Verklaring van toepasselijkheid 2024

Yards Deurwaardersdiensten B.V.

Document index

Auteur	Yards Deurwaarders BV.
Document naam	“Verklaring van toepasselijkheid 2024”
Datum	20-01-2025
Distributie	Extern
Versie / status	1.1
Classificatie	Publiek

Document historie

Versie	Toelichting	Auteur	Datum
0.1	Initiële document setup	Ramon Hartman	17-12-2024
0.2	Check en aanpassingen	Mike Oostwal	*20-12-2024*
1.0	Definitieve versie	Mike Oostwal	*20-12-2024*
1.1	Tekstuele aanpassingen op verzoek KIWA	Mike Oostwal	*20-01-2025*

1. Inleiding

Dit document omvat de Verklaring van Toepasselijkheid (VVT) ten behoeve van de certificering voor de ISO27001 standaard.
De doelstelling van dit document is het identificeren van de toepasselijke beheersmaatregelen welke geïmplementeerd dienen te zijn om de bedreigingen tegen Yards en haar bedrijfsprocessen te controleren en te managen. De beheersmaatregelen zijn geïdentificeerd op basis van de in de ISO27001 standaard opgenomen beheersmaatregelen benoemd in Annex 1 van de ISO 27001 norm.
Per beheersmaatregel wordt de toepasselijkheid weergegeven, als uitgangspunt is hierbij gesteld dat alle geselecteerde beheersmaatregelen zijn geïmplementeerd/toegepast tenzij, dan wordt een verklaring voor het "niet toepassen" of "niet van toepassing verklaren" gegeven.
Voor de van toepassing zijnde beheersmaatregel wordt verwezen naar de gedefinieerde ISO27002 'best practices' richtlijnen welke specifiek zijn gemaakt voor toepassing in de Yards bedrijfsprocessen.

1.1. Directie verklaring

De directie van, Yards Deurwaardersdiensten B.V., verklaart hierbij te voldoen aan de gestelde criteria van de NEN-ISO/IEC 27001:2017 en accepteert het restrisico van eventueel niet genomen maatregelen voor het volgende toepassingsgebied:

Minnelijke & gerechtelijke (incasso)werkzaamheden

Zoals uitgevoerd binnen de bedrijfsprocessen van Yards en haar bedrijfslocatie.
Het gehanteerde kwaliteits- en informatiebeveiligingsmanagement systeem is van toepassing op de bedrijfsprocessen van Yards en geldt voor alle vaste en tijdelijke werknemers van Yards.
Directie van Yards Deurwaardersdiensten B.V.

Naam: Paul Tabor
Functie: CEO
Datum: 20-01-2025

Handtekening

2. Verklaring van toepasselijkheid

2.1. Toelichting

Uitgangspunt bij het opstellen van de verklaring van toepassing is dat alle beheersmaatregelen worden toegepast tenzij.

De VVT is weergegeven in de volgende tabel met de volgende kolommen:

De eerste twee kolommen geven het nummer en de beschrijving van de ISO27001 annex 1 domeinen, sub-domeinen en beheersmaatregelen weer.

Kolom drie geeft de selectie reden van de beheersmaatregel weer,

- hetzij voortkomend uit de risicoanalyse aangeduid met R_x (x verwijzend naar het risico nummer in het risicoregister.) of R_{syst} (Verwijst naar het resultaat van de bedrijfs (informatie)systeemwaardering.)
- geselecteerd als baseline op basis van “best practices”,
- of voortkomend uit een directe verplichting uit de ISO 27001.

Kolom vier, vijf en zes geven waarin het beleid is terug te vinden, dit kan dus staan in:

- Wet- en regelgeving
- Contractuele overeenkomst
- Beleid van de organisatie

In de laatste kolom wordt aangegeven of de beheersmaatregel is geïmplementeerd ja of nee. Indien de norm of beheersmaatregel niet is geïmplementeerd wordt dit benoemt.
Noot, indien gewenst of noodzakelijk kan via de Yards compliance manager inzage worden verkregen in het risico register.

2.2 Verklaring van toepasselijkheid ISO27001 Annex-1

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
A.5	Organisatorische beheersmaatregelen							
A.5.1.	Beleidsregels voor informatiebeveiliging	Informatiebeveiligingsbeleid en onderwerp specifieke beleidsregels moeten worden gedefinieerd, goedgekeurd door het management, gepubliceerd, gecommuniceerd aan en erkend door relevant personeel en relevante belanghebbenden en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, te worden beoordeeld.	ISO27001 5.1/5.2/9.3 $R_{6,7,8,9,11,12,14}$	Ja			X	Ja
A.5.2.	Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen overeenkomstig	ISO27001$_{5.3}$ $R_{14,43,83,85}$	Ja			X	Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
		de behoeften van de organisatie.						
A.5.3.	Functiescheiding	Conflicterende taken en conflicterende verantwoordelijkheidsgebieden moeten te worden gescheiden.	R14,43,83,85,102,120,121,122,123,136	Ja			X	Ja
A.5.4.	Management verantwoordelijkheden	Het management moet van al het personeel eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de onderwerpspecifieke beleidsregels en procedures van de organisatie.	ISO27001 5.1 R78,80,84,123,124,144,145,147	Ja	X		X	Ja
A.5.5.	Contact met overheidsinstanties	De organisatie moet contact met de relevante instanties leggen en te onderhouden.	ISO27001 4.2 R1,4,5,11,12,13,14	Ja			X	Ja
A.5.6.	Contact met speciale belangengroepen	De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en te onderhouden.	ISO27001 4.2 R1,4,5,146,147	Ja	X	X		Ja
A.5.7.	Informatie en analyses over dreigingen	Informatie met betrekking tot informatiebeveiligingsdreiging	R148	Ja	X		X	Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
		en moet worden verzameld en geanalyseerd om informatie en analyses over dreigingen te produceren.						
A.5.8.	Informatiebeveiliging in projectmanagement	Informatiebeveiliging moet worden geïntegreerd in projectmanagement.	R informatiesystemen $R_{17,81,146,149}$	Ja			X	Ja
A.5.9.	Inventariseren van informatie en andere gerelateerde bedrijfsmiddelen	Er moet een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, worden opgesteld en onderhouden.	Basis $ISO27001_{7.1}$ R informatiesystemen $R_{85,119}$	Ja			X	Ja
A.5.10.	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen moet worden vastgesteld en geïmplementeerd.	Basis R_{86}	Ja			X	Ja
A.5.11.	Retourneren van bedrijfsmiddelen	Personeel en andere belanghebbenden, al naargelang de situatie, moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij	Basis $R_{23,87,119}$	Ja			X	Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
		beëindiging van hun dienstverband, contract of overeenkomst retourneren.						
A.5.12.	Classificeren van informatie	Informatie moet worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante belanghebbenden.	ISO27001$_{7.5.3}$ R$_{24,88,102}$	Ja			X	Ja
A.5.13.	Labelen van informatie	Om informatie te labelen moet een passende reeks procedures worden vastgesteld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Basis R$_{89,115}$	Ja			X	Ja
A.5.14.	Overdragen van informatie	Er moeten regels, procedures of overeenkomsten voor informatieoverdracht zijn vastgesteld voor alle soorten van overdracht binnen de organisatie en tussen de organisatie en andere partijen.	Basis ISO27001$_{7.5.3}$ R$_{35,88,116,117,118}$	Ja		X		Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
A.5.15.	Toegangsbeveiliging	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.	Basis $R_{45,83,88,90,102}$	Ja	X		X	Ja
A.5.16	Identiteitsbeheer	De volledige levenscyclus van identiteiten moet worden beheerd.	$R_{25,45,91}$	Ja	X	X	X	Ja
A.5.17.	Beheer van authenticatie-informatie	De toewijzing en het beheer van authenticatie-informatie moet worden beheerst door middel van een beheerproces waarvan het informeren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	Basis $R_{26,45,88}$	Ja	X	X	X	Ja
A.5.18.	Toegangsrechten	Toegangsrechten met betrekking tot informatie en andere gerelateerde bedrijfsmiddelen moeten worden verstrekt, beoordeeld, aangepast en verwijderd	$R_{27,28,29,92}$	Ja	X		X	Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
		overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de organisatie.						
A.5.19.	Informatiebeveiliging in leveranciersrelaties	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 beheren.	Basis $R_{30,131,140,141}$	Ja	X	X	X	Ja
A.5.20.	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Relevante informatiebeveiligingseisen moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie te worden overeengekomen.	ISO27001$_{8.1}$ R_{30}	Ja		X		Ja
A.5.21.	Beheren van informatiebeveiliging in de ICT-keten	Er moeten processen en procedures worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-	Basis R_{30}	Ja	X	X		Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
		producten en -diensten te beheren.						
A.5.22.	Monitoren, beoordelen en beheren van wijzigingen van leveranciersdiensten	De organisatie moet de informatiebeveiligingspraktijken en de leveranciersdiensten regelmatig monitoren, beoordelen, evalueren en veranderingen daaraan te beheren.	R informatiesystemen $R_{19,22,30,132}$	Ja	X	X		Ja
A.5.23.	Informatiebeveiliging voor het gebruik van clouddiensten	Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten moeten overeenkomstig de informatiebeveiligingseisen van de organisatie worden opgesteld.	R_{30}	Ja	X	X		Ja
A.5.24	Plannen en voorbereiden van beheer van informatiebeveiliging	De organisatie moet plannen opstellen voor, en zich voor te bereiden op, het beheren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.	ISO27001 $_{10.1}$ $R_{92,150}$	Ja	X		X	Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
A.5.25.	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en te beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	ISO27001$_{10.1}$ R$_{151,152,153}$	Ja	X		X	Ja
A.5.26.	Reageren op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	R$_{153}$	Ja	X		X	Ja
A.5.27.	Leren van informatiebeveiligingsincidenten	Kennis die is opgedaan met informatiebeveiligingsincidenten moet worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	ISO27001$_{10.1}$ R$_{31,58,59,110,154}$	Ja	X		X	Ja
A.5.28.	Verzamelen van bewijsmateriaal	De organisatie moet procedures vaststellen en te implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.	ISO27001$_{10.1}$ R$_{114}$	Ja	X		X	Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
A.5.29.	Informatiebeveiliging tijdens een verstoring	De organisatie moet plannen maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	R informatiesystemen R32,76,77,81,130,131,139,141	Ja	X	X	X	Ja
A.5.30.	ICT-gereedheid voor bedrijfscontinuïteit	De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstelling en en ICT-continuïteitseisen.	R32,33,40,53,66,127	Ja	X	X	X	Ja
A.5.31.	Wettelijke, statutaire, regelgevende en contractuele eisen	Eisen van 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 vastgesteld, gedocumenteerd en actueel gehouden.	R1,2,3,4,5,33	Ja	X		X	Ja
A.5.32.	Intellectuele eigendomsrechten	De organisatie moet passende procedures implementeren om intellectuele eigendomsrechten te beschermen.	Basis R5,10,41	Ja	X	X	X	Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
A.5.33.	Beschermen van registraties	Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	Basis $R_{15,41,88,113}$	Ja	X	X	X	Ja
A.5.34	Privacy en bescherming van persoonsgegevens	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 te voldoen.	Basis $R_{5,11,41,45,88,107,136}$	Ja	X			Ja
A.5.35.	Onafhankelijke beoordeling van informatiebeveiliging	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.	ISO27001$_{9.2}$ $R_{154,155}$	Ja			X	Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
A.5.36.	Naleving van beleid, regels en normen voor informatiebeveiliging	De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie moet regelmatig worden beoordeeld.	ISO27001$_{9.2/10.1}$ R$_{154,155}$	Ja			X	Ja
A.5.37.	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar te worden gesteld aan het personeel dat ze nodig heeft.	Basis R$_{81,92,93}$	Ja			X	Ja
A.6	Beheersmaatregelen gericht op mensen							
A.6.1.	Screening	De achtergrond van alle kandidaten die in aanmerking komen voor posities binnen de organisatie moet worden gecontroleerd voordat ze bij de organisatie in dienst treden en daarna op gezette tijden te worden herhaald. Hierbij behoort rekening te worden gehouden met de toepasselijke wet- en regelgeving, voorschriften en	R$_{79,95,96}$	Ja	X			Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
		ethische overwegingen, en deze controle behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.						
A.6.2.	Arbeidsovereenkomst	In arbeidsovereenkomsten moet worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.	ISO27001$_{5.3}$ R$_{97,98}$	Ja	X	X		Ja
A.6.3.	Bewustwording van, opleiding en training in informatiebeveiliging	Personeel van de organisatie en relevante belanghebbenden moet een passend(e) bewustwording van, opleiding, training en bijscholing in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, krijgen.	ISO27001$_{7.3}$ R$_{2,3,4,78,79,80,81,99,123,124,125,129,142,147}$	Ja			X	Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
A.6.4.	Disciplinaire procedure	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.	Basis R5,34,78,80,100, 101,123,125,129	Ja		X	X	Ja
A.6.5.	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	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.	R informatiesystemen R34,80,81,102,	Ja		X	X	Ja
A.6.6.	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, moeten worden geïdentificeerd, gedocumenteerd, regelmatig	Basis R34	Ja		X		Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
		te worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.						
A.6.7.	Werken op afstand	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.	Basis $R_{17,18,35,37}$	Ja		X		Ja
A.6.8.	Melden van informatiebeveiligings-gebeurtenissen	De organisatie moet voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden.	$ISO27001_{10.1}$ R_{110}	Ja			X	Ja
A.7	Fysieke beheersmaatregelen							
A.7.1.	Fysieke beveiligingszones	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken.	R informatiesystemen $R_{36,111,112,125}$	Ja			X	Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
A.7.2.	Fysieke toegangsbeveiliging	Beveiligde zones moeten worden beschermd door passende toegangscontroles en toegangspunten.	Basis R36,109,111,112, 125, 129,142	Ja			X	Ja
A.7.3.	Beveiligen van kantoren, ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.	R informatiesystemen R36,111,112,125, 129	Ja			X	Ja
A.7.4.	Monitoren van de fysieke beveiliging	Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.	R111,112,125	Ja	X			Ja
A.7.5.	Beschermen tegen fysieke en omgevingsdreigingen	Er moet bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen van de infrastructuur, worden ontworpen en geïmplementeerd.	Basis R126	Ja		X		Ja
A.7.6.	Werken in beveiligde zones	Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd.	R36,88	Ja			X	Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
A.7.7.	'Clear desk' en 'Clear screen'	Er moeten 'clear desk'-regels voor papieren documenten en verwijderbare opslagmedia en 'clear screen'-regels voor informatieverwerkende faciliteiten worden gedefinieerd en op passende wijze ten uitvoer worden gebracht.	R informatiesystemen R_{109}	Ja			X	Ja
A.7.8.	Plaatsen en beschermen van apparatuur	Apparatuur moet veilig worden geplaatst en beschermd.	R informatiesystemen $R_{17,111,112,125}$	Ja		X		Ja
A.7.9.	Beveiligen van bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd.	R informatiesystemen $R_{37,38}$	Ja			X	Ja
A.7.10.	Opslagmedia	Opslagmedia moet worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie.	Basis R informatiesystemen $R_{39,102,}$	Ja			X	Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
A.7.11.	Nutsvoorzieningen	Informatieverwerkende faciliteiten moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	R informatiesystemen $R_{17,127,128}$	Ja		X		Ja
A.7.12.	Beveiligen van bekabeling	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen onderschepping, interferentie of beschadiging.	R informatiesystemen R_{129}	Ja		X		Ja
A.7.13.	Onderhoud van apparatuur	Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.	R informatiesystemen $R_{17,40,67}$	Ja		X		Ja
A.7.14.	Veilig verwijderen of hergebruiken van apparatuur	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	R informatiesystemen R_{41}	Ja		X		Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
		worden verwijderd of hergebruikt.						
A.8	Technische beheersmaatregelen							
A.8.1.	'User endpoint devices'	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' moet worden beschermd.	Basis R_{42}	ja			X	Ja
A.8.2.	Speciale toegangsrechten	Het toewijzen en gebruik van speciale toegangsrechten moet worden beperkt en beheerd.	R_{43}	Ja			X	Ja
A.8.3.	Beperking toegang tot informatie	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen moet worden beperkt overeenkomstig het vastgestelde onderwerp specifieke beleid inzake toegangsbeveiliging.	$R_{88,120,121,122}$	Ja			X	Ja
A.8.4.	Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd.	n.v.t.	Nee			X	Nee, Yards beheert geen software bron- of programmacode

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
A.8.5.	Beveiligde authenticatie	Er moeten beveiligde authenticatietechnologieën en -procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke of aanvullende beleid inzake toegangsbeveiliging.	R_{45}	Ja	X		X	Ja
A.8.6.	Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en afgestemd overeenkomstig de huidige en verwachte capaciteitseisen.	Basis $R_{46,137}$	Ja		X		Ja
A.8.7.	Bescherming tegen malware	Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn.	Basis $R_{16,48}$	Ja			X	Ja
A.8.8.	Beheer van technische kwetsbaarheden	Er moet informatie worden verkregen over technische kwetsbaarheden van in gebruik zijnde informatiesystemen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden	ISO27001 9.2 R informatiesystemen $R_{16,49,121,122}$	Ja			X	Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
		geëvalueerd en er behorende passende maatregelen te worden getroffen.						
A.8.9.	Configuratie management	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.	R_{50}	Ja			X	Ja
A.8.10.	Wissen van informatie	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moet worden gewist als deze niet langer nodig is.	$R_{51,88}$	Ja	X		X	Ja
A.8.11.	Maskeren van gegevens	Gegevens moeten worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels, en bedrijfseisen van de organisatie, rekening	n.v.t.	Nee				Nee, Yards vind maskeren niet noodzakelijk daar persoonlijke gegevens worden beschermd

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
		houdend met de toepasselijke wetgeving.						door autorisatiebeheer en geheime adressen van debiteuren binnen gerechtsdeurwaardersoftware.
A.8.12	Voorkomen van gegevenslekken (Data leakage prevention)	Maatregelen om gegevenslekken te voorkomen moeten worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.	R107,108	Ja	X		X	Ja
A.8.13	Back-up van informatie	Back-ups van informatie, software en systemen moeten worden bewaard en regelmatig te worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups.	R informatiesystemen R52,53,54	Ja	X	X	X	Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
A.8.14	Redundantie van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	R informatiesystemen $R_{55,56}$	Ja		X	X	Ja
A.8.15	Logging	Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	R informatiesystemen $R_{57,58}$	Ja			X	Ja
A.8.16	Monitoren van activiteiten	Netwerken, systemen en toepassingen moeten worden gemonitord op afwijkend gedrag en er behoren passende maatregelen te worden genomen om potentiële informatiebeveiligingsincidenten te evalueren.	$R_{57,59}$	Ja			X	Ja
A.8.17	Kloksynchronisatie	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt,	R informatiesystemen $R_{60,61}$	Ja		X	X	Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
		moeten worden gesynchroniseerd met goedgekeurde tijdsbronnen.						
A.8.18	Gebruik van speciale systeemhulpmiddelen	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, moet worden beperkt en nauwkeurig te worden gecontroleerd.	$R_{62,88}$	Ja		X	X	Ja
A.8.19	Installeren van software op operationele systemen	Er moeten procedures en maatregelen worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.	R informatiesystemen $R_{63,64}$	Ja		X	X	Ja
A.8.20	Beveiliging netwerkcomponenten	Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	R_{65}	Ja		X	X	Ja
A.8.21	Beveiliging netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten moeten	Basis $R_{66,67}$	Ja		X	X	Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
		worden geïdentificeerd, geïmplementeerd en gemonitord.						
A.8.22	Netwerksegmentatie	Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd.	Basis $R_{68,69,88}$	Ja		X	X	Ja
A.8.23	Toepassen van webfilters	De toegang tot externe websites moet worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.	R_{70}	Ja			X	Ja
A.8.24	Cryptografische maatregelen	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, moeten worden gedefinieerd en geïmplementeerd.	Basis R informatiesystemen $R_{71,72,}$	Ja			X	Nee, Yards beheert geen cryptografie maar gebruiken het wel, uitbesteed
A.8.25.	Beveiligen tijdens de ontwikkelingscyclus	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast.	n.v.t.	Nee				Nee, Yards kent geen interne software

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
								ontwikkeling.
A.8.26.	Toepassingsbeveiligingseisen	Er moeten eisen aan de informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	n.v.t.	Ja			X	Yards kent geen interne software ontwikkeling maar heeft wel beleid ten aanzien van het aanschaffen van software.
A.8.27.	Veilige systeemarchitectuur en technische uitgangspunten	Uitgangspunten voor het ontwerpen van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen.	n.v.t.	Nee				Nee, Yards kent geen interne software ontwikkeling.
A.8.28	Veilig coderen	Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling.	n.v.t.	Nee				Nee, Yards kent geen interne software ontwikkeling.

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
A.8.29.	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Processen voor het testen van de beveiliging moeten worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.	n.v.t.	Nee				Nee, Yards kent geen interne software ontwikkeling.
A.8.30.	Uitbestede systeemontwikkeling	De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.	n.v.t.	Nee				Nee, Yards kent geen interne software ontwikkeling.
A.8.31	Scheiding van ontwikkel-, test- en productie-omgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd.	Basis $R_{73,74}$	Ja		X	X	Ja
A.8.32	Wijzigingsbeheer	Wijzigingen in informatieverwerkingsfaciliteit en en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer.	$R_{16,20,75,121,122}$	Ja			X	Ja
A.8.33	Testgegevens	Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.	Basis $R_{103,104,105,106}$	Ja	X		X	Ja

#	Omschrijving	Beschrijving beheersmaatregel	Risk/Basis /n.v.t	Van toepassing?	Wet- en regelgeving	Contractuele overeenkomst	Beleid van de organisatie	Geïmplementeerd? Zo nee waarom:
A.8.34	Bescherming van informatiesystemen tijden audits	Audits en andere borgingsactiviteiten waarbij operationele systemen worden beoordeeld moeten worden gepland en overeengekomen tussen de tester en het verantwoordelijke management.	ISO27001$_{9.1}$ R$_{45}$	Ja			X	Ja