Focusgebied	Onderdeel	Gap	Prioriteit	Impact	Doel	Beoogd effect
Mens	Awareness programma	Average	+++	+++	Verhogen van het informatiebeveiligingsbewustzijn van de organisatie	Medewerkers van de organisatie gaan bewust en veilig om met informatie. Verhogen van Vertrouwelijkheid van informatie in informatiesystemen, vermindering van aantal en verlaging van impact van beveiligingsincidenten en datalekken. Voorkomen imagoschade en financiele schade door boetes en claims.
Proces, Techniek	Rol gebaseerde toegang / autorisatiematrix	Average	+++	+++	Eenduidige, procesgerichte autorisatiematrix, inclusief Functies, Rollen en Toegangsniveau, welke als basis dient voor de technische inrichting van toegang tot informatiesystemen	Toegang tot informatie is beperkt tot bevoegd personeel. Verhogen van Vertrouwelijkheid van informatie in informatiesystemen, vermindering van aantal en verlaging van impact van beveiligingsincidenten en datalekken. Voorkomen imagoschade en financiele schade door boetes en claims
Mens, Proces	B.01 norm (webapplicaties)	Average	+++	+++	specifieke aandacht voor webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer in het informatiebeveiligingsbeleid	Verhogen van Beschikbaarheid, Integriteit en Vertrouwelijkheid van informatie in webapplicaties die gebruik maken van DigiD, succesvolle ENSIA-audit, behoud van DigiD aansluiting (x4), Voorkomen van onderbrekingen in digitale dienstverlening. Voorkomen imagoschade.
Proces	Baselinetoets	Average	+++	+++	Actueel inzicht in stavaza informatiebeveiliging van informatie conform geldende richtlijnen, inclusief GAP-analyse	Effectiviteit van informatiebeveiligingsmaatregelen verhogen, succesvolle ENSIA-audit, voldoen aan wet- en regelgeving (BIO 2.0 / NIS2)
Proces	Beleid wet politiegegevens	Average	+++	+++	Formuleren van beleidsregels inzake politiegegevens.	Voldoen aan wet- en regelgeving (Wpg), succesvolle Wpg audit

Proces	Beveiligingsambitie bepalen	Average	+++	+++	Bepalen van informatiebeveiligingsdoelstellingen, met specifieke aandacht voor de nieuwste industrieontwikkelingen.	Strategie/roadmap informatiebeveiliging 2025-2027.
Proces, Techniek	Certificaatbeheer	Average	+++	+++	Borging van certificaat/sleutelbeheer van informatiesystemen binnen de organisatie, inlusief verantwoordelijkheiden, bevoegdheden en de aanschaf van ondersteunende systemen.	Elimineren van Single Point of Failure in huidig proces, verhogen van Beschikbaarheid en Vertrouwelijkheid van informatie in informatiesystemen
Proces	Cybercrime response plan	Average	+++	+++	Borging van de organisatie, processen en procedures rondom de behandeling van informatiebeveiligingsincidenten met een ontwrichtend karakter in een bedrijfscontinuïteitsplan.	Organisatie voorbereid op een cybercrisis, voorkomen van onderbrekingen in dienstverlening. Voorkomen imagoschade.
Techniek	Device en port control	Average	+++	+++	Implementatie van technische maatregelen ter bevordering van de beveiliging van o.a. netwerkapparatuur	Verhogen van Integriteit en Vertrouwelijkheid van informatie in informatiesystemen
Proces	Informatiebeveiligingsbeleid update	Average	+++	+++	Actueel en vastgesteld informatiebeveiligingsbeleid	Bevorderen Beschikbaarheid, Integriteit en Vertrouwelijkheid van informatie.
Techniek	Mobile security (Intune)	Average	+++	+++	Implementatie van technische en procesmatige maatregelen ter bevordering van de beveiliging van werkplekken.	Verhogen van Beschikbaarheid en Vertrouwelijkheid van informatie in informatiesystemen
Mens, Proces, Techniek	NIS2	Poor	+++	+++	Tijdige implementatie van benodigde beheersmaatrgelen om te voldoen aan de NIS2 richtlijn.	Voldoen aan wet- en regelgeving (Cyberbeveiligingswet (Cbw), verwachte intreding Augustus 2025)
Techniek	Remote acces / 2 factor	Average	+++	+++	Implementatie van technische maatregelen ter bevordering van de beveiliging van toegang tot systemen.	Toegang tot informatie is beperkt tot bevoegd personeel. Verhogen van Vertrouwelijkheid van informatie in informatiesystemen, vermindering van aantal en verlaging van impact van beveiligingsincidenten en datalekken. Voorkomen imagoschade en financiele schade door boetes en claims

Proces	Risicoregister	Average	+++	+++	Bepalen van actuele risico's voor de informatiebeveiliging van processen en systemen binnen de organisatie	Verhogen effectiviteit van maatregelen ter bevorderdering van de Beschikbaarheid, Integriteit en Vertrouwelijkheid van informatie binnen de organisatie.
Proces, Techniek	SIEM/SOC	Poor	+++	+++	Tijdige implementatie van technische (SIEM) en organisatorige (SOC) maatregelen om te voldoen aan de BIO 2.0 en NIS2 richtlijnen	Effectiviteit van informatiebeveiligingsmaatregelen verhogen, succesvolle ENSIA-audit, voldoen aan wet- en regelgeving (BIO 2.0, NIS2/Cbw)
Proces	Suwinet beleid	Average	+++	+++	Formuleren van beleidsregels inzake Suwi gegevens.	Voldoen aan wet- en regelgeving (BIO 2.0), succesvolle ENSIA audit
Proces	Tactische procedures uitwerken	Average	+++	+++	Implementatie van tactische processen en procedures ten behoeve van diverse normen uit de BIO 2.0 en NIS2	Verhogen effectiviteit van maatregelen ter bevorderdering van de Beschikbaarheid, Integriteit en Vertrouwelijkheid van informatie binnen de organisatie.
Proces	Actualiseren technische security procedures	Average	++	+++	Implementatie van technische processen en procedures ten behoeve van diverse normen uit de BIO 2.0 en NIS2	Verhogen effectiviteit van maatregelen ter bevorderdering van de Beschikbaarheid, Integriteit en Vertrouwelijkheid van informatie binnen de organisatie.
Techniek	Open standaarden email (DNSsec, DMARC)	Good	++	++	Implementatie van technische maatregelen ter bevordering van de beveiliging van e-mail verkeer.	Verhogen van Vertrouwelijkheid van informatie in informatiesystemen, vermindering van aantal en verlaging van impact van beveiligingsincidenten en datalekken.
Techniek	Disc & file encryptie	Average	++	++	Implementatie van technische maatregelen ter bevordering van de beveiliging van de opslag van informatie op Sharepoint, werkplekken en mobiele telefoons	Verhogen van Vertrouwelijkheid van informatie in informatiesystemen, vermindering van aantal en verlaging van impact van beveiligingsincidenten en datalekken.
Proces	Security audits	Average	++	++	Uitvoeren intern/externe informatiebeveiligingsaudits	Organisatie is aantoonbaar "in control" op informatiebeveiligingsgebied.

Mens, Proces	Functieprofielen ciso en so	Average	++	+	Actuualitastie van functie- en rolbeschrijving ten behoeve van Informatiebeveiligingsbeleid, cybercrime response plan, ISMS.	Verhogen effectiviteit van maatregelen ter bevorderdering van de Beschikbaarheid, Integriteit en Vertrouwelijkheid van informatie binnen de organisatie. Voldoen aan wet- en regelgeving (BIO 2.0, Wcb)
Proces	ISMS	Average	++	+	Managementsysteem voor informatiebeveiliging conform ISO27001 / BIO, ondergebracht in een ondersteunend systeem (Recourse)	Verhogen effectiviteit van maatregelen ter bevorderdering van de Beschikbaarheid, Integriteit en Vertrouwelijkheid van informatie binnen de organisatie. Voldoen aan wet- en regelgeving (BIO 2.0, Wcb)
Proces, Techniek	Password safe	Poor	+	+	Implementatie van technische maatregelen ter bevordering van de beveiliging van toegang tot systemen.	Toegang tot informatie is beperkt tot bevoegd personeel. Verhogen van Vertrouwelijkheid van informatie in informatiesystemen, vermindering van aantal en verlaging van impact van beveiligingsincidenten en datalekken. Voorkomen imagoschade en financiele schade door boetes en claims
Techniek	Logging	Average	+	+	Implementatie van technische maatregelen ter bevordering van de beveiliging van informatiesystemen	Verhogen van Integriteit en Vertrouwelijkheid van informatie in informatiesystemen
Mens, Proces	Security instructie (OGD)	Average	+	+	Verhogen van het informatiebeveiligingsbewustzijn van de organisatie	Medewerkers IM zijn bewust van informatiebeveiligingsmaatregelen, processen en procedures. Verhogen van effectiviteit personeel, verlaging van impact van beveiligingsincidenten.