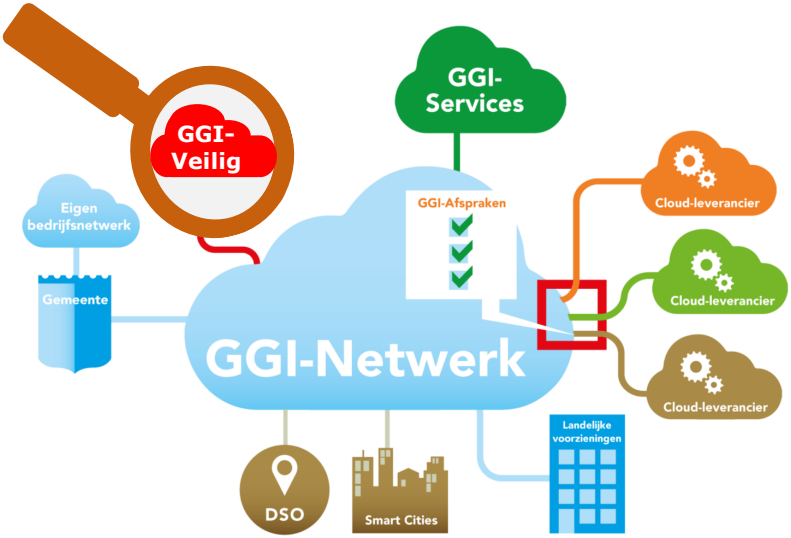
Gemeentelijke Gemeenschappelijke Infrastructuur (GGI) / GGI-Veilig-VDW



Eenvoudiger en veiliger digitaal dienstverlenen

GGI-Veilig / Volwassenheidsmodel Digitale Weerbaarheid

juni 2018

www.da2020.nl/ggi

VOORWOORD

Gemeenten hebben in het kader van de Digitale Agenda 2020 en de uitvoeringsbeweging "Samen Organiseren" de VNG opdracht gegeven tot onder andere het realiseren van de Gemeentelijke Gemeenschappelijke Infrastructuur (GGI).

De GGI creëert een veilige, samenhangende digitale infrastructuur waardoor samenwerken tussen gemeenten met andere overheden beter, veiliger en makkelijker wordt.

Eén van die onderdelen van GGI is GGI-Veilig. GGI-Veilig is een producten en diensten portfolio op het gebied van de operationele informatiebeveiliging en wordt in opdracht van gemeenten[1] verworven. Een nadere toelichting op GGI-Veilig is opgenomen in het boekje "Gemeentelijke Gemeenschappelijke Infrastructuur / GGI-Veilig"

Voor één van de onderdelen van het GGI-Veilig producten en diensten portfolio (SIEM/SOC dienstverlening) geldt dat voor de effectieve inzet ervan er een bepaalde mate van "digitale volwassenheid" aanwezig moet zijn.

Als handreiking voor het bepalen van het niveau van "volwassenheid digitale weerbaarheid" is het GGI-Veilig-Volwassenheidsmodel Digitale Weerbaarheid (GGI-Veilig-VDW) opgesteld. GGI-Veilig-VDW is een eenvoudig en praktisch

[1] Onder gemeenten wordt (in het vervolg) begrepen alle Nederlandse gemeenten (uitgezonderd Bonaire, Sint Eustatius en Saba) en alle samenwerkingsverbanden op basis van de Wet Gemeenschappelijke Regelingen dan wel samenwerkingsverbanden waarin een gemeente een belang heeft.

toepasbaar model voor self assessment. Het is gebaseerd op internationale Security Management Maturity modellen. Dit model wordt in dit boekje gepresenteerd.

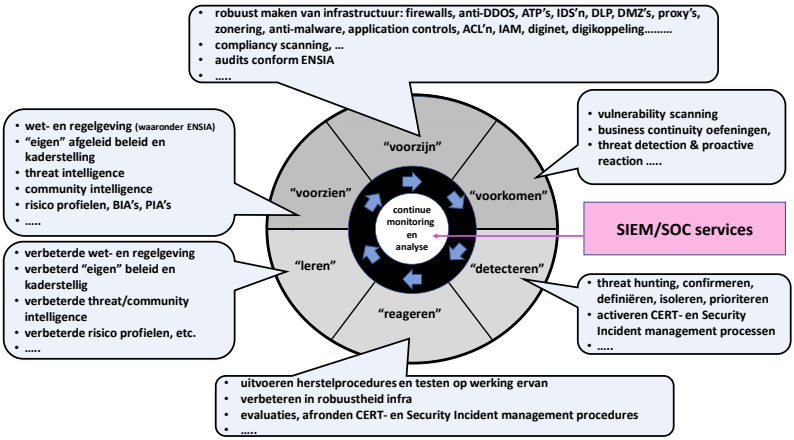
Informatie over GGI, over alle onderdelen van GGI en het introductiefilmpje GGI zijn te vinden op www.da2020.nl/ggi .

Inhoudsopgave

1. WAAROM EEN GGI-VEILIG-VDW

Gemeenten zijn en blijven te allen tijde zelf verantwoordelijk voor de betrouwbaarheid van hun gegevensbeheer en hun informatievoorziening c.q. voor de informatiebeveiliging.

GGI-Veilig is een collectieve voorziening voor gemeenten op het gebied van de operationele informatiebeveiliging. GGI-Veilig omvat een producten en diensten portfolio dat gebruikt kan worden bij de inrichting, uitvoering en borging van het informatiebeveiligingsproces. Het biedt gemeenten daarmee op een ontzorgende manier ondersteuning bij het realiseren en in stand houden van hun digitale weerbaarheid.



Informatiebeveiliging als een continu werkend cyclish proces

Het GGI-Veilig portflolio kan op hoofdlijnen worden onderverdeeld in drie groepen producten/diensten, die in een nauwe onderlinge samenhang de informatiebeveiliging op zowel de gemeentelijke bedrijfsnetwerken/ICT-infrastructuren

als de GGI-infrastructuur kunnen vormgeven. De product/dienst groepen zijn:

- Producten/diensten op het gebied van de “klassieke” preventieve middelen zoals firewalls, antivirus, mail filtering, indringer detectiesystemen, etc.
- Producten/diensten voor de continue monitoring en analyse: SIEM/SOC services.
- Expertise diensten, ter ondersteuning van gemeenten bij het gebrek aan kennis en capaciteit.

Zoals bekend is continue monitoring en analyse van gedrag en acties op de digitale infrastructuur (SIEM/SOC services) in het digitale tijdperk een noodzakelijke aanvullende maatregel om voldoende digitaal weerbaar te kunnen zijn en blijven. De geldende wet- en regelgeving vormen daarbij belangrijke drivers voor het nemen van deze aanvullende maatregel.

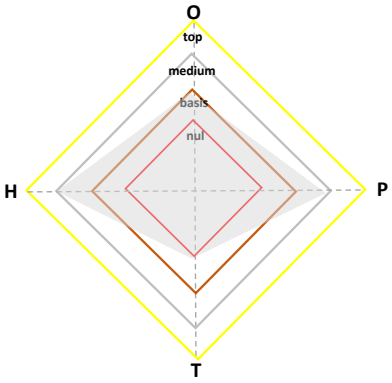
Het inrichten van de monitoring en analyse functie (SIEM/SOC services) is echter een complexe aangelegeheid.

GGI-Veilig-VDW is opgezet als een hulpmiddel voor gemeenten bij het bepalen van wat gedaan moet worden om voldoende gereed te voor het effectief kunnen inzetten van de SIEM/SOC services en het geeft een beeld van de mate van volwassenheid op het terrein van digitale weerbaarheid.

2. HOE IS GGI-VEILIG-VDW OPGEZET

GGI-Veilig-VDW is, zoals aangegeven, gebaseerd op een aantal internationale Security Management Maturity modellen. Het bestaat uit situatie beschrijvingen waarmee de volwassenheid op de aandachtsgebieden Organisatie (O), Personeel (H), Processen (P) en Techniek (T) vanuit de optiek van digitale weerbaarheid kan worden omschreven. De omschrijvingen per aandachtsgebied beschrijven daarbij 4 niveaus (nul, basis, medium, top) van volwassenheid digitale weerbaarheid.

Op basis van bovenstaande kenmerken kan met onderstaand rapportagemodel op eenvoudige manier zichtbaar gemaakt worden op welke volwassenheidsniveau digitale weerbaarheid de organisatie zich bevindt.



Als algemeen uitgangspunt voor de organisatorische gereedheid voor implementatie SIEM/SOC services kan het niveau basis gehanteerd worden met de bereidheid de acties te ondernemen om op niveau medium te komen.

3. DE GGI-VEILIG-VDW NIVEAU BESCHRIJVINGEN

3.1 Beschrijving situatie niveau nul

O-1: Het portefeuillehouderschap informatiebeveiliging is niet eenduidig belegd bij één van de leden van het college van B&W dan wel bij één van de directieleden van een gemeentelijk samenwerkingsverband.

O-2: Het uitvoeren/evalueren/actualiseren van de bedrijfsrisicoanalyse digitale weerbaarheid is geen geïntegreerd onderdeel van de jaarlijkse bedrijfsplan c.q. beleidsplan cyclus uitgevoerd dan wel onderdeel van een jaarlijkse evaluatie/actualisatie van het informatiebeveiligingsbeleid.

O-3: Er is geen gestructureerde aanpak voor het creëren en onderhouden van awareness digitale weerbaarheid en het herkennen en melden van mogelijke security/privacy incidenten.

O-4: De organisatie heeft geen actueel inzicht in de mate waarin zij BIG en AVG compliant zijn en welke maatregelen er genomen moeten worden om dat te bereiken.

H-1: De functieprofielen van de informatiebeveiligingsfunctie in de organisatie zijn kwalitatief en kwantitatief niet / onvoldoende in lijn met het informatiebeveiligingsbeleid om de daarbij gestelde doelen te kunnen realiseren.

H-2: Er is, als onderdeel van de jaarlijks bedrijfs-/beleidsplan cyclus, geen gestructureerd opleiding/trainings programma om de kennis/kunde van de IB-specialisten op niveau te krijgen (voor nieuw) en te houden (voor bestaand) en voor kennisdeling met IB-specialisten buiten de eigen organisatie.

H-3: Er is geen vastgestelde gedragscode voor IB-specialisten.

H-4: Er is geen minimum operationeel beschikbare IB-capaciteit vastgesteld en er is geen gestructureerd vervangingsplan hoe de IB-capaciteit op voldoende niveau te houden tijdens ziekte, verlof, langdurige opleiding/training, vertrek, etc.

P-1: Er zijn geen vastgestelde processen voor risicomanagement (voor het onderkennen, classificeren en vaststellen van organisatie risico's digitale weerbaarheid) en business continuity management (bedrijfscontinuïteit plan incl. de herstelprocessen ingeval van uitval c.q. verstoring van systemen/processen bedrijfsvoering/dienstverlening als gevolg van een (security) incident).

P-2: Er zijn geen processen en protocollen opgesteld hoe intern en extern gecommuniceerd moet worden ingeval van een security incident.

P-3: Aan de security/privacy aspecten is in de beheerprocessen van de organisatie (nagenoeg) geen aandacht besteed; denk hierbij aan de IV/IT beheerprocessen zoals incident-, wijzigingen-, configuratie/certificaat, IV/IT-architectuur-,

applicatie/database- en release managent, inkoop processen producten/diensten, organisatiebeheer processen zoals organisatiewijzigingen, in- door- en uitstroom processen, toekennen rollen/rechten.

P-4: Er is geen proces securitymonitoring, incidentdetectie en opvolging op de digitale infrastructuur ingericht waardoor security incidenten ontdekt kunnen worden. Incidentmeldingen komen van buiten de informatiebeveiligingsfunctie en opvolging is altijd reactief.

T-1: Ter ondersteuning van de uitvoering van het informatiebeveiligingsbeleid beschikt de organisatie niet over een ISM systeem[2]; de voor de uitvoering benodigde documentatie is in diverse bestanden opgeslagen en wordt door de CISO/IBF beheerd.

T-2: De organisatie beschikt niet over een systeem (of meerdere systemen) voor configuratiebeheer ICT middelen, (technisch) wijzigingenbeheer, certificaatbeheer (hfd ICT is eigenaar/beheerder) en autorisatiebeheer en (functioneel) wijzigingenbeheer (hfd IM is eigenaar/beheerder). Compliancy beoordelingen vinden niet plaats.

T-3: De organisatie beschikt niet over een systeem voor (security) incidentmelding, logging & tracking (workflow

[2] Zie IBD: ISMS

management functie) waarmee een audittrail kan worden opgebouwd van (wijze van) melding tot en met herstel.

T-4: De organisatie beschikt niet over een systeem voor geautomatiseerde security incident detectie.

3.2 Beschrijving situatie niveau basis

O-1: Het portefeuillehouderschap informatiebeveiliging is eenduidig belegd bij één van de leden van het college van B&W dan wel bij één van de directieleden van een gemeentelijk samenwerkingsverband.

O-2: De organisatierisico's digitale weerbaarheid zijn in kaart gebracht en worden periodiek geëvalueerd/bijgesteld, wanneer nodig wordt het informatiebeveiligingsbeleidsplan bijgesteld. Voor de digitale weerbaarheid zijn hierbij de belangrijkste assets die horen bij de risico's bepaald. Vervolgens is bepaald hoe gedetecteerd wordt of deze risico's manifest worden en is deze detectie ingericht.

O-3: Er wordt aandacht besteed aan het creëren en onderhouden van awareness digitale weerbaarheid bij alle ambtenaren en eventueel ingehuurd personeel en het herkennen en melden van mogelijke security/privacy incidenten.

O-4: Er wordt aandacht besteed aan de mate waarin de organisatie BIG en AVG compliant is en welke maatregelen er genomen zouden moeten worden om dat te bereiken.

H-1: De functieprofielen van de informatiebeveiligings-functie in de organisatie zijn kwalitatief en kwantitatief eenmalig getoetst of e.e.a. in lijn is met het vastgestelde informatiebeveiligingsbeleid om de daarbij gestelde doelen te kunnen realiseren en wordt dit wanneer nodig in lijn gebracht.

H-2: Er is, als onderdeel van de jaarlijks bedrijfs-/beleidsplan cyclus, geen gestructureerd opleiding/training programma om de kennis/kunde van de IB-specialisten op niveau te krijgen (voor nieuw) en te houden (voor bestaand) en voor kennisdeling met IB-specialisten buiten de eigen organisatie. Er is wel een opleidings-/trainingsbudget voor IB-specialisten op basis van de algemene organisatienormen.

H-3: Er is een vastgestelde gedragscode voor IB-specialisten.

H-4: Er is wel een minimum operationeel beschikbare IB-capaciteit vastgesteld maar er is geen gestructureerd vervangingsplan hoe de IB-capaciteit op voldoende niveau te houden tijdens ziekte, verlof, langdurige opleiding/training, vertrek, etc..

P-1: Er zijn processen voor risicomanagement (voor het onderkennen, clasificeren en vaststellen van organisatie risico's digitale weerbaarheid) en business continuity management (bedrijfscontinuïteit plan incl. de herstelprocessen ingeval van uitval c.q. verstoring van systemen/processen bedrijfsvoering/dienstverlening als gevolg van een (security) incident).

P-2: Er zijn vastgestelde processen en protocollen hoe intern en extern gecommuniceerd moet worden ingeval van een security incident.

P-3: De security/privacy aspecten zijn in de beheerprocessen van de organisatie benoemd; denk hierbij aan de IV/IT beheerprocessen zoals incident-, wijzigingen-, configuratie/certificaat-, IV/IT-architectuur-, ontwikkel- en release managent, inkoop processen producten/diensten, organisatiebeheer processen zoals organisatiewijzigingen, in- door- en uitstroom processen, toekennen rollen/rechten.

P-4: Er is een proces security monitoring, incident detectie en opvolging op de digitale infrastructuur ingericht waardoor security incidenten mogelijk ontdekt worden. Dit gebeurt reactief.

T-1: Ter ondersteuning van de uitvoering van het informatiebeveiligingsbeleid beschikt de organisatie over een ISM systeem; de portefeuillehouder informatiebeveiliging is eigenaar van het systeem en de CISO is houder/beheerder van het systeem. Het ISMS wordt niet actief gebruikt bij de jaarlijkse bedrijfs- en beleidsplan cyclus en jaarlijkse actualisatie van het informatiebeveiligingsbeleids-plan.

T-2: De organisatie beschikt over een systeem (of meerdere systemen) voor configuratiebeheer ICT middelen, (technisch) wijzigingenbeheer, certificaatbeheer (hfd ICT is eigenaar/beheerder) en autorisatiebeheer en (functioneel) wijzigingenbeheer (hfd IM is eigenaar/beheerder). Compliancy beoordelingen vinden

plaats op basis van de vastgelegde informatie in het systeem/de systemen. De systemen worden actief gebruik bij de processen waaraan zij ondersteunend zijn en de juistheid, actualiteit en volledigheid van de in de systemen opgeslagen gegevens wordt periodiek gecontroleerd en geven derhalve op moment van compliancy meeting een voldoende betrouwbaar beeld van de werkelijkheid.

T-3: De organisatie beschikt over een systeem voor (security) incident melding, logging & tracking (workflow management functie) waarmee een audittrail wordt vastgelegd van (wijze van) melding tot en met herstel.

T-4: De organisatie beschikt over een of meerdere systemen voor de collectie en analyse van logdata voor reactieve security incident detectie. Na detectie en classificatie worden de bestuurlijke processen voor security incident opvolging, communicatie en business continuity geactiveerd.

3.3 Beschrijving situatie niveau medium

O-1: Het portefeuillehouderschap informatiebeveiliging is eenduidig belegd bij één van de leden van het college van B&W dan wel bij één van de directieleden van een gemeentelijk samenwerkingsverband en binnen de organisatie is dat voor een ieder bekend.

O-2: De organisatierisico's digitale weerbaarheid zijn in kaart gebracht en worden jaarlijks geëvalueerd/bijgesteld als onderdeel van de jaarlijkse bedrijfsplan c.q. beleidsplan cyclus en jaarlijkse evaluatie en bijstelling van het

informatiebeveiligingsbeleidsplan. Voor de digitale weerbaarheid zijn hierbij de belangrijkste assets die horen bij de risico's bepaald. Vervolgens is bepaald hoe gedetecteerd gaat worden of deze risico's manifest kunnen worden en is deze detectie ingericht.

O-3: Er wordt structureel periodiek aandacht besteed aan het creëren en onderhouden van awareness digitale weerbaarheid bij alle ambtenaren en eventueel ingehuurd personeel met specifieke aandacht op het voorkomen maar zeker ook reageren op en melden van security incidenten.

O-4: Er wordt structureel als onderdeel van de jaarlijkse bedrijfsplan c.q. beleidsplan cyclus van de aandacht besteed aan de mate waarin de organisatie BIG en AVG compliant (compliancy scan, BIG-toets, etc.) is, wat de kwetsbaarheden in de ICT-infrastructuur zij (vulnerability scan) en welke maatregelen genomen zouden moeten worden om compliancy te bereiken en de kwetsbaarheiden op te lossen. De te nemen maatregelen worden opgenomen in het informatiebeveiligings-beleidsplan.

H-1: Periodiek worden de functieprofielen van de informatiebeveiligingsfunctie in de organisatie kwalitatief en kwantitatief getoetst op de ontwikkelingen in het vakgebied en het vigerende informatiebeveiligingsbeleid om de daarbij gestelde doelen te kunnen realiseren en wordt e.e.a. wanneer nodig aangepast.

H-2: Er is, als onderdeel van de jaarlijks bedrijfs-/beleidsplan cyclus, een jaarlijks opleiding/training plan voor de IB-

functionarissen dat gebaseerd is op de algemene organisatienormen. Er wordt op gestructureerde wijze aan kennisdeling gedaan met IB-specialisten buiten de eigen organisatie.

H-3: Er is een vastgestelde gedragscode voor IB-specialisten, welke door de IB-specialisten ondertekend is.

H-4: Er is een minimum operationeel beschikbare IB-capaciteit vastgesteld en er is een gestructureerd vervangingsplan hoe de IB-capaciteit op voldoende niveau te houden tijdens ziekte, verlof, langdurige opleiding/training, vertrek, etc.

P-1: De processen voor risicomanagement (voor het onderkennen, classificeren en vaststellen van organisatie risico's digitale weerbaarheid) en business continuity management (bedrijfscontinuïteit plan incl. de herstelprocessen ingeval van uitval c.q. verstoring van systemen/processen bedrijfsvoering/dienstverlening als gevolg van een (security) incident) zijn in OPZET (vastgesteld), BESTAAN (ingericht) en WERKING (periodiek uitgevoerd/beoefend) in de organisatie aantoonbaar geborgd.

P-2: Er zijn vastgestelde processen en protocollen hoe intern en extern gecommuniceerd moet worden ingeval van een security incident en hoe de verslaggeving/verantwoording daarover dient plaats te vinden

P-3: De security/privacy aspecten zijn in de beheerprocessen van de organisatie in OPZET, BESTAAN en WERKING

aantoonbaar geborgd; denk hierbij aan de IV/IT beheerprocessen zoals incident-, wijzigingen-, configuratie/certificaat-, IV/IT-architectuur-, ontwikkel- en release managent, inkoop processen producten/diensten, organisatiebeheer processen zoals organisatiewijzigingen, in- door- en uitstroom processen, toekennen rollen/rechten.

P-4: Het proces security monitoring, incident detectie en opvolging op de digitale infrastructuur is zowel proactief als reactief binnen de reguliere bedrijfstijden in OPZET, BESTAAN en WERKING geborgd en wordt ondersteund door tooling. Hierbij wordt regelmatig gekeken naar het veranderende dreigingslandschap voor de gemeente (Threat Intelligence, Community Intelligence). Eventuele veranderingen hierin worden meegenomen in de monitoring en maatregelen die getroffen zijn.

T-1: Ter ondersteuning van de uitvoering van het informatiebeveiligingsbeleid beschikt de organisatie over een ISM systeem; de portefeuillehouder informatiebeveiliging is en voelt zich eigenaar van het systeem en de CISO is houder/beheerder van het systeem. Het ISMS wordt actief gebruikt bij de jaarlijkse bedrijfs- en beleidsplan cyclus en jaarlijkse actualisatie van het informatiebeveiligingsbeleidsplan.

T-2: De organisatie beschikt over een systeem (of meerdere systemen) voor configuratiebeheer ICT middelen, (technisch) wijzigingenbeheer, certificaatbeheer (hfd ICT is eigenaar/beheerder) en autorisatiebeheer en (functioneel) wijzigingenbeheer (hfd IM is

eigenaar/beheerder). Compliancy beoordelingen vinden plaats op basis van de vastgelegde informatie in het systeem/de systemen. De systemen worden actief gebruik bij de processen waaraan zij ondersteunend zijn en deze processen zijn in OPZET, BESTAAN en WERKING controleerbaar geborgd. De in de systemen opgeslagen gegevens geven derhalve op moment van compliancy meeting een betrouwbaar beeld van de werkelijkheid.

T-3: De organisatie beschikt over een systeem voor (security) incident melding, logging & tracking (workflow management functie) waarmee een audittrail wordt vastgelegd van (wijze van) melding tot en met herstel. Het systeem is gekoppeld aan/ maakt onderdeel uit van service asset & configuratie beheersysteem en/of ISM systeem

T-4: De organisatie beschikt over een Security Information en Event Management systeem (SIEM) voor monitoring, analyse en proactieve en reactieve security incident detectie en compliancy en vulnerability scanning. De bijbehorende SIEM/SOC processen zijn in OPZET, BESTAAN en WERKING geborgd en gekoppeld aan de bestuurlijke processen voor security incident opvolging, communicatie en business continuity.

3.4 Beschrijving situatie niveau top

O-1: Het portefeuillehouderschap informatiebeveiliging is eenduidig belegd bij één van de leden van het college van B&W dan wel bij één van de directieleden van een gemeentelijk samenwerkingsverband en binnen de

organisatie treedt de betreffende functionaris actief en zichtbaar op als ambassadeur digitale weerbaarheid.

O-2: De organisatierisico's digitale weerbaarheid zijn in kaart gebracht en worden jaarlijks geëvalueerd als onderdeel van de jaarlijkse bedrijfsplan c.q. beleidsplan cyclus en het informatiebeveiligingsbeleidsplan wordt hierop aangepast als ook na majeure beveiligingsincidenten. Over de risico's digitale weerbaarheid en de (effectiviteit van de) beheersingsmaatregelen wordt periodiek (minimaal 1x per jaar) gerapporteerd aan alle stakeholders (College, Raad, directeuren uitvoering, medewerkers, burgers, enz.).Voor de digitale weerbaarheid zijn hierbij de belangrijkste assets die horen bij de risico's bepaald/herzien. Vervolgens wordt bepaald hoe gedetecteerd kan worden of en hoe deze risico's manifest kunnen worden, is/wordt deze detectie ingericht, de te nemen set mitigerende maatregelen bepaald en de uitvoering daarvan actief bewaakt.

O-3: Er wordt structureel periodiek aandacht besteed aan het creëren en onderhouden van awareness digitale weerbaarheid bij alle ambtenaren en eventueel ingehuurd personeel met specifieke aandacht op het voorkomen maar zeker ook reageren op en melden van security incidenten. De effecten hiervan worden gemeten en hierover wordt aan de stakeholders gerapporteerd.

O-4: Er wordt structureel als onderdeel van de jaarlijkse bedrijfsplan c.q. beleidsplan cyclus van de aandacht besteed aan de mate waarin de organisatie BIG en AVG compliant (compliancy scan, BIG-toets, etc.) is, wat de

kwetsbaarheden in de ICT-infrastructuur zij (vulnerability scan) en welke maatregelen genomen zouden moeten worden om compliancy te bereiken en de kwetsbaarheiden op te lossen. De te nemen maatregelen worden opgenomen in het informatiebeveiligings-beleidsplan, begroot en op realisatie wordt door de bestuurlijk verantwoordelijke actief gestuurd.

H-1: Jaarlijks worden de functieprofielen van de informatiebeveiligingsfunctie in de organisatie kwalitatief en kwantitatief getoetst op de ontwikkelingen in het vakgebied, het geactualiseerde risicoprofiel van de organisatie en het vigerende informatiebeveiligingsbeleid om de daarbij gestelde doelen te kunnen realiseren en wordt e.e.a. wanneer nodig aangepast.

H-2: Er is, als onderdeel van de jaarlijks bedrijfs-/beleidsplan cyclus, een gestructureerd opleiding/training programma dat gebaseerd is op de algemene organisatienormen en wanneer nodig een "plus" vanwege de dynamiek in het vakgebied om de kennis/kunde van de IB-specialisten op niveau te houden. Er wordt ook op gestructureerde wijze aan kennisdeling gedaan met IB-specialisten buiten de eigen organisatie.

H-3: Er is een vastgestelde gedragscode voor IB-specialisten, welke door de IB-specialisten ondertekend is en waarop handhaving is ingericht

H-4: Er is een minimum operationeel beschikbare IB-capaciteit vastgesteld, er is een gestructureerd vervangingsplan hoe de IB-capaciteit op voldoende niveau te houden tijdens ziekte, verlof, langdurige opleiding/training,

vertrek, etc. en de werking daarvan wordt jaarlijks geëvalueerd en wanneer nodig bijgesteld.

P-1: De processen voor risicomanagement (voor het onderkennen, classificeren en vaststellen van organisatie risico's digitale weerbaarheid) en business continuity management (bedrijfscontinuïteit plan incl. de herstelprocessen ingeval van uitval c.q. verstoring van systemen/processen bedrijfsvoering/dienstverlening als gevolg van een security incident) zijn in OPZET (vastgesteld), BESTAAN (ingericht) en WERKING (periodiek uitgevoerd/beoefend) in de organisatie aantoonbaar geborgd. Over de WERKING wordt periodiek (minimaal 1x per jaar) gerapporteerd aan alle stakeholders.

P-2: Er zijn vastgestelde processen en protocollen opgesteld hoe intern en extern gecommuniceerd moet worden ingeval van een security incident, hoe de verslaggeving/verantwoording daarover dient plaats te vinden en deze worden periodiek (minimaal 1x jaarlijks) geoefend, geëvalueerd en waar nodig bijgesteld.

P-3: De security/privacy aspecten zijn in de beheerprocessen van de organisatie in OPZET, BESTAAN en WERKING aantoonbaar geborgd; denk hierbij aan de IV/IT beheerprocessen zoals incident-, wijzigingen-, configuratie/certificaat-, IV/IT-architectuur-, ontwikkel- en release managent, inkoop processen producten/diensten, organisatiebeheer processen zoals organisatiewijzigingen, in-door- en uitstroom processen, toekennen rollen/rechten. De processen worden periodiek

geëvalueerd en het proces van continuous improvement is ingericht en geborgd.

P-4: Het proces security monitoring, incident detectie en opvolging op de digitale infrastructuur is zowel proactief als reactief zowel binnen als buiten de reguliere bedrijfstijden in OPZET, BESTAAN en WERKING geborgd en wordt ondersteund door tooling. De aspecten van het aangesloten zijn op en kunnen verwerken van Threat Intelligence, Community Intelligence, Threat Hunting en Threat Response (vernemen/onderkennen van veranderingen in dreigingslandschap voor de gemeente, het actief monitoren daarop en het kunnen nemen van mitigerende maatregelen) zijn hier integraal onderdeel van. De security monitoring proces wordt periodiek geëvalueerd en het proces van continuous improvement is ingericht en geborgd.

T-1: Ter ondersteuning van de uitvoering van het informatiebeveiligingsbeleid beschikt de organisatie over een ISM systeem; de portefeuillehouder informatiebeveiliging is en voelt zich eigenaar van het systeem en de CISO is houder/beheerder van het systeem. Het ISMS wordt actief gebruikt bij de jaarlijkse bedrijfs- en beleidsplan cyclus en jaarlijkse actualisatie van het informatiebeveiligingsbeleidsplan. De werking en effectiviteit wordt periodiek geëvalueerd en het proces van continuous improvement is ingericht en geborgd.

T-2: De organisatie beschikt over een systeem (of meerdere systemen) voor configuratiebeheer ICT middelen, (technisch) wijzigingenbeheer, certificaatbeheer (hfd ICT

is eigenaar/beheerder) en autorisatiebeheer en (functioneel) wijzigingenbeheer (hfd IM is eigenaar/beheerder). Compliancy beoordelingen vinden plaats op basis van de vastgelegde informatie in het systeem/de systemen. De systemen worden actief gebruik bij de processen waaraan zij ondersteunend zijn en deze processen zijn in OPZET, BESTAAN en WERKING controleerbaar geborgd. De in de systemen opgeslagen gegevens geven derhalve op moment van compliancy meeting een betrouwbaar beeld van de werkelijkheid; de compliancy en kwetsbaarheden meeting ICT infrastructuur gebeurt met de T4 tooling op de "live" ICT infrastructuur en is v.w.b. configuratiebeheer daarmee tevens een extra controle middels op de configuratiebeheer database.

T-3: De organisatie beschikt over een systeem voor (security) incident melding, logging & tracking (workflow management functie) waarmee een audittrail wordt vastgelegd van (wijze van) melding tot en met herstel. Het systeem is gekoppeld aan/ maakt onderdeel uit van service asset & configuratie beheersysteem en/of ISM systeem. Het (security) incident managementproces waaraan het ondersteuning biedt is in OPZET, BESTAAN e, WERKING geborgd. De werking en effectiviteit van het systeem in combinatie met het proces wordt periodiek geëvalueerd en het proces van continuous improvement is ingericht en geborgd.

T-4: De organisatie beschikt over een Security Information en Event Management systeem (SIEM) voor monitoring, analyse en proactieve en reactieve security incident

detectie en compliancy en vulnerabilty scanning. De bijbehorende SIEM/SOC processen zijn in OPZET, BESTAAN en WERKING geborgd en gekoppeld aan de bestuurlijke processen voor security incident opvolging, communicatie en business continuity. De werking en effectiviteit van het stelsel van systemen en processen wordt periodiek geëvalueerd en verantwoord en het proces van continuous improvement is ingericht en geborgd.

Meer Informatie

VNG Realisatie:	www.vngrealisatie.nl
VNG:	www.vng.nl
Digitale Agenda2020:	www.da2020.nl
GGI:	www.da2020.nl/ggi
GEMMA:	www.gemmaonline.nl
IBD:	www.ibdgemeenten.nl
Inkoopvoorwaarden:	www.gibit.nl
Accountmanagers:	www.da2020.nl/contact

Peter Klaver, projectmanager GGI: 06-36341374;
peter.klaver@vng.nl

Jeroen Schuuring, plv projectmanager GGI: 06-15681100;
jeroen.schuuring@vng.nl

Jan van Zessen, projectleider GGI-Veilig: 06-53766890;
jan.vanzessen@vng.nl