# Een zichtbaar betrouwbaar, weerbaar en integer MKB – zo bereik je dat

## Weerbaar tegen digitale ondermijning met het CYRA-normenkader "NDO"

Factsheet Normenkader Digitale Ondermijning ("NDO")
Versie 2.0. | november 2024

Digitale ondermijning kent een breed scala van aanvalsmethoden en technieken die kwaadwillenden gebruiken om schade aan te richten, gegevens te stelen, systemen te compromitteren en andere illegale activiteiten uit te voeren in de digitale wereld. Uit politieonderzoeken blijkt dat bedrijven die geïnfiltreerd zijn, dan wel uit eigen wil betrokken zijn bij criminele activiteiten, hun preventieve cybermaatregelen ofwel cyberhygiëne niet op orde hadden. Met het Normenkader Digitale Ondermijning krijg je meer grip op bescherming van informatie tegen ondermijnende activiteiten.

## Achtergrond

Ondermijning is te omschrijven als de schadelijke maatschappelijke effecten van georganiseerde misdaad. Zij tast daarmee de beoogde en legale werking van de maatschappij aan. Waar kwaadwillenden (beïnvloed door criminele organisaties) gebruik maken van de digitale infrastructuur, komt men op het gebied van de digitale ondermijning.

Kenmerkend voor veel ondermijnende criminaliteit is dat mensen binnen een bedrijf ('insiders') worden ingezet om de (digitale) infrastructuur te kunnen gebruiken. De modus operandi van de georganiseerde misdaad en de bijbehorende drugsimport maakt bijvoorbeeld exclusief gebruik van insiders. De rol van deze insiders is de basis voor de uitwerking van de controls binnen het Normenkader Digitale Ondermijning. In deze publicatie worden de ontwikkelde controls toegelicht.

## Doelgroep

Deze factsheet is geschreven voor personen die binnen hun organisatie een rol hebben bij het adviseren van MKB-ers in de bescherming van hun informatie en infrastructuur tegen misbruik door criminelen. Het Normenkader Digitale Ondermijning is ontwikkeld voor alle bedrijven die weerbaar willen zijn tegen digitale ondermijning.

## Partners

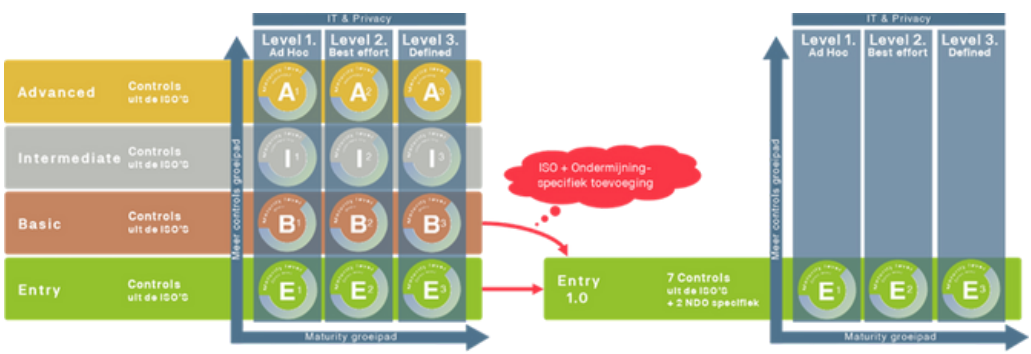
Het Normenkader Digitale Ondermijning is ontwikkeld samen met de publieke partners van de Stichting FERM, waaronder de politie en de douane.

# Opbouw van de controls

Het Normenkader Digitale Ondermijning is een set van 9 controls waarvan in de praktijk wordt verondersteld dat deze effectief zijn tegen ondermijning. De controls zijn gebaseerd op het CYRA-model. CYRA staat voor “CYberRAting”. Het CYRA-model heeft tot doel het (cyber)weerbaard maken van organisaties. Dit kan een opmaat zijn naar ISO 27001 certificering.


Met CYRA kan je een deelcertificaat halen, waarmee je aan je klanten kan aantonen wat je doet op het vlak van cyberweerbaarheid. CYRA is voor elke ondernemer in Nederland als standaard bereikbaar en met name geschikt voor kleinere bedrijven.

Het bestaande framework CYRA is nu uitgebreid met een set extra controls om de weerbaarheid tegen specifiek digitale ondermijning te vergroten. De controls hebben voornamelijk betrekking op het beperken van het zogenaamde insider risk. Dit is het risico dat mensen werkzaam binnen de organisatie al dan niet bewust informatie (door)geven die door criminelen gebruikt wordt. Dit risico wordt beperkt door enerzijds ondermijning-specifieke toevoegingen op bestaande CYRA-controls (add-ons) op te nemen, en anderzijds door aan CYRA nieuwe specifieke ondermijningscontrols toe te voegen (extensions).



# Overzicht van de controls

**Organisatie**

Beleidsregels voor informatiebeveiliging en privacy
- *Add-on*: Beleidsregels over digitale ondermijning

Informatie en analyse over dreigingen
- *Add-on*: Dreigingsinformatie/-analyse over 'insider threat'

Inventarisatie van informatie en andere samenhangende bedrijfsmiddelen
- *Add-on*: Bedrijfsmiddelen vanuit het oogpunt van 'insider threat'

Classificatie van informatie
- *Add-on*: Koppeling met vertrouwelijkheid van informatie something

**Personeel**

Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
- *Add-on*: Herkennen van ondermijning

**Techniek**

'User endpoint devices'
- *Add-on*: Maatregelen omtrent privé en zakelijk gebruik

Genereren, bewaren en beoordelen
- *Add-on*: Specifieke instellingen en controle van logs

**Nieuw: Ondermijning specifiek**
- Meldpunt Ondermijning
- Screening van personeel

**Bruikbaar en begrijpelijk: uit de praktijk**

Het Normenkader kent beheersmaatregelen die door elk bedrijf kunnen worden ingezet om minder vatbaar te zijn voor digitale ondermijning. Gedurende de ontwikkeling van deze set controls heeft een pilot plaatsgevonden om de beheersmaatregelen op bruikbaarheid en begrijpelijkheid te toetsen. Uit deze praktijktoets is gebleken dat met de nieuwe beheersmaatregelen een flinke stap gezet kan worden in het digitaal weerbaar worden als MKB.

**Weerbaar en betrouwbaar MKB**

Het gebruik van het Normenkader Digitale Ondermijning is net als het gebruik van de CYRA controls vrijblijvend. Je start met de self-assessment om het niveau te toetsen. Daarbij kies je voor een van de standaard-treden van CYRA, zoals Entry of Basic, en voor het nieuwe Normenkader Digitale Ondermijning. Zodra je als bedrijf je gewenste niveau zelf hebt getoetst en denkt klaar te zijn voor toetsing, kun je de audit aanvragen.

**Het certificaat**

Wanneer je als bedrijf een audit aanvraagt en succesvol afrondt, ontvang je een certificaat. Omdat je als bedrijf ook het CYRA-niveau laat toetsen, krijg je een certificaat voor het CYRA-niveau met de graad van volwassenheid, én, daarbij als toevoeging het behalen van het Normenkader Digitale Ondermijning. Met dit certificaat kan een bedrijf aantonen niet alleen alert te zijn op mogelijke ondermijnende activiteiten, maar daar ook specifieke maatregelen op te hebben getroffen. De geldigheidsduur van de toevoeging is gelijk aan die van het CYRA-certificaat, namelijk 3 jaar.

**Meer informatie**

Kijk voor meer informatie over het CYRA model en het Normenkader Digitale Ondermijning op https://cyberrating.nl/digitale-ondermijning/

**UITGAVE**
Stichting FERM
Wilhelminakade 909
World Port Center
3072 AP Rotterdam

**Meer informatie**
https://cyberrating.nl/digitale-ondermijning/
November 2024