IT Risico Management en Business Continuity Management

Van theorie naar praktijk

IT-risico management: *het proces van het identificeren, beoordelen en beheersen van risico's die de informatiebeveiliging van een organisatie kunnen beïnvloeden.*

Business Continuity Management: het proces van het identificeren, beoordelen en beheersen van potentiële bedreigingen die de continuïteit van kritieke bedrijfsprocessen kunnen verstoren

Henk Links

Edo Meinema

26 juni 2025

Versie 2.0

Agenda (10:45 – 12:10)

10:45 – 11:15 Van OZON naar Risicomanagement

11:15 – 11:40 Koffiepauze

11:45 – 12:10 Risico Management in het MBO

Agenda (10:45 – 12:10)

10:45 – 11:15 Van OZON naar Risicomanagement

11:15 – 11:40 Koffiepauze

11:45 – 12:10 Risico Management in het MBO

(N)OZON -> CRISIS-MANAGEMENT -> CONTINUÏTEITS-MANAGEMENT -> RISICO-MANAGEMENT

CRISIS-MANAGEMENT	**CONTINUÏTEITS-MANAGEMENT**	**RISICO-MANAGEMENT**
• Cyberaanval • Acute verstoring systemen • Protest van studenten	• Back-up- en herstelprocedures • Alternatieve onderwijsvoorzieningen • Uitwijklocaties Examens	• IT-risico's • Wet- en regelgeving • Financiële risico's
REACTIEF (beperking schade)	voorbereidend/herstellend (behoud processen)	PROACTIEF (behalen van doelen)
INCIDENT (respons/escalatie)		**DREIGING** (kans en impact)
BOB-methode Communicatie	Business Impact Analyse Herstelplannen	Inventarisatie/Analyse Mitigerende maatregelen

scenario kaart

risico kaart

Wie hanteert een risico gebaseerde aanpak van de statements uit het NBA-kader?

Domein 3: Risk Management

Kader voor Information Risk Management	RM.01	VW3	(a) Er is organisatiebreed beleid voor (Information) Risk Management dat is goedgekeurd door het senior management. (b) Het beleid en de procesbeschrijving geven aan hoe om te gaan met de essentiële elementen van Risk Management (risicobereidheid/-profiel, risico-eigenaarschap, risicoproces, risicobeoordeling, risicomitigatie en risico-acceptatie). (c) Het kader voor Information Risk Management is in lijn met het kader voor organisatiebreed Risk Management en omvat componenten als strategie, programma's, projecten en uitvoering. (d) Classificatie van informatierisico's gebeurt op basis van een set van algemeen geldende karakteristieken vanuit het kader voor organisatiebreed Risk Management en getroffen maatregelen voor informatierisico's zijn gestandaardiseerd en geprioriteerd, waarbij rekening gehouden wordt met kans, impact en restrisico's. (e) Voor dit risicokader is een training geïmplementeerd.
Risicobeoordeling	RM.02	VW3	(a) Risicoanalyses worden uitgevoerd volgens vooraf vastgestelde intervallen en methoden, als onderdeel van het Risk Management proces en het kader voor Information Risk Management. (b) De risicoanalysemethodiek is in lijn met bedrijfsbehoeften en identificeert belangrijke bedrijfsrisico's (incl. kroonjuwelen). (c) De geïdentificeerde informatierisico's worden kwalitatief en/of kwantitatief beoordeeld gebruikmakend van het Risk Management proces/kader voor Information Risk Management of good practice bronnen. (d) Afwijkingen van de risicobereidheid of het risicoprofiel met betrekking tot risicobeperkende maatregelen worden aan het (senior) management gerapporteerd.
Plan voor behandeling en beperking van risico's (incl. risicoacceptatie)	RM.03	VW3	(a) Er is een proces geïmplementeerd om (nieuwe) risico's formeel vast te leggen en op te nemen in een risico-actieplan. (b) Restrisico's en maatregelen zijn geïdentificeerd, geanalyseerd en gedocumenteerd (in een risicoregister of -actieplan). (c) De geïdentificeerde maatregelen of acceptatie van restrisico's zijn gedocumenteerd, goedgekeurd door het (senior) management en toegewezen aan een (risico)eigenaar. (d) De voortgang van implementatie van risicobeperkende maatregelen en eventuele afwijkingen worden gemonitord. (e) Het risico-actieplan wordt onderhouden en aangepast indien nodig. Het senior management is eigenaar van het risico-actieplan. Aanvulling 3.0: (f) Organisatie heeft expliciet afgewogen of restrisico's buiten risicobereidheid dienen te worden verzekerd, en als verzekeren relevant wordt geacht, dan is deze verzekering ook afgesloten.

Doel van het volwassenheidsmodel

Het volwassenheidsmodel heeft tot doel de auditors alsmede de directies van organisaties een leidraad en handvatten te geven waarmee zij doelgericht en op pragmatische wijze hun organisaties kunnen ondersteunen bij het meten, bepalen en verbeteren van het volwassenheidsniveau van informatiebeveiliging.

In eerste instantie kan het model door het verantwoordelijk management en/of de (interne) auditafdeling gebruikt worden voor het toetsen van het volwassenheidsniveau van informatiebeveiliging op basis van de geïmplementeerde beheersmaatregelen.

Om tot het gewenste volwassenheidsniveau te komen, moeten er vanuit de organisatie specifieke context (kansen en risico's) onderbouwde keuzes worden gemaakt om bepaalde maatregelen wel of niet te treffen ("comply or explain"). Ondersteunend hieraan biedt het model te verwachte beheersmaatregelen per volwassenheidsniveau.

Toepassing van het volwassenheidsmodel

Zoals eerder beschreven geeft het model op conceptueel niveau inzicht in welke informatiebeveiligings- c.q. cybersecuritymaatregelen per volwassenheidsniveau redelijkerwijs verwacht mogen worden. Het geeft hiermee een handreiking om het volwassenheidsniveau te meten, te bepalen en te verbeteren. Maar natuurlijk blijven de genoemde beheersmaatregelen altijd een enigszins subjectief karakter hebben. Het volwassenheidsmodel is richtinggevend en daarmee een goed instrument om de dialoog aan te gaan met het verantwoordelijk management of andere stakeholders.

Het vaststellen van het gewenste volwassenheidsniveau wordt in belangrijke mate bepaald door de aard van de business c.q. processen, soort gegevens van de organisatie, de beschikbare applicaties en infrastructuur alsmede externe factoren c.q. dreigingen. Deze zaken alsmede de specifieke risico's en risicobereidheid van de organisatie zijn bepalend hoe hoog de lat voor de organisatie moeten liggen.

NBA Volwassenheidsmodel Informatiebeveiliging

(12 domeinen; 69 statements)

1	Governance	GO.01	Informatiebeveiliging Strategie
		GO.02	Informatiebeveiliging Beleid
		GO.03	Informatiebeveiliging Plan / Roadmap
		GO.04	Enterprise Architectuur
		GO.05	Onafhankelijke Assurance
2	Organisatie	OR.01	Eigenaarschap, Rollen, Aansprakelijkheid en Verantwoordelijkheden
		OR.02	Functiescheiding
3	Risicomanagement	RM.01	Raamwerk voor informatierisicobeheer
		RM.02	Risicobeoordeling
		RM.03	Risicoactie- en mitigatieplan (inclusief risicoacceptatie)
4	Human Resource	HR.01	Werving
		HR.02	Certificering, training en opleiding
		HR.03	Afhankelijkheid van individuen
		HR.04	Functiewijziging en/of beëindiging
		HR.05	Kennisdeling
		HR.06	Veiligheidsbewustzijn (Security Awareness)
5	Configuratie Management	CO.01	Identificatie en onderhoud van configuratie-items
		CO.02	Configuratiedatabase en baseline
6	Incident Management	IM.01	Incident Management
		IM.02	Incident Escalatie
		IM.03	Incidentrespons op (cyber)beveiligingsincidenten
		IM.04	Problem management
7	Change Management	CH.01	Standaarden en procedures voor het wijzigingsproces
		CH.02	Impactanalyse, prioritering en autorisatie
		CH.03	Spoedwijzigingen
		CH.04	Testomgeving
		CH.05	Testen van wijzigingen
		CH.06	Promotie naar productie
8	Systeemontwikkeling	SD.01	Methodologie veilige ontwikkeling en implementatie van software
		SD.02	Ontwikkelaarstoegang tot productie
		SD.03	Gegevensconversie en/of migratie
9	Data Management	DM.01	Eigenaarschap van gegevens (en systeem)
		DM.02	Dataclassificatie
		DM.03	Beveiligingsvereisten voor gegevensbeheer
		DM.04	Opslag- en bewaarregelingen
		DM.05	Uitwisseling van (gevoelige) gegevens
		DM.06	Verwijdering van informatie

10	Identity & Access Management	ID.01	Toegangsregels
		ID.02	Beheer van toegangsrechten
		ID.03	Gebruikers met verhoogde toegangsrechten (Super Users)
		ID.04	Envelop procedure
		ID.05	Periodieke beoordeling van toegangsrechten
11	Security Management	SM.01	Beveiligingsbasisregels
		SM.02	Authenticatiemechanismen
		SM.03	Mobiele apparaten en telewerken
		SM.04	Logging
		SM.05	Testen, bewaking en monitoring van informatiebeveiliging
		SM.06	Patchbeheer
		SM.07	Beheer van bedreigingen en kwetsbaarheden
		SM.08	Bescherming en beschikbaarheid van infrastructuurbronnen
		SM.09	Onderhoud van de infrastructuur
		SM.10	Beheer van cryptografische sleutels
		SM.11	Netwerkbeveiliging
		SM.12	Beheer van malware-aanvallen
		SM.13	Bescherming van beveiligingstechnologie
12	Fysieke Toegangsbeveiliging	PH.01	Fysieke beveiligingsmaatregelen
		PH.02	Beheer van fysieke toegangsrechten
13	Computer Operations	OP.01	Taakverwerking
		OP.02	Backup- en herstelprocedures
		OP.03	Capaciteits- en prestatiebeheer
14	Business Continuity Management	BC.01	Bedrijfscontinuïteitsplanning (Business Continuity Planning)
		BC.02	Testen van noodherstel (disaster recovery)
		BC.03	Externe opslag van backupmedia
		BC.04	Gegevensreplicatie
		BC.05	Crisismanagement
15	Supply Chain Management	SC.01	Service Level Agreement
		SC.02	Service Level Management
		SC.03	Risicobeheer van leveranciers
		SC.04	Interne controle bij externe dienstverleners (service providers)

(SM) Security Management	
11.51 (SM.06)	**Patchmanagement**
Risico	Afwezigheid van patches of beveiligingsoplossingen kan ertoe leiden dat bekende kwetsbaarheden worden misbruikt om ongeautoriseerde toegang tot de IT-infrastructuur te verkrijgen.
Doel	Beschikbare patches en/of beveiligingsfixes worden geïnstalleerd in overeenstemming met vooraf vastgesteld en goedgekeurd beleid (inclusief dat voor besturingssystemen, databases en geïnstalleerde applicaties) en aanbevelingen van CSIRT en/of leveranciers.
Volwassenheidsniveau 1	(a) Er is geen beleid voor patchmanagement. (b) Individuele risicoanalyse voor kwetsbaarheden en patches. (c) Ad-hoc-installatie van patches en/of beveiligingsfixes.
Volwassenheidsniveau 2	(a) Er is een informeel beleid voor patchmanagement. (b) Risico's op kwetsbaarheden en installatie van patches/fixes worden gemanaged maar niet gedocumenteerd. (c) Patches worden vaak geïmplementeerd met onvoldoende oog voor informatiebeveiliging.
Volwassenheidsniveau 3	(a) Er is een formeel vastgelegd beleid voor patchmanagement. (b) Patchmanagement is op organisatieniveau geïmplementeerd en gedocumenteerd, in lijn met Change Management. (c) Patches worden in de basis overgenomen in samenwerking met CSIRT. (d) IT-personeel check handmatig de patchlevels van besturingssystemen, databases en applicaties.
Volwassenheidsniveau 4	(a) De effectiviteit van patchmanagement wordt regelmatig geëvalueerd. Deze evaluaties worden gedocumenteerd en verbeteringen worden bepaald. (b) Patchmanagement dient te worden gedreven door risico's en niet enkel door compliance.
Volwassenheidsniveau 5	(a) Er zijn automatische controles op patchlevels en alerts voor IT-personeel (maar geen automatische installatie van patches). (b) Rapportages worden automatisch gegenereerd voor het senior management.

Effect van ICT-falen

Visie, Missie en Strategie

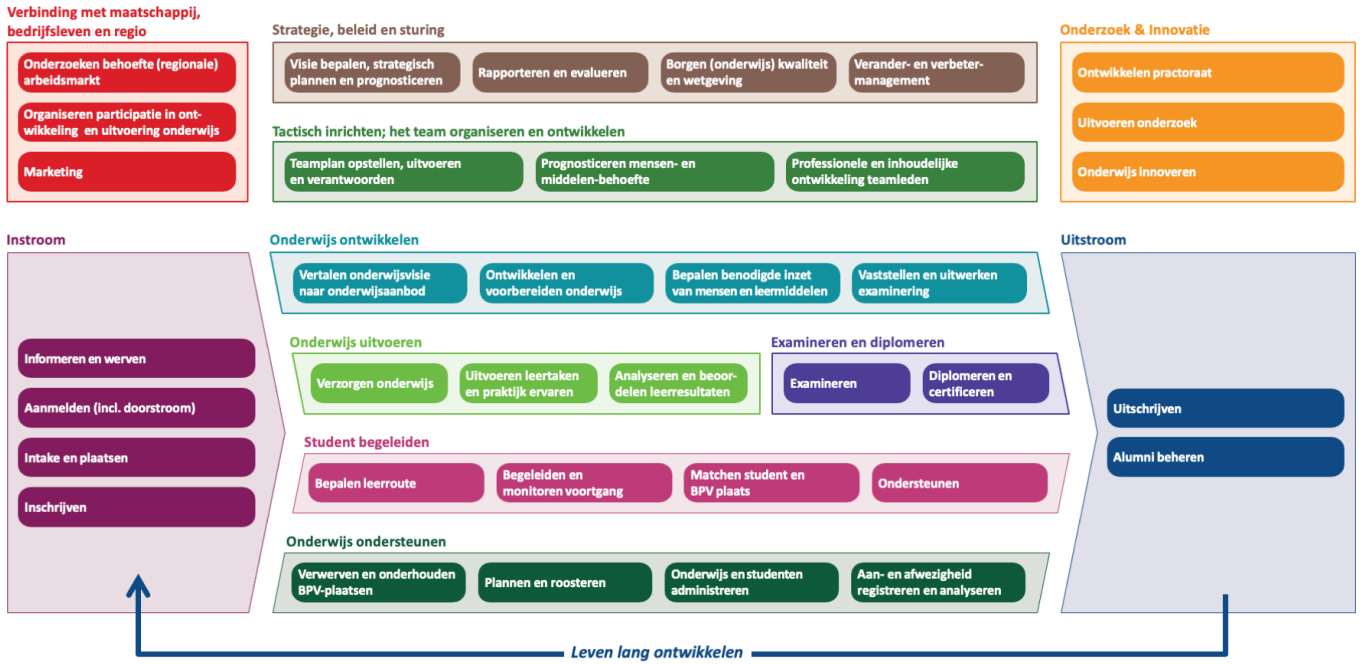
Organisatiedoelstellingen

Bedrijfsprocessen

Informatie

Applicaties

Wie heeft een Business Impact Analyse uitgevoerd op de HORA/MORA?



RTO

RPO

RM.01	VW3	(a) Er is organisatiebreed beleid voor (Information) Risk Management dat is goedgekeurd door het senior management. (b) Het beleid en de procesbeschrijving geven aan hoe om te gaan met de essentiële elementen van Risk Management (risicobereidheid/-profiel, risico-eigenaarschap, risicoproces, risicobeoordeling, risicomitigatie en risico-acceptatie). (c) Het kader voor Information Risk Management is in lijn met het kader voor organisatiebreed Risk Management en omvat componenten als strategie, programma's, projecten en uitvoering. (d) Classificatie van informatierisico's gebeurt op basis van een set van algemeen geldende karakteristieken vanuit het kader voor organisatiebreed Risk Management en getroffen maatregelen voor informatierisico's zijn gestandaardiseerd en geprioriteerd, waarbij rekening gehouden wordt met kans, impact en restrisico's. (e) Voor dit risicokader is een training geïmplementeerd.
BC.01	VW3	(a) Business- en IT-continuïteitsplannen zijn gedefinieerd, geïntegreerd en goedgekeurd door het senior management. (b) De organisatie heeft een bedrijfsimpactanalyse uitgevoerd, op basis waarvan recovery-time doelen zijn bepaald en volledig gedocumenteerde IT-herstelplannen en business continuïteitsplannen zijn opgesteld om deze doelen te bereiken. (c) De plannen betreffen ook gebruikershandleidingen, rollen, verantwoordelijkheden, crisismanagement, communicatieprocessen en de testmethode.

BCM

Generiek

templates

1. Voer een Business Impact Analyse (BIA) uit op de processen
2. Classificeer de onderliggende IT-infrastructuur, systemen en applicaties m.b.v. BIV

BCM

templates

1. Ontwikkel herstelplannen
2. Op basis van scenario's

Risicomanagement

templates

1. Identificeer en analyseer Risico's
2. Op basis van scenario's

🔍 Verschil tussen een Risicokaart en een Scenariokaart

- Een **risicokaart** helpt je om te voorkomen dat er iets misgaat, door risico’s te analyseren en te beheersen.

- Een **scenariokaart** helpt je om voorbereid te zijn op het moment dat er tóch iets misgaat, en de schade te beperken.

🔍 Verschil tussen een Risicokaart en een Scenariokaart

Aspect	Risicokaart	Scenariokaart
Doel	In kaart brengen en beoordelen van risico's op kans en impact	Voorbereiden op en plannen van reactie op verstorende scenario's
Focus	Individuele risico's die een proces of doel kunnen bedreigen	Concrete gebeurtenissen of scenario's met brede gevolgen
Gebruik	Risicomanagement: preventie, prioritering en beheersmaatregelen	BCM: continuïteitsplan(ning), crisismanagement
Dimensies	Kans, impact, risicoscore, rest-risico	Tijdslijn, scenarioverloop, gevolgen, afhankelijkheden
Output	Risicomatrix, top-risicolijst, beheersmaatregelen	Actieplannen, herstelstrategieën, worst case-analyse

📘 Risicokaart

RISICO	KANS	IMPACT	RISICOSCORE	BEHEERSMAATREGEL
ICT-storing tijdens tentamens	Hoog	Hoog	9	Back-up systemen, papieren tentamens paraat
Docententekort	Middel	Hoog	6	Flexibele inzet, gastdocenten
Onvoldoende cyberbeveiliging	Hoog	Hoog	9	Awareness training, firewalls, audits
Laag studentenaantal bij opleiding	Middel	Middel	4	Marketingcampagne, opleiding herstructureren

Een risicokaart zou bovenstaande gegevens visualiseren in een risicomatrix waarbij bijvoorbeeld ‘Kans’ op de X-as en ‘Impact’ op de Y-as staat.

Scenariokaart

Grootschalige uitval van het digitale leerplatform (bijv. door cyberaanval)

Onderdeel	Beschrijving
Scenario	Het leerplatform is gedurende 5 dagen niet beschikbaar
Trigger	Ransomware-aanval op de centrale server
Gevolgen	Onderwijs stilgelegd, studenten missen deadlines, reputatieschade
Kritieke processen	Lesgeven, toetsen, communicatie met studenten
Afhankelijkheden	ICT, communicatiesystemen, toetssoftware
Hersteltijd (RTO)	Binnen 48 uur (doelstelling)
Herstelacties	Overschakelen op alternatieve platforms, communicatie via mail & intranet
Verantwoordelijken	ICT-coördinator, crisismanager, directie

Een **scenariokaart** visualiseert dit proces vaak met een tijdslijn en betrokken afdelingen, en ondersteunt beslissingen tijdens crisissituaties.

(N)OZON -> CRISIS-MANAGEMENT -> CONTINUÏTEITS-MANAGEMENT -> RISICO-MANAGEMENT

CRISIS-MANAGEMENT	**CONTINUÏTEITS-MANAGEMENT**	**RISICO-MANAGEMENT**
• Cyberaanval • Acute verstoring systemen • Protest van studenten	• Back-up- en herstelprocedures • Alternatieve onderwijsvoorzieningen • Uitwijklocaties Examens	• IT-risico's • Wet- en regelgeving • Financiële risico's
REACTIEF (beperking schade)	voorbereidend/herstellend (behoud processen)	PROACTIEF (behalen van doelen)
INCIDENT (respons/escalatie)		**DREIGING** (kans en impact)
BOB-methode Communicatie	Business Impact Analyse Herstelplannen	Inventarisatie/Analyse Mitigerende maatregelen

scenario kaart

risico kaart

SURF mbo digitaal

SURF Security Expertise Centrum

mbo digitaal

PROGRAMMA Cyberveiligheid

- Template Bedrijfscontinuïteitsbeheer Beleid
  → 05 november 2024 BC.01, BC.02, BC.05
- Template Standaard Bedrijfscontinuïteitsplan
  → 03 december 2024 BC.01, BC.02, BC.05
- Template Bedrijfsimpactanalyse BIA
  → 11 december 2024 BC.01, BC.05
- Stappenplan Bedrijfscontinuïteitsbeheer
  → 03 december 2024 BC.01, BC.02, BC.05
- Template Scenariokaart Cyber
  → 03 december 2024 BC.01, BC.05
- Handleiding Tabletop oefeningen
  → 14 oktober 2024 BC.01, BC.02, BC.05

Gedaan:

- mbo referentie BIA *(processen)*
- mbo referentie BIV *(applicaties)*

MORA

- template herstelplan
- scenariokaarten

Mee bezig:

- Voorbeelden herstelplan
- Voorbeelden scenariokaarten
- Best Practices

Maturity Workshops:

- Business Continuïteitsmanagement
  -> toepassen BIA <-> risicomanagement

Agenda (10:45 – 12:10)

10:45 – 11:15 Van OZON naar Risicomanagement

11:15 – 11:40 Koffiepauze

11:45 – 12:10 Risico Management in het MBO

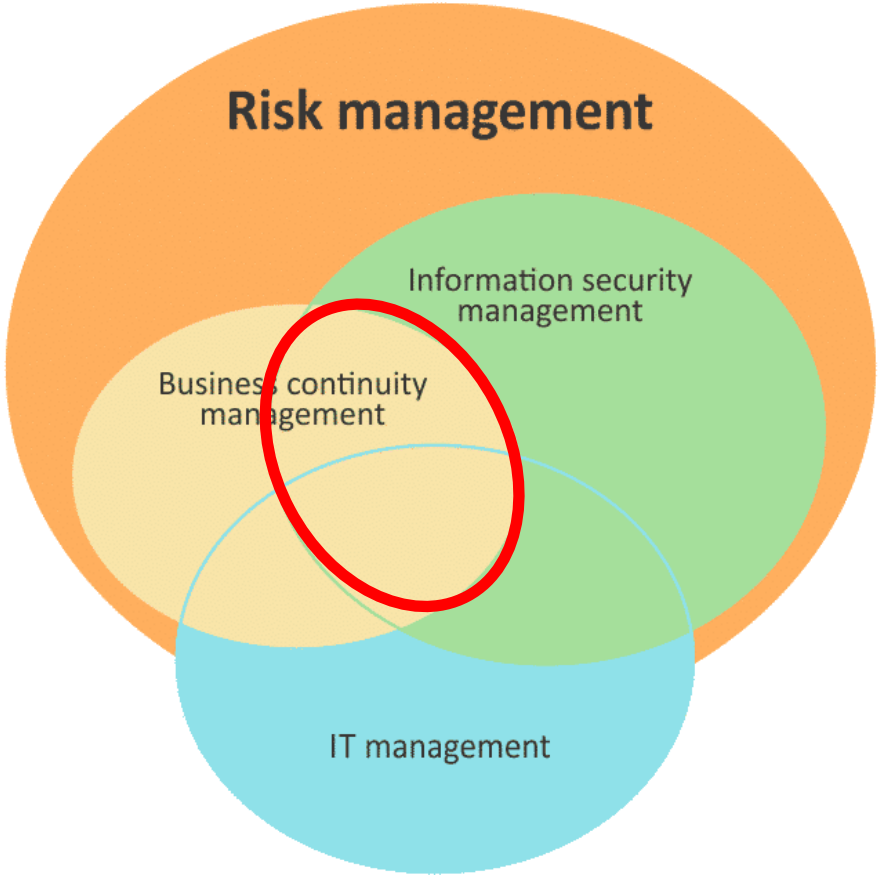
Agenda (10:45 – 12:10)

10:45 – 11:15 Van OZON naar Risicomanagement

11:15 – 11:40 Koffiepauze

11:45 – 12:10 Risico Management in het MBO

Business Continuity Management in het MBO



De relatie tussen Risicomanagement en Business Continuity Management

Risico Management in het MBO

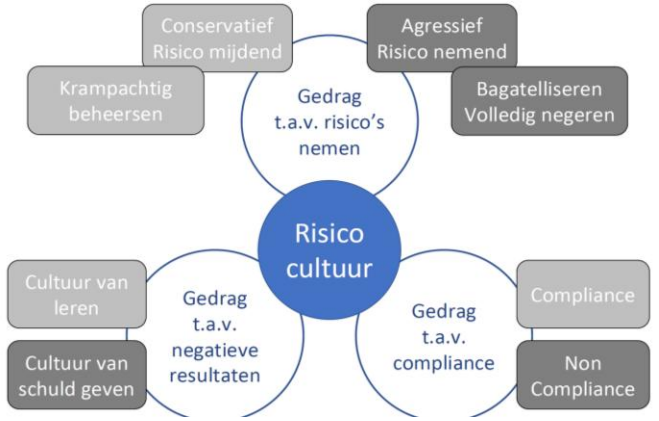
- Context
- Processen
- Kroonjuwelen
- Eigenaarschap en rollen
- Risicobereidheid / Risicomatrix
- Beleid

Context

De basis (RM.01)	Risicobeoordeling	Behandelplan	Rapporteren
•Context •Processen •Kroonjuwelen •Verantwoordelijkheid / Eigenaarschap •Risicobereidheid (IT) •Beleid			

- Visie, Missie, Doelstelling
- Organogram
- Middelen (personeel/financieel)
- Wet- en regelgeving
- Risicocultuur

} Jaarrekening



Processen

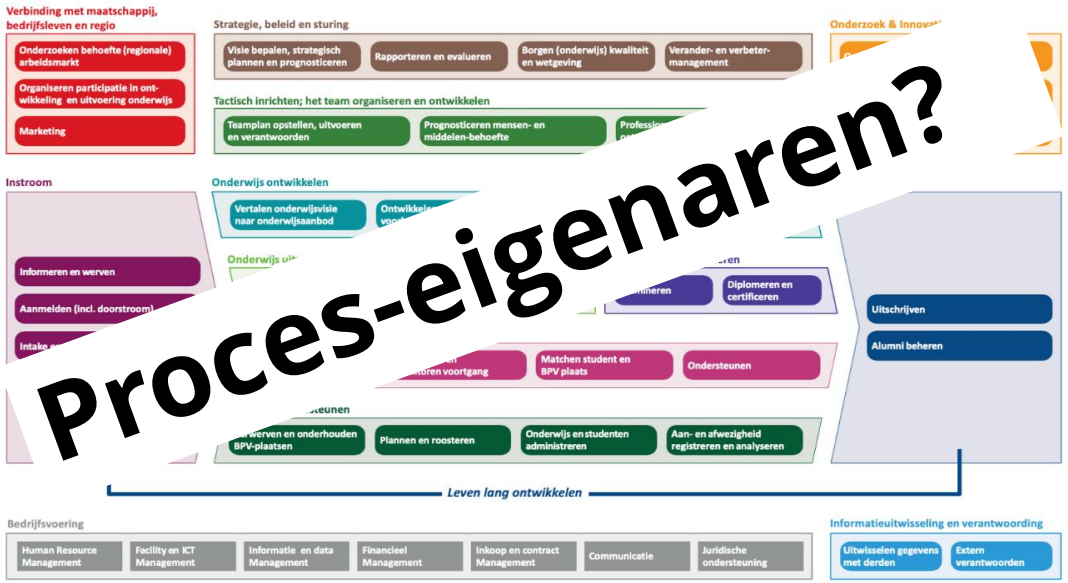
De basis (RM.01)

- Context
- Processen
- Kroonjuwelen
- Verantwoordelijkheid / Eigenaarschap
- Risicobereidheid (IT)
- Beleid

Risicobeoordeling

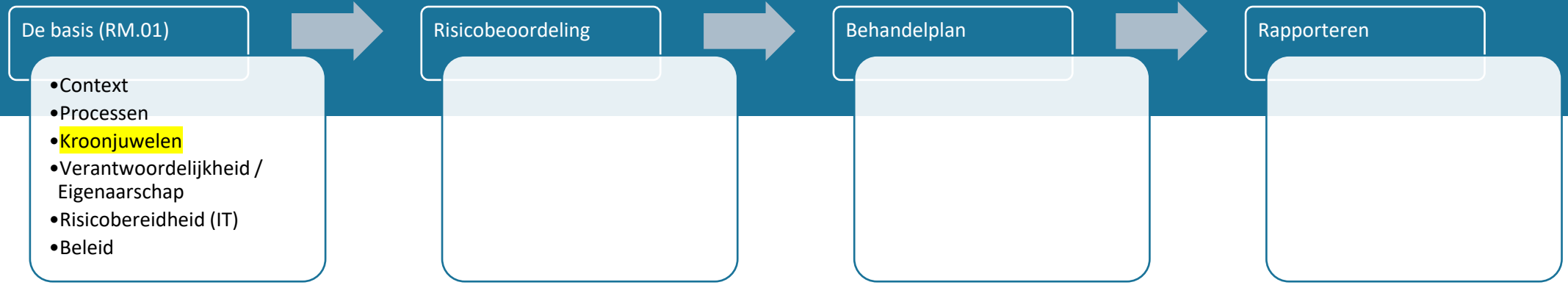
Behandelplan

Rapporteren



https://mora.mbodigitaal.nl/index.php/Hoofdpagina

Kroonjuwelen

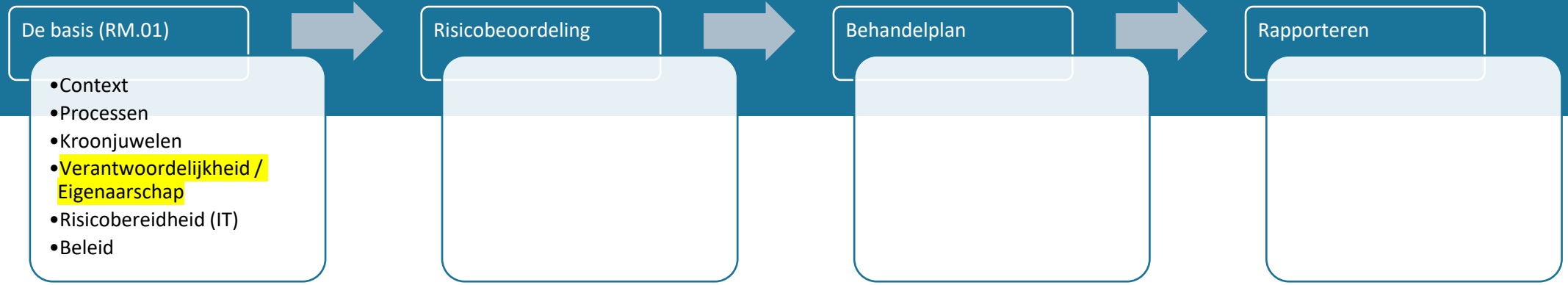


Bepaal kroonjuwelen aan de hand van classificatie van:

- Data
- Systeem
- Proces

- BIV-classificatie (data & systeem)
- Business Impact Analyse (proces)
- Metafoor van Burcht en open stad

Verantwoordelijkheid/Eigenaarschap



Risico-eigenaren:

- Begrijpen de risico's
- Geven risicobereidheid aan
- Beslissen

- RACI-template van SURF (NBA)
- Proceseigenaren (MORA/HORA)
- Vaststelling vindt plaats bij 'beleid'

Eigenaarschap RA~~SCI~~

R
Responsible

Verantwoordelijk voor de uitvoering van een taak of activiteit.

Zorgt ervoor dat het werk wordt gedaan en legt verantwoording af aan degene die accountable is.

A
Accountable

Eindverantwoordelijk voor de taak of activiteit. Heeft de bevoegdheid om beslissingen te nemen en goedkeuring te geven.

Er is slechts één persoon accountable voor elke taak.

S
Supportive

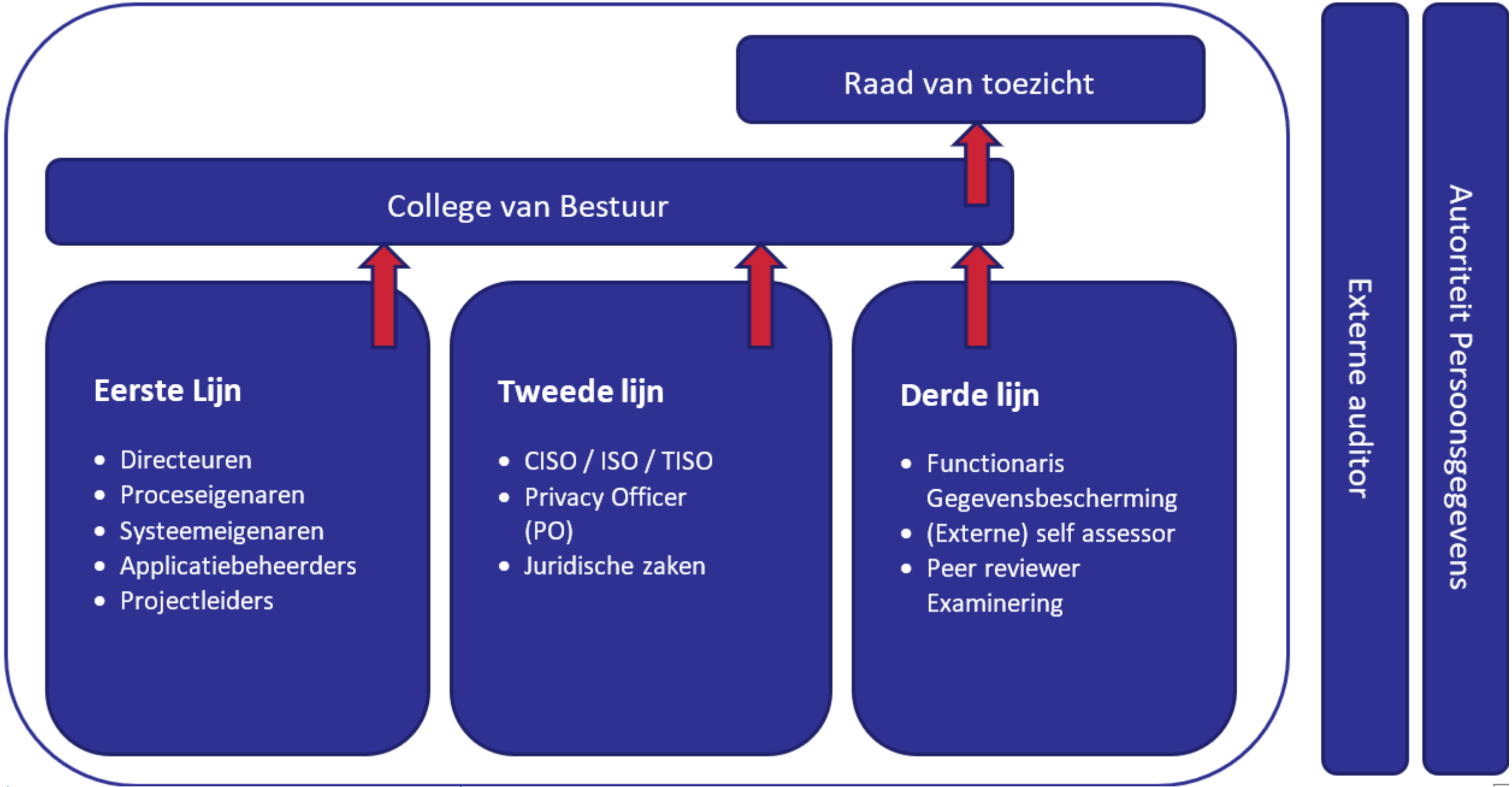
Personen die

C
Consulted

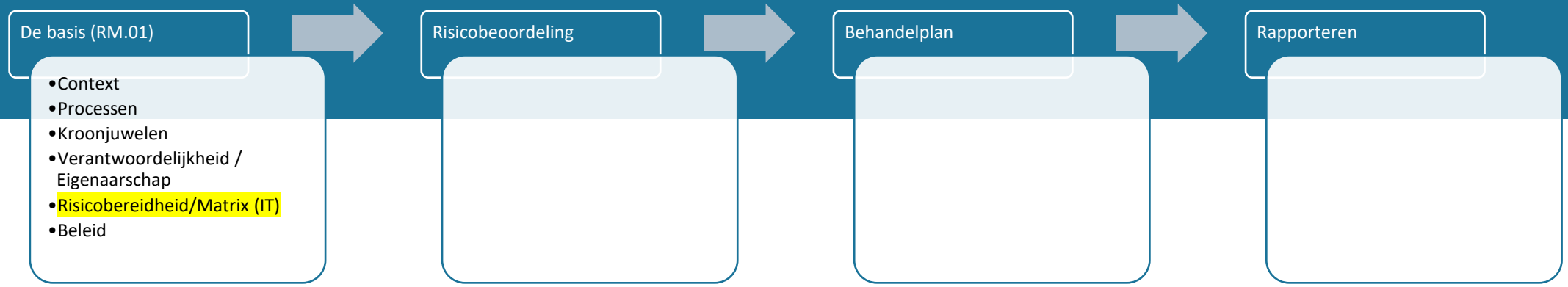
I
Informed

updates

		Directeur Personeel & Organis	Manager Personeel & Organis	Directeur Finance & Control	Directeur Facilitair	Manager Inkoop	Manager Services	Directeur ICT/IM	Manager ICT	Manager Informatie Manager	Manager Service Delivery	(C)ISO	Privacy Officer	Functionaris Gegevensbesch	Interim Controlling	College van bestuur	
		1e LIJN										2e LIJN		3e LIJN		CvB	
Governance																	
G01 Strategie	1.1 Strategie (mbt informatiebeveiliging)											R	C			A	
G02 Beleid	1.2 Beleid	R		R	R			R				R	C			A	
G03 Architectuur	1.4 Architectuur							R								A	
G04 Organisatie	2.1 Eigenaarschap, rollen, verantwoording en verantwoordelijkheid	R		R	R			R				R	C			A	
	2.2 Functiescheiding	R		R	R			R				R	C			A	
G05 Risk Management	3.1 Framework voor risk management							C				R	C			A	
	3.2 Risico beoordeling	R		R	R			R				R	C			A	
	3.3 Plan voor het behandelen van risico's	R		R	R			R				R	C			A	
G06 Roadmap	1.3 Planning / roadmap	R		R	R			R				R	C			A	
G07 Assurance	1.5 Onafhankelijke assurance			R										R	R	A	
Processen																	
P08 Human Resources	4.1 Werving	A	R									C	C				
	4.2 Certificering, Training en scholing	A/R	R	R	R			R				C	C				
	4.3 Afhankelijkheid van individuen	A/R	R	R	R			R				C	C				
	4.4 Verandering of beeindigen van functie	A	R	R	R			R				C	C				
	4.5 Kennisdeling	A/R		R	R			R				C	C				
	4.6 Veiligheidsbewustzijn	A						R				C	C				
	5.1 Identificatie en onderhoud van configuratie-items				A		R					C					
	5.2 Configuratiedatabase en baseline				A		R		R			C					
	6.1 Incident management				A		R		R			C	C				


Raad van toezicht
College van Bestuur
Eerste Lijn
Directeuren
Proceseigenaren
Systeemeigenaren
Applicatiebeheerders
Projectleiders
Tweede lijn
CISO / ISO / TISO
Privacy Officer (PO)
Juridische zaken
Derde lijn
Functionaris Gegevensbescherming
(Externe) self assessor
Peer reviewer Examinering
Externe auditor
Autoriteit Persoonsgegevens

Aan de slag: De basis – Risicobereidheid



Aan de slag: Risicobereidheid/Risicoprofiel

1. De mate van risico die een organisatie bereid is te accepteren bij het nastreven van haar doelstellingen.
2. Kan verschillen per onderwerp:
   - Financieel
   - Compliance
   - Operationeel
   - Strategisch
   - ...

Aan de slag: Risicoclassificatie/Risicomatrix

IMPACT	Minimaal	Aanzienlijk	Ernstig	Kritiek	Catastrofaal
	Minor	Significant	Serious	Critical	Catastrophic
	Er wordt niet of nauwelijks hinder ondervonden door de gebeurtenis en het kan volledig hersteld worden met beperkte middelen.	Het geraakte system of proces functioneert tijdelijk niet naar behoren door uitval van beschikbaarheid, integriteit en/of vertrouwelijkheid. De consequenties voor de organisatie zijn zwaar, maar te overkomen	Het geraakte systeem of proces functioneert niet meer en moet hersteld worden, met flinke reputatieschade en financiële en/of juridische gevolgen. En/of heeft het tot onveilige situaties geleid.	De impact is groot. De geraakte organisatie functioneert niet meer, en zal er niet of nauwelijks meer van kunnen herstellen. Ook diens partners worden dus geraakt. En/of het heeft zwaar letsel tot gevolg.	De impact is direct en immens. Alle aangesloten onderwijsinstellingen kampen met serieuze problemen en dat raakt ook nationale belangen. En/of het heeft dood tot gevolg
	1	2	3	4	5
Categorie:					
Financieel	Schade is lager dan €5.000	Schade ligt tussen €5001 en €20.000	Schade ligt tussen €20.001 en €300.000	Schade ligt tussen €300.001 en €1.500.000	Schade is groter dan €1.500.000
Imago	Geen/hoogst onwaarschijnlijke imagoschade.	Nauwelijks negatieve publiciteit. Een klein aantal negatieve berichten in lokale media (inclusief losse uitingen op sociale media).	Negatieve berichtgeving in de lokale media gedurende een paar dagen (inclusief commotie op sociale media). Vereist voorzichtige PR.	Aanhoudende negatieve berichtgeving in de natioale media (inclusief grote commotie op sociale media).	Aanhoudende negatieve berichtgeving in de landelijke of internationale media (inclusief zeer grote commotie op sociale media).
Onderwijs	Geen verstoring op het onderwijs.	Hooguit verstoring van een beperkt aantal activiteiten op een academie/instituut/dienst of vakgroep.	Verstoring van een deel van het onderwijs (zoals een deel van academies/instituten of vakgroepen).	Verstoring van een groot deel van het onderwijs op een of meer academies/instituten.	Merendeel van het onderwijs wordt onmogelijk op een of meer academies/instituten.
Onderwijsaccreditatie	Geen invloed op onderwijscertificatie.	Bepaalde invloed op onderwijscertificatie.	Extra toezicht op onderwijscertificatie.	Beperking van onderwijscertificatie.	Verlies van onderwijscertificatie.
Onderzoek	Geen verstoring op onderzoek.	Korte onderbrekingen in lopend onderzoek, voornamelijk reeds publieke of niet-gevoelige data.	Niet openbare onderzoeksgegevens, langdurige onderbreking of invalidatie van onderzoek.	Publicatiebeperkingen, reputatieschade aan onderzoeker of instelling, patenten of contractuele afspraken.	Verregaande contractuele verplichtingen, uitsluiting toekomstige subsidies of levensbedreigend onderzoek.
Bedrijfsvoering	Geen verstoring op bedrijfsvoering.	Hooguit verstoring van een beperkt aantal activiteiten van de bedrijfsvoering.	Verstoring van een deel van de bedrijfsvoering.	Verstoring van een groot deel van de bedrijfsvoering.	Merendeel / geheel van het bedrijfsvoering wordt onmogelijk.

Categorie:

- Financieel
- Imago
- Onderwijs
- Onderwijsaccreditatie
- Onderzoek
- Bedrijfsvoering
- Wet/regelgeving
- AVG
- Betrokkenen
- Strategie
- Omgeving
- Gebouwen
- Juridisch & Governance
- Studenten werving
- Medewerkers
- Technologie

Aan de slag: Risicobereidheid/Risicoprofiel

Opdracht 1:

Laat Microsoft Copilot een risicoprofiel voorstellen op basis van het jaarverslag van jouw organisatie.

Voorbeeld van een prompt:

Je bent CISO bij een onderwijsinstelling en verantwoordelijk voor het opstellen van het IT risicoprofiel van de onderwijsinstelling. Dit doe je in overleg met het bestuur. Doe een voorstel voor het risicoprofiel van de onderwijsinstelling op basis van de informatie die te vinden is op de website <website onderwijsinstelling> en onderliggende pagina's. Geef een verwijzing naar de oorspronkelijke tekst ter validatie.

Aan de slag: Risicoclassificatie/Risicomatrix

Opdracht 2:

~~A: Maak je eigen risicoclassificatie/risicomatrix op basis van de SURF-template of de aangepaste template~~

B:Laat Microsoft Copilot een risicomatrix voorstellen op basis van het jaarverslag van jouw organisatie.

Voorbeeld:

Doe een voorstel voor de impact-categorieën financieel, imago, onderwijs, wet- en regelgeving, AVG voor een schaal op basis van 'zeer klein', 'klein', 'gemiddeld', 'hoog' en 'zeer hoog' voor schades door informatiebeveiligingsincidenten op basis van informatie uit het jaarverslag dat is te vinden op de volgende locatie: *<jaarverslag op website onderwijsinstelling>*. Geef het antwoord weer in tabelvorm

Aan de slag: De basis – Risicobereidheid

De basis (RM.01)	Risicobeoordeling	Behandelplan	Rapporteren
• Context • Processen • Kroonjuwelen • Verantwoordelijkheid / Eigenaarschap • Risicobereidheid/Matrix (IT) • Beleid