

Verklaring van toepasselijkheid ISO27001:2017 + A11: 2020

KWIZ versie 1.4 van 21-1-2022

| | | | Van toepassing? | Geïmplementeerd? | Wet | Contract | Risico analyse | Niet van toepassing want: |
|---|--------------------------------------|---|-----------------|------------------|-----|----------|----------------------------------|---------------------------|
| A.5 | Beveiligingsbeleid | | | | | | | |
| Norm | Omschrijving | Beheersmaatregel | Van toepassing? | Geïmplementeerd | Wet | Contract | Risk Assessment / Best Practices | Onderbouwing uitsluiting |
| A.5 IB-beleid | | | | | | | | |
| A.5.1 Aansturing door de directie van de IB | | | | | | | | |
| Doelstelling: Het verschaffen van directieaansturing van en -steun voor IB in overeenstemming met bedrijfseisen en relevante wet- en regelgeving. | | | | | | | | |
| A.5.1.1 | Beleidsregels voor IB | Ten behoeve van IB moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. | j | j | | | X | |
| A.5.1.2 | Beoordelen van het IB-beleid | Het beleid voor IB moet met geplande tussenpozen of als zich significante veranderingen voordoen, worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is. | j | j | | | X | |
| A.6 Organiseren van IB | | | | | | | | |
| A.6.1 Interne organisatie | | | | | | | | |
| Doelstelling: Een beheerkader vaststellen om de implementatie en uitvoering van de IB binnen de organisatie te initiëren en te beheersen. | | | | | | | | |
| A.6.1.1 | Rollen en verantwoordelijkheden IB | Alle verantwoordelijkheden bij IB moeten worden gedefinieerd en toegewezen. | j | j | | | X | |
| A.6.1.2 | Scheiding van taken | Conflicterende taken en verantwoordelijkheidsgebieden moeten worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de <u>bedrijfsmiddelen van de organisatie te verminderen</u> . | j | j | | | X | |
| A.6.1.3 | Contact met overheidsinstanties | Er moeten passende contacten met relevante overheidsinstanties worden onderhouden. | j | j | X | | x | |
| A.6.1.4 | Contact met speciale belangengroepen | Er moeten passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden. | j | j | | | X | |
| A.6.1.5 | IB in projectbeheer | IB moet aan de orde komen in projectbeheer, ongeacht het soort project. | j | j | | X | X | |
| A.6.2 Mobiele apparatuur en telewerken | | | | | | | | |
| Doelstelling: Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur. | | | | | | | | |
| A.6.2.1 | Beleid voor mobiele apparatuur | Beleid en ondersteunende beveiligingsmaatregelen moeten worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheersen. | j | j | | X | X | |
| A.6.2.2 | Telewerken | Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt bereikt, verwerkt of opgeslagen. | j | j | | X | X | |
| A.7 Veilig personeel | | | | | | | | |
| A.7.1 Voorafgaand aan het dienstverband | | | | | | | | |
| Doelstelling: Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de functies waarvoor zij in aanmerking komen. | | | | | | | | |
| A.7.1.1 | Screening | Verificatie van de achtergrond van alle kandidaten voor een dienstverband moet worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's. | j | j | | | X | |
| A.7.1.2 | Arbeidsvoorwaarden | De contractuele overeenkomst met medewerkers en contractanten moet hun verantwoordelijkheden voor IB en die van de organisatie vermelden. | j | j | | x | X | |
| A.7.2 Tijdens het dienstverband | | | | | | | | |
| Doelstelling: Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van IB en deze nakomen. | | | | | | | | |

| | | | | | | | | |
|--|--|---|---|---|--|---|---|--|
| A.7.2.1 | Directieverantwoordelijkheden | De directie moet van alle medewerkers en contractanten eisen dat ze IB toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie. | j | j | | | X | |
| A.7.2.2 | Bewustzijn, opleiding en training ten aanzien van IB | Alle medewerkers van de organisatie en, voor zover relevant, contractanten moeten een passende bewustzijnsopleiding en -training krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie. | j | j | | | X | |
| A.7.2.3 | Disciplinaire procedure | Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de IB. | j | j | | | X | |
| A.7.3 Beëindiging en wijziging van dienstverband | | | | | | | | |
| Doelstelling: Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband. | | | | | | | | |
| A.7.3.1 | Beëindiging of wijziging van verantwoordelijkheden van het dienstverband | Verantwoordelijkheden en taken met betrekking tot IB die van kracht blijven na beëindiging of wijziging van het dienstverband moeten worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer worden gebracht. | j | j | | | X | |
| A.8 Beheer van bedrijfsmiddelen | | | | | | | | |
| A.8.1 Verantwoordelijkheid voor bedrijfsmiddelen | | | | | | | | |
| Doelstelling: Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren. | | | | | | | | |
| A.8.1.1 | Inventariseren van bedrijfsmiddelen | Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten worden geïdentificeerd, en van deze bedrijfsmiddelen moet een inventaris worden opgesteld en onderhouden. | j | j | | X | X | |
| A.8.1.2 | Eigendom van bedrijfsmiddelen | Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een eigenaar hebben. | j | j | | X | X | |
| A.8.1.3 | Aanvaardbaar gebruik van bedrijfsmiddelen | Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten regels worden geïdentificeerd, gedocumenteerd en geïmplementeerd. | j | j | | | X | |
| A.8.1.4 | Teruggeven van bedrijfsmiddelen | Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst teruggeven. | j | j | | | X | |
| A.8.2 Informatieclassificatie | | | | | | | | |
| Doelstelling: Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie. | | | | | | | | |
| A.8.2.1 | Classificatie van informatie | Informatie moet worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging. | j | j | | | X | |
| A.8.2.2 | Informatie labelen | Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie. | j | j | | | X | |
| A.8.2.3 | Behandelen van bedrijfsmiddelen | Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie. | j | j | | | X | |
| A.8.3 Behandelen van media | | | | | | | | |
| Doelstelling: Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen. | | | | | | | | |
| A.8.3.1 | Beheer van verwijderbare media | Voor het beheren van verwijderbare media moeten procedures worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld. | j | j | | | X | |
| A.8.3.2 | Verwijderen van media | Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures. | j | j | | | X | |
| A.8.3.3 | Media fysiek overdragen | Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport. | j | j | | | X | |
| A.9 Toegangsbeveiliging | | | | | | | | |
| A.9.1 Bedrijfseisen voor toegangsbeveiliging | | | | | | | | |
| Doelstelling: Toegang tot informatie en informatieverwerkende faciliteiten beperken. | | | | | | | | |
| A.9.1.1 | Beleid voor toegangsbeveiliging | Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en IB-eisen. | j | j | | | X | |

| | | | | | | | | |
|--|--|--|---|---|--|---|---|--|
| A.9.1.2 | Toegang tot netwerken en netwerkdiensten | Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. | j | j | | | X | |
| A.9.2 Beheer van toegangsrechten van gebruikers | | | | | | | | |
| Doelstelling: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen. | | | | | | | | |
| A.9.2.1 | Registratie en uitschrijving van gebruikers | Een formele registratie- en uitschrijvingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. | j | j | | X | X | |
| A.9.2.2 | Gebruikers toegang verlenen | Een formele gebruikerstoegangsverleningsprocedure moet worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken. | j | j | | | X | |
| A.9.2.3 | Beheren van speciale toegangsrechten | Het toewijzen en gebruik van bevoorrechte toegangsrechten moeten worden beperkt en gecontroleerd. | j | j | | | X | |
| A.9.2.4 | Beheer van geheime authenticatie-informatie van gebruikers | Het toewijzen van geheime authenticatie-informatie moet worden beheerd via een formeel beheersproces. | j | j | | | X | |
| A.9.2.5 | Beoordeling van toegangsrechten van gebruikers | Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen. | j | j | | | X | |
| A.9.2.6 | Toegangsrechten intrekken of aanpassen | De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten moeten bij beëindiging van hun dienstverband, contract of overeenkomst worden verwijderd, en bij wijzigingen moeten ze worden aangepast. | j | j | | | X | |
| A.9.3 Gebruikersverantwoordelijkheden | | | | | | | | |
| Doelstelling: Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie-informatie. | | | | | | | | |
| A.9.3.1 | Geheime authenticatie-informatie gebruiken | Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie. | j | j | | | X | |
| A.9.4 Toegangsbeveiliging van systeem en toepassing | | | | | | | | |
| Doelstelling: Onbevoegde toegang tot systemen en toepassingen voorkomen. | | | | | | | | |
| A.9.4.1 | Beperking toegang tot informatie | Toegang tot informatie en systeemfuncties van applicaties moet worden beperkt in overeenstemming met het beleid voor toegangscontrole. | j | j | | | X | |
| A.9.4.2 | Beveiligde inlogprocedures | Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerd door een beveiligde inlogprocedure. | j | j | | | X | |
| A.9.4.3 | Systeem voor wachtwoordbeheer | Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen. | j | j | | | X | |
| A.9.4.4 | Speciale systeemhulpmiddelen gebruiken | Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen moet worden beperkt en nauwkeurig worden gecontroleerd. | j | j | | | X | |
| A.9.4.5 | Toegangsbeveiliging op programmabroncode | Toegang tot de programmabroncode moet worden beperkt. | j | j | | | X | |
| A.10 Cryptografie | | | | | | | | |
| A.10.1 Cryptografische beheersmaatregelen | | | | | | | | |
| Doelstelling: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen. | | | | | | | | |
| A.10.1.1 | Beleid inzake het gebruik van cryptografische beheersmaatregelen | Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd. | j | j | | | X | |
| A.10.1.2 | Sleutelbeheer | Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels moet tijdens hun gehele levenscyclus een beleid worden ontwikkeld en geïmplementeerd. | j | j | | | X | |

| A.11 Fysieke beveiliging en beveiliging van de omgeving | | | | | | | |
|--|---|--|---|---|---|---|---|
| A.11.1 Beveiligde gebieden | | | | | | | |
| Doelstelling: Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie voorkomen. | | | | | | | |
| A.11.1.1 | Fysieke beveiligingszone | Beveiligingszones moeten worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten. | j | j | | X | X |
| A.11.1.2 | Fysieke toegangsbeveiliging | Beveiligde gebieden moeten worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt. | j | j | | X | X |
| A.11.1.3 | Kantoren, ruimten en faciliteiten beveiligen | Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast. | j | j | | | X |
| A.11.1.4 | Beschermen tegen bedreigingen van buitenaf | Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast. | j | j | | X | X |
| A.11.1.5 | Werken in beveiligde gebieden | Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast. | j | j | | | X |
| A.11.1.6 | Laad- en loslocatie | Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, moeten worden beheerst, en zo mogelijk worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden. | j | j | | | x |
| A.11.2 Apparatuur | | | | | | | |
| Doelstelling: Verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen. | | | | | | | |
| A.11.2.1 | Plaatsing en bescherming van apparatuur | Apparatuur moet zo worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind. | j | j | | | X |
| A.11.2.2 | Nutsvoorzieningen | Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen. | j | j | | | X |
| A.11.2.3 | Beveiliging van bekabeling | Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade. | j | j | X | | X |
| A.11.2.4 | Onderhoud van apparatuur | Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen. | j | j | | | X |
| A.11.2.5 | Verwijdering van bedrijfsmiddelen | Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring. | j | j | | | X |
| A.11.2.6 | Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein | Bedrijfsmiddelen die zich buiten het terrein bevinden, moeten worden beveiligd, waarbij rekening moet worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie. | j | j | | | X |
| A.11.2.7 | Veilig verwijderen of hergebruiken van apparatuur | Alle onderdelen van de apparatuur die opslagmedia bevatten, moeten worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of veilig zijn overschreven. | j | j | | | X |
| A.11.2.8 | Onbeheerde gebruikersapparatuur | Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is. | j | j | | | X |
| A.11.2.9 | 'Clear desk'- en 'clear screen'-beleid | Er moet een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten worden ingesteld. | j | j | | | X |
| A.12 Beveiliging bedrijfsvoering | | | | | | | |
| A.12.1 Bedieningsprocedures en verantwoordelijkheden | | | | | | | |
| Doelstelling: Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen. | | | | | | | |
| A.12.1.1 | Gedocumenteerde bedieningsprocedures | Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben. | j | j | | | X |

| | | | | | | | | |
|--|--|--|---|---|--|---|---|--|
| A.12.1.2 | Wijzigingsbeheer | Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de IB moeten worden beheerst. | j | j | | | X | |
| A.12.1.3 | Capaciteitsbeheer | Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste <u>stelsysteemprestaties te waarborgen</u> . | j | j | | | X | |
| A.12.1.4 | Scheiding van ontwikkel-, test- en productieomgevingen | Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen. | j | j | | | X | |
| A.12.2 Bescherming tegen malware | | | | | | | | |
| Doelstelling: Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware. | | | | | | | | |
| A.12.2.1 | Beheersmaatregelen tegen malware | Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend <u>bewustzijn van gebruikers</u> . | j | j | | | X | |
| A.12.3 Back-up | | | | | | | | |
| Doelstelling: Beschermen tegen het verlies van gegevens. | | | | | | | | |
| A.12.3.1 | Back-up van informatie | Regelmatig moeten back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een <u>overeengekomen back-upbeleid</u> . | j | j | | | X | |
| A.12.4 Verslaglegging en monitoren | | | | | | | | |
| Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen. | | | | | | | | |
| A.12.4.1 | Gebeurtenissen registreren | Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en IB-gebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig <u>worden beoordeeld</u> . | j | j | | | X | |
| A.12.4.2 | Beschermen van informatie in logbestanden | Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang. | j | j | | | X | |
| A.12.4.3 | Logbestanden van beheerders en operators | Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld. | j | j | | | X | |
| A.12.4.4 | Kloksynchronisatie | De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met één <u>referentietijdbron</u> . | j | j | | | X | |
| A.12.5 Beheersing van operationele software | | | | | | | | |
| Doelstelling: De integriteit van operationele systemen waarborgen. | | | | | | | | |
| A.12.5.1 | Software installeren op operationele systemen | Om het op operationele systemen installeren van software te beheersen moeten <u>procedures worden geïmplementeerd</u> . | j | j | | | X | |
| A.12.6 Beheer van technische kwetsbaarheden | | | | | | | | |
| Doelstelling: Benutting van technische kwetsbaarheden voorkomen. | | | | | | | | |
| A.12.6.1 | Beheer van technische kwetsbaarheden | Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt moet tijdig worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken. | j | j | | X | X | |
| A.12.6.2 | Bepalingen voor het installeren van software | Voor het door gebruikers installeren van software moeten regels worden <u>vastgesteld en geïmplementeerd</u> . | j | j | | | X | |
| A.12.7 Overwegingen betreffende audits van informatiesystemen | | | | | | | | |
| Doelstelling: De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken. | | | | | | | | |
| A.12.7.1 | Beheersmaatregelen betreffende audits van informatiesystemen | Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, moeten zorgvuldig worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren. | j | j | | | X | |
| A.13 Communicatiebeveiliging | | | | | | | | |
| A.13.1 Beheer van netwerkbeveiliging | | | | | | | | |
| Doelstelling: De bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten waarborgen. | | | | | | | | |

| | | | | | | | | |
|--|---|---|---|---|--|---|---|--|
| A.13.1.1 | Beheersmaatregelen voor netwerken | Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen. | j | j | | | X | |
| A.13.1.2 | Beveiliging van netwerkdiensten | Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten. | j | j | | X | X | |
| A.13.1.3 | Scheiding in netwerken | Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden. | j | j | | | X | |
| A.13.2 Informatietransport | | | | | | | | |
| Doelstelling: Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit. | | | | | | | | |
| A.13.2.1 | Beleid en procedures voor informatietransport | Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn. | j | j | | X | X | |
| A.13.2.2 | Overeenkomsten over informatietransport | Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen. | j | j | | X | X | |
| A.13.2.3 | Elektronische berichten | Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn. | j | j | | X | X | |
| A.13.2.4 | Vertrouwelijkheids- of geheimhoudings-overeenkomst | Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen moeten worden vastgesteld, regelmatig worden beoordeeld en gedocumenteerd. | j | j | | X | X | |
| A.14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen | | | | | | | | |
| A.14.1 Beveiligingseisen voor informatiesystemen | | | | | | | | |
| Doelstelling: Waarborgen dat IB integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken. | | | | | | | | |
| A.14.1.1 | Analyse en specificatie van IB-eisen | De eisen die verband houden met IB moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen. | j | j | | X | X | |
| A.14.1.2 | Toepassingsdiensten op openbare netwerken beveiligen | Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, moet worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging. | j | j | | X | X | |
| A.14.1.3 | Transacties van toepassingsdiensten beschermen | Informatie die deel uitmaakt van transacties van toepassingsdiensten moet worden beschermd ter voorkoming van onvolledige overdracht, foutieve routing, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vernieuwvuldigen of afsnellen. | j | j | | | X | |
| A.14.2 Beveiliging in ontwikkelings- en ondersteunende processen | | | | | | | | |
| Doelstelling: Bewerkstelligen dat IB wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen. | | | | | | | | |
| A.14.2.1 | Beleid voor beveiligd ontwikkelen | Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast. | j | j | | | X | |
| A.14.2.2 | Procedures voor wijzigingsbeheer met betrekking tot systemen | Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele controleprocedures voor wijzigingsbeheer. | j | j | | | X | |
| A.14.2.3 | Technische beoordeling van toepassingen na wijzigingen bedieningsplatform | Als bedieningsplatforms zijn veranderd, moeten bedrijfskritische toepassingen worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie. | j | j | | | X | |

| | | | | | | | | |
|--|---|--|---|---|--|---|---|---|
| A.14.2.4 | Beperkingen op wijzigingen aan softwarepakketten | Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd. | j | j | | | X | |
| A.14.2.5 | Principes voor engineering van beveiligde systemen | Principes voor de engineering van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen. | j | j | | | X | |
| A.14.2.6 | Beveiligde ontwikkelomgeving | Organisaties moeten beveiligde ontwikkelomgevingen vaststellen en passend beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling. | j | j | | | X | |
| A.14.2.7 | Uitbestede softwareontwikkeling | Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie. | n | n | | | | KWIZ besteedt geen systeemontwikkeling uit. |
| A.14.2.8 | Testen van systeembeveiliging | Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest. | j | j | | | X | |
| A.14.2.9 | Systeemacceptatie-tests | Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld. | j | j | | X | X | |
| A.14.3 Testgegevens | | | | | | | | |
| Doelstelling: Bescherming waarborgen van gegevens die voor het testen zijn gebruikt. | | | | | | | | |
| A.14.3.1 | Bescherming van testgegevens | Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd. | j | j | | | X | |
| A.15 Leveranciersrelaties | | | | | | | | |
| A.15.1 IB in leveranciersrelaties | | | | | | | | |
| Doelstelling: De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers. | | | | | | | | |
| A.15.1.1 | IB-beleid voor leveranciersrelaties | Met de leverancier moeten de IB-eisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, worden overeengekomen en gedocumenteerd. | j | j | | X | X | |
| A.15.1.2 | Opnemen van beveiligingsaspecten in leveranciers-overeenkomsten | Alle relevante IB-eisen moeten worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt. | j | j | | X | X | |
| A.15.1.3 | Toelevingsketen van informatie- en communicatie-technologie | Overeenkomsten met leveranciers moeten eisen bevatten die betrekking hebben op de IB-risico's in verband met de toelevingsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie. | j | j | | X | X | |
| A.15.2 Beheer van dienstverlening van leveranciers | | | | | | | | |
| Doelstelling: Een overeengekomen niveau van IB en dienstverlening in overeenstemming met de leverancierovereenkomsten handhaven. | | | | | | | | |
| A.15.2.1 | Monitoring en beoordeling van dienstverlening van leveranciers | Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen. | j | j | | X | X | |
| A.15.2.2 | Beheer van veranderingen in de dienstverlening van leveranciers | Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor IB, moeten worden beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's. | j | j | | X | X | |
| A.16 Beheer van IB-incidenten | | | | | | | | |
| A.16.1 Beheer van IB-incidenten en -verbeteringen | | | | | | | | |
| Doelstelling: Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van IB-incidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging. | | | | | | | | |
| A.16.1.1 | Verantwoordelijkheden en procedures | Directieverantwoordelijkheden en -procedures moeten worden vastgesteld om een snelle, doeltreffende en ordelijke respons op IB-incidenten te bewerkstelligen. | j | j | | | X | |
| A.16.1.2 | Rapportage van IB-gebeurtenissen | IB-gebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd. | j | j | | | X | |

| | | | | | | | | |
|----------|--|--|---|---|--|--|---|--|
| A.16.1.3 | Rapportage van zwakke plekken in de IB | Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie moet worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de IB registreren en rapporteren. | j | j | | | X | |
| A.16.1.4 | Beoordeling van en besluitvorming over IB-gebeurtenissen | IB-gebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geïnclassificeerd als IB-incidenten. | j | j | | | X | |
| A.16.1.5 | Respons op IB-incidenten | Op IB-incidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures. | j | j | | | X | |
| A.16.1.6 | Lering uit IB-incidenten | Kennis die is verkregen door IB-incidenten te analyseren en op te lossen moet worden gebruikt om de waarschijnlijkheid van toekomstige incidenten te verkleinen. | j | j | | | X | |
| A.16.1.7 | Verzamelen van bewijsmateriaal | De organisatie moet procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen. | j | j | | | X | |

A.17 IB-aspecten van bedrijfscontinuïteitsbeheer

A.17.1 IB-continuïteit

Doelstelling: IB-continuïteit moet worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.

| | | | | | | | | |
|----------|---|--|---|---|--|---|---|--|
| A.17.1.1 | IB-continuïteit plannen | De organisatie moet haar eisen voor IB en voor de continuïteit van het IB-beheer in ongunstige situaties, bijv. een crisis of een ramp, vaststellen. | j | j | | X | X | |
| A.17.1.2 | IB-continuïteit implementeren | De organisatie moet processen, procedures en beheersmaatregelen vaststellen, documenteren, implementeren en handhaven om het vereiste niveau van continuïteit voor IB tijdens een ongunstige situatie te waarborgen. | j | j | | X | X | |
| A.17.1.3 | IB-continuïteit verifiëren, beoordelen en evalueren | De organisatie moet de ten behoeve van IB-continuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties. | j | j | | X | X | |

A.17.2 Redundante componenten

Doelstelling: Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen.

| | | | | | | | | |
|----------|--|---|---|---|--|---|---|--|
| A.17.2.1 | Beschikbaarheid van informatieverwerkende faciliteiten | Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen. | j | j | | X | X | |
|----------|--|---|---|---|--|---|---|--|

A.18 Naleving

A.18.1 Naleving van wettelijke en contractuele eisen

Doelstelling: Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende IB en beveiligingseisen.

| | | | | | | | | |
|----------|---|---|---|---|---|---|---|--|
| A.18.1.1 | Vaststellen van toepasselijke wetgeving en contractuele eisen | Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen moeten voor elk informatiesysteem en de organisatie expliciet worden vastgesteld, gedocumenteerd en actueel gehouden. | j | j | X | X | X | |
| A.18.1.2 | Intellectuele eigendomsrechten | Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen moeten passende procedures worden geïmplementeerd. | j | j | X | X | X | |
| A.18.1.3 | Beschermen van registraties | Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave. | j | j | X | X | X | |
| A.18.1.4 | Privacy en bescherming van persoonsgegevens | Privacy en bescherming van persoonsgegevens moeten, voor zover van toepassing, worden gewaarborgd in overeenstemming met relevante wet- en regelgeving. | j | j | X | X | X | |
| A.18.1.5 | Voorschriften voor het gebruik van cryptografische beheersmaatregelen | Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving. | j | j | X | X | X | |

A.18.2 IB-beoordelingen

Doelstelling: Verzekeren dat IB wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie.

| | | | | | | | | |
|----------|---|---|---|---|--|--|---|--|
| A.18.2.1 | Onafhankelijke beoordeling van IB | De aanpak van de organisatie ten aanzien van het beheer van IB en de implementatie ervan (bijv. beheersdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor IB), moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen worden beoordeeld | j | j | | | X | |
| A.18.2.2 | Naleving van beveiligingsbeleid en normen | [A11] > Leidinggevenden moeten regelmatig de naleving van de informatieverwerking en -procedures binnen hun[<A11] verantwoordelijkheidsgebied beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging | j | j | | | X | |
| A.18.2.3 | Beoordeling van technische naleving | Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor IB. | j | j | | | X | |