KEMBIT

KEMBIT Operations - Statement of Applicability ISO 27001

Auteur: Jeremy Erkens / Johan van der Velde
Datum: 12-sep-2024

Document specificaties

Type	SoA ISO 27001	Relatienummer	10007
Kenmerk	Management Systeem	Documentclassificatie	Vertrouwelijk
Auteur	J. Erkens / J. v.d. Velde	Contactpersoon	Quality Manager
Versie	8.0	E-mail Contactpersoon	qa@kembit.nl
Datum	12-sep-2024	Telefoon Contactpersoon	+31 (0) 885700500

Disclaimer

KEMBIT

Inhoudsopgave

1 Introductie

Deze Statement of Applicability (SoA) ondersteunt en is gebaseerd op onderstaande normeringen:

- 27001:2023 - ISO 27001 is een ISO standaard voor informatiebeveiliging.

Het doel van dit document is het definiëren van de maatregelen welke binnen het Management Systeem van KEMBIT Operations van wel of niet van toepassing zijn.

1.1 Belangrijke wijziging 2022

Met ingang van 7 september 2022 zijn de KEMBIT bedrijven KEMBIT Consultancy B.V. en KEMBIT Services B.V. samengevoegd tot KEMBIT Operations B.V. De certificering en deze Statement of Applicability zijn van toepassing op de diensten van het voormalig KEMBIT Services B.V. en (nog) niet voor de diensten van het voormalige KEMBIT Consultancy. Tijdens de eerstvolgende audit in 2023 wordt hiervoor de scope uitgebreid zodat alle diensten die door KEMBIT Operations geleverd worden gecertificeerd zijn inclusief de diensten Detachering en Project Management.

1.2 Belangrijke wijziging 2024

In 2022 en 2023 heeft ISO nieuwe versies van ISO 27001 uitgebracht. Omdat de ISO 27001 en NEN 7510-1 niet meer synchroon lopen wat betreft de nummering van de maatregelen, heeft KEMBIT Operations B.V. de SoA opgesplitst. Er is een aparte SoA opgesteld voor NEN 7510.

In hoofdstuk 3 zijn alle beheersmaatregelen genoteerd en wordt aangegeven welke maatregelen van toepassing zijn en of deze geïmplementeerd zijn. Hierbij is gebruik gemaakt van bijlage A van de NEN 7510-1 norm. Voor maatregelen die wel van toepassing zijn maar nog niet geïmplementeerd, heeft KEMBIT Operations B.V. een implementatieplan opgesteld met een planning en een verantwoordelijke eigenaar.

1.3 Verantwoordelijkheden

Onderstaand overzicht laat de verantwoordelijke voor dit document zien.

- Accountable:
  - Quality Manager
  - Informatie Manager
- Responsible:
  - Directeur Operations

1.4 Definities

Een overzicht van gebruikte definities is terug te vinden in het document:

- KEMBIT - Management Systeem - **Hoofdstuk 3: KEMBIT - MS - Begrippenlijst.pdf**.

1.5 Gerelateerde documenten

Voor onze klanten is een ingekorte versie gemaakt van de SoA, hierin zijn hoofdstuk 1 is niet opgenomen. De ingekorte versies zijn op de KEMBIT website geplaatst, onder certificeringen: Certificeringen | KEMBIT

- KEMBIT Operations - MS - SoA NEN7510-1_online_versie.pdf
- KEMBIT Operations - MS - SoA ISO27001_online_versie.pdf

2 Statements

2.1 Organisatorische beheersmaatregelen 5

2.1.1 Beleidsregels voor Informatiebeveiliging 5.1

Doelstelling: De voortdurende geschiktheid, toereikendheid, doeltreffendheid van de sturing en ondersteuning door het management overeenkomstig de bedrijfseisen van wet- en regelgeving, statutaire en contractuele eisen bewerkstelligen.

Ref. no.:	5.1	Item:	Beleidsregels voor informatiebeveiliging		
ISO 27001	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.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.2 Rollen en verantwoordelijkheden bij informatiebeveiliging 5.2

Doelstelling: Een gedefinieerde, goedgekeurde en duidelijk te begrijpen structuur voor de implementatie, uitvoering en het beheer van informatiebeveiliging binnen de organisatie inrichten.

Ref. no.:	5.2	Item:	Rollen en verantwoordelijkheden bij informatiebeveiliging		
ISO 27001	Rollen en verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.3 Functiescheiding 5.3

Doelstelling: Het risico op fraude, fouten en het omzeilen van beheersmaatregelen voor informatiebeveiliging verminderen.

Ref. no.:	5.3	Item:	Functiescheiding		
ISO 27001	Conflicterende taken en conflicterende verantwoordelijkheden moeten worden gescheiden.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.4 Managementverantwoordelijkheden 5.4

Doelstelling: Bewerkstelligen dat het management zijn rol bij informatiebeveiliging begrijpt en maatregelen neemt om ervoor te zorgen dat al het personeel zich bewust is van zijn verantwoordelijkheden op het gebied van informatiebeveiliging en deze ook nakomt.

Ref. no.:	5.4	Item:	Managementverantwoordelijkheden		
ISO 27001	Het management moet van al het personeel eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de onderwerpspecifieke beleidsregels en procedures van de organisatie.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.5 Contact met overheidsinstanties 5.5

Doelstelling: Een passende stroom van informatie met betrekking tot informatiebeveiliging tussen de organisatie en relevante juridische, regelgevende en toezichthoudende instanties bewerkstelligen.

Ref. no.:	5.5	Item:	Contact met overheidsinstanties		
ISO 27001	De organisatie moet contact met relevante instanties leggen en onderhouden.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.6 Contact met speciale belangengroepen 5.6

Doelstelling: Een passende stroom van informatie met betrekking tot informatiebeveiliging bewerkstelligen.

Ref. no.:	5.6	Item:	Contact met speciale belangengroepen		
ISO 27001	De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en onderhouden.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.7 Informatie en analyses over dreigingen 5.7

Doelstelling: Bewustwording bieden van de mogelijke bedreigingen voor de organisatie zodat de passende mitigerende maatregelen kunnen worden getroffen.

Ref. no.:	5.7	Item:	Informatie en analyses over dreigingen		
ISO 27001	Informatie met betrekking tot informatiebeveiligingsdreigingen moet worden verzameld en geanalyseerd om informatie over dreigingen te produceren.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.8 Informatiebeveiliging in projectmanagement 5.8

Doelstelling: Ervoor zorgen dat informatiebeveiligingsrisico's binnen projecten om en te leveren producten en diensten gedurende de gehele levenscyclus van het project op doeltreffende wijze binnen het projectmanagement worden aangepakt.

Ref. no.:	5.8	Item:	Informatiebeveiliging in projectmanagement		
ISO 27001	Informatiebeveiliging moet worden geïntegreerd in projectmanagement.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.9 Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen 5.9

Doelstelling: De informatie en andere gerelateerde bedrijfsmiddelen van de organisatie identificeren om de informatiebeveiliging ervan te behouden en passend eigenaarschap toe te wijzen.

Ref. no.:	5.9	Item:	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen		
ISO 27001	Er moet een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, worden opgesteld en onderhouden.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.10 Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen 5.10

Doelstelling: Waarborgen dat informatie en andere gerelateerde bedrijfsmiddelen passen worden beschermd, gebruikt en behandeld.

Ref. no.:	5.10	Item:	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen		
ISO 27001	Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen moeten worden geïdentificeerd, gedocumenteerd en geïmplementeerd.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.11 Retourneren van bedrijfsmiddelen 5.11

Doelstelling: De bedrijfsmiddelen van de organisatie beschermen als onderdeel van de procedure voor het wijzigen of beëindigen van het dienstverband, het contract of de overeenkomst.

Ref. no.:	5.11	Item:	Retourneren van bedrijfsmiddelen		
ISO 27001	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.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.12 Classificeren van informatie 5.12

Doelstelling: Bewerkstelligen dat het identificeren van en het inzicht in de beschermingsbehoeften voor de organisatie in overeenstemming zijn met het belang ervan voor de organisatie.

Ref. no.:	5.12	Item:	Classificeren van informatie		
ISO 27001	Informatie moet worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante eisen van belanghebbenden.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.13 Labelen van informatie 5.13

Doelstelling: Het communiceren van de dataclassificatie van informatie mogelijk maken en het automatiseren van informatieverwerking en -beheer ondersteunen.

Ref. no.:	5.13	Item:	Labelen van informatie		
ISO 27001	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.14 Overdragen van informatie 5.14

Doelstelling: Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met externe belanghebbende.

Ref. no.:	5.14	Item:	Overdragen van informatie		
ISO 27001	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.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.15 Toegangsbeveiliging 5.15

Doelstelling: Toegang voor bevoegden bewerkstelligen en toegang voor onbevoegden tot informatie en andere gerelateerde bedrijfsmiddelen voorkomen.

Ref. no.:	5.15	Item:	Toegangsbeveiliging		
ISO 27001	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.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.16 Identiteitsbeheer 5.16

Doelstelling: De unieke identificatie van personen en systemen die toegang hebben tot de informatie en andere gerelateerde bedrijfsmiddelen van de organisatie, en een juiste toewijzing van toegangsrechten mogelijk maken.

Ref. no.:	5.16	Item:	Identiteitsbeheer		
ISO 27001	De volledige levenscyclus van identiteiten moet worden beheerd.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.17 Authenticatie-informatie 5.17

Doelstelling: Goede authenticatie bewerkstelligen en fouten van authenticatieprocessen voorkomen.

Ref. no.:	5.17	Item:	Authenticatie-informatie		
ISO 27001	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.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.18 Toegangsrechten 5.18

Doelstelling: Bewerkstelligen dat de toegang tot informatie en andere gerelateerde bedrijfsmiddelen wordt vastgesteld en goedgekeurd overeenkomstig met de bedrijfseisen.

Ref. no.:	5.18	Item:	Toegangsrechten		
ISO 27001	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.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.19 Informatiebeveiliging in leveranciersrelaties 5.19

Doelstelling: Een overeengekomen niveau van informatiebeveiliging in leveranciersrelaties in stand houden.

Ref. no.:	5.19	Item:	Informatiebeveiliging in leveranciersrelaties		
ISO 27001	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.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.20 Adresseren van informatiebeveiliging in leveranciersovereenkomsten 5.20

Doelstelling: Een overeengekomen niveau van informatiebeveiliging in de leveranciersrelaties in stand houden.

Ref. no.:	5.20	Item:	Adresseren van informatiebeveiliging in leveranciersovereenkomsten		
ISO 27001	Relevante informatiebeveiligingseisen moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie worden overeengekomen.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.21 Beheren van informatiebeveiliging in de ICT-toeleveringsketen 5.21

Doelstelling: Een overeengekomen niveau van informatiebeveiliging in leveranciersrelaties in stand houden.

Ref. no.:	5.21	Item:	Beheren van informatiebeveiliging in de ICT-toeleveringsketen		
ISO 27001	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.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.22 Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten 5.22

Doelstelling: Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.

Ref. no.:	5.22	Item:	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten		
ISO 27001	De organisatie moet de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig monitoren, beoordelen, evalueren en veranderingen daaraan beheren.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.23 Informatiebeveiliging voor het gebruik van clouddiensten 5.23

Doelstelling: Informatiebeveiliging voor gebruik van clouddiensten specificeren en beheren.

Ref. no.:	5.23	Item:	Informatiebeveiliging voor het gebruik van clouddiensten		
ISO 27001	Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten moeten overeenkomstig de informatiebeveiligingseisen van de organisatie worden opgesteld.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.24 Plannen en voorbereiden van het beheer van informatiebeveiligings- incidenten 5.24

Doelstelling: Een snelle, doeltreffende, consistente en geordende reactie op informatiebeveiligingsincidenten, met inbegrip van communicatie over informatiebeveiligingsgebeurtenissen, bewerkstelligen.

Ref. no.:	5.24	Item:	Plannen en voorbereiden van het beheer van informatiebeveiligings- incidenten		
ISO 27001	De organisatie moet plannen opstellen voor, en zich voorbereiden op, het beheren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatie- beveiligingsincidenten te definiëren, vast te stellen en te communiceren.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.25 Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen 5.25

Doelstelling: Doeltreffende, categorisering en prioritering van informatiebeveiligingsgebeurtenissen bewerkstelligen.

Ref. no.:	5.25	Item:	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	
ISO 27001	De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.		**Applicable**	Ja
			Geïmplementeerd	Ja
			Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.26 Reageren op informatiebeveiligingsincidenten 5.26

Doelstelling: Een doeltreffende reactie op informatiebeveiligingsincidenten bewerkstelligen.

Ref. no.:	5.26	Item:	Reageren op informatiebeveiligingsincidenten	
ISO 27001	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.		**Applicable**	Ja
			Geïmplementeerd	Ja
			Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.27 Leren van informatiebeveiligingsincidenten 5.27

Doelstelling: De waarschijnlijkheid of de gevolgen van toekomstige incidenten verminderen.

Ref. no.:	5.27	Item:	Leren van informatiebeveiligingsincidenten	
ISO 27001	Kennis die is opgedaan met informatiebeveiligingsincidenten moet worden gebruikt om de en voor informatiebeveiliging te versterken en te verbeteren.		**Applicable**	Ja
			Geïmplementeerd	Ja
			Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.28 Verzamelen van bewijsmateriaal 5.28

Doelstelling: In het kader van disciplinaire en gerechtelijke stappen consistent en doeltreffend beheer bewerkstelligen van bewijsmateriaal in verband met informatiebeveiligingsincidenten.

Ref. no.:	5.28	Item:	Verzamelen van bewijsmateriaal		
ISO 27001	De organisatie moet procedures vaststellen en implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.29 Informatiebeveiliging tijdens een verstoring 5.29

Doelstelling: Informatie en andere gerelateerde bedrijfsmiddelen tijdens een verstoring beschermen.

Ref. no.:	5.29	Item:	Informatiebeveiliging tijdens een verstoring		
ISO 27001	De organisatie moet plannen maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.30 ICT-gereedheid voor bedrijfscontinuïteit 5.30

Doelstelling: De beschikbaarheid van de informatie en andere gerelateerde bedrijfsmiddelen van de organisatie tijdens een verstoring waarborgen.

Ref. no.:	5.30	Item:	ICT-gereedheid voor bedrijfscontinuïteit		
ISO 27001	De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoel- stellingen en ICT-continuïteitseisen.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.31 Wettelijke, statutaire, regelgevende en contractuele eisen 5.31

Doelstelling: De naleving bewerkstelligen van wettelijke, statutaire, regelgevende en contractuele eisen in verband met informatiebeveiliging.

Ref. no.:	5.31	Item:	Wettelijke, statutaire, regelgevende en contractuele eisen	
ISO 27001	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.		**Applicable**	Ja
			Geïmplementeerd	Ja
			Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.32 Intellectuele-eigendomsrechten 5.32

Doelstelling: De naleving bewerkstelligen van wet- en regelgeving, statutaire en contractuele eisen in verband met intellectuele-eigendomsrechten en het gebruik van gepatenteerde producten.

Ref. no.:	5.32	Item:	Intellectuele-eigendomsrechten	
ISO 27001	De organisatie moet passende procedures implementeren om intellectuele-eigendomsrechten te beschermen.		**Applicable**	Ja
			Geïmplementeerd	Ja
			Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.33 Beschermen van registraties 5.33

Doelstelling: Registraties behoren te worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.

Ref. no.:	5.33	Item:	Beschermen van registraties	
ISO 27001	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.		**Applicable**	Ja
			Geïmplementeerd	Ja
			Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.34 Privacy en bescherming van persoonsgegevens 5.34

Doelstelling: De naleving bewerkstelligen van wet- en regelgeving, statutaire en contractuele eisen met betrekking tot de informatiebeveiligingsaspecten voor de bescherming van persoonsgegevens.

Ref. no.:	5.34	Item:	Privacy en bescherming van persoonsgegevens	
ISO 27001	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.		**Applicable**	Ja
			Geïmplementeerd	Ja
			Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.35 Privacy en bescherming van persoonsgegevens 5.35

Doelstelling: Waarborgen dat de organisatie continue een geschikte, toereikende en doeltreffende aanpak voor het beheer van informatiebeveiliging hanteert.

Ref. no.:	5.35	Item:	Onafhankelijke beoordeling van informatiebeveiliging	
ISO 27001	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.		**Applicable**	Ja
			Geïmplementeerd	Ja
			Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.36 Naleving van beleid, regels en normen voor informatiebeveiliging 5.36

Doelstelling: Bewerkstelligen dat informatiebeveiliging in overeenstemming met informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en normen van de organisatie wordt geïmplementeerd en uitgevoerd.

Ref. no.:	5.36	Item:	Onafhankelijke beoordeling van informatiebeveiliging	
ISO 27001	De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie moet regelmatig worden beoordeeld.		**Applicable**	Ja
			Geïmplementeerd	Ja
			Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

2.1.37 Gedocumenteerde bedieningsprocedures 5.37

Doelstelling: De correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen.

Ref. no.:	5.37	Item:	Onafhankelijke beoordeling van informatiebeveiliging		
ISO 27001	Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar worden gesteld aan het personeel dat ze nodig heeft.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

3 Mensgerichte beheersmaatregelen 6

3.1.1 Screening 6.1

Doelstelling: Bewerkstelligen dat al het personeel in aanmerking komt en geschikt is voor de functies waarvoor zij worden overwogen en dat zij hiervoor gedurende hun dienstverband in aanmerking blijven komen en geschikt blijven.

Ref. no.:	6.1	Item:	Screening		
ISO 27001	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.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

3.1.2 Arbeidsovereenkomst 6.2

Doelstelling: Bewerkstelligen dat personeel begrijpt wat hun verantwoordelijkheden zijn op het gebied van informatiebeveiliging voor de rollen waarvoor zij in aanmerking komen.

Ref. no.:	6.2	Item:	Arbeidsovereenkomst		
ISO 27001	In arbeidsovereenkomsten moet worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

3.1.3 Bewustwording van, opleiding en training in informatiebeveiliging 6.3

Doelstelling: Ervoor zorgen dat personeel en relevante belanghebbenden zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.

Ref. no.:	6.3	Item:	Bewustwording van, opleiding en training in informatiebeveiliging	
ISO 27001	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.		**Applicable**	Ja
			Geïmplementeerd	Ja
			Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

3.1.4 Disciplinaire procedure 6.4

Doelstelling: Bewerkstelligen dat personeel en andere relevante belanghebbende de gevolgen begrijpen van schending van het informatiebeveiligingsbeleid, personeel en andere relevante belanghebbenden ervan weerhouden zich schuldig te maken aan een schending, en personeel en andere relevante belanghebbende die zich schuldig hebben gemaakt aan een schending op de juiste manier aanpakken.

Ref. no.:	6.4	Item:	Disciplinaire procedure	
ISO 27001	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.		**Applicable**	Ja
			Geïmplementeerd	Ja
			Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

3.1.5 Vertrouwelijkheids- of geheimhoudingsovereenkomsten 6.5

Doelstelling: De belangen van de organisatie beschermen als onderdeel van de wijzigings- of beëindigingsprocedure van dienstverband of contracten.

Ref. no.:	6.5	Item:	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	
ISO 27001	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.		**Applicable**	Ja
			Geïmplementeerd	Ja
			Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

3.1.6 Vertrouwelijkheids- of geheimhoudingsovereenkomsten 6.6

Doelstelling: De vertrouwelijkheid van informatie waartoe personeel of externe partijen toegang hebben handhaven.

Ref. no.:	6.6	Item:	Vertrouwelijkheids- of geheimhoudingsovereenkomsten		
ISO 27001	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.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

3.1.7 Werken op afstand 6.7

Doelstelling: De beveiliging van informatie waarborgen wanneer personeel op afstand werkt.

Ref. no.:	6.7	Item:	Werken op afstand		
ISO 27001	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.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

3.1.8 Melden van informatiebeveiligingsgebeurtenissen 6.8

Doelstelling: Tijdige, consistente en doeltreffende melding ondersteunen van informatiebeveiligingsgebeurtenissen tijdig via passende kanalen melden.

Ref. no.:	6.8	Item:	Melden van informatiebeveiligingsgebeurtenissen		
ISO 27001	De organisatie moet voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligings- gebeurtenissen tijdig via passende kanalen kan melden.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

4 Fysieke beheersmaatregelen 7

4.1.1 Fysieke beveiligingszones 7.1

Doelstelling: Onbevoegde fysieke toegang tot, schade aan en interferentie en andere gerelateerde bedrijfsmiddelen van de organisatie voorkomen.

Ref. no.:	7.1	Item:	Fysieke beveiligingszones		
ISO 27001	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

4.1.2 Fysieke toegangsbeveiliging 7.2

Doelstelling: Bewerkstelligen dat er alleen bevoegde fysieke toegang tot de informatie en andere gerelateerde bedrijfsmiddelen van de organisatie plaatsvindt.

Ref. no.:	7.2	Item:	Fysieke toegangsbeveiliging		
ISO 27001	Beveiligde zones moeten worden beschermd door passende toegangsbeveiligingsmaatregelen en toegangspunten.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

4.1.3 Beveiligen van kantoren, ruimten en faciliteiten 7.3

Doelstelling: Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en andere gerelateerde bedrijfsmiddelen van de organisatie in kantoren, ruimten en faciliteiten voorkomen.

Ref. no.:	7.3	Item:	Beveiligen van kantoren, ruimten en faciliteiten		
ISO 27001	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

4.1.4 Monitoren van de fysieke beveiliging 7.4

Doelstelling: Onbevoegde fysieke toegang detecteren en ontmoedigen.

Ref. no.:	7.4	Item:	Monitoren van de fysieke beveiliging		
ISO 27001	Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.			**Applicable**	Nee
				Geïmplementeerd	Nee
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item niet van toepassing.	

4.1.5 Beschermen tegen fysieke en omgevingsdreigingen 7.5

Doelstelling: De gevolgen van gebeurtenissen die voortvloeien uit fysieke en omgevingsbedreigingen, voorkomen of beperken.

Ref. no.:	7.5	Item:	Beschermen tegen fysieke en omgevingsdreigingen		
ISO 27001	Er moet bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen voor de infrastructuur, worden ontworpen en geïmplementeerd.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

4.1.6 Werken in beveiligde zones 7.6

Doelstelling: Informatie en andere gerelateerde bedrijfsmiddelen in beveiligde zones beschermen tegen schade en onbevoegde verstoring door personeel dat in deze zones aan het werk is.

Ref. no.:	7.6	Item:	Werken in beveiligde zones		
ISO 27001	Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

4.1.7 ‘Clear desk’ en ‘clear screen’ 7.7

Doelstelling: De risico’s op onbevoegde toegang behoort tot, verlies van en schade aan informatie op bureaus, schermen en op andere toegankelijke plaatsen tijdens en buiten de gebruikelijke werkuren beperken.

Ref. no.:	7.7	Item:	‘Clear desk’ en ‘clear screen’		
ISO 27001	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.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

4.1.8 Plaatsen en beschermen van apparatuur 7.8

Doelstelling: De risico’s op fysieke en omgevingsdreigingen en op toegang door onbevoegden en schade beperken.

Ref. no.:	7.8	Item:	‘Clear desk’ en ‘clear screen’		
ISO 27001	Apparatuur moet veilig worden geplaatst en beschermd.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

4.1.9 Beveiligen van bedrijfsmiddelen buiten het terrein 7.9

Doelstelling: Bedrijfsmiddelen buiten het gebruiken en/of terrein behoren te worden beschermd.

Ref. no.:	7.9	Item:	Beveiligen van bedrijfsmiddelen buiten het terrein		
ISO 27001	Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

4.1.10 Opslagmedia 7.10

Doelstelling: Uitsluitend geoorloofde openbaring, wijziging, verwijdering of vernietiging van informatie op opslagmedia bewerkstelligen.

Ref. no.:	7.10	Item:	Opslagmedia		
ISO 27001	Opslagmedia moeten worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

4.1.11 Nutsvoorzieningen 7.11

Doelstelling: Verlies, schade of compromittering van informatie en andere gerelateerde bedrijfsmiddelen of onderbreking van de bedrijfsvoering van de organisatie vanwege verstoring en ontregeling van ondersteunende nutsvoorzieningen voorkomen.

Ref. no.:	7.11	Item:	Opslagmedia		
ISO 27001	Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

4.1.12 Beveiligen van bekabeling 7.12

Doelstelling: Verlies, schade, diefstal of compromittering van informatie en andere gerelateerde bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie in verband met voedings- en communicatiekabels voorkomen.

Ref. no.:	7.12	Item:	Beveiligen van bekabeling		
ISO 27001	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen onderschepping, interferentie of beschadiging.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

4.1.13 Onderhoud van apparatuur 7.13

Doelstelling: Verlies, schade, diefstal of compromittering van informatie en andere gerelateerde bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie door gebrekkig onderhoud voorkomen.

Ref. no.:	7.13	Item:	Onderhoud van apparatuur		
ISO 27001	Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

4.1.14 Veilig verwijderen of hergebruiken van apparatuur 7.14

Doelstelling: Het lekken van informatie via af te voeren of te hergebruiken apparatuur voorkomen.

Ref. no.:	7.14	Item:	Veilig verwijderen of hergebruiken van apparatuur		
ISO 27001	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.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5 Technologische beheersmaatregelen 8

5.1.1 User endpoint devices' 8.1

Doelstelling: Informatie beschermen tegen de risico's als gevolg van het gebruik van 'user endpoint devices'

Ref. no.:	8.1	Item:	User endpoint devices'		
ISO 27001	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.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.2 Speciale toegangsrechten 8.2

Doelstelling: Bewerkstelligen dat alleen bevoegde gebruikers, softwarecomponenten en diensten speciale toegangsrechten krijgen.

Ref. no.:	8.2	Item:	Speciale toegangsrechten		
ISO 27001	Het toewijzen en het gebruik van speciale toegangsrechten moet worden beperkt en beheerd.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.3 Beperking toegang tot informatie 8.3

Doelstelling: Uitsluitend bevoegde toegang bewerkstelligen en onbevoegde toegang tot informatie en andere gerelateerde bedrijfsmiddelen voorkomen.

Ref. no.:	8.3	Item:	Beperking toegang tot informatie		
ISO 27001	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen moet worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.4 Toegangsbeveiliging op broncode 8.4

Doelstelling: Voorkomen dat er ongeoorloofde functionaliteit wordt geïntroduceerd, vermijden dat onbedoelde of kwaadwillige wijzigingen plaatsvinden en de vertrouwelijkheid behouden van waardevol intellectueel eigendom.

Ref. no.:	8.4	Item:	Toegangsbeveiliging op broncode		
ISO 27001	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.5 Beveiligde authenticatie 8.5

Doelstelling: bewerkstelligen dat een gebruiker of een entiteit veilig wordt geauthenticeerd wanneer toegang tot systemen, toepassingen en diensten wordt verleend.

Ref. no.:	8.5	Item:	Beveiligde authenticatie		
ISO 27001	Er moeten beveiligde authenticatietechnologieën en -procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke beleid inzake toegangsbeveiliging.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.6 Capaciteitsbeheer 8.6

Doelstelling: De vereiste capaciteit van informatieverwerkende faciliteiten, personeel, kantoren en andere faciliteiten behoren te worden gedefinieerd, rekening houdend met belang van de betrokken systemen en processen voor de organisatie.

Ref. no.:	8.6	Item:	Capaciteitsbeheer		
ISO 27001	Het gebruik van middelen moet worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.7 Bescherming tegen malware 8.7

Doelstelling: Waarborgen dat informatie en andere gerelateerde bedrijfsmiddelen beschermd zijn tegen malware.

Ref. no.:	8.7	Item:	Capaciteitsbeheer		
ISO 27001	Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebuikersbewustzijn.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.8 Beheer van technische kwetsbaarheden 8.8

Doelstelling: Misbruik van technische kwetsbaarheden voorkomen.

Ref. no.:	8.8	Item:	Beheer van technische kwetsbaarheden		
ISO 27001	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.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.9 Configuratiebeheer 8.9

Doelstelling: Garanderen dat hardware, software, diensten en netwerken correct met de vereisten beveiligingsinstellingen functioneren en de configuratie niet door ongeautoriseerde of onjuiste wijzigingen wordt gewijzigd.

Ref. no.:	8.9	Item:	Beheer van technische kwetsbaarheden		
ISO 27001	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.10 Wissen van informatie 8.10

Doelstelling: Onnodige openbaarmaking van gevoelige informatie voorkomen en aan de eisen van wet- en regelgeving, statutaire en contractuele eisen voor het wissen van informatie voldoen.

Ref. no.:	8.10	Item:	Wissen van informatie		
ISO 27001	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moet worden gewist als deze niet langer vereist is.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.11 Maskeren van gegevens 8.11

Doelstelling: De openbaarmaking van gevoelige informatie met inbegrip van persoonsgegevens beperken en aan de eisen van wet- en regelgeving, statutaire en contractuele eisen voldoen.

Ref. no.:	8.11	Item:	Wissen van informatie		
ISO 27001	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.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.12 Voorkomen van gegevenslekken (data leakage prevention) 8.12

Doelstelling: OM de ongeoorloofde openbaarmaking en extractie van informatie door personen of systemen te detecteren en voorkomen.

Ref. no.:	8.12	Item:	Voorkomen van gegevenslekken		
ISO 27001	Maatregelen om gegevenslekken te voorkomen moeten worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.13 Back-up van informatie 8.13

Doelstelling: Herstel mogelijk maken na verlies van gegevens of systemen.

Ref. no.:	8.13	Item:	Back-up van informatie		
ISO 27001	Back-ups van informatie, software en systemen moeten worden bewaard en regelmatig worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.14 Redundantie van informatieverwerkende faciliteiten 8.14

Doelstelling: De ononderbroken werking van informatieverwerkende faciliteiten waarborgen.

Ref. no.:	8.14	Item:	Back-up van informatie		
ISO 27001	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.15 Logging 8.15

Doelstelling: Gebeurtenissen registreren, bewijs genereren, de integriteit van informatie in logbestanden waarborgen, onbevoegden toegang voorkomen, informatiebeveiligingsgebeurtenissen identificeren die tot een informatiebeveiligingsincident kunnen leiden en onderzoeken ondersteunen.

Ref. no.:	8.15	Item:	Logging		
ISO 27001	Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, worden geproduceerd, opgeslagen, beschermd en geanalyseerd.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.16 Monitoren van activiteiten 8.16

Doelstelling: Afwijkend gedrag en potentiële informatiebeveiligingsincidenten detecteren.

Ref. no.:	8.16	Item:	Monitoren van activiteiten		
ISO 27001	Netwerken, systemen en toepassingen moeten worden gemonitord op afwijkend gedrag en er moeten passende maatregelen worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.17 Kloksynchronisatie 8.17

Doelstelling: De correlatie en analyse van beveiligingsgerelateerde gebeurtenissen en andere geregistreerde gegevens mogelijk maken en onderzoeken bij informatiebeveiligingsincidenten ondersteunen.

Ref. no.:	8.17	Item:	Monitoren van activiteiten		
ISO 27001	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdbronnen.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.18 Gebruik van speciale systeemhulpmiddelen 8.18

Doelstelling: Bewerkstelligen dat het gebruik van systeemhulpmiddelen geen schade toebrengt aan systeem- en toepassingsbeheersmaatregelen voor informatiebeveiliging.

Ref. no.:	8.18	Item:	Monitoren van activiteiten		
ISO 27001	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om en voor systemen en toepassingen te omzeilen, moet worden beperkt en nauwkeurig worden gecontroleerd.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.19 Installeren van software op operationele systemen 8.19

Doelstelling: De integriteit van operationele systemen garanderen en voorkomen dat misbruik wordt gemaakt van technische kwetsbaarheden.

Ref. no.:	8.19	Item:	Monitoren van activiteiten		
ISO 27001	Er moeten procedures en maatregelen worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.20 Beveiliging netwerkcomponenten 8.20

Doelstelling: Informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten beschermen tegen compromittering via netwerk.

Ref. no.:	8.20	Item:	Beveiliging netwerkcomponenten		
ISO 27001	Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.21 Beveiliging van netwerkdiensten 8.21

Doelstelling: De beveiliging bij het gebruik van netwerkdiensten waarborgen.

Ref. no.:	8.21	Item:	Beveiliging netwerkcomponenten		
ISO 27001	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.22 Netwerksegmentatie 8.22

Doelstelling: Het netwerk opsplitsen met beveiligingsgrenzen en het verkeer ertussen op basis van de bedrijfsbehoeften beheersen.

Ref. no.:	8.22	Item:	Netwerksegmentatie		
ISO 27001	Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.23 Toepassen van webfilters 8.23

Doelstelling: Systemen beschermen om te voorkomen dat deze door malware worden gecompromitteerd en om toegang tot ongeoorloofde internetbronnen te voorkomen.

Ref. no.:	8.23	Item:	Toepassen van webfilters		
ISO 27001	De toegang tot externe websites moet worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.			**Applicable**	Ja
				Geïmplementeerd	Nee
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.24 Netwerksegmentatie 8.24

Doelstelling: Correctheid en doeltreffend gebruik bewerkstelligen van cryptografie om de vertrouwelijkheid, authenticiteit of integriteit van informatie overeenkomstig de bedrijfs- en informatiebeveiligingseisen te beschermen en met inachtneming van eisen van wet- en regelgeving, statutaire en contractuele eisen met betrekking tot cryptografie.

Ref. no.:	8.24	Item:	Gebruik van cryptografie		
ISO 27001	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, moeten worden gedefinieerd en geïmplementeerd.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.25 Beveiligen tijdens de ontwikkelcyclus 8.25

Doelstelling: bewerkstelligen dat informatiebeveiliging binnen de veilige ontwikkelcyclus van software en systemen wordt ontworpen en geïmplementeerd.

Ref. no.:	8.25	Item:	Beveiligen tijdens de ontwikkelcyclus		
ISO 27001	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.26 Toepassingsbeveiligingseisen 8.26

Doelstelling: Garanderen dat alle informatiebeveiligingseisen te worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.

Ref. no.:	8.26	Item:	Toepassingsbeveiligingseisen		
ISO 27001	Er moeten eisen aan de informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.27 Veilige systeemarchitectuur en technische uitgangspunten 8.27

Doelstelling: Waarborgen dat informatiesystemen veilig worden ontworpen, geïmplementeerd en beheerd binnen de ontwikkelingslevenscyclus.

Ref. no.:	8.27	Item:	Veilige systeemarchitectuur en technische uitgangspunten		
ISO 27001	Uitgangspunten voor het ontwerpen van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.28 Veilig coderen 8.28

Doelstelling: Waarborgen dat vellige software wordt geschreven waardoor het aantal potentiële informatiebeveiligingskwetsbaarheden in de software wordt beperkt.

Ref. no.:	8.28	Item:	Veilig coderen		
ISO 27001	Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.29 Testen van de beveiliging tijdens ontwikkeling en acceptatie 8.29

Doelstelling: Valideren of aan de informatiebeveiligingseisen wordt voldaan wanneer toepassingen of code in de productieomgeving worden uitgerold.

Ref. no.:	8.29	Item:	Testen van de beveiliging tijdens ontwikkeling en acceptatie		
ISO 27001	Processen voor het testen van de beveiliging moeten worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.30 Uitbestede systeemontwikkeling 8.30

Doelstelling: Garanderen dat de door de organisatie vereiste informatiebeveiligingsmaatregelen bij uitbestede systeemontwikkeling te sturen, bewaken en beoordelen.

Ref. no.:	8.30	Item:	Uitbestede systeemontwikkeling		
ISO 27001	De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.			**Applicable**	Nee
				Geïmplementeerd	Nee
				Verantwoording: KEMBIT besteed geen systeemontwikkeling werkzaamheden uit aan derden.	

5.1.31 Scheiding van ontwikkel-, test- en productieomgevingen 8.31

Doelstelling: De productieomgeving en de gegevens beschermen tegen compromittering door ontwikkel- en testactiviteiten.

Ref. no.:	8.31	Item:	Scheiding van ontwikkel-, test- en productieomgevingen		
ISO 27001	De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.32 Wijzigingsbeheer 8.32

Doelstelling: De informatiebeveiliging behouden tijdens het uitvoeren van wijzigingen.

Ref. no.:	8.32	Item:	Scheiding van ontwikkel-, test- en productieomgevingen		
ISO 27001	Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.33 Testgegevens 8.33

Doelstelling: De relevantie van het testen en de bescherming van operationele gegevens die voor het testen worden gebruikt, waarborgen.

Ref. no.:	8.33	Item:	Scheiding van ontwikkel-, test- en productieomgevingen		
ISO 27001	Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	

5.1.34 Bescherming van informatiesystemen tijdens audits 8.34

Doelstelling: De impact van audittests en andere auditactiviteiten op operationele systemen en bedrijfsprocessen tot een minimum beperken.

Ref. no.:	8.34	Item:	Bescherming van informatiesystemen tijdens audits		
ISO 27001	Audittests en andere auditactiviteiten waarbij operationele systemen worden beoordeeld, moeten worden gepland en overeengekomen tussen de tester en het verantwoordelijke management.			**Applicable**	Ja
				Geïmplementeerd	Ja
				Verantwoording: Op basis van de uitkomsten van de risicoanalyse, verklaart KEMBIT dit item van toepassing.	