

# Veiligheidsregio's en digitale veiligheid

Op welke manieren kan een veiligheidsregio bijdragen aan digitale veiligheid? Op basis van literatuuronderzoek, interviews met experts en desk research, zijn dit onze aanbevelingen.

## ZEKER DOEN

### Cybergevolgbestrijding

De effecten bestrijden van een incident met een digitale oorzaak.



### Risico's in kaart brengen

Risico-analyse van digitale verstoringen met maatschappelijke impact.



### Cybercrisismanagement

Ondersteuning van organisaties die getroffen zijn door cyberincident, in ieder geval bij gemeenten.



## AAN TE RADEN OM TE DOEN

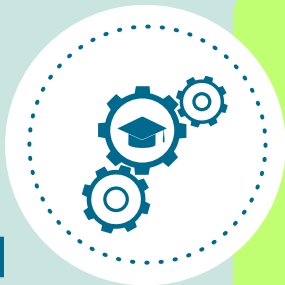
### Platform

Kennis vergaren en delen, netwerk opzetten, partners koppelen bij incidenten.



### OTO

Opleiden en trainen van crisisfunctionarissen en CISO's, cyberoefeningen (laten) organiseren.



## MISSCHIEN DOEN

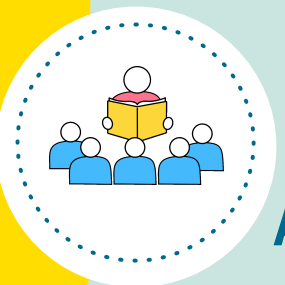
### Deelname NRN

Als veiligheidsregio's een eigen CERT hebben kan die deelnemen aan het Nationaal Respons Netwerk.



### Voorlichting

Over digitale risico's. Mogelijk bij partners. Misschien bij burgers,



## AAN TE RADEN OM NIET DOEN

### Vergunningen controleren

Cyber meenemen bij vergunningsplichtige activiteiten. Wel nodig, maar niet voor veiligheidsregio.



## NIET DOEN

### Digitale brandweer

Incident respons vanuit de veiligheidsregio.



**Scherp**