Assests en systemen	**Data en informatie**	**Mensen**	**Procedures en processen**	**Partners en derde partijen**	**Risico's en Bedreigingen**	**Andere maatregelen**
Identify	Identify	Identify	Identify	Identify	Identify	Identify
CMDB	Inventarisatie en Classificatie	Identity management Systeem	Centrale tool	CMDB	Key Control Framework	Geen
Inventarisatie & Classificatie	dataclassificitatie to do	HR Proces / in&uitstroom	Conform ITIL	Inkoop en contractmanagement, Security Annex,	RIA's, classificeren, dreigingsbeeld	Externe scan
Netwerk scanning	Geen maatregelen	Awareness campagnes voor bepaalde doelgroepen (bv omgang met vertrouwelijke info/	Belangrijkste info beveiliging procedures&processen beschreven	Alleen inkoop bij bekende lev's, inzicht in alle (betaalde) derden	met name op Cloud	Governance zorgen door organisatie aanpassingen/ TBV duidelijk in organisatie
Assets Business Impact analyse	Geen retentiebeleid	Screening	Onderdeel van kwaliteitsmanagementsysteem / Policy house	voldoen aan SLA's, certificeringen, ISO 27001/2, externe toets, audits, toezicht,	Business Impact Analyse	We beoordelen de impact van nieuwe/veranderde wet- en regelgeving.
Risk Assessment		Geen maatregelen	Tbv Architectuurteam / IT Control framework	Onderdeel van Identity man.sys.	Risico workshops (jaarlijks) / strategisch/ operationeel	We maken gebruik van diverse bronnen om kennis te nemen van
Beschikbaarheidsanalyse		VOG	Nog niet in een tool	Spendanalyse gedaan op lev's, specifieke maatregelen in place	IV risicoanalyse uitvoeren, compliance en mitigerende	
		Conform Wet (aanpak schijnconstructies)			Gericht op hackers, terrorisme, insider, outsider, natuurlijke	
		AO richtlijnen				

Assests en systemen	**Data en informatie**	**Mensen**	**Procedures en processen**	**Partners en derde partijen**	**Risico's en Bedreigingen**	**Andere maatregelen**
Protect	Protect	Protect	Protect	Protect	Protect	Protect
			Er zijn Business Process Owners aangesteld die in zekere zin de			
Volgens security architectuur	Versleuteling	Access management	verantwoordelijkheid hebben hun	gecontroleerde toegang (VPN)	Improve system patching	Network zoning
Endpoint beveiliging anti-malware, IDS (intrusion detection prevention), IPS, identity- & Firewall, Antimalware, monitoring, etc.	Accessmanagement; toegangscontrole, logging toegang,	Onderzoek bij Sollicitatie / geheimhouding bij arbeidscontract/ screening	Autorisatie mechanismes	monitoring dat dienst geleverd worden conform contract rapportage, controls, evaluatie risk en complience	geen	dashboard security controls
systemen gehardend conform CIS bencgmark	Impact GDPR	Incidentele en rudimentaire awareness campagnes gericht op Mensen niet onnodig veel rechten geven	Geen business continuity process and disaster recovery process controle AO		Architectuur mensen; te makkelijk te hacken, te vriendelijk.	versleuteling van informatie
zonering, toegangscontrole en -beperkingen obv passen vernieuwen van firewalls, encryptie, antivirus/malware, hardening, patches installeren, gedragscode's, informatie over (on)veilig gedrag op portal, werken volgens ISO27001/NEN7510 in zijn algemeenheid	DataLossPrevention systeem VPN verbinding Encryptie van verkeerstromen + opslag afh. Van classificatie	continue/ jaarlijkse awareness campagne Toegangscontrole op locatie/ info over de locatie ivm risico's	ITIL bescherming processen Informatiebeveiliging als onderdeel van ontwikkel- en wijzigingsprocessen, waaronder secure software development, testen van systemen inclusief security testen, gereguleerd change management proces. - patch management		System patching verbeteren evaluatie/ mitigerende beheersmaatregelen tegen risico's en bedreigingen	
Netwerk segmentatie Firewall / DMZ		Verplichte information risk management training	Dekkende procedures en processen		Maatregelen zijn aanwezig in risk maps	
Uitwijkmogelijkheid naar 2e	Role based access	Personeelsreglement voor info beveiliging, voorlichting en	Deze zijn in een systeem opgeslagen waar met			
Basisbeveiliging	Dagelijkse backup	training	toegangsbeveiliging			

Organisatorische-, procedurele-, technische- en bouwkundige maatregelen en elektronische voorzieningen die anti virus maatregelen versleuteling van informatie op deze assets regelmatig vulnerability scans om kwetsbaarheden zichtbaar te maken patch management IPS Op het vlak van systemen doen we veel: - Firewalls om geen gevoelige gegevens weg te geven - Netwerkzonering om gevoelige onderdelen van het netwerk af te schermen - Aanvullende maatregelen in het netwerk om aanvallen te detecteren en af te vangen - Antivirus software en scanning	logische toegangsbeperkingen (accounts, rechten, wachtwoorden) encryptie, bewaarbeleid Momenteel is beveiliging gericht op tooling. Voor data centric beveiliging worden de eerste stappen genomen.

Assests en systemen Detect	**Data en informatie** Detect	**Mensen** Detect	**Procedures en processen** Detect	**Partners en derde partijen** Detect	**Risico's en Bedreigingen** Detect	**Andere maatregelen** Detect
Endpoint protectie Anti virus/malware, vulnerability scans Monitoren en scannen SIEM technologie geïnstalleerd Zero trust model in het network. brand/inbraakalarmen (fysiek), intrusion detection (logisch) IDS Systeem Mini SOC ingericht Penetratietesten uitvoeren	DLP systems Data anlytics tbv integriteitscontrole /Logging en monitoring om ongeautoriseerde Virusscanner Cloud usage review scan Spam and phishing detection Network security monitoring, logging, auditing	Pasjescontrole, tourniquettes Werving van personeel voor SOC. Iedere virusmelding wordt beoordeeld of er een 'foei-mailtje' verstuurd moet worden screening, logging, auditing bijhouden mislukte inlogpogingen, logging van Geen Multi layer security detection Controle op gevolgd Melden van incidenten (door Bewustwordingsprogramma Procedure om bij vermoeden van misbruik onderzoek te doen	Checks en rapportages CSIRT organisatie optuigen / Security Operation Centre processen Audits Geen maatregelen Multi layer detaction AO conform informatie beveiligingsbeleid Conform informatie	Third Party Memorandum, audit Informatie van partners inlezen in SIEM/SOC. toezicht / controls geimpementeerde ISO27001 beheersmaatregelen melden van incidenten Logging en monitoring van derde partijen	Acteren op SOC bevindingen architectuur papieren tijgers; TPM's zijn makkelijk maar vaak niet transparant/duidelijk genoeg. Geen maatregelen Through active threat hunting. External threat intelligence verklaringen evaluatie bedreigingen intellingence verzamelen en Opgenomen in de aanwezige risk We gebruiken informatie uit diverse bronnen om bekende	Service Desk uitgebreid informeren over datalekken en Usage of external intelligence data monitoring en logging DDOS aanvallen of ongeautoriseerde toegang infrastructuur en Geen

Assests en systemen Respond	**Data en informatie** Respond	**Mensen** Respond	**Procedures en processen** Respond	**Partners en derde partijen** Respond	**Risico's en Bedreigingen** Respond	**Andere maatregelen** Respond
Monitoring en response	Monitoring en response	geen	Incident proces (vereenvoudigd)	Continuiteitseisen en voorziening in de contracten met relevante	beheersen van risico's en bedreigingen	sigalering van events naar derden partners in de IV keten en

Incident proces	Incident proces	continuiteitsplannen	Auditproces (incl. proces	security incident management	opgenomen in risk maps	Rapportage van security
IDS	applicatielog beoordelen op onrechtmatige mutatie - of	Bewustwordingstraining	Periodieke aanpassingen	laten mitigeren van incidenten bij partners	Incidentproces	
afspraken met beveiligers (3rd party)	Procedure datalekken in geval er een lek geweest is	Through Health, Safety, Social and Environmental process	Secrutity incident management proces	Audit verslag 3e partijen		
mobile device mgt ingericht om te kunnen wipen op afstand		check integriteit				
escalatieprocedures opgesteld (inhoudelijk en qua communicatie	Reserve kopieen	taken en verantwoordelijkheden rollen/functies	gebeuretnissen/ technische events vastleggen in AO	incidentproces-afspraak /SLA		
Escalatieprotocol bij serviceprovider	business continuity management	testen van response plannen				
Endpoint Detect and Respond system in place	disaster recovery planning Forensic investigation	oefenen van cyber crisis Incidentproces	Crisis management proces Incident response procedure Procedure datalekken	Geen		
beoordelen systeemlogs op ongeautoriseerde toegang	applicatielog beoordelen op onrechtmatige mutatie - of	CSIRT	communicatieprotocol om te reageren op een incident			
business continuity management						
disaster recovery planning	Excalatieprotocol na incident					
Forensic investigation						
Backup & Continuïteitsplannen: dubbele uitvoering						

Assests en systemen	**Data en informatie**	**Mensen**	**Procedures en processen**	**Partners en derde partijen**	**Risico's en Bedreigingen**	**Andere maatregelen**
Recover	Recover	Recover	Recover	Recover	Recover	Recover
Backup & Restore / reservekopieen	Backup & Restore / reservekopieen	continuity plannen	Execution of business continuity plan and Disaster recovery plan.	contract afspraken over beschikbaarheid	Geen	Geen
Continuiteitsplannen	Continuiteitsplannen	3rd party levert personeel uit pool	actuele crisisplannen , procedures en processen voor calamiteiten	betrekken bij evaluatie van incidenten,	Opgenomen in de risk maps	uitdragen en jaarlijks beoefenen met crisismanagementteam
Evaluatie van incidenten &	Evaluatie van incidenten &	bewustwordingstrainingen	Testen van plannen	Vervanging bij ziekte binnen	beheersen, inventarisatie risico's	
		bewustwording vergroten door te communiceren over incidenten,	Business continuity / Disaster recovery	communicatie in de IV keten inclusief voorbereiding		
business continuity management	business continuity management	veilig en onveilig gedrag		afstemming ervan	continuity plannen	
disaster recovery planning	disaster recovery planning	Testen van plannen				
periodieke recoverytests van delen van systemen etc	periodieke recoverytests van delen van systemen etc	Through Health, Safety, Social and Environmental process				
Gedeeltelijke uitwijk backup/recovery (VM's)	Gedeeltelijke uitwijk backup/recovery (VM's)					
Changes, redundantie	Changes, redundantie					
monitoren eventuele vervolgacties rondom inhoudelijke preventieve	monitoren eventuele vervolgacties rondom inhoudelijke preventieve					

Welke andere maatregelen zijn er genomen om informatiebeveiliging binnen
Awareness via Mailings/ Onboarding e-learning
Intratnet pagina actueel houden
Inrichten security op C-level
Awareness programma / bewustwordingscampagne per doelgroep van personeel

risicoworkshops bij kritische projecten onder leiding van
beoordeling leveranciers in inkooptrajecten volgens vast
periodiek beoordelen bestaande

Hoe houd je controle op dit hele proces van identificeren, beschermen, ontdekken, reageren en herstellen, welke
Management, Privacy, Risk & Audit en Security overleg
Daarnaast vindt periodiek een benchmark plaats op de status
Work in progress, PDCA cycle: PD gaan goed, check en act moeten
ISO27001 processen staan en worden actief gebruikt
Jaarlijks tot 3 jaarlijks reviewen van beleid en strategiedocumentatie
Jaarlijkse externe audits door accountant EN andere externe
1x per 3 jaar herzien documentatie Business continuity en security
1x per jaar uitvoeren van NIST framework is being used within the Information Risk
rapporteren aan lijnmanagement over de status
Overleg en rapportage over informatiebeveiliging op RvB niveau
Overleg en rapportage over intensieve samenwerking met de operationele (IT) mensen

wordt periodiek geëvalueerd of er afdoende maatregelen getroffen zijn of dat aanvullende maatregelen nodig zijn.

Het informatie beveiligingsbeleid uitvoeren en de naleving hiervan controleren middels assessments

Hoe vaak worden maatregelen	
Jaarlijks	8x
Soms frequenter	5x

Sommige 3-yearly *Toelichting:* Jaarlijks tot 3 jaarlijks reviewen van beleid en strategiedocumentatie; Jaarlijkse externe audits door accountant en andere externe partijen; Regelmatig wordt gecontroleerd of het informatiebeveiligingsbeleid en procedures worden nageleefd. Maakt ook onderdeel uit van de 1x per 2 jaar is het doel. sommige vaker, meeste minder vaak. Beleid wordt aangepast aan de hand van feedback uit projecten of de technologie ontwikkelingen.	4x

Welke maatregelen zijn het meest effectief (kosten/opbrengsten) en hoe
Awareness en bescherming. Veel support in budget en daad op C- Patching van systemen en werkplekken is geautomatiseerd, platform voor beide ook. Combinatie brengt We hebben het risicomanagement rondom informatiebeveiliging opgenomen in het algemene risicomanagement. Dat is effectief, efficient en beter voor het draagvlak. De meeste collega's hebben een zakelijk mobile device. Daardoor is de noodzaak van web access Back up van data en systemen. Gerealiseerd in datacenter protect and detect awareness uitdragen middels commitment via het management. tijdige signalering van risico en bedreigingen die de business in Normale maatregel zoals anti-virus. Kunnen deelnemen aan de

Logische toegangsbeveiliging tot systemen. Er is een koppeling tussen het personeelssysteem en active directory waardoor we zeker weten dat alleen mensen

Zijn fysieke beveiliging, informatiebeveiliging, cyber veiligheid en persoonlijke data beveiliging ieder apart geadresseerd binnen jouw	
Organisch	2x
Apart	6x
Samen	3x
Toelichting:	
Apart. Fysiek = facilities, IB/Cyber = Security office, Persoonlijke	
Deze onderwerpen zijn gedeeltelijk belegd bij verschillende personen, echter er vindt wel regelmatig overleg	
Vaak organisatorisch verdeeld echter worden functioneel	
Kwaliteit van de samenwerking	

In hoeverre is jouw Board geïnteresseerd in deze maatregelen / procedures	
Zeer. Goed overleg.	7x
redelijk, vooral hands-on/praktisch; lijkt alsof de (achtergrond)kennis	4x
Niet	0x
Toelichting:	
Board is wel geïnteresseerd in status van informatiebeveiliging, maar niet zozeer in specifieke	
Indirect. Af en toe wordt onze CIO gevraagd om een status update te geven over deze onderwerpen	
Deze zijn geinteresseerd en worden periodiek geinformeerd	

Dit is het einde van de enquête, als je nog iets wilt delen, laat het
Ik vond het een moeilijk in te vullen model. Dat kwam niet zozeer door het gebruik van het NIST model maar nog meer door