Round Table Information Security

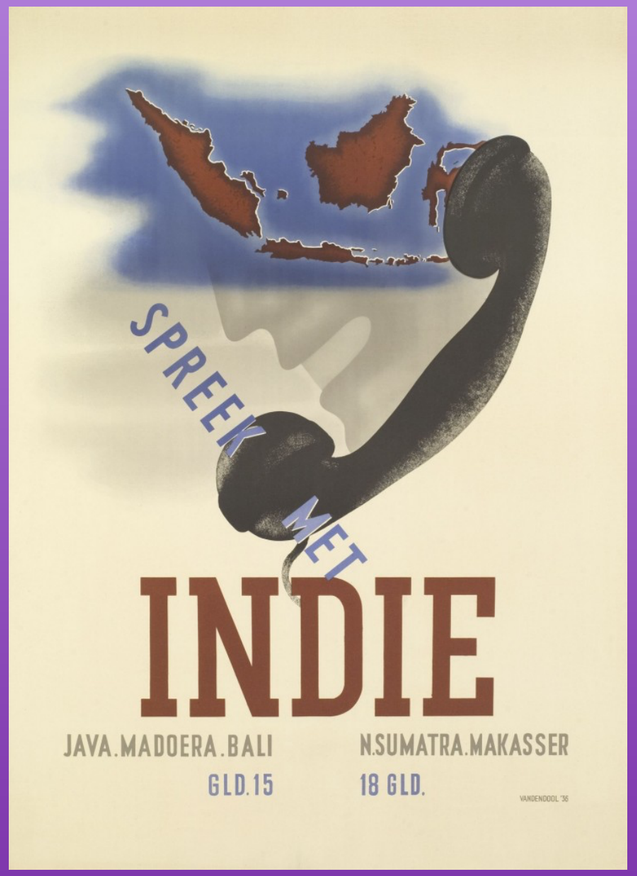
Tijd voor een CISO !

Radio Kootwijk, 29 april 2022

In Audit
Information Security

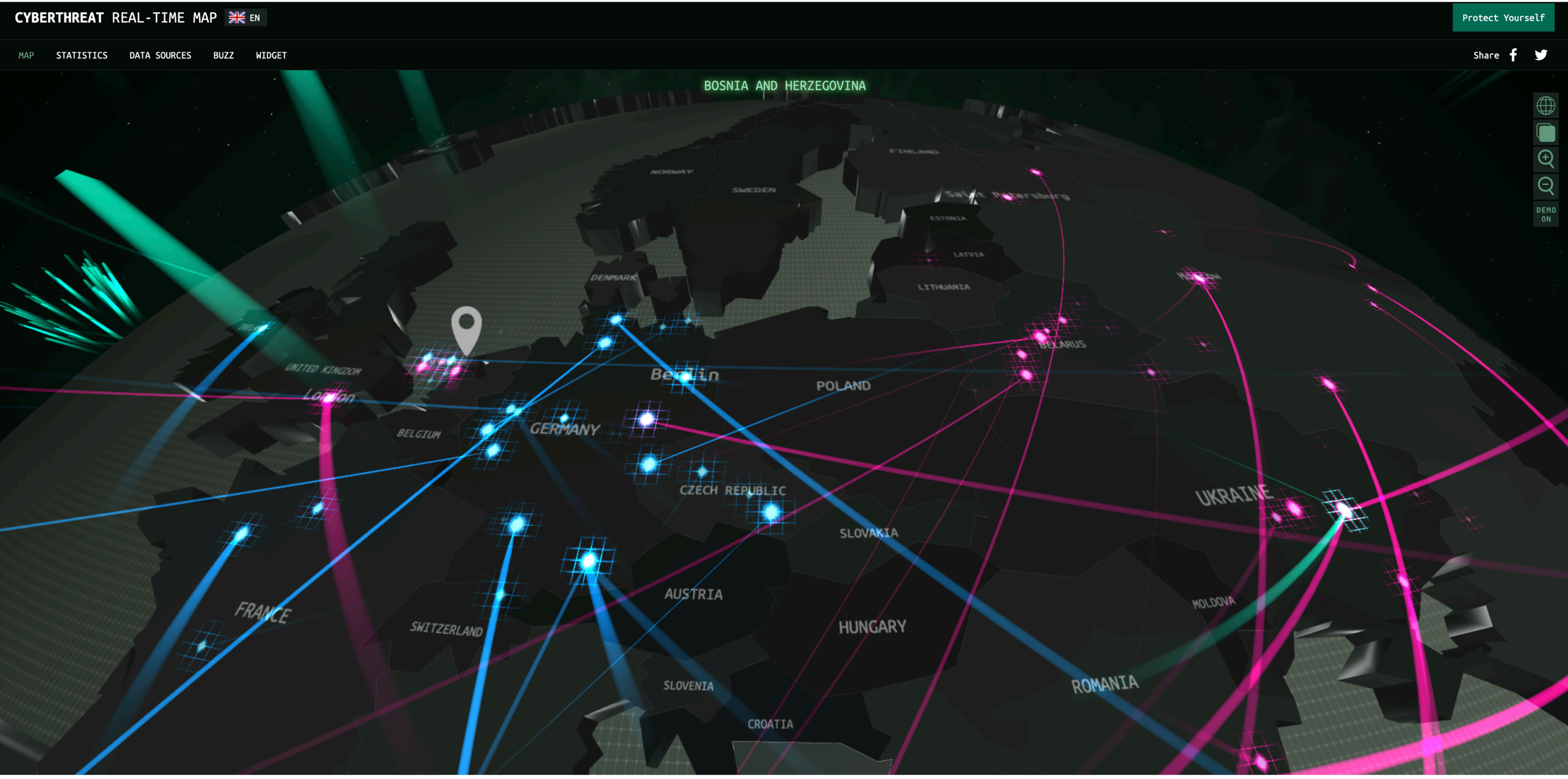
Op 7 januari 1929 stelde koningin-moeder Emma de radio-telefoonverbinding met Nederlands-Indië officieel in gebruik. Dat gebeurde met de legendarische woorden:
‘Hallo Bandoeng, hallo Bandoeng hoort u mij?’

Nu kon het Nederlandse publiek met Nederlands-Indië bellen.



InAudit Information Security BV

Shared Service Centre voor Informatiebeveiliging

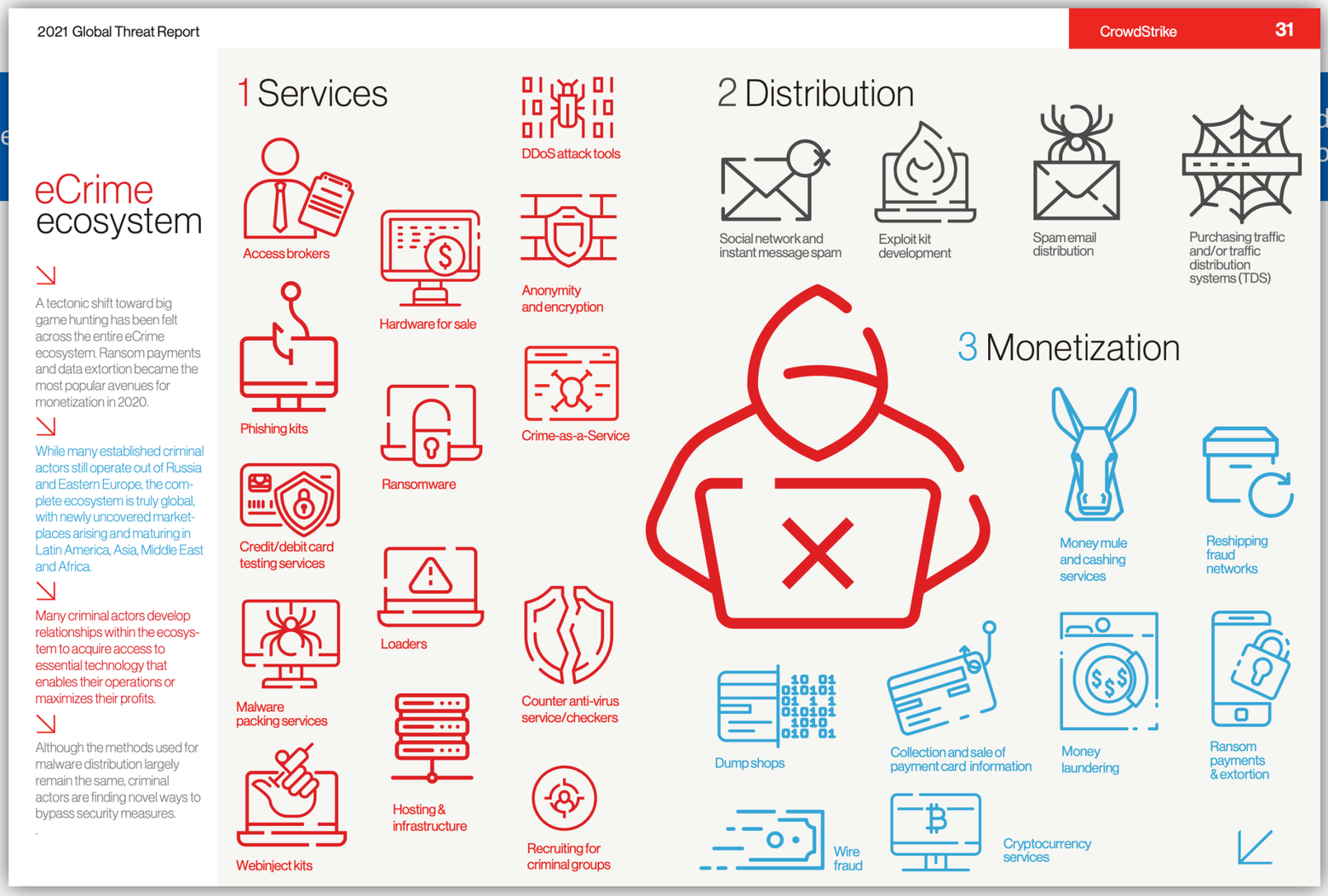


https://cybermap.kaspersky.com

Cyber kill chain

Er zit handel in iedere fase

Reconnaissance → We… → …d and …ol → Actions on objectives



Cyberellende, hoe dan?

1) Gebrek aan beleid en inzicht
2) Verlies van laptops, telefoons, USB-sticks etc
3) “Pathetic Passwords”
4) Verzuim om de computers te “locken”
5) (vreemde) USB-sticks
6) Public Wifi en Sharing Wifi
7) IoT devices
8) Phishing luck
9) “Being social”

1) Geen (offline) back-up of nooit getest
2) Geen draaiboek en/of fallback scenario’s
3) Geen inzicht in de infrastructuur
4) Geen training, geen kennis of ervaring

Wat maakt het een ramp?

CYBER SECURITY

Wat weet u ervan ?

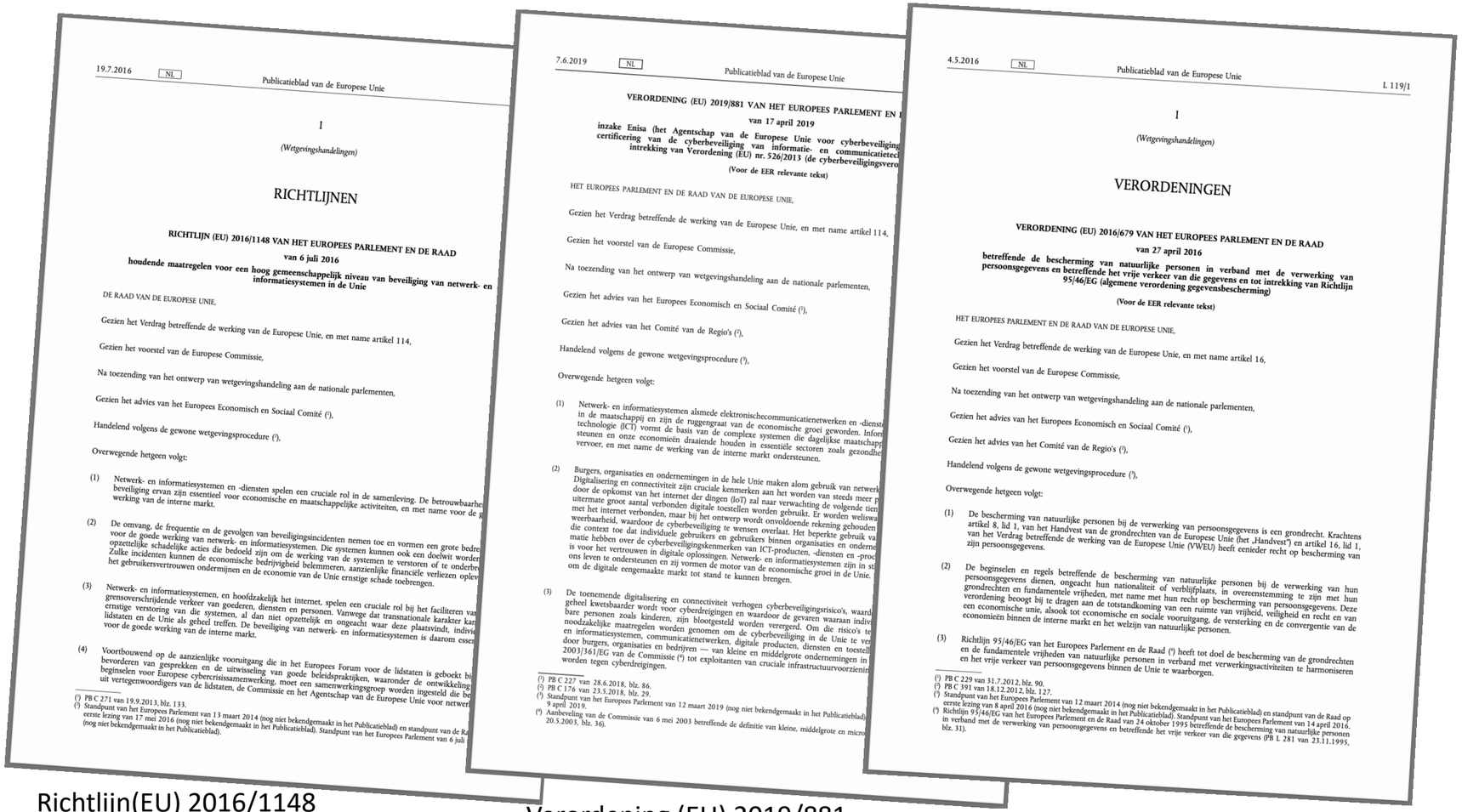
…

Informatiebeveiliging is niet alleen cybersecurity

Cybersecurity als onderdeel van risicomanagement

Maar wel een onderdeel dat specifieke competenties vergt

Europese wet- en regelgeving



19.7.2016 NL Publicatieblad van de Europese Unie

I

(Wetgevingshandelingen)

RICHTLIJNEN

RICHTLIJN (EU) 2016/1148 VAN HET EUROPEES PARLEMENT EN DE RAAD

van 6 juli 2016

houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 114,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Gezien het advies van het Europees Economisch en Sociaal Comité (1),

Handelend volgens de gewone wetgevingsprocedure (2),

Overwegende hetgeen volgt:

(1) Netwerk- en informatiesystemen en -diensten spelen een cruciale rol in de samenleving. De betrouwbaarhe beveiliging ervan zijn essentieel voor economische en maatschappelijke activiteiten, en met name voor de g werking van de interne markt.

(2) De omvang, de frequentie en de gevolgen van beveiligingsincidenten nemen toe en vormen een grote bedre voor de goede werking van netwerk- en informatiesystemen. Die systemen kunnen ook een doelwit worden opzettelijke schadelijke acties die bedoeld zijn om de werking van de systemen te verstoren of te onderbr Zulke incidenten kunnen de economische bedrijvigheid belemmeren, aanzienlijke financiële verliezen oplev het gebruikersvertrouwen ondermijnen en de economie van de Unie ernstige schade toebrengen.

(3) Netwerk- en informatiesystemen, en hoofdzakelijk het internet, spelen een cruciale rol bij het faciliteren va grensoverschrijdende verkeer van goederen, diensten en personen. Vanwege dat transnationale karakter kar ernstige verstoring van die systemen, al dan niet opzettelijk en ongeacht waar deze plaatsvindt, indivi lidstaten en de Unie als geheel treffen. De beveiliging van netwerk- en informatiesystemen is daarom esse voor de goede werking van de interne markt.

(4) Voorbouwend op de aanzienlijke vooruitgang die in het Europees Forum voor de lidstaten is geboekt bi bevorderen van gesprekken en de uitwisseling van goede beleidspraktijken, waaronder de ontwikkeling beginselen voor Europese cybercrisissamenwerking, moet een samenwerkingsgroep worden ingesteld die be uit vertegenwoordigers van de lidstaten, de Commissie en het Agentschap van de Europese Unie voor netwer

(1) PB C 271 van 19.9.2013, blz. 133.
(2) Standpunt van het Europees Parlement van 13 maart 2014 (nog niet bekendgemaakt in het Publicatieblad) en standpunt van de R eerste lezing van 17 mei 2016 (nog niet bekendgemaakt in het Publicatieblad). Standpunt van het Europees Parlement van 6 juli (nog niet bekendgemaakt in het Publicatieblad).

7.6.2019 NL Publicatieblad van de Europese Unie

VERORDENING (EU) 2019/881 VAN HET EUROPEES PARLEMENT EN

van 17 april 2019

inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging certificering van de cyberbeveiliging van informatie- en communicatietec intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsvero

(Voor de EER relevante tekst)

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 114,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Gezien het advies van het Europees Economisch en Sociaal Comité (1),

Gezien het advies van het Comité van de Regio's (2),

Handelend volgens de gewone wetgevingsprocedure (3),

Overwegende hetgeen volgt:

(1) Netwerk- en informatiesystemen alsmede elektronischecommunicatienetwerken en -dienst in de maatschappij en zijn de ruggengraat van de economische groei geworden. Infor technologie (ICT) vormt de basis van de complexe systemen die dagelijkse maatschapp steunen en onze economieën draaiende houden in essentiële sectoren zoals gezondhe vervoer, en met name de werking van de interne markt ondersteunen.

(2) Burgers, organisaties en ondernemingen in de hele Unie maken alom gebruik van netwerk Digitalisering en connectiviteit zijn cruciale kenmerken aan het worden van steeds meer p door de opkomst van het internet der dingen (IoT) zal naar verwachting de volgende tien uitermate groot aantal verbonden digitale toestellen worden gebruikt. Er worden weliswa met het internet verbonden, maar bij het ontwerp wordt onvoldoende rekening gehouden weerbaarheid, waardoor de cyberbeveiliging te wensen overlaat. Het beperkte gebruik va die context toe dat individuele gebruikers en gebruikers binnen organisaties en onderne matie hebben over de cyberbeveiligingskenmerken van ICT-producten, -diensten en -proc is voor het vertrouwen in digitale oplossingen. Netwerk- en informatiesystemen zijn in st ons leven te ondersteunen en zij vormen de motor van de economische groei in de Unie. om de digitale eengemaakte markt tot stand te kunnen brengen.

(3) De toenemende digitalisering en connectiviteit verhogen cyberbeveiligingsrisico's, waard geheel kwetsbaarder wordt voor cyberdreigingen en waardoor de gevaren waaraan indiv bare personen zoals kinderen, zijn blootgesteld worden verergerd. Om die risico's te noodzakelijke maatregelen worden genomen om de cyberbeveiliging in de Unie te ver en informatiesystemen, communicatienetwerken, digitale producten, diensten en toestell door burgers, organisaties en bedrijven — van kleine en middelgrote ondernemingen in 2003/361/EG van de Commissie (4) tot exploitanten van cruciale infrastructuurvoorzienir worden tegen cyberdreigingen.

(1) PB C 227 van 28.6.2018, blz. 86.
(2) PB C 176 van 23.5.2018, blz. 29.
(3) Standpunt van het Europees Parlement van 12 maart 2019 (nog niet bekendgemaakt in het Publicatieblad) 9 april 2019.
(4) Aanbeveling van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro 20.5.2003, blz. 36).

4.5.2016 NL Publicatieblad van de Europese Unie L 119/1

I

(Wetgevingshandelingen)

VERORDENINGEN

VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD

van 27 april 2016

betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)

(Voor de EER relevante tekst)

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 16,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Gezien het advies van het Europees Economisch en Sociaal Comité (1),

Gezien het advies van het Comité van de Regio's (2),

Handelend volgens de gewone wetgevingsprocedure (3),

Overwegende hetgeen volgt:

(1) De bescherming van natuurlijke personen bij de verwerking van persoonsgegevens is een grondrecht. Krachtens artikel 8, lid 1, van het Handvest van de grondrechten van de Europese Unie (het „Handvest") en artikel 16, lid 1, van het Verdrag betreffende de werking van de Europese Unie (VWEU) heeft eenieder recht op bescherming van zijn persoonsgegevens.

(2) De beginselen en regels betreffende de bescherming van natuurlijke personen bij de verwerking van hun persoonsgegevens dienen, ongeacht hun nationaliteit of verblijfplaats, in overeenstemming te zijn met hun grondrechten en fundamentele vrijheden, met name met hun recht op bescherming van persoonsgegevens. Deze verordening beoogt bij te dragen aan de totstandkoming van een ruimte van vrijheid, veiligheid en recht en van een economische unie, alsook tot economische en sociale vooruitgang, de versterking en de convergentie van de economieën binnen de interne markt en het welzijn van natuurlijke personen.

(3) Richtlijn 95/46/EG van het Europees Parlement en de Raad (3) heeft tot doel de bescherming van de grondrechten en de fundamentele vrijheden van natuurlijke personen in verband met verwerkingsactiviteiten te harmoniseren en het vrije verkeer van persoonsgegevens binnen de Unie te waarborgen.

(1) PB C 229 van 31.7.2012, blz. 90.
(2) PB C 391 van 18.12.2012, blz. 127.
(3) Standpunt van het Europees Parlement van 12 maart 2014 (nog niet bekendgemaakt in het Publicatieblad). Standpunt van het Europees Parlement van 14 april 2016, eerste lezing van 8 april 2016 (nog niet bekendgemaakt in het Publicatieblad).
(4) Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PB L 281 van 23.11.1995, blz. 31).

Richtlijn(EU) 2016/1148
(NIS Directive)

Verordening (EU) 2019/881
(Cybersecurity Act)

Verordening (EU) 2016/679
(AVG – Algemene Verordening Gegevensbescherming)

Vergelijking Good Practice document DNB met EIOPA guidelines

Nieuws onder de zon ?

Good Practice - Information security 2019/2020

Introduction

This Good Practices document provides the institutions under our supervision with practical guidance on the implementation of control measures to ensure the integrity, continuous availability and security of electronic data processing.

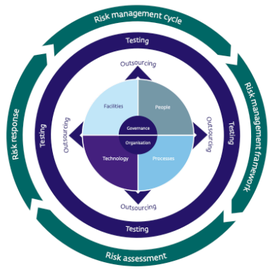
Based on a risk analysis, institutions implement control measures aimed at managing their information security and cybersecurity risks. These control measures should be in line with nature, scale and complexity of the risks associated with the institution's activities and the complexity of its organisational structure. These control measures are not limited to technological solutions (*Technology*), they also address human actions (*People*), *Processes* and *Facilities*.

In addition, institutions assess the design, existence and operating effectiveness of control measures on a regular basis as part of their *Risk management cycle*, in order to deal with constantly changing information security and cyberthreat risks. They improve or replace any control measures that are not effective. Institutions set up their *Governance* and *Organisation* in such a way as to steer this process.

Also, institutions ensure that they are in control of information security and cybersecurity regarding outsourced activities (*Outsourcing*) and that they *Test* their resilience to cyberthreats. This Good Practices document includes the *maturity model* that we use to assess information security and cybersecurity risk management levels at the institutions under our supervision.

Reader's guide

The Good Practices document is based on the following model:



The Good Practices document can be approached from the following two perspectives.

1. As an overview of the relevant control measures for each of the elements in the model, summarised for managers and policymakers.
   The main control measures that are relevant to an institution are explained in brief, with examples.
   The role of management in implementing and monitoring the control measures is also addressed.

2. As a detailed list of control measures, including additional examples.
   There are links to the relevant control measures under each of the elements in the model. For the sake of readability each control measure is listed under one element in the model only, while a control measure may be relevant to multiple elements.

You can access the elements through the links in the Contents tab. There are also separate tabs for the Q&A on Information security and for the maturity model.

EIOPA

EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS AUTHORITY

EIOPA-BoS-20/600

Richtsnoeren betreffende beveiliging en governance van informatie- en communicatietechnologie

Eiopa – Westhafen Tower, Westhafenplatz 1 - 60327 Frankfurt – Germany - Tel.: + 49 69-951119-20;
Fax: + 49 69-951119-19; e-mail: info@eiopa.europa.eu site: www.eiopa.europa.eu

NIEUW en VERPLICHT: de CISO

Chief Information Security Officer

De information security officer

Rol binnen de governance (Guideline 7)

➢ Nieuwe sleutelfunctie ?

- Ondernemingen moeten
  - binnen hun governancesysteem en in overeenstemming met het evenredigheidsbeginsel,
- een informatiebeveiligingsfunctie opzetten,
- waarbij de verantwoordelijkheden worden toegewezen aan *een specifieke persoon*.

- De onderneming moet de *onafhankelijkheid en objectiviteit* van deze informatiebeveiligingsfunctie waarborgen
- door deze *op passende wijze te scheiden* van
  - *processen inzake ICT-activiteiten*
  - *en bedrijfsvoering.*

- De functie moet verslag uitbrengen aan het AMSB
  (bestuur en/of de raad van commissarissen)

De information security officer

Rol binnen de governance

➢ Taken van de CISO

a) Voorbereiden beleidslijnen voor informatiebeveiliging (en controle op uitrol);
b) Periodiek en ad-hoc rapporteren aan het bestuur over de status van informatiebeveiliging
c) Informatiebeveiligingsmaatregelen monitoren;
d) Waarborgen dat dienstverrichters aan de beleidslijnen voldoen;
e) Informeren van medewerkers over informatiebeveiligingsbeleid, opleidings- & awareness sessies
f) Onderzoek van operationele of veiligheidsincidenten (en rapporteren aan bestuur).

e) waarborgen dat alle medewerkers en dienstverrichters die toegang hebben tot informatie en systemen, op passende wijze zijn geïnformeerd over de beleidslijnen voor informatiebeveiliging, bijvoorbeeld door middel van opleidings- en bewustmakingssessies voor informatiebeveiliging;

DNB trekt de touwtjes aan

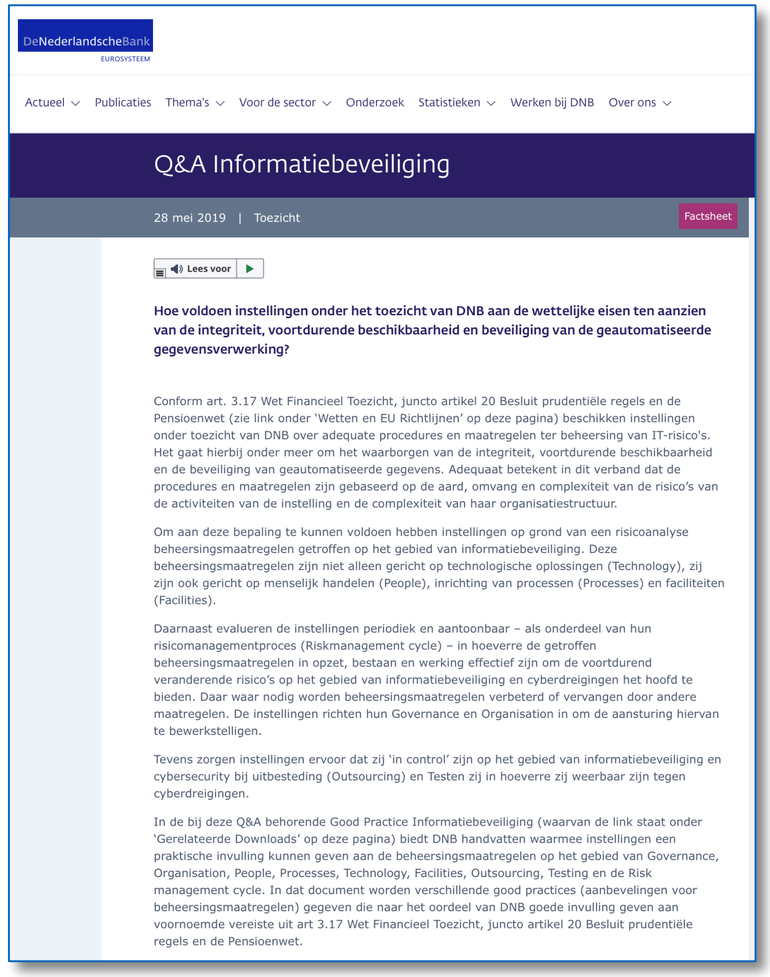
Het volwassenheidsniveau moet omhoog

DNB trekt de touwtjes aan

SBA-IB (Sectorbrede uitvraag informatiebeveiliging)

- **Doelstelling:**
- Volwassenheidsniveau naar 3 of 4
  (Q&A Informatiebeveiliging)
- Uiterlijk 31 juni 2023 op niveau
- Plan van aanpak (31 maart 2022)

- **Nieuwe Self-assessment:**
  - Verklaring van de directie: ‘naar waarheid ingevuld’
  - Onafhankelijke verklaring van de IAF
    (of een andere externe deskundige)



DeNederlandscheBank
EUROSYSTEEM

Actueel | Publicaties | Thema's | Voor de sector | Onderzoek | Statistieken | Werken bij DNB | Over ons

Q&A Informatiebeveiliging

28 mei 2019 | Toezicht

Factsheet

Lees voor

Hoe voldoen instellingen onder het toezicht van DNB aan de wettelijke eisen ten aanzien van de integriteit, voortdurende beschikbaarheid en beveiliging van de geautomatiseerde gegevensverwerking?

Conform art. 3.17 Wet Financieel Toezicht, juncto artikel 20 Besluit prudentiële regels en de Pensioenwet (zie link onder ‘Wetten en EU Richtlijnen’ op deze pagina) beschikken instellingen onder toezicht van DNB over adequate procedures en maatregelen ter beheersing van IT-risico's. Het gaat hierbij onder meer om het waarborgen van de integriteit, voortdurende beschikbaarheid en de beveiliging van geautomatiseerde gegevens. Adequaat betekent in dit verband dat de procedures en maatregelen zijn gebaseerd op de aard, omvang en complexiteit van de risico’s van de activiteiten van de instelling en de complexiteit van haar organisatiestructuur.

Om aan deze bepaling te kunnen voldoen hebben instellingen op grond van een risicoanalyse beheersingsmaatregelen getroffen op het gebied van informatiebeveiliging. Deze beheersingsmaatregelen zijn niet alleen gericht op technologische oplossingen (Technology), zij zijn ook gericht op menselijk handelen (People), inrichting van processen (Processes) en faciliteiten (Facilities).

Daarnaast evalueren de instellingen periodiek en aantoonbaar – als onderdeel van hun risicomanagementproces (Riskmanagement cycle) – in hoeverre de getroffen beheersingsmaatregelen in opzet, bestaan en werking effectief zijn om de voortdurend veranderende risico’s op het gebied van informatiebeveiliging en cyberdreigingen het hoofd te bieden. Daar waar nodig worden beheersingsmaatregelen verbeterd of vervangen door andere maatregelen. De instellingen richten hun Governance en Organisation in om de aansturing hiervan te bewerkstelligen.

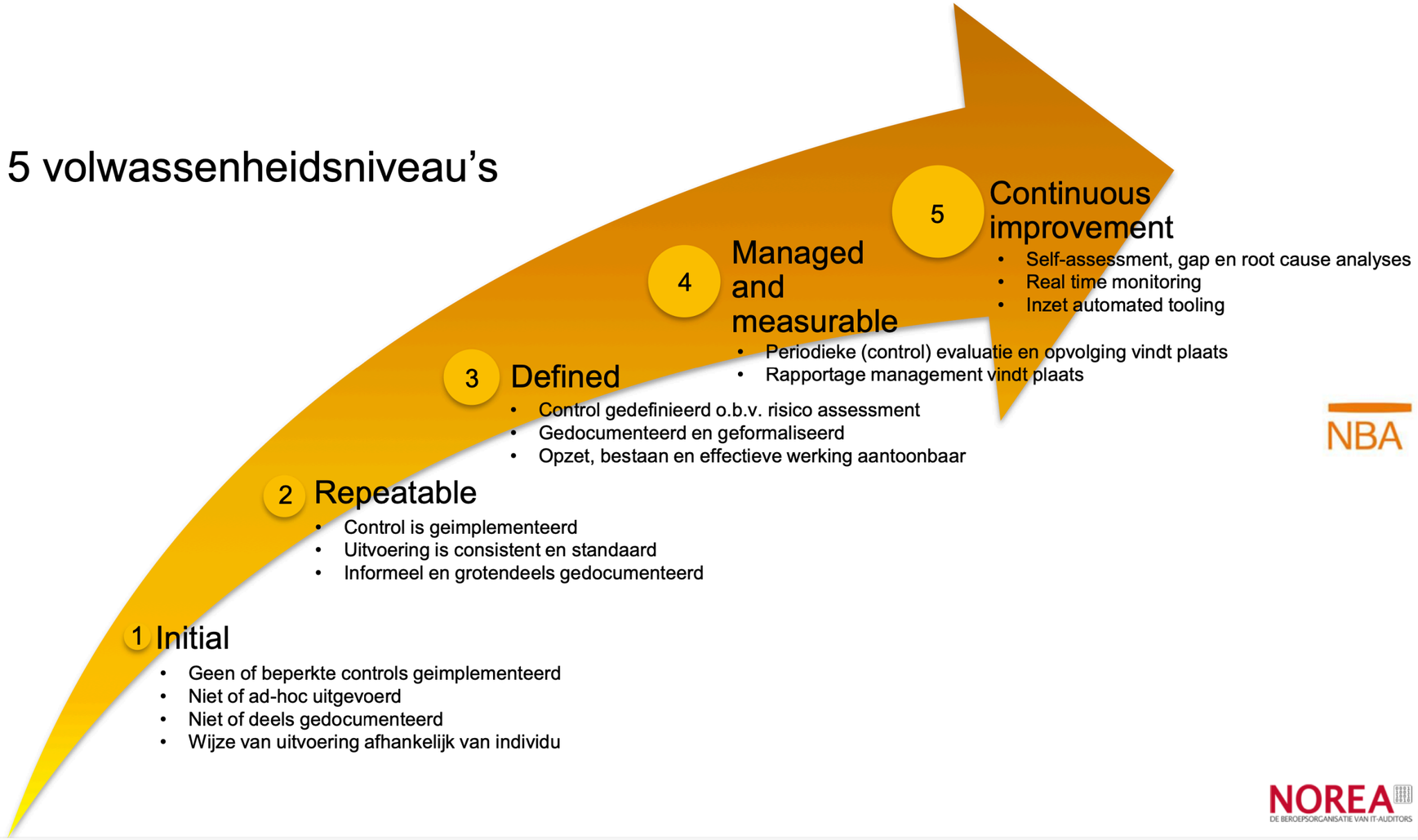
Tevens zorgen instellingen ervoor dat zij ‘in control’ zijn op het gebied van informatiebeveiliging en cybersecurity bij uitbesteding (Outsourcing) en Testen zij in hoeverre zij weerbaar zijn tegen cyberdreigingen.

In de bij deze Q&A behorende Good Practice Informatiebeveiliging (waarvan de link staat onder ‘Gerelateerde Downloads’ op deze pagina) biedt DNB handvatten waarmee instellingen een praktische invulling kunnen geven aan de beheersingsmaatregelen op het gebied van Governance, Organisation, People, Processes, Technology, Facilities, Outsourcing, Testing en de Risk management cycle. In dat document worden verschillende good practices (aanbevelingen voor beheersingsmaatregelen) gegeven die naar het oordeel van DNB goede invulling geven aan voornoemde vereiste uit art 3.17 Wet Financieel Toezicht, juncto artikel 20 Besluit prudentiële regels en de Pensioenwet.

DNB trekt de touwtjes aan

SBA-IB (Sectorbrede uitvraag informatiebeveiliging)

5 volwassenheidsniveau's



1 Initial
- Geen of beperkte controls geimplementeerd
- Niet of ad-hoc uitgevoerd
- Niet of deels gedocumenteerd
- Wijze van uitvoering afhankelijk van individu

2 Repeatable
- Control is geimplementeerd
- Uitvoering is consistent en standaard
- Informeel en grotendeels gedocumenteerd

3 Defined
- Control gedefinieerd o.b.v. risico assessment
- Gedocumenteerd en geformaliseerd
- Opzet, bestaan en effectieve werking aantoonbaar

4 Managed and measurable
- Periodieke (control) evaluatie en opvolging vindt plaats
- Rapportage management vindt plaats

5 Continuous improvement
- Self-assessment, gap en root cause analyses
- Real time monitoring
- Inzet automated tooling

NBA

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Volwassenheidsniveau 3 en 4

Aantoonbaarheid en toetsing werking

Volwassenheidsmeting

Maturity Indication Level 1 **Initial** "Initial Controls are not, or only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.	Maturity Indication Level 2 **Repeatable** Controls are in place and executed in a structured and consistent, but informal, manner.	Maturity Indication Level 3 **Defined** Controls are documented and executed in a structured and formal manner. Execution of control can be proved, is tested and effective.	Maturity Indication Level 4 **Managed and measurable** The effectiveness of the control is periodically assessed and improved when necessary. This assessment is documented.	Maturity Indication Level 5 **Continuous improvement** An enterprisewide risk and control programme provides continuous and effective control and risk issues resolution.	Actual Maturity Indication Level
- Information and/or cyber security activities or measures are implemented and/or executed on an ad-hoc basis.	- A strategy and vision has been defined, but has not been formally accepted.	- Strategy and vision has been approved by senior management. - Strategy and mission is actively communicated to employees, contractors and business partners.	- Strategy and vision are acknowledged as leading for all activities and measures regarding information and cyber security. - Alignment with strategy and vision is documented where applicable. - The validity and feasibility of the strategy and vision is periodically verified.	- Strategy also addresses how IT will help business objectives to be realized. - If necessary, the strategy or vision is adjusted to keep pace with business objectives and external developments.	2
- No policy defined. - Some policy statements drafted.	- A (information) security policy has been defined and covers most relevant aspects of information security.	- Policy has been approved by senior management. - Policy is actively communicated to employees, contractors and business partners (suppliers) and is made available as hard copy or digital document via intranet. - Policy is part of the security awareness program. - Compliance with policy is assessed on ad-hoc basis.	- The (information) security policy has been embedded into / adopted by the organization and translated into underlying procedures, baselines and instructions. - Policy is evaluated, updated and reapproved by senior management on a periodic basis.	- Compliance with (information) security policy is periodically reported to senior management.	2
- No information or cyber security plan or roadmap defined. - A few individual IT security projects have been defined and/or in progress.	- An information and/or cyber security plan or roadmap has been defined and covers all relevant business objectives, risks and compliance requirements.	- The plan or roadmap has been approved by senior management. - The plan has been translated into required (information) security policies and procedures together with appropriate investments in services, personnel, software and hardware. - Related polices and procedures are communicated to stakeholders and users.	- The information and/or cyber security plan is implemented and supported via enforced (information) security policies, procedures, required services, personnel, software and hardware. - There is a process for periodically evaluating and updating the information and/or cyber security plan and for forcing appropriate levels of management review and approval of changes.	- The information and/or cyber security plan versus related project portfolio are periodically monitored for e.g. progress, threats, feasibility and extent to which business requirements are met, including benefit tracking. - Reports submitted to senior management.	3

NBA

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Volwassenheidsniveau 3 en 4

Opleggen, uitleggen, trainen of overtuigen ?

InAudit BV
692volgers
Gepromoot

Een beknopt overzicht van wat wetenschappelijke onderzoek ons vertelt over de invloed van intrinsieke motivatie op de werkvloer.

Hoe stimuleer je intrinsieke motivatie bij medewerkers? 🚀 Downloaden

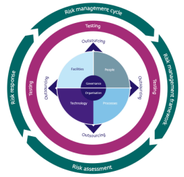
inaudit.nl

Ethical hacking & pen-testing

Aantoonbaarheid en toetsing werking

Testing

Testing



DNB verstaat onder dit element

Onderzoek toont aan dat het (laten) uitvoeren van Security testing effectief is om informatiebeveiliging en cyberweerbaarheid van instellingen continu te verbeteren. Security *Testing* kan zich richten op verschillende elementen uit het model van deze Q&A. Een test kan bijvoorbeeld zijn gericht op zwakheden in de infrastructuur (*Technology*), maar ook op menselijke gedrag en menselijk handelen (*People*) of op zwakke plekken in de toegang tot gebouwen (*Facilities*). De scope van Security testing kan zich richten op de interne organisatie, maar kan ook de belangrijke uitbestedingen meenemen.

Relevante beheersingsmaatregelen voor de instelling

DNB let erop dat de instelling op grond van een risicoanalyse en actuele cyberdreigingen bepaalt welke soorten beveiligingstests worden uitgevoerd alsmede de scope en diepgang van die tests. Daarbij is de aard en frequentie van deze testen afhankelijk van het risicoprofiel van de instelling. Een voorbeeld hierbij is dat de instelling verschillende typen beveiligingstests kan of laat uitvoeren, waaronder pentests gericht op de beveiliging van infrastructuur en applicaties, red teaming, het testen van de fysieke beveiliging en het testen van menselijk handelen in relatie tot informatiebeveiliging en cybersecurity. Deze testen kunnen uitgevoerd worden door interne of extern ingehuurde partijen.

Daarnaast let DNB erop dat de instelling na gaat dat de partij die de beveiligingstests uitvoert voldoende geëquipeerd is om dergelijke tests uit te voeren (hebben zij de juiste kennis en ervaring, certificeringen en referenties?). Een voorbeeld hierbij is dat de instelling op basis van een risicoanalyse *een jaarplan* maakt voor de uit te voeren soorten security tests.

Rol van het bestuur bij de implementatie van deze beheersmaatregelen

Het bestuur van de instelling is eindverantwoordelijk voor het aansturen, monitoren en uit laten voeren van Security testing.

U kunt hierbij bijvoorbeeld denken aan de volgende aspecten:

- Het bestuur stelt voldoende middelen beschikbaar om periodiek security tests te laten uitvoeren.
- Het bestuur houdt in het oog dat de scope van security tests de verschillende elementen uit het model van deze Good Practice omvat en daarbij rekening houdt bij het laten uitvoeren van de tests.
- Het bestuur zorgt ervoor dat in de RvB vergadering de uitkomsten van security tests worden besproken. Verder zorgt het bestuur ervoor dat met passende maatregelen opvolging wordt gegeven aan de constateerde risico's.

Beheersingsmaatregelen:

22.1 Penetration testing and ethical hacking

22

Ethical hacking & pen-testing

	21.2	Physical access
Testing		
	22	**Testing**
	22.1	Penetration testing and ethical hacking

Aantoonbaarheid & toetsing

Geautomatiseerde ondersteuning

key2control

Home | Oplossingen | Nieuws | Klanten | Partners | Over Key2Control | Contact | Vraag een demo aan

Informatiebeveiliging

Met Key2Control software heeft jouw organisatie aantoonbaar grip op alle vereisten om informatie en persoonsgegevens te bewaren, beveiligen en te beschermen. Dankzij de software is jouw organisatie volledig voorbereid op een audit of certificering.

Jouw uitdaging | Onze oplossing | Normenkaders | Meer weten

Onze oplossing

Key2Control software beschikt over een compleet Information Security Management System (ISMS). Dit ISMS ondersteunt het proces van A tot Z. Het ISMS is gebaseerd op het PDCA-kwaliteitsmodel van Deming en de ISO, NEN en BIO standaarden. Elk normenkader is in Key2Control voorzien van toelichtingen en werkinstructies op normniveau. Specifieke stuurvragen en voor gedefinieerde Act- en Check-maatregelen ondersteunen de normen.

In de software kunnen taken worden aangemaakt bij elke maatregel zodat deze terechtkomt bij andere medewerkers. Het is mogelijk om op elk moment verantwoording af te leggen op basis van realtime informatie dankzij standaard rapportages. Met enkele muisklikken genereert het ISMS bijvoorbeeld een verklaring van toepasselijkheid, jaarplan en voortgangsrapportage. Dankzij de dashboards ben je altijd op de hoogte van de actuele status. De verzamelde bewijslast wordt auditproof opgeslagen in de versleutelde omgeving.

Uw organisatie in control met InAudit Information Security

Kunnen wij u helpen ?

WELKOM
UNNEN WIJ U HELPEN?

Inhoud

Expertises van InAudit ...3
Interview met Berry Debrauwer ...4
Gedrag & Cultuur ...6
Puzzel ... 9
Interview met Donatus ...10
Waardevolle inzichten van ONVZ ...12
De wereld van ...14

InAudit timmert al ruim 8 jaar aan de weg met
organisaties. Onze kennis en expertise van audit, risicomana
datakwaliteit, finance en alle verplichtingen vanuit De Nederlandse Bank
vreemd. Het voelt goed om te weten dat onze klanten onze dienstverlening waarderen e
ons het vertrouwen geven om de interne audit uit te voeren.

Naast alle ontwikkelingen op gebied van interne audit hebben wij niet stil gezeten. Wij ervaren dat nieuwe disciplir
veel raakvlakken vertonen met de interne audit en van toegevoegde waarde zijn voor onze dienstverlening aan o
klanten. Afgelopen jaren hebben wij onze expertise uitgebreid met datakwaliteit, gedrag & cultuur en informa
security.
Met de komst van nieuwe expertises vinden wij het belangrijk om onderscheid aan te brengen. Natuurlijk was
bekend met het vertrouwde blauwe logo van InAudit. Naast deze bekende logo's gaat u ons ook op andere man
tegenkomen. Dat wil zeggen: hetzelfde herkenbare en vertrouwde logo maar dan in een andere kleur. Op
manier willen wij toch onderscheid aanbrengen in onze dienstverlening. Wij lichten het hier graag toe:

InAudit Audit Services - De naam zegt het al. Wij bieden oplossingen voor uw uitdagingen op het gebied van interne audit. Uitbesteding van de interne auditfunctie is onze kerncompetentie. Daarnaast springen we ons ook bij als tijdelijke oplossing of voeren we specifieke audits uit op gebieden waarop wij ons hebben gespecialiseerd.

InAudit Advies – Als wij u kunnen ondersteu
andere gebieden dan interne audit, dan doen
graag. Om de onafhankelijkheid van audit te
doen we dat vanuit InAudit Advies. InAudit Ad
zekere zin de nieuwe naam van het vroegere Inf

In Audit Services

In Audit Advies

InAudit Gedrag & Cultuur – Onderzoeken op het gebied van gedrag en cultuur hoeven niet uitsluitend als onderdeel van een audit plaats te vinden. Vanuit InAudit Gedrag & Cultuur kunnen wij ook het operationele management helpen met onderzoeken naar risicocultuur, groepsdynamiek en aanspreekgedrag en 'awareness'.

InAudit Information Security – Hieronde
zoals het ontwikkelen
informatiebeveiligingsbeleid bij onze
strategische adviezen voor tactische e
maatregelen en het creëren van awa
organisaties. Informatiebeveiliging word
een zelfstandige sleutelfunctie. Voor ver
uitbesteding de logische keuze.

In Audit
In Audi
Information Se

InAudit Information Security BV

Landgoed De Wildbaan
Spankerenseweg 16
6974 BC Leuvenheim
055-5782921
www.inaudit.nl