Tekst verwijderd]*

Bij het opstellen van planningen voor het bereiken van de informatiebeveiligingsdoelstellingen moet de organisatie vaststellen:

- h) wat er zal worden gedaan;
- i) welke middelen er nodig zijn;
- j) wie verantwoordelijk is;
- k) wanneer het zal zijn voltooid; en
- l) hoe de resultaten zullen worden geëvalueerd.

6.3 Planning van wijzigingen

Wanneer de organisatie besluit dat er een noodzaak is voor wijzigingen in het managementsysteem voor informatiebeveiliging, moeten de wijzigingen worden uitgevoerd volgens een geplande werkwijze.

* Nederlandse voetnoot: De tekst is niet overgenomen in deze vertaling, omdat de strekking ervan identiek is aan die van het nieuwe opsommingsdeel g).

7 Ondersteuning

7.1 Middelen

De organisatie moet de middelen vaststellen en beschikbaar stellen die nodig zijn voor het inrichten, implementeren, onderhouden en continu verbeteren van het managementsysteem voor informatiebeveiliging.

7.2 Competentie

De organisatie moet:

- a) de benodigde competentie vaststellen van de perso(o)n(en) die onder haar gezag werkzaamheden verricht(en) die de prestaties van haar informatiebeveiliging beïnvloeden;
- b) bewerkstelligen dat deze personen competent zijn op basis van de juiste opleiding, training of ervaring;
- c) indien van toepassing, acties ondernemen om de benodigde competentie te verwerven, en de doeltreffendheid van de ondernomen acties evalueren; en
- d) geschikte gedocumenteerde informatie als bewijs van competentie bewaren.

OPMERKING Toepasbare acties kunnen bijv. zijn: het voorzien in training van, het begeleiden van of het in een andere functie benoemen van huidige medewerkers; of het inhuren of contracteren van competente personen.

7.3 Bewustzijn

Personen die werkzaamheden verrichten onder het gezag van de organisatie, moeten zich bewust zijn van:

- a) het informatiebeveiligingsbeleid;
- b) hun bijdrage aan de doeltreffendheid van het managementsysteem voor informatiebeveiliging, met inbegrip van de voordelen van verbeterde informatiebeveiligingsprestaties; en
- c) de gevolgen van het niet voldoen aan de eisen van het managementsysteem voor informatiebeveiliging.

7.4 Communicatie

De organisatie moet vaststellen welke interne en externe communicatie relevant is voor het managementsysteem voor informatiebeveiliging, inclusief:

- a) waarover te communiceren;
- b) wanneer te communiceren;
- c) met wie te communiceren;
- d) hoe te communiceren.

7.5 Gedocumenteerde informatie

7.5.1 Algemeen

Het managementsysteem voor informatiebeveiliging van de organisatie moet onder andere bevatten:

- a) de gedocumenteerde informatie die dit document vereist; en
- b) de gedocumenteerde informatie die de organisatie nodig acht voor de doeltreffendheid van het managementsysteem voor informatiebeveiliging.

OPMERKING De uitgebreidheid van gedocumenteerde informatie voor een managementsysteem voor informatiebeveiliging kan van organisatie tot organisatie verschillen vanwege:

- 1) de omvang van de organisatie en het type van haar activiteiten, processen, producten en diensten;
- 2) de complexiteit van de processen en hun interacties; en
- 3) de competentie van de mensen.

7.5.2 Creëren en actualiseren

Bij het creëren en actualiseren van gedocumenteerde informatie moet de organisatie zorgen voor (een) passend(e):

- a) identificatie en beschrijving (bijv. een titel, datum, auteur of referentienummer);
- b) format (bijv. taal, softwareversie, afbeeldingen) en media (bijv. papier, elektronisch); en
- c) beoordeling en goedkeuring van geschiktheid en toereikendheid.

7.5.3 Beheersing van gedocumenteerde informatie

Gedocumenteerde informatie zoals het managementsysteem voor informatiebeveiliging en dit document vereisen, moet worden beheerst om te bewerkstelligen dat:

- a) de informatie beschikbaar is en geschikt is voor gebruik, waar en wanneer het nodig is; en
- b) de informatie afdoende is beveiligd (bijv. tegen het verlies van vertrouwelijkheid, oneigenlijk gebruik en aantasting).

Voor het beheersen van gedocumenteerde informatie moet de organisatie, voor zover van toepassing, invulling geven aan de volgende activiteiten:

- c) distributie, toegang, het terugvinden alsmede het gebruik;
- d) opslag en behoud, inclusief behoud van leesbaarheid;
- e) beheersing van wijzigingen (bijv. versiebeheer); en
- f) bewaring en vernietiging.

Gedocumenteerde informatie van externe oorsprong die de organisatie nodig acht voor de planning en uitvoering van het managementsysteem voor informatiebeveiliging moet bij de situatie passend worden geïdentificeerd, en worden beheerst.

OPMERKING Toegang kan impliceren een besluit tot toestemming om de gedocumenteerde informatie alleen in te zien, of tot toestemming en bevoegdheid om de gedocumenteerde informatie in te zien en te wijzigen enz.

8 Uitvoering

8.1 Operationele planning en beheersing

Om te voldoen aan de eisen en om de in hoofdstuk 6 vastgestelde acties te implementeren moet de organisatie de benodigde processen plannen, implementeren en beheersen, door:

- criteria vast te stellen voor de processen;
- procesbeheersing te implementeren in overeenstemming met de criteria.

Gedocumenteerde informatie moet beschikbaar zijn in de omvang die nodig is om het vertrouwen te hebben dat de processen volgens planning zijn uitgevoerd.

De organisatie moet geplande wijzigingen beheersen en de consequenties van onbedoelde wijzigingen beoordelen, en zo nodig maatregelen treffen om nadelige effecten tegen te gaan.

De organisatie moet bewerkstelligen dat door externen geleverde processen, producten of diensten die relevant zijn voor het managementsysteem voor informatiebeveiliging, worden beheerst.

8.2 Risicobeoordeling van informatiebeveiliging

De organisatie moet, met geplande tussenpozen of zodra belangrijke veranderingen worden voorgesteld of zich voordoen, risicobeoordelingen voor informatiebeveiliging uitvoeren, rekening houdend met de in 6.1.2 a) vastgestelde criteria.

De organisatie moet gedocumenteerde informatie bewaren over de resultaten van de risicobeoordelingen voor informatiebeveiliging.

8.3 Informatiebeveiligingsrisico's behandelen

De organisatie moet het risicobehandelingsplan voor informatiebeveiliging implementeren.

De organisatie moet gedocumenteerde informatie bewaren over de resultaten van de risicobehandeling voor informatiebeveiliging.

9 Evaluatie van de prestaties

9.1 Monitoren, meten, analyseren en evalueren

De organisatie moet vaststellen:

- a) wat moet worden gemonitord en gemeten, met inbegrip van processen en beheersmaatregelen voor informatiebeveiliging;
- b) de methoden voor het, voor zover van toepassing, monitoren, meten, analyseren en evalueren om valide resultaten te bewerkstelligen. Om als valide te worden te beschouwd behoren de resultaten van de geselecteerde methoden te kunnen worden vergeleken en gereproduceerd;

- c) wanneer moet worden gemonitord en gemeten;
- d) wie moet monitoren en meten;
- e) wanneer de resultaten van het monitoren en meten moeten worden geanalyseerd en geëvalueerd;
- f) wie deze resultaten moet analyseren en evalueren.

Gedocumenteerde informatie moet beschikbaar zijn als bewijs van de resultaten.

De organisatie moet de prestaties van de informatiebeveiliging en de doeltreffendheid van het managementsysteem voor informatiebeveiliging evalueren.

9.2 Interne audit

9.2.1 Algemeen

De organisatie moet met geplande tussenpozen interne audits uitvoeren om informatie te verkrijgen of het managementsysteem voor informatiebeveiliging:

a) voldoet aan

- 1) de eigen eisen van de organisatie voor haar managementsysteem voor informatiebeveiliging;
- 2) de eisen van dit document;

b) doeltreffend is geïmplementeerd en onderhouden.

9.2.2 Intern auditprogramma

De organisatie moet (een) auditprogramma('s) plannen, vaststellen, implementeren en onderhouden, met inbegrip van de frequentie, methoden, verantwoordelijkheden, planningseisen en rapportage.

Bij het inrichten van het (de) interne auditprogramma('s) moet de organisatie rekening houden met het belang van de betrokken processen en met de resultaten van voorgaande audits.

De organisatie moet:

- a) de auditcriteria voor en de reikwijdte van elke audit definiëren;
- b) auditoren selecteren en audits uitvoeren zodanig dat de objectiviteit en de onpartijdigheid van het auditproces worden bewerkstelligd;
- c) bewerkstelligen dat de resultaten van de audits worden gerapporteerd aan het relevante management.

Gedocumenteerde informatie moet beschikbaar zijn als bewijs van de implementatie van het (de) audit programma('s) en de auditresultaten.

9.3 Management review

9.3.1 Algemeen

Het topmanagement moet met geplande tussenpozen het managementsysteem voor informatiebeveiliging van de organisatie beoordelen om de continue geschiktheid, toereikendheid en doeltreffendheid ervan te bewerkstelligen.

9.3.2 Input voor de management review

Bij de management review moet onder andere rekening worden gehouden met:

- a) de status van acties die zijn voortgekomen uit voorgaande management reviews;
- b) wijzigingen in externe en interne belangrijke punten (issues) die relevant zijn voor het managementsysteem voor informatiebeveiliging;
- c) wijzigingen in de behoeften en verwachtingen van de belanghebbenden die relevant zijn voor het managementsysteem voor informatiebeveiliging;
- d) feedback over de prestaties van de informatiebeveiliging, met inbegrip van trends in:
 - 1) afwijkingen en corrigerende maatregelen;
 - 2) resultaten van monitoren en meten;
 - 3) auditresultaten;
 - 4) het voldoen aan informatiebeveiligingsdoelstellingen;
- e) feedback van belanghebbenden;
- f) resultaten van risicobeoordeling en de status van het risicobehandelingsplan;
- g) kansen voor continue verbetering.

9.3.3 Resultaten van de management review

De resultaten van de management reviews moeten beslissingen omvatten met betrekking tot kansen voor continue verbetering en de noodzaak voor wijzigingen in het managementsysteem voor informatiebeveiliging.

Gedocumenteerde informatie moet beschikbaar zijn als bewijs van de resultaten van de management reviews.

10 Verbetering

10.1 Continue verbetering

De organisatie moet continu de geschiktheid, toereikendheid en doeltreffendheid van het managementsysteem voor informatiebeveiliging verbeteren.

10.2 Afwijkingen en corrigerende maatregelen

Wanneer zich een afwijking voordoet, moet de organisatie:

a) op de afwijking reageren, en indien van toepassing:

- 1) maatregelen treffen om de afwijking te beheersen en te corrigeren;
- 2) de consequenties aanpakken;

b) de noodzaak evalueren om maatregelen te treffen om de oorzaken van de afwijking weg te nemen, zodat de afwijking zich niet herhaalt of zich niet elders voordoet, door:

- 1) de afwijking te beoordelen;
- 2) de oorzaken van de afwijking vast te stellen; en
- 3) vast te stellen of zich gelijksoortige afwijkingen voordoen of kunnen voordoen;

c) de benodigde maatregelen implementeren;

d) de doeltreffendheid van getroffen corrigerende maatregelen beoordelen; en

e) zo nodig, wijzigingen aanbrengen in het managementsysteem voor informatiebeveiliging.

Corrigerende maatregelen moeten passend zijn voor de effecten van de opgetreden afwijkingen.

Gedocumenteerde informatie moet beschikbaar zijn als bewijs van:

- f) de aard van de afwijkingen en de vervolgens getroffen maatregelen;
- g) de resultaten van corrigerende maatregelen.

Bijlage A

(normatief)

Referentie voor beheersmaatregelen voor informatiebeveiliging

De in tabel A.1 opgenomen beheersmaatregelen voor informatiebeveiliging zijn rechtstreeks afgeleid van en afgestemd met de in ISO/IEC 27002:2022 [1], hoofdstuk 5 t/m 8 opgenomen beheersmaatregelen en moeten in context met 6.1.3 worden gebruikt.

Tabel A.1 — Beheersmaatregelen voor informatiebeveiliging

5	Organisatorische beheersmaatregelen	
5.1	Beleidsregels voor informatiebeveiliging	Beheersmaatregel Informatiebeveiligingsbeleid en onderwerpspecifieke beleidsregels moeten worden gedefinieerd, goedgekeurd door het management, gepubliceerd, gecommuniceerd aan en erkend door relevant personeel en relevante belanghebbenden en met geplande tussenpozen en als zich significante wijzigingen voordoen, worden beoordeeld.
5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Beheersmaatregel Rollen en verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.
5.3	Functiescheiding	Beheersmaatregel Conflicterende taken en conflicterende verantwoordelijkheden moeten worden gescheiden.
5.4	Managementverantwoordelijkheden	Beheersmaatregel Het management moet van al het personeel eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de onderwerpspecifieke beleidsregels en procedures van de organisatie.
5.5	Contact met overheidsinstanties	Beheersmaatregel De organisatie moet contact met de relevante instanties leggen en onderhouden.
5.6	Contact met speciale belangengroepen	Beheersmaatregel De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en onderhouden.
5.7	Informatie en analyses over dreigingen	Beheersmaatregel Informatie met betrekking tot informatiebeveiligingsdreigingen moet worden verzameld en geanalyseerd om informatie over dreigingen te produceren.

5.8	Informatiebeveiliging in projectmanagement	Beheersmaatregel Informatiebeveiliging moet worden geïntegreerd in projectmanagement.
5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Beheersmaatregel Er moet een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, worden opgesteld en onderhouden.
5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Beheersmaatregel Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen moeten worden geïdentificeerd, gedocumenteerd en geïmplementeerd.
5.11	Retourneren van bedrijfsmiddelen	Beheersmaatregel Personeel en andere belanghebbenden, al naargelang de situatie, moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst retourneren.
5.12	Classificeren van informatie	Beheersmaatregel Informatie moet worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante eisen van belanghebbenden.
5.13	Labelen van informatie	Beheersmaatregel Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.
5.14	Overdragen van informatie	Beheersmaatregel Er moeten regels, procedures of overeenkomsten voor informatieoverdracht zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.
5.15	Toegangsbeveiliging	Beheersmaatregel Er moeten regels op basis van bedrijfs- en informatiebeveiligingseisen worden vastgesteld en geïmplementeerd om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen.
5.16	Identiteitsbeheer	Beheersmaatregel De volledige levenscyclus van identiteiten moet worden beheerd.

5.17	Authenticatie-informatie	Beheersmaatregel De toewijzing en het beheer van authenticatie-informatie moet worden beheerst door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.
5.18	Toegangsrechten	Beheersmaatregel Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen moeten worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de organisatie.
5.19	Informatiebeveiliging in leveranciersrelaties	Beheersmaatregel Er moeten processen en procedures worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met het gebruik van producten of diensten van de leverancier te beheersen.
5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Beheersmaatregel Relevante informatiebeveiligingseisen moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie worden overeengekomen.
5.21	Beheren van informatiebeveiliging in de ICT-toeleveringsketen	Beheersmaatregel Er moeten processen en procedures worden bepaald en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheersen.
5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	Beheersmaatregel De organisatie moet de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig monitoren, beoordelen, evalueren en veranderingen daaraan beheren.
5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Beheersmaatregel Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten moeten overeenkomstig de informatiebeveiligingseisen van de organisatie worden opgesteld.
5.24	Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	Beheersmaatregel De organisatie moet plannen opstellen voor, en zich voorbereiden op, het beheren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.
5.25	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	Beheersmaatregel De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.

5.26	Reageren op informatiebeveiligingsincidenten	Beheersmaatregel Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.
5.27	Leren van informatiebeveiligingsincidenten	Beheersmaatregel Kennis die is opgedaan met informatiebeveiligingsincidenten moet worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.
5.28	Verzamelen van bewijsmateriaal	Beheersmaatregel De organisatie moet procedures vaststellen en implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.
5.29	Informatiebeveiliging tijdens een verstoring	Beheersmaatregel De organisatie moet plannen maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.
5.30	ICT-gereedheid voor bedrijfscontinuïteit	Beheersmaatregel De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen.
5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Beheersmaatregel Wettelijke, statutaire, regelgevende en contractuele eisen die relevant zijn voor informatiebeveiliging en de aanpak van de organisatie om aan deze eisen te voldoen, moeten worden geïdentificeerd, gedocumenteerd en actueel gehouden.
5.32	Intellectuele-eigendomsrechten	Beheersmaatregel De organisatie moet passende procedures implementeren om intellectuele-eigendomsrechten te beschermen.
5.33	Beschermen van registraties	Beheersmaatregel Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.
5.34	Privacy en bescherming van persoonsgegevens	Beheersmaatregel De organisatie moet de eisen met betrekking tot het behoud van privacy en de bescherming van persoonsgegevens volgens de toepasselijke wet- en regelgeving en contractuele eisen identificeren en eraan voldoen.
5.35	Onafhankelijke beoordeling van informatiebeveiliging	Beheersmaatregel De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan, met inbegrip van mensen, processen en technologieën, moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, worden beoordeeld.

5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	Beheersmaatregel De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie moet regelmatig worden beoordeeld.
5.37	Gedocumenteerde bedieningsprocedures	Beheersmaatregel Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar worden gesteld aan het personeel dat ze nodig heeft.
6	Mensgerichte beheersmaatregelen	
6.1	Screening	Beheersmaatregel De achtergrond van alle kandidaten voor een dienstverband moet worden gecontroleerd voordat ze bij de organisatie in dienst treden en daarna op gezette tijden worden herhaald. Hierbij moet rekening worden gehouden met de toepasselijke wet- en regelgeving en ethische overwegingen, en deze controle moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.
6.2	Arbeidsovereenkomst	Beheersmaatregel In arbeidsovereenkomsten moet worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.
6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Beheersmaatregel Personeel van de organisatie en relevante belanghebbenden moeten een passende bewustwording van, opleiding en training in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, krijgen.
6.4	Disciplinaire procedure	Beheersmaatregel Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen personeel en andere belanghebbenden die zich schuldig hebben gemaakt aan een schending van het informatiebeveiligingsbeleid.
6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	Beheersmaatregel Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband, moeten worden gedefinieerd, gehandhaafd en gecommuniceerd aan relevant personeel en andere belanghebbenden.
6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Beheersmaatregel Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, moeten worden geïdentificeerd, gedocumenteerd, regelmatig worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.

6.7	Werken op afstand	Beheersmaatregel Wanneer personeel op afstand werkt, moeten er beveiligingsmaatregelen worden geïmplementeerd om informatie te beschermen die buiten het gebouw en/of terrein van de organisatie wordt ingezien, verwerkt of opgeslagen.
6.8	Melden van informatiebeveiligingsgebeurtenissen	Beheersmaatregel De organisatie moet voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden.
7	Fysieke beheersmaatregelen	
7.1	Fysieke beveiligingszones	Beheersmaatregel Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken.
7.2	Fysieke toegangsbeveiliging	Beheersmaatregel Beveiligde zones moeten worden beschermd door passende toegangsbeveiligingsmaatregelen en toegangspunten.
7.3	Beveiligen van kantoren, ruimten en faciliteiten	Beheersmaatregel Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.
7.4	Monitoren van de fysieke beveiliging	Beheersmaatregel Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.
7.5	Beschermen tegen fysieke en omgevingsdreigingen	Beheersmaatregel Er moet bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen voor de infrastructuur, worden ontworpen en geïmplementeerd.
7.6	Werken in beveiligde zones	Beheersmaatregel Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd.
7.7	'Clear desk' en 'clear screen'	Beheersmaatregel Er moeten 'clear desk'-regels voor papieren documenten en verwijderbare opslagmedia en 'clear screen'-regels voor informatieverwerkende faciliteiten worden gedefinieerd en op passende wijze worden afgedwongen.
7.8	Plaatsen en beschermen van apparatuur	Beheersmaatregel Apparatuur moet veilig worden geplaatst en beschermd.
7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Beheersmaatregel Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd.

7.10	Opslagmedia	Beheersmaatregel Opslagmedia moeten worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie.
7.11	Nutsvoorzieningen	Beheersmaatregel Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.
7.12	Beveiligen van bekabeling	Beheersmaatregel Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen onderschepping, interferentie of beschadiging.
7.13	Onderhoud van apparatuur	Beheersmaatregel Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te garanderen.
7.14	Veilig verwijderen of hergebruiken van apparatuur	Beheersmaatregel Onderdelen van de apparatuur die opslagmedia bevatten, moeten worden gecontroleerd om te waarborgen dat gevoelige gegevens en gelicentieerde software zijn verwijderd of veilig zijn overschreven voordat ze worden verwijderd of hergebruikt.
8	Technologische beheersmaatregelen	
8.1	'User endpoint devices'	Beheersmaatregel Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' moet worden beschermd.
8.2	Speciale toegangsrechten	Beheersmaatregel Het toewijzen en het gebruik van speciale toegangsrechten moet worden beperkt en beheerd.
8.3	Beperking toegang tot informatie	Beheersmaatregel De toegang tot informatie en andere gerelateerde bedrijfsmiddelen moet worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.
8.4	Toegangsbeveiliging op broncode	Beheersmaatregel Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd.
8.5	Beveiligde authenticatie	Beheersmaatregel Er moeten beveiligde authenticatietechnologieën en -procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke beleid inzake toegangsbeveiliging.

8.6	Capaciteitsbeheer	Beheersmaatregel Het gebruik van middelen moet worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen.
8.7	Bescherming tegen malware	Beheersmaatregel Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn.
8.8	Beheer van technische kwetsbaarheden	Beheersmaatregel Er moet informatie worden verkregen over technische kwetsbaarheden van in gebruik zijnde informatiesystemen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en er moeten passende maatregelen worden getroffen.
8.9	Configuratiebeheer	Beheersmaatregel Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.
8.10	Wissen van informatie	Beheersmaatregel In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moet worden gewist als deze niet langer vereist is.
8.11	Maskeren van gegevens	Beheersmaatregel Gegevens moeten worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels, en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving.
8.12	Voorkomen van gegevenslekken (data leakage prevention)	Beheersmaatregel Maatregelen om gegevenslekken te voorkomen moeten worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.
8.13	Back-up van informatie	Beheersmaatregel Back-ups van informatie, software en systemen moeten worden bewaard en regelmatig worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups.
8.14	Redundantie van informatieverwerkende faciliteiten	Beheersmaatregel Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.

8.15	Logging	Beheersmaatregel Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, worden geproduceerd, opgeslagen, beschermd en geanalyseerd.
8.16	Monitoren van activiteiten	Beheersmaatregel Netwerken, systemen en toepassingen moeten worden gemonitord op afwijkend gedrag en er moeten passende maatregelen worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren.
8.17	Kloksynchronisatie	Beheersmaatregel De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdbronnen.
8.18	Gebruik van speciale systeemhulpmiddelen	Beheersmaatregel Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, moet worden beperkt en nauwkeurig worden gecontroleerd.
8.19	Installeren van software op operationele systemen	Beheersmaatregel Er moeten procedures en maatregelen worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.
8.20	Beveiliging netwerkcomponenten	Beheersmaatregel Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.
8.21	Beveiliging van netwerkdiensten	Beheersmaatregel Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord.
8.22	Netwerksegmentatie	Beheersmaatregel Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd.
8.23	Toepassen van webfilters	Beheersmaatregel De toegang tot externe websites moet worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.
8.24	Gebruik van cryptografie	Beheersmaatregel Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, moeten worden gedefinieerd en geïmplementeerd.

8.25	Beveiligen tijdens de ontwikkelcyclus	Beheersmaatregel Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast.
8.26	Toepassingsbeveiligingseisen	Beheersmaatregel Er moeten eisen aan de informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.
8.27	Veilige systeemarchitectuur en technische uitgangspunten	Beheersmaatregel Uitgangspunten voor het ontwerpen van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen.
8.28	Veilig coderen	Beheersmaatregel Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling.
8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Beheersmaatregel Processen voor het testen van de beveiliging moeten worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.
8.30	Uitbestede systeemontwikkeling	Beheersmaatregel De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.
8.31	Scheiding van ontwikkel-, test- en productieomgevingen	Beheersmaatregel Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd.
8.32	Wijzigingsbeheer	Beheersmaatregel Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer.
8.33	Testgegevens	Beheersmaatregel Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.
8.34	Bescherming van informatiesystemen tijdens audits	Beheersmaatregel Audittests en andere auditactiviteiten waarbij operationele systemen worden beoordeeld, moeten worden gepland en overeengekomen tussen de tester en het verantwoordelijke management.

Bibliografie

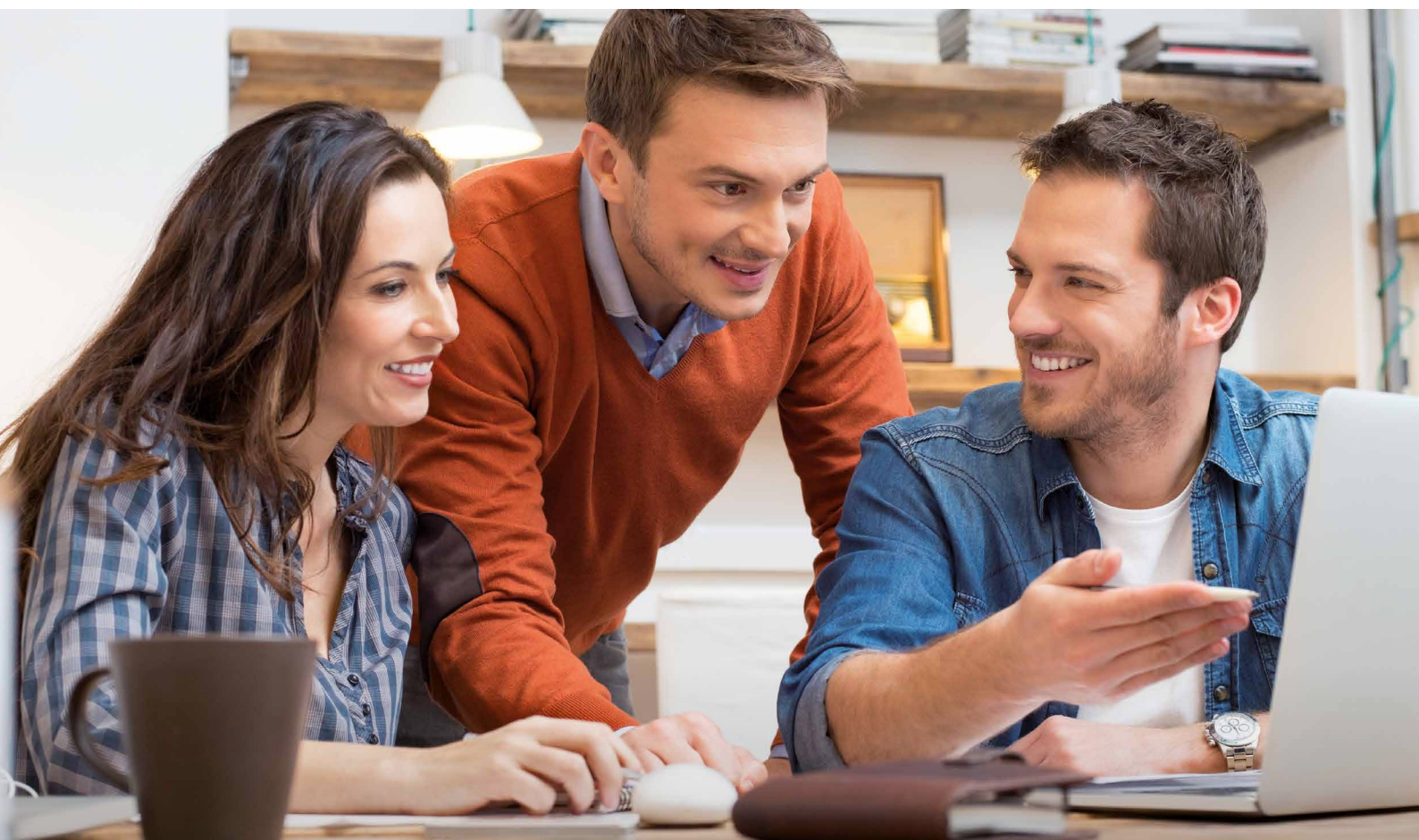
- [1] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection – Information security controls*
- [2] ISO/IEC 27003, *Information technology – Security techniques – Information security management systems – Guidance*
- [3] ISO/IEC 27004, *Information technology – Security techniques — Information security management – Monitoring, measurement, analysis and evaluation*
- [4] ISO/IEC/DIS 27005, *Information security, cybersecurity and privacy protection – Guidance on managing information security risks*
- [5] ISO 31000:2018, *Risk management – Guidelines*
- [6] ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, 2012

Waarom betaalt u voor een norm?

Normen zijn afspraken voor en door de markt. Het zijn afspraken over zaken waarmee iedereen te maken heeft. Bijvoorbeeld over gezondheidszorg, financiële dienstverlening, veiligheid en maatschappelijk verantwoord ondernemen. Zonder deze afspraken zou het leven een stuk complexer zijn. Normen zorgen voor verbetering van producten, diensten en processen. Op de werkvloer, in de omgang met elkaar en in de samenleving als geheel.

De afspraken worden gemaakt door belanghebbende partijen. Een belanghebbende partij kan een producent, ondernemer, dienstverlener, gebruiker, maar ook de overheid of een consumenten- of onderzoeksorganisatie zijn. Een breed draagvlak is belangrijk. De afspraken komen onder begeleiding van NEN tot stand en mogen niet strijdig zijn met andere geldige NEN-normen.

NEN is een stichting en heeft geen winstoogmerk. De diensten die NEN levert – van het bijeenbrengen van partijen en het maken en vastleggen van de afspraken tot het bieden van hulp bij de toepassing van de normen – moeten worden bekostigd. Daarom betalen alle deelnemende partijen voor het normalisatieproces en betaalt u als gebruiker voor normen, trainingen en andere producten.



Altijd de actuele norm?

Nooit meer zoeken in de systemen en zelf de vraag stellen:
'Heb ik de laatste versie van NEN-EN-ISO/IEC 27001:2023 nl?'

Via het digitale platform NEN Connect heeft u altijd toegang tot de meest actuele versie van deze norm. Vervallen versies blijven ook beschikbaar. Met een licentie kan de norm via NEN Connect altijd en overal makkelijk geraadpleegd worden, zowel online als offline.

Kies voor slimmer werken en bekijk onze mogelijkheden op www.nenconnect.nl.

Meer informatie over de mogelijkheden

Onze Klantenservice is bereikbaar maandag tot en met vrijdag, van 8.30 uur tot 17.00 uur.

Telefoon: 015 2 690 391

E-mail: klantenservice@nen.nl

nen
connect