# Versnellingsprogramma Informatieveiligheid

Samen slimmer met data

VR ISAC

Veiligheidsregio's werken samen aan een toekomstbestendige digitale informatievoorziening en **robuuste ICT-infrastructuur**. Dit stelt veiligheidsregio's in staat om te beschikken over alle informatie die voor risicobeheersing, crisisbeheersing en incidentbestrijding cruciaal is. Het is van groot belang dat deze informatie tijdig beschikbaar is, betrouwbaar is en dat informatie niet in verkeerde handen valt. Het versnellingsprogramma informatieveiligheid biedt hiervoor een gefaseerde aanpak.

**Fase 1** van het versnellingsprogramma informatieveiligheid heeft tot doel om veiligheidsregio's op het gebied van informatie-beveiliging te helpen om **de basis op orde** te krijgen. Het programma ondersteunt daarin door te voorzien in een gestructureerde aanpak, heldere uitgangspunten en een toolkit.

**Fase 2** richt zich op het vergroten van de **cyberweerbaarheid** van veiligheidsregio's. Deze weerbaarheid wordt concreet gemaakt door het inrichten van een landelijk SOC (Security Operations Centre) en een landelijk CERT (Cyber Emergency Response Team). Samen met de VR-ISAC vormt dit het cybersecurity-netwerk, dat aan de hand van actuele dreigingsinformatie cyberincidenten voorkomt of sneller oplost en adequaat opschaalt als zich een cybercrisis voordoet. Het cybersecurity-netwerk werkt samen met ketenpartners (bijv. NCSC, politie) en netwerkpartners (bijv. IBD, Z-CERT) en kan veiligheidsregio's adviseren in geval van digitale ontwrichting.

**Fase 3** loopt parallel met fase 1 en 2 en voorziet in **borging** met governance, audits, subsidieonderzoek en juridische kaders.

## 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

Ketenverantwoorde-lijkheden en -afhankelijkheden nemen toe. Daarom verbinden het IFV en alle regio's zich solidair aan dit 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.

## 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.

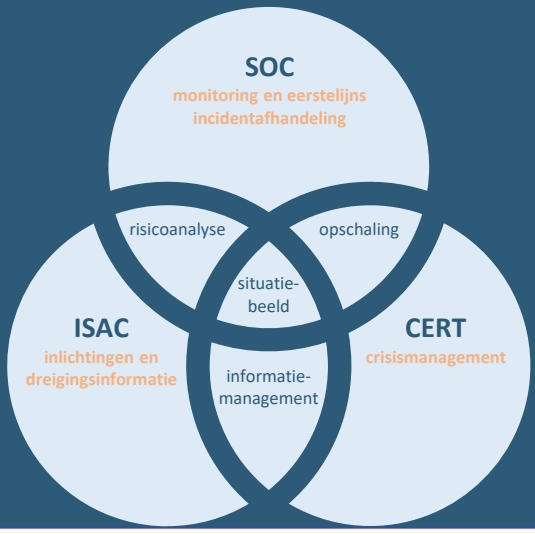
### Aansluiten

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.

## Cybersecurity Netwerk




## 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.