Versnellingsplan Informatieveiligheid

Programma Informatievoorziening

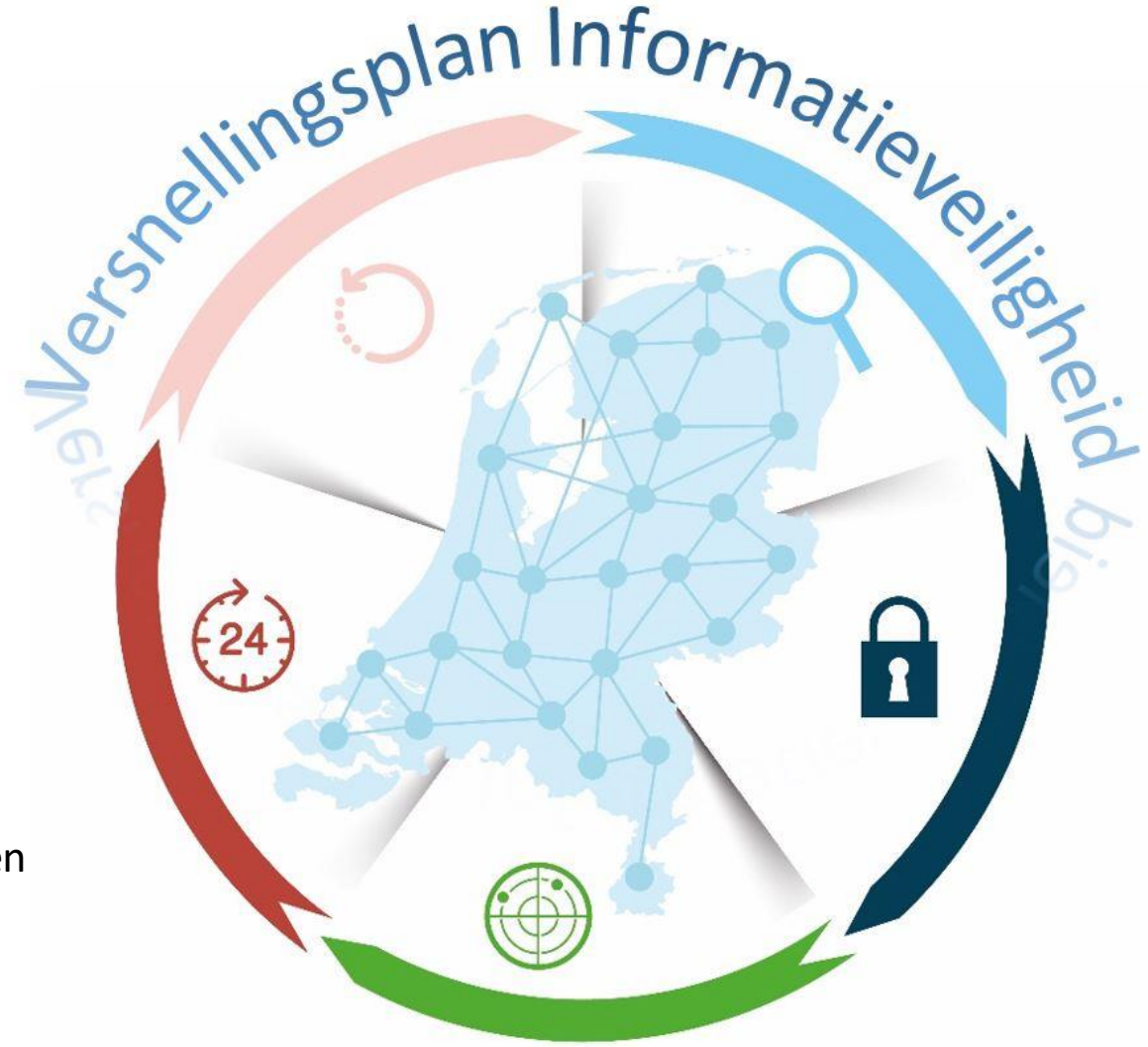
21 september 2021

Aanleiding

- Digitale dreigingen en risico op datalekken blijven toenemen
- Laatste collegiale toetsing informatieveiligheid liet zien dat onderlinge verschillen toenemen en dat er verbetermogelijkheden zijn
- Cybercrisis bij de VNOG of de ‘coronalek’ bij de GGD onderstrepen noodzaak goed inzicht te hebben in (de opslag van) je gegevens én deze goed te beveiligen.
- Landelijk staat cyber hoog op de agenda
- Nationaal Crisisplan-Digitaal (Min.JenV) en het Nationaal Responskader Cyber (Min. BZK).
- **Veiligheidsberaad besluit eind 2020 te doen opdracht te geven voor een landelijk versnellingsplan informatieveiligheid.**
- **De VR-ISAC en het IFV werken dit samen uit in nauwe afstemming met de landelijke vakgroep Informatieveiligheid en de werkgroep digitale ontwrichting onder de vlag van het Programma Informatievoorziening.**

Versnellingsplan Informatieveiligheid – in het kort

- **Het versnellingsplan informatieveiligheid biedt een gefaseerde, samenhangende aanpak voor een extra impuls aan de digitale weerbaarheid van individuele veiligheidsregio's, het IFV én uiteindelijk van Nederland**
- Veiligheidsregio's hebben een inspanningsverplichting om op **1 januari in 2023 te voldoen aan de BIO** als landelijke norm voor informatiebeveiliging.
- Bovendien geven de veiligheidsregio's en het IFV gezamenlijk uitvoering aan de noodzakelijke stappen voor een **optimale aansluiting en informatiepositie in de functionele keten**. Het verkrijgen van een OKTT-status en onderzoek naar een CERT en SOC voor veiligheidsregio's horen hierbij.
- En vergroten we het **bewustzijn over en van** (handelingen met effect op) **informatieveiligheid** bij medewerkers in de veiligheidsregio met onder andere bewustwordingscampagnes.



Zie 13 t/m 17 voor de activiteiten en uitgangspunten per fase

Het Programma Informatievoorziening werkt aan het voorkomen van uitval van de eigen en gezamenlijke informatievoorziening en het voorbereiden op de gevolgen hiervan, en draagt bij aan het beperken van maatschappelijke ontwrichting door digitale verstoringen.

Het versnellingsplan past naadloos in het thema *Continuiteit* van het Programma IV 2020-2025:

Onze maatschappij digitaliseert in hoog tempo en dit brengt, naast kansen, ook nieuwe afhankelijkheden en risico's met zich mee. Van veiligheidsregio's wordt verwacht om samen met andere belanghebbenden te komen tot een veilige en gezonde fysieke leefomgeving. Partners hierbij zijn onder andere gemeenten, politie, provincies, omgevingsdiensten, waterschappen en het Rijk. In de steeds meer gedigitaliseerde wereld van nu is er een wederzijdse afhankelijkheid. Gedeelde data faciliteren deze samenwerking. Bij crisisbeheersing en rampen- en incidentbestrijding kan gedacht worden aan de gevolgen van een grootschalige digitale ontwrichting, een zogenoemde ongekende crisis. Digitale weerbaarheid (ook van de eigen informatievoorziening) is een belangrijk thema op de managementagenda's.

Bij digitale verstoringen wordt onderscheid gemaakt tussen de interne informatievoorziening van de veiligheidsregio's zelf en de crisisbeheersing naar aanleiding van digitale verstoringen.

De afbakening voor het Programma IV betreft de interne informatievoorziening. In het programma is wel aandacht voor de afstemming op de activiteiten die in de crisisbeheersing ondernomen worden. Er is hiervoor een nauwe samenwerking met de werkgroep 'Digitale ontwrichting & Cyber" (opdrachtgever RCDV) waarbij de werkgroep zich vooral op de externe factoren focust; cybergevolgbestrijding en cyberwaakzaamheid. Daarnaast is het mogelijke effect onderkend die de investering in de interne bedrijfsvoering kan hebben op de cybergevolgbestrijding.

Concrete doelen die op dit thema zijn geformuleerd:

- Continuïteit informatievoorziening van de meldkamer op orde (bijdragen i.s.m. LMS);
- Inzicht in kwetsbaarheden eigen informatievoorziening middels een Information Sharing and Analysis Centre (ISAC) om hierop te kunnen anticiperen;
- Werkbare oplossingen ten behoeve van redundantie, het managen van businesscontinuïteit;
- Eigen informatiebeveiliging op orde. Van Basisline Informatiebeveiliging Gemeenten (BIG) naar Baseline Informatiebeveiliging Overheid (BIO);

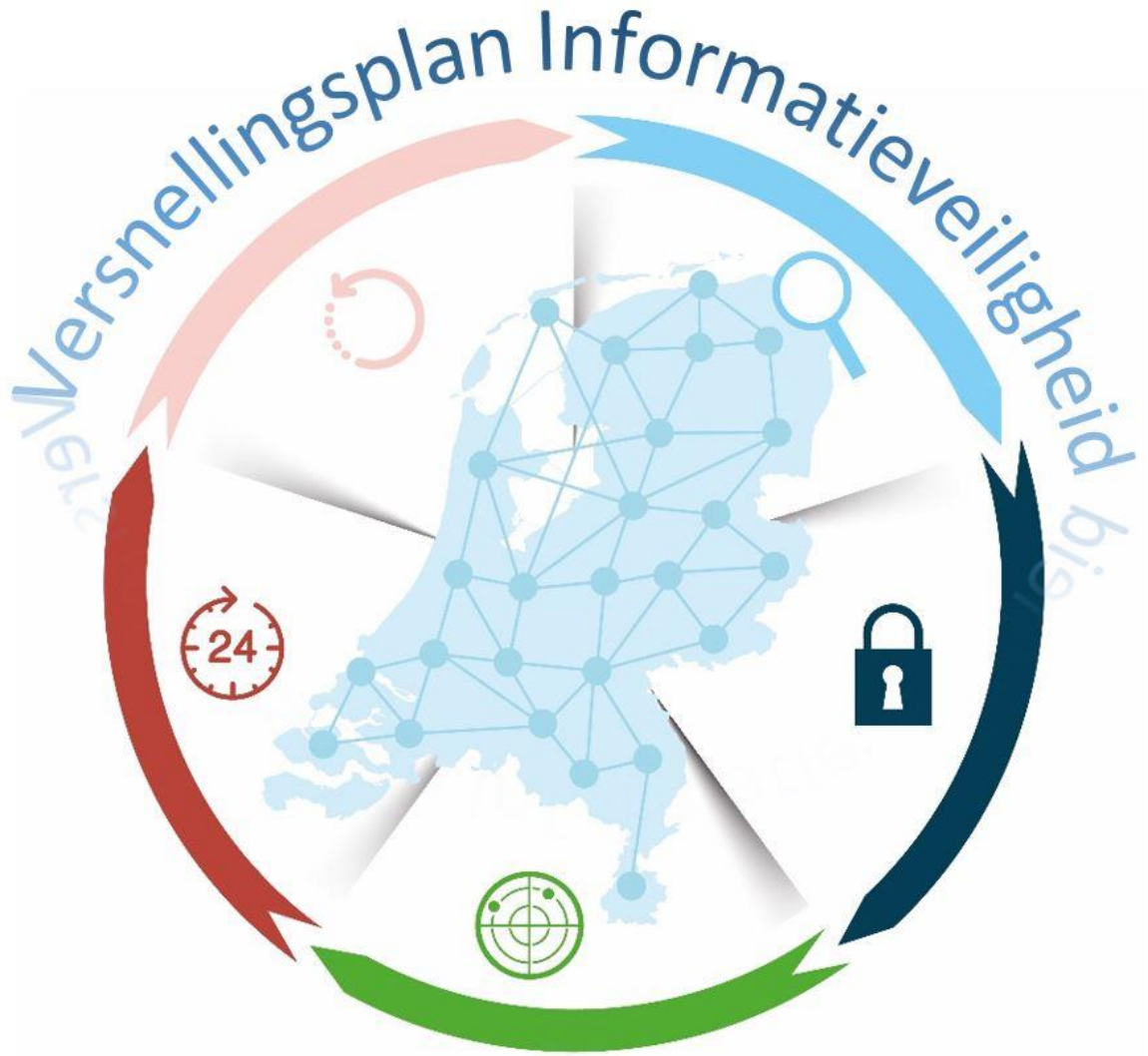
Communicatiedoelen versnellingsplan

- Medewerkers van de veiligheidsregio's, het IFV, het netwerk van het Programma IV en de aanspreekpunten in de regio **informeren** over ontwikkelingen rond het versnellingsplan en inhoudelijke onderwerpen en thema's (kennis).
- Het **bewustzijn** over en van (eigen handelen op) informatieveiligheid **vergroten** (kennis/houding).
- **Samenhang bewaken** en **context bieden.**
- **De weg wijzen.** Zorgen dat de informatie toegankelijk is en men weet welke informatie waar te vinden is.

Boodschap

- **Gezamenlijk hebben we een missie om de digitale weerbaarheid op zowel regionaal niveau als landelijk niveau optimaal vorm te geven en zo bij te dragen aan een veiliger Nederland.**

- Informatieveiligheid is een thema van **álle medewerkers**
- Maak een **stappenplan** om de basis op orde te krijgen en informatieveiligheid op het juiste niveau brengen.
- In veel regio's zijn **(grote) investeringen noodzakelijk.**



Doelgroepen	Middel
Contactpersonen regio	Kick-off sessies, themasessies, digitale inloopsessies?, mail, DSR Vakgroep informatieveiligheid
Directeuren BV/directie VR	Via DBV
IFV werkgroep digitale weerbaarheid, incl. afdeling communicatie IFV	Via programmamanager IV (Guus) en adviseur (Ricardo)
IFV directie	Via manager Dienst informatievoorziening (Frank)
IFV medewerkers	IFV Connect, Yammer
VR medewerkers	Animatie, implementatieloket, bewustwordingscampagnes
Collega's netwerk Programma IV	DSR Programma IV, nieuwsbrief Programma IV
IV-Board, NIM, NICT	Presentatie tijdens reguliere bijeenkomst, mail
Vakgroep Informatieveiligheid	DSR informatieveiligheid, mail, inloopsessie?
Architectuurboard	Presentatie tijdens reguliere bijeenkomst, mail

Communicatiemiddelen algemeen

Het is belangrijk dat iedereen hetzelfde beeld heeft bij het versnellingsplan. Omdat het plan uit veel verschillende onderdelen bestaat, is het risico groot op ruis in de communicatie en verlies van overzicht en samenhang. Eenzelfde 'startbeeld' is wenselijk. Daarnaast goed om tijdens de gehele looptijd breed te blijven communiceren over dit onderwerp.

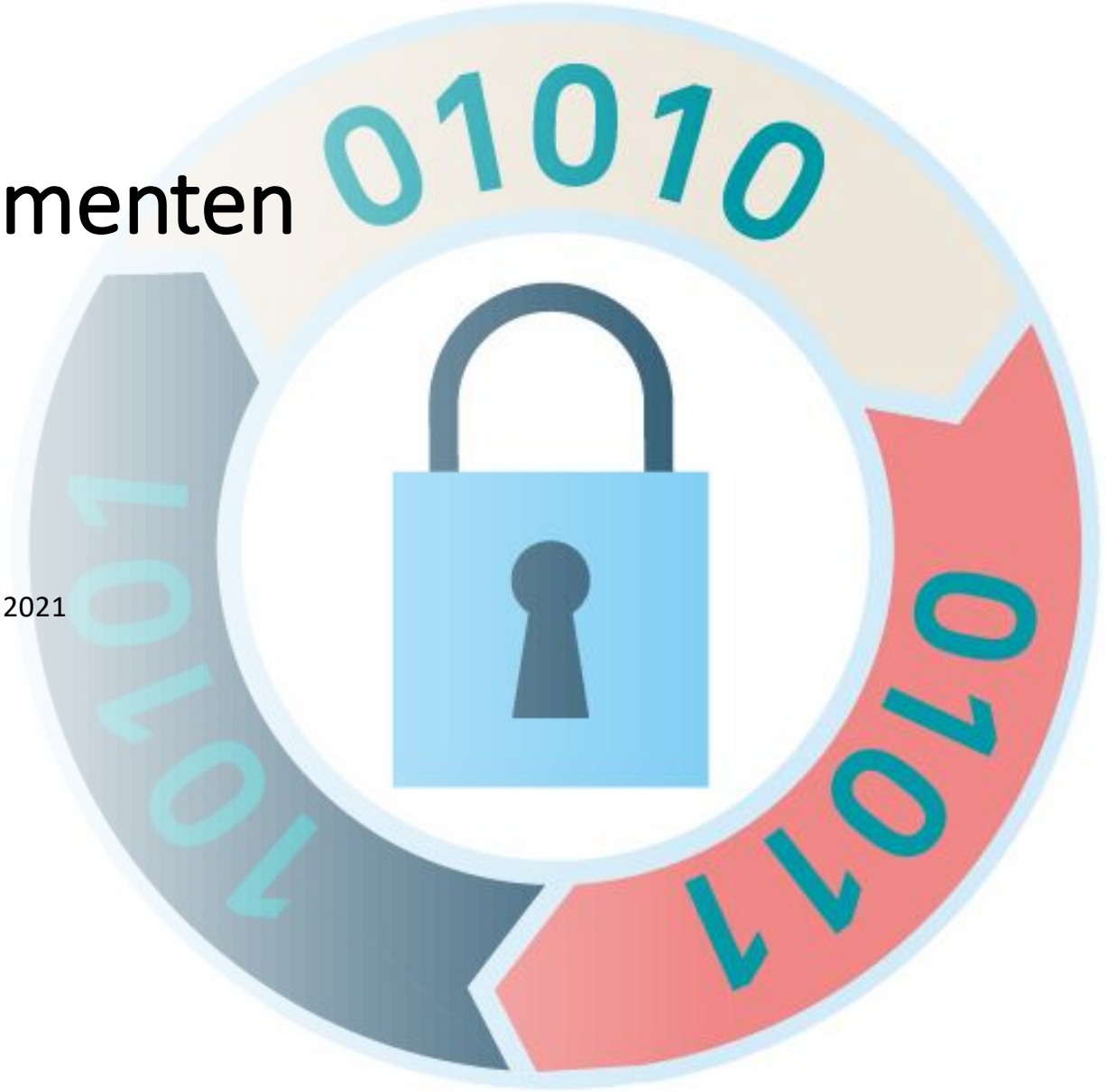
- Een **animatie** die houdbaar is gedurende het hele traject kan voor alle doelgroepen deze belangrijke functie hebben. Ook kan het heel goed worden ingezet als eerste communicatiemiddel in een bewustwordingscampagne.
- **Filmpjes** a la dit voorbeeld kunnen hetzelfde doel dienen en mogelijk worden ingezet rond de inrichting van een SOC/CERT.
- Voor de bewustwordingscampagnes kunnen we vanuit het Programma IV landelijk content ontwikkelen die regio's kunnen hergebruiken of delen. Denk hierbij aan het schrijven en delen van **artikelen** over informatieveiligheid of het maken van **podcasts** over dit onderwerp. Daarnaast verzamelen we voorbeelden van bewustwordingscampagnes voor een toolkit.

- De tweede editie van het Platform voor crisismanagement van het IFV stond in het teken van digitale weerbaarheid. Hier kunnen we nog artikelen uit delen.
- Ook kunnen we de expertise van de VR-ISAC benutten om **presentaties (op verzoek)** te geven, bijvoorbeeld **over lessons learned bij crises**, zoals de VNOG hack.
- **Oefenen/leerarena's** zijn ook goede middelen om tijdens de bewustwordingscampagne in te zetten.

Planning/communicatiemomenten

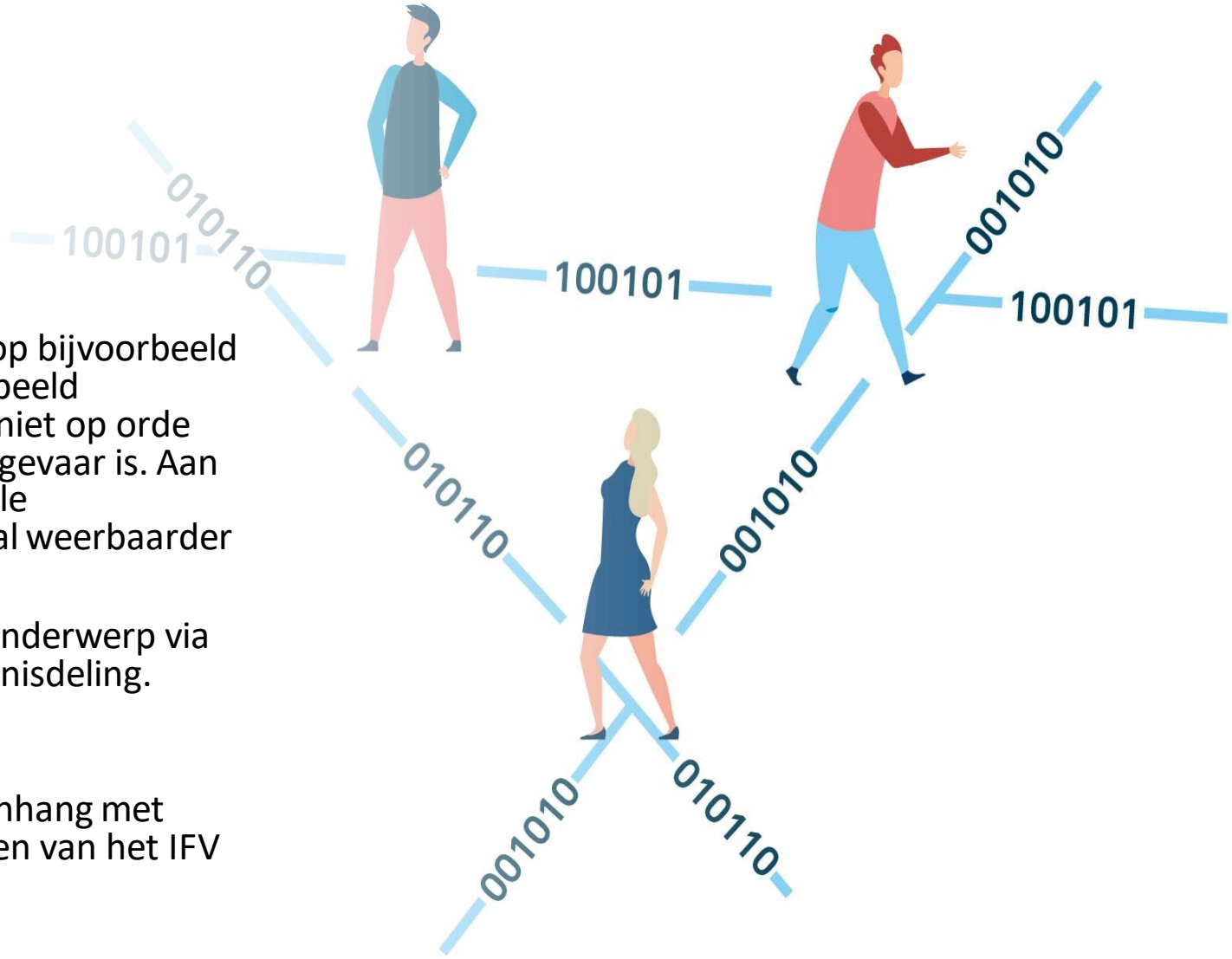
Omdat de fasen in het versnellingsplan parallel aan elkaar lopen (zie slide 18) is een faseovergang geen duidelijk communicatiemoment. Wél zijn er een aantal andere momenten te markeren, die gedurende de looptijd verder kunnen worden ingevuld:

• Kick-off sessies voor de regionale contactpersonen	• Zomer 2021
• Terugblik kick-off sessies	• Eind september 2021
• Start invullen van regionale voortgangsrapportages	• Begin oktober
• Start van bewustwordingcampagne(s)	• Najaar 2021
• Verkrijgen van de OKTT status voor de VR-ISAC	• Sept/nov
• Nieuwsbrief Programma IV Instelling SOC en CERT	• ? 2022
• Brandweerevent	• 7, 8 oktober
• IV-event	• 30 november
• Tussenstand BIO (interne berichtgeving)	• Voorjaar 2021
• Streven behaald	• 30 juni 2022
• Einde versnellingsplan	• 1 januari 2023



Aandachtspunten

- We communiceren naar buiten toe vooral reactief, op bijvoorbeeld vragen. We zijn enigszins terughoudend omdat het beeld voorkomen moet worden dat veiligheidsregio's het niet op orde hebben en daarmee de veiligheid voor de burger in gevaar is. Aan de andere kant liften we mee op de beweging die alle overheidsorganisaties momenteel maken om digitaal weerbaarder te worden. We zijn geen uitzondering.
- Ook kunnen nieuwsberichten en artikelen over dit onderwerp via deze kanalen worden verspreid in het kader van kennisdeling. Indien relevant worden deze ook geplaatst in het implementatieloket op IFV.nl.
- Voor het programmateam is het belangrijk de samenhang met andere activiteiten die onder verschillende afdelingen van het IFV plaatsvinden te bewaken.



Contact

Openbare informatie op het implementatieloket IFV

Hier vind je onder andere ook veelgestelde vragen en antwoorden en links naar interessante handreikingen en documenten.

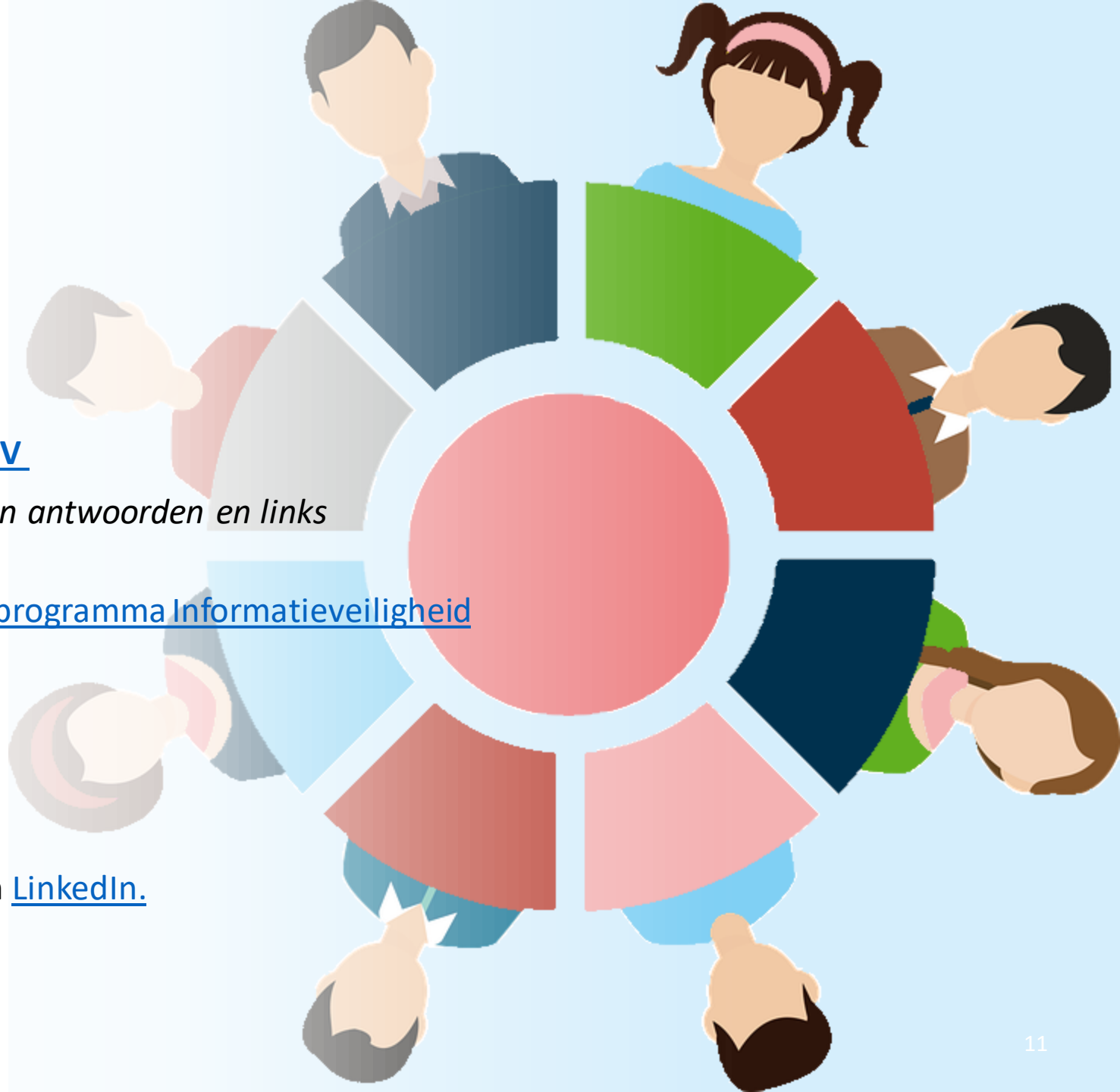
Samenwerkingsomgeving SharePoint: Versnellingsprogramma Informatieveiligheid

Vragen? programmaiv@ifv.nl

Achtergrondinfo:

Programma Informatievoorziening brandweer.nl en LinkedIn.

Abonneer je op onze nieuwsbrieven



Bijlagen

Fase 1 Basis op orde (2021-2023)

Landelijke activiteiten (vanuit Programma IV i.s.m. VR-ISAC):

- **Visiedocumenten** en uitgangspunten opstellen en communiceren (2021)
- **Toolkit BIO** met handreikingen/zelftests e.d. beschikbaar stellen via IFV.nl (vertrouwelijke documenten alleen met de contactpersonen van de regio).
- Front office voor vragen inrichten en uitvoeren (**Implementatieloket**) (2021)
- Verzamelen van regionale **voortgangsinformatie** voor POI/RCDV (najaar 2021)
- **Staat van informatieveiligheid** uitvoeren (2022)
- **Tools voor bewustwordingcampagnes** (informatieveilig zijn en blijven + cyberweerbaar worden en blijven) beschikbaar stellen en landelijke awareness-activiteiten ontplooien.
- **Ontwikkelen security architectuur** (i.s.m. landelijke Architectuurboard en vakgroep informatieveiligheid) 2022
- Onderzoek **Herziening softwarecatalogus** (idem en VNG) eind 2021
- **BIV-classificaties uitwerken** (doorontwikkeling informatieplattegrond)
- **Communicatie** (doorlopend)

Regionale activiteiten (door veiligheidsregio's zelf):

- Opstellen van een **implementatieplan** met prioriteiten, een planning en budget
- Leveren van **voortgangsinformatie**
- **Bewustwordingscampagnes** in de regio's voeren (bewustwording ELO/les- en leerstof)
- **Implementatie van de BIO**

Basis op orde - uitgangspunten

BIO is de norm

Regio's en IFV voldoen aan de wettelijk vastgestelde Baseline Informatiebeveiliging Overheid (BIO).

Regio's + IFV zelf verantwoordelijk

Het op orde brengen van een basisniveau van informatie-beveiliging is een verantwoordelijkheid van regio's en het IFV zelf.

Commitment

Collectieve belangen en afhankelijkheden nemen toe. Daarom verbinden het IFV en alle regio's zich aan het programma.

Landelijke activiteiten

Het Programma IV voorziet in de dekking van kosten voor landelijke ontwikkel-activiteiten.

Regionale capaciteit

Regio's voorzien zelf in het budget en de capaciteit die nodig is voor de uitvoering van het versnellings-programma in hun organisatie.

Samenhang

Het programma geeft invulling aan het *Programma IV – Continuïteit* en volgt het bestuurlijk routeboek Digitale Ontwrichting en het Nationaal Crisisplan Digitaal.

Fase 2: Vergroten cyberweerbaarheid (2021-2023)

Landelijke activiteiten (vanuit Programma IV i.s.m. VR-ISAC):

- **Haalbaarheidsstudie CERT en SOC** voor veiligheidsregio's (2021)
- Definitie aansluitvoorwaarden (2022)
- **Waakvlamfunctie inrichten** (2021)
- **Tijdelijke SOC-voorziening** voor beheerde voorzieningen (2021-2022)
- **OKTT-status** VR-ISAC (tussenstap naar CERT/SOC, 2021)
- **Inrichten en operationaliseren van een SOC** (Security Operations Centre) **en een CERT** (Cyber Emergency Response Team). (2022-2023)
- **Opschaling en samenwerking SOC/CERT/ISAC oefenen en trainen (2021-2022)**
- **Oefenen** (intern-netwerk-keten, 2023)

Regionale activiteiten (door veiligheidsregio's zelf):

- **Implementatie van de BIO**
- Leveren van **voortgangsinformatie**
- **Bewustwordingscampagnes i**n de regio's voeren
- **Inrichten en operationaliseren van een SOC een CERT**
- **Opschaling en samenwerking SOC/CERT/ISAC oefenen en trainen**
- **Oefenen** (intern-netwerk-keten)

Cyberweerbaarheid - uitgangspunten

Randvoorwaarde

De basis moet op orde zijn om te kunnen starten met de ontwikkeling van cyber-weerbaarheid.

Waakzaam

Informatie en infrastructuur worden 24/7 bewaakt in een landelijk SOC, die ook de eerstelijns respons levert bij beveiligings-incidenten.

Slagvaardig

Een landelijk cyber-responsteam(CERT) wordt geactiveerd wanneer een regio, IFV, of landelijke voorziening wordt getroffen door een majeur incident of cybercrisis.

Collectief

De ontwikkeling van het SOC en CERT is een collectieve voorziening voor en van 25 regio's en het IFV samen.

Aansluiten

Aansluiten op het NCSC Nationaal Detectie Netwerk verloopt via het digitale verkeersplein.

Netwerk-samenwerking

Het programma biedt de basis voor structurele samenwerking met respons- netwerken van medeoverheden en keten- en samenwerkings-partners.

Fase 3: Borging (parallel aan fase 1 en 2)

Landelijke activiteiten (vanuit Programma IV i.s.m. VR-ISAC):

- Ontwerp **governance model** (2021)
- Onderzoek **subsidiemogelijkheden** (2021)
- Ontwerp **juridische kaders**
- Ontwerp **auditsystematiek**
- **Audits** (2024)

Regionale activiteiten (door veiligheidsregio's zelf):

- **Audits** (2024)

Borging - uitgangspunten

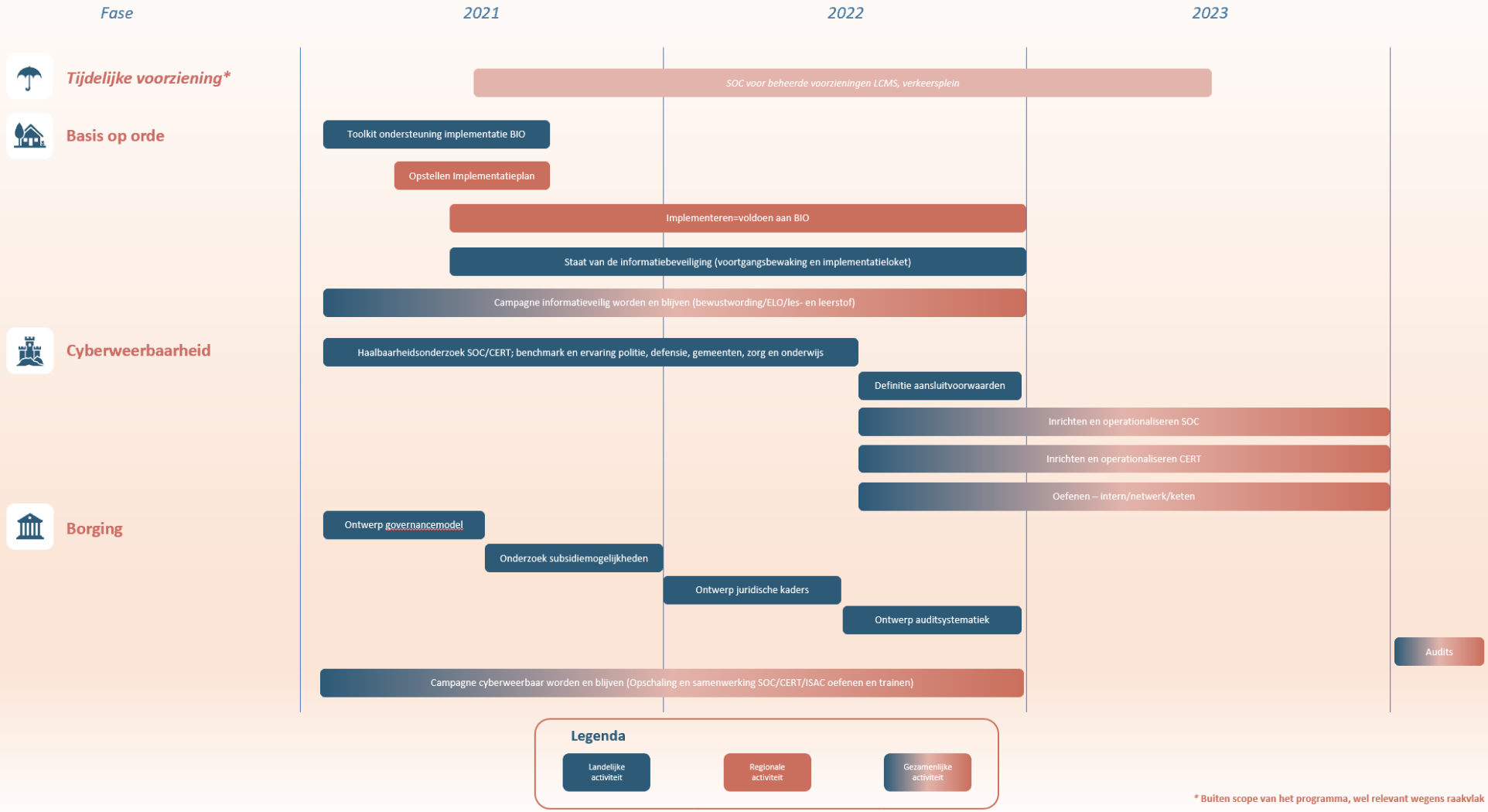
Als de basis op orde is en de cyberweerbaarheid is op peil, dan is het zaak om op niveau te blijven. Voor de borging van het normniveau en de cyberweerbaarheid zijn dit de uitgangspunten:

- Veiligheidsregio's en het IFV hebben, naast technische maatregelen, organisatorische maatregelen getroffen om informatieveiligheid en cyberweerbaarheid structureel in hun **governance** en PDCA-cyclus te verankeren;
- Het programma zal voorstellen uitwerken voor een **audit**systematiek op basis waarvan het normniveau collegiaal of professioneel kan worden getoetst;

Voor de inrichting van een sectorale SOC en/of CERT zijn Rijksbijdragen of **subsidies** niet ongebruikelijk, deze mogelijkheden zullen in het programma nader worden onderzocht;

Voor de onderlinge verhoudingen (en verantwoordelijkheden) tussen het cybersecuritynetwerk, het IFV en de veiligheidsregio's zullen heldere **juridische kaders** geschetst worden.

Plan van aanpak versnellingsprogramma Informatieveiligheid



Een samenwerking van: