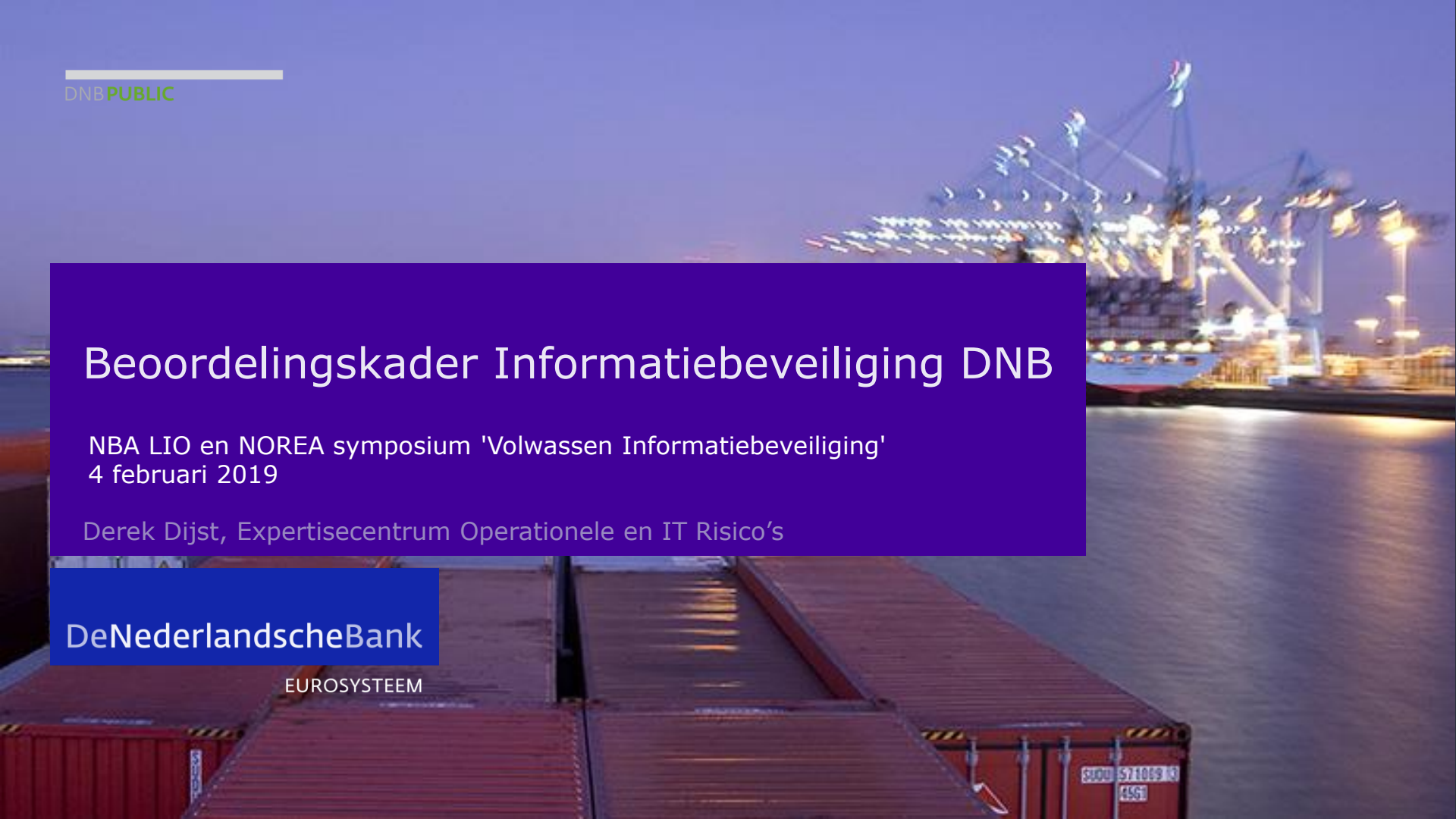
DNBPUBLIC



Beoordelingskader Informatiebeveiliging DNB

NBA LIO en NOREA symposium 'Volwassen Informatiebeveiliging'
4 februari 2019

Derek Dijst, Expertisecentrum Operationele en IT Risico's

DeNederlandscheBank

EUROSYSTEEM

Agenda

DNB PUBLIC

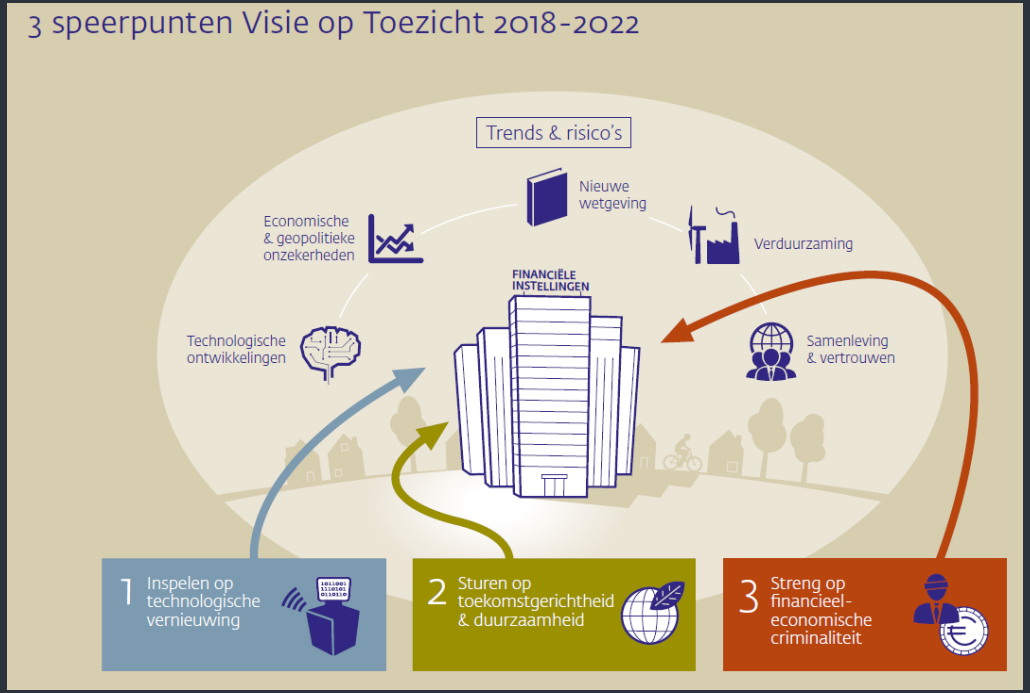
Toezicht door DNB
Beoordelingskader Informatiebeveiliging DNB
Ervaringen beoordelingskader
Waarnemingen 2018
Aandacht voor uitbesteding
Thema’s 2019

Agenda

- Toezicht door DNB
- Beoordelingskader Informatiebeveiliging DNB
- Ervaringen beoordelingskader
- Waarnemingen 2018
- Aandacht voor uitbesteding
- Thema's 2019

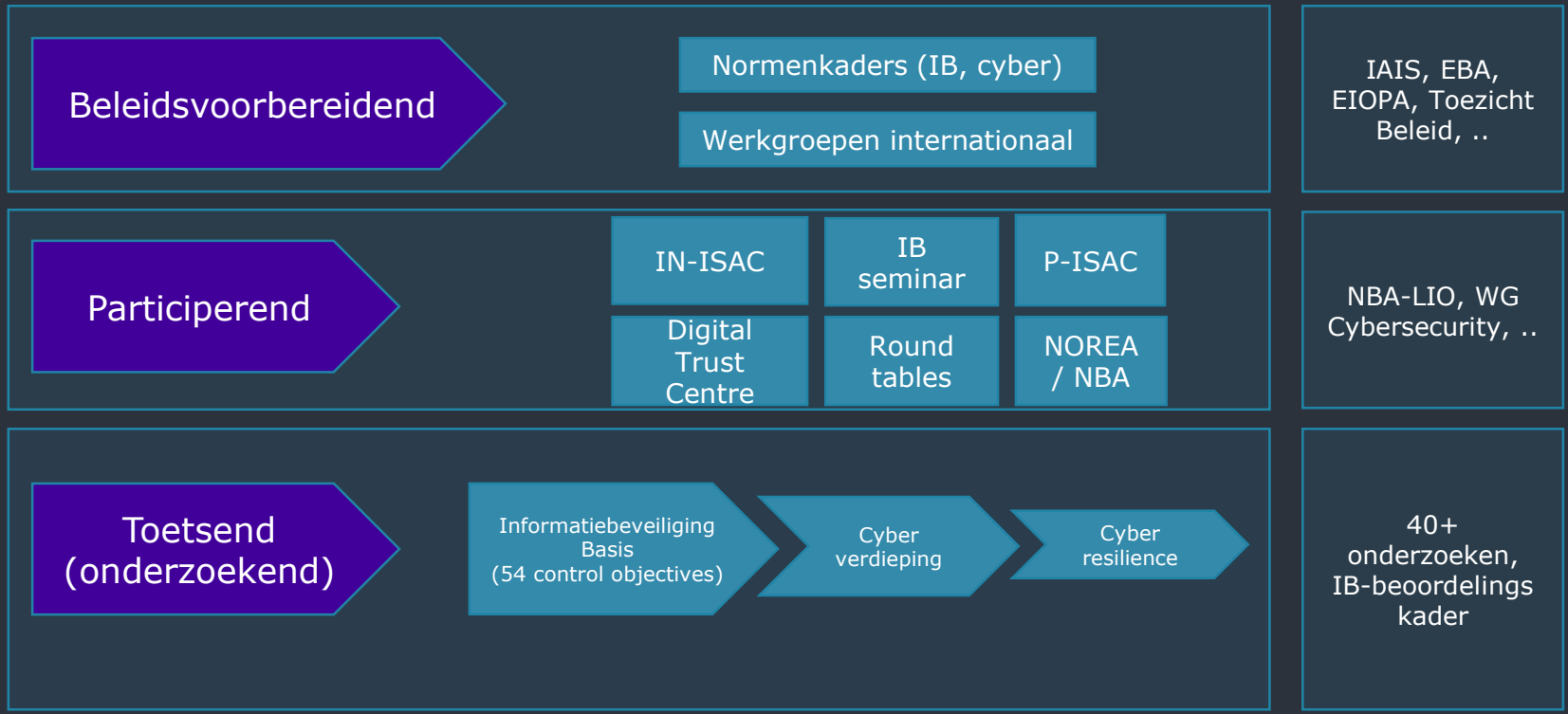
Toezicht door DNB

1. DNB speelt in op technologische vernieuwing
2. DNB stuurt op toekomstgerichtheid en duurzaamheid
3. DNB is streng op financieel-economische criminaliteit



Cybersecurity - toezichtsperspectief

DNB PUBLIC



Agenda

DNB PUBLIC

Toezicht door DNB

Beoordelingskader Informatiebeveiliging DNB

Ervaringen beoordelingskader

Waarnemingen 2018

Aandacht voor uitbesteding

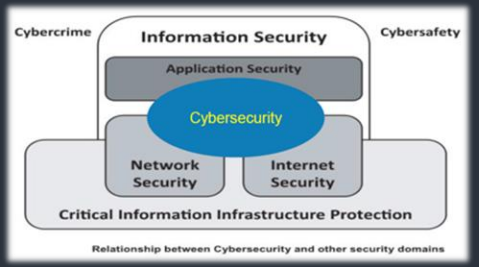
Thema's 2019

Beoordelingskader DNB

Beheersing van informatiebeveiligingsrisico's (inclusief cyberrisico's)

Opzet beoordelingskader

- Instellingen beoordelen zelf hun volwassenheidsniveau
- DNB toetst en stelt minimum vereist volwassenheidsniveau
- Kader 54 controls, principle based, aard van de risico's
- Jaarlijkse selectie van instellingen
- Kader geaccepteerd door sector (vaak onderdeel van risk-framework instelling)
  - Initiatieven om kader verder uit te werken (NBA-LIO)
- Meer nadruk op risicomanagement (en gewenst niveau -4-)

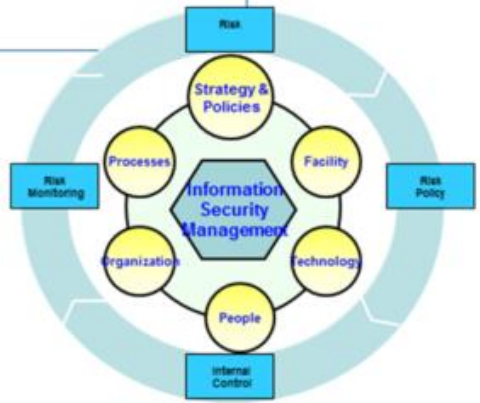


Bron: isaca.org

Update van beoordelingskader

2010 - 2018

IB kader:
- 54 controls
- Points to Consider
- Maturity Level
- 6 Domeinen
- Self assessment



2019 ....

IB+ kader:
Aanpassingen:
- Aantal controls (nieuw en vervallen)
- Aanscherping Points to Consider
- Guidance document Q&A website DNB

Ongewijzigd:
- Maturity Level
- 6 Domeinen
- Self assessment

Feedback ISACs, branche organisaties, werkgroepen, ..

Agenda

DNB PUBLIC

Toezicht door DNB
Beoordelingskader Informatiebeveiliging DNB
Ervaringen beoordelingskader
Waarnemingen 2018
Aandacht voor uitbesteding
Thema's 2019

Kwaliteit van ontvangen assessments

DNB PUBLIC

Aandachtspunten:

1) Scoping van de assessments
2) Interpretatie en onderbouwing volwassenheidsniveau's
3) Kwaliteit van de onafhankelijke review op het assessment (intern en extern)
4) Uitbestedingsketen

Gebruik het kader als instrument

DNB PUBLIC

- Raamwerk helpt de organisatie bij het inrichten van informatiebeveiliging
- Gericht op het behalen van doelstellingen
- Cobit is door DNB als uitgangspunt gebruikt
- Het beoordelingskader vormt een basis. Geen papieren exercitie!

Andere activiteiten zijn ook belangrijk voor de weerbaarheid van de instelling (bijv. pen-testing en oefeningen).

Agenda

DNB PUBLIC

Toezicht door DNB
Beoordelingskader Informatiebeveiliging DNB
Ervaringen beoordelingskader
Waarnemingen 2018
Aandacht voor uitbesteding
Thema's 2019

Belangrijkste waarnemingen 2018

DNB PUBLIC

1) Uitdaging: op niveau brengen en houden van maatregelen

2) Inzicht: meer inzicht in maatregelen in de uitbestedingsketen is nodig

3) Aandacht: meer aandacht nodig voor cybersecurity dreigingen en -maatregelen

Agenda

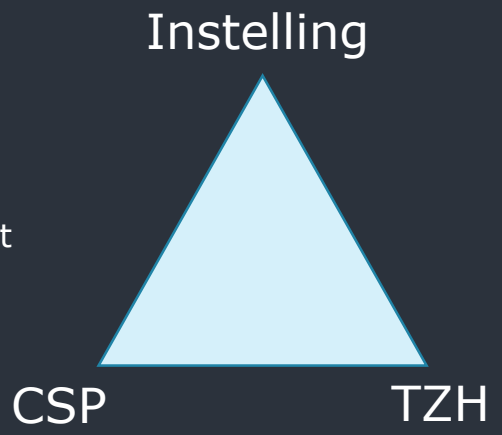
DNB PUBLIC

Toezicht door DNB
Beoordelingskader Informatiebeveiliging DNB
Ervaringen beoordelingskader
Waarnemingen 2018
Aandacht voor uitbesteding
Thema's 2019

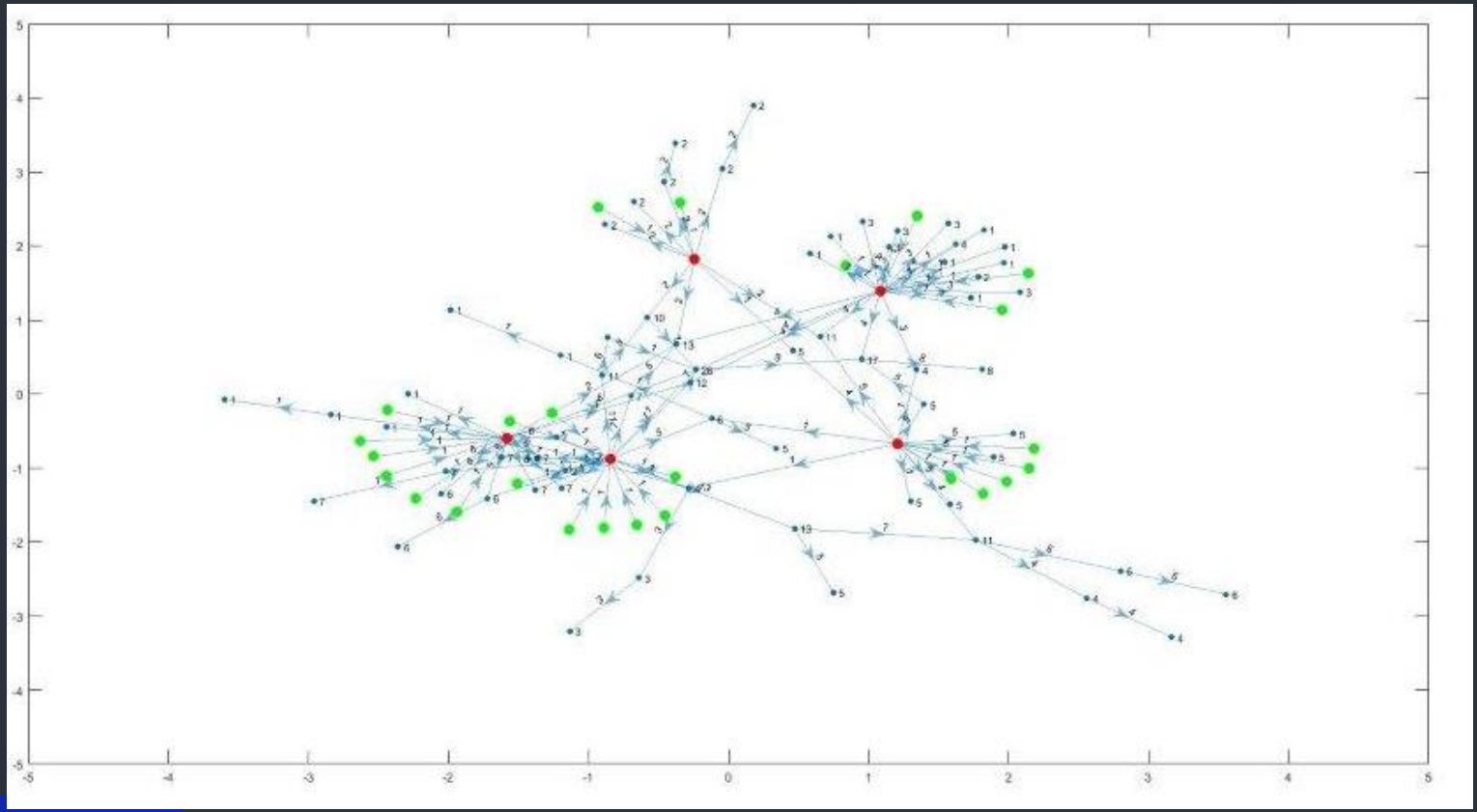
Uitbesteding/cloud - toezichtsperspectief

DNB PUBLIC

- DNB al sinds 2010 met Cloud bezig
  - Contacten met BigTechs
  - Cloud guidance (2011)
  - Thema-onderzoek naar IT uitbesteding en Cloud (2018)
  - Cloud meldingsproces sinds 2011. In 2018 over naar Digitaal Loket Toezicht (DLT)
  - Aandacht vanuit toezicht neemt komende jaren toe



Concentratierisico



Uitbesteding/cloud - toezichtsperspectief

DNB PUBLIC

Belangrijkste bevindingen onderzoeken 2018

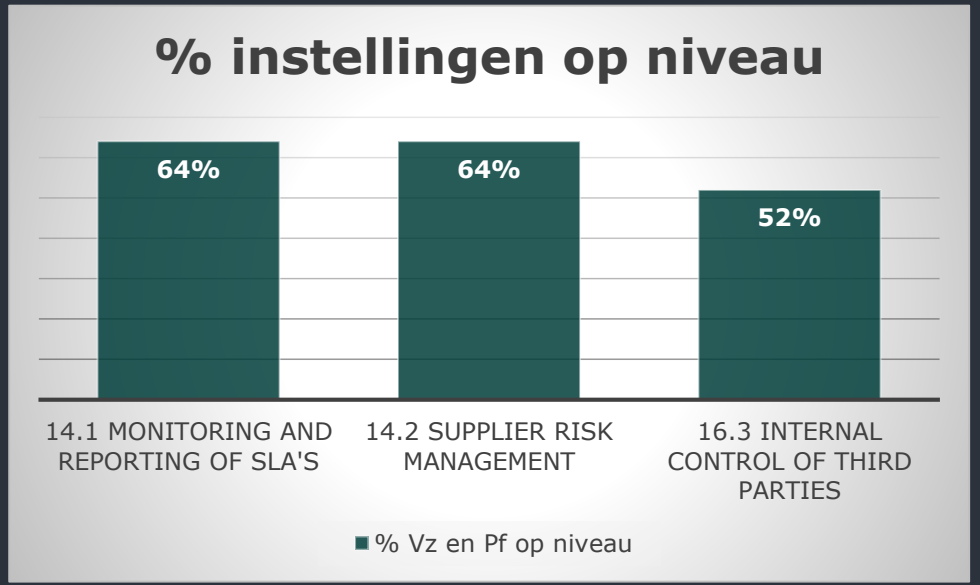
- Uitbestedingen worden niet structureel centraal geregistreerd
- Geen reguliere managementinformatie over de actuele uitbestedingsrisico's (30%)
- Evaluatie van dienstverleners behoeft verbetering in zowel frequentie als kwaliteit (30%)
- Ontbreken van wettelijke verplichte clausules (vooral bij onderuitbestedingen); 25% van de contracten voldoet niet aan wet- en regelgeving
- Inrichting Business Continuity Management onvoldoende (35%)
- Onvoldoende zekerheid (assurance) beschikbaar bij instellingen over de kwaliteit van geleverde diensten (40%)
- De service level rapportages (KPI's) stellen de instellingen ook niet altijd in staat om de prestaties en gemaakte afspraken te controleren (30%)

DeNederlandscheBank
EUROSYSTEEM

Controls op uitbesteding

Relevante controls die vaak niet op minimum niveau zitten:

- Monitoring and Reporting of SLA's (14.1)
- Supplier Risk management (14.2)
- Internal controls of third parties (16.3)



Impact op overige controledoelstellingen

Niet effectieve controls voor het beheersen van IB-risico's op belangrijke uitbesteding, heeft mogelijk ook impact op eigen instelling.

Voorbeeld: uitbesteding IT-infrastructuur

16	Monitoring		
16.1	Security testing, surveillance and monitoring		3
16.2	Monitoring of internal control framework		4
16.3	Internal control of third parties		1
16.4	Evaluation of compliance with external requirements		3
16.5	Independent assurance		3

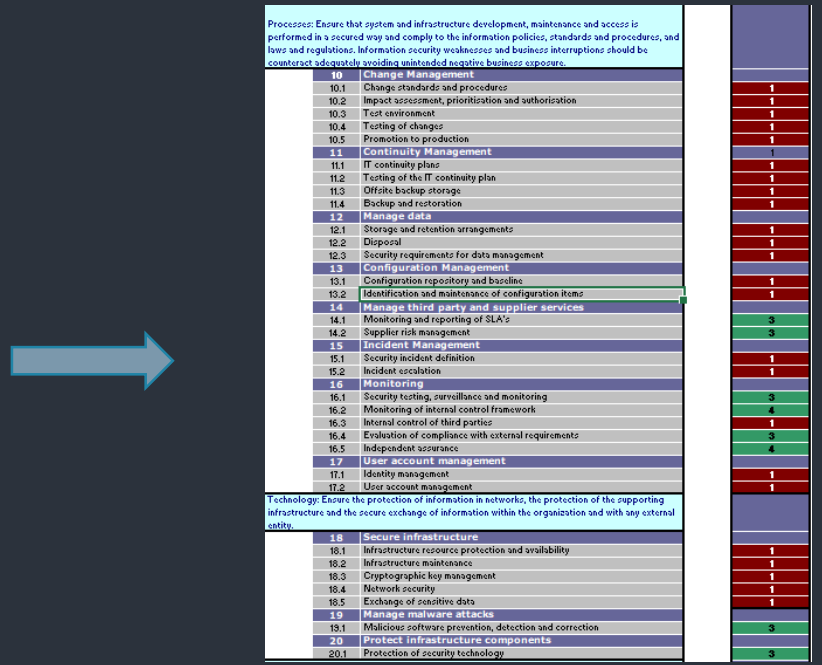
Impact op overige controledoelstellingen

DNB PUBLIC

Niet effectieve controls voor het beheersen van IB-risico's op belangrijke uitbesteding, heeft mogelijk ook impact op eigen instelling.

Voorbeeld: uitbesteding IT-infrastructuur

16	Monitoring	
16.1	Security testing, surveillance and monitoring	3
16.2	Monitoring of internal control framework	4
16.3	Internal control of third parties	1
16.4	Evaluation of compliance with external requirements	3
16.5	Independent assurance	3



Processes: Ensure that system and infrastructure development, maintenance and access is performed in a secured way and comply to the information policies, standards and procedures, and laws and regulations. Information security weaknesses and business interruptions should be counteract adequately avoiding unintended negative business exposure.		
10	Change Management	
10.1	Change standards and procedures	1
10.2	Impact assessment, prioritisation and authorisation	1
10.3	Test environment	1
10.4	Testing of changes	1
10.5	Promotion to production	1
11	Continuity Management	1
11.1	IT continuity plans	1
11.2	Testing of the IT continuity plan	1
11.3	Offsite backup storage	1
11.4	Backup and restoration	1
12	Manage data	
12.1	Storage and retention arrangements	1
12.2	Disposal	1
12.3	Security requirements for data management	1
13	Configuration Management	
13.1	Configuration repository and baseline	1
13.2	Identification and maintenance of configuration items	1
14	Manage third party and supplier services	
14.1	Monitoring and reporting of SLA's	3
14.2	Supplier risk management	3
15	Incident Management	
15.1	Security incident definition	1
15.2	Incident escalation	1
16	Monitoring	
16.1	Security testing, surveillance and monitoring	3
16.2	Monitoring of internal control framework	4
16.3	Internal control of third parties	1
16.4	Evaluation of compliance with external requirements	3
16.5	Independent assurance	4
17	User account management	
17.1	Identity management	1
17.2	User account management	1
Technology: Ensure the protection of information in networks, the protection of the supporting infrastructure and the secure exchange of information within the organization and with any external entity.		
18	Secure infrastructure	
18.1	Infrastructure resource protection and availability	1
18.2	Infrastructure maintenance	1
18.3	Cryptographic key management	1
18.4	Network security	1
18.5	Exchange of sensitive data	1
19	Manage malware attacks	
19.1	Malicious software prevention, detection and correction	3
20	Protect infrastructure components	
20.1	Protection of security technology	3

Agenda

DNB PUBLIC

Toezicht door DNB
Beoordelingskader Informatiebeveiliging DNB
Ervaringen beoordelingskader
Waarnemingen 2018
Aandacht voor uitbesteding
Thema's 2019

Thema’s 2019

DNB PUBLIC

Aandacht voor:

- Datakwaliteit
- IB & Cyberonderzoeken

Hartelijk dank voor uw aandacht

d.s.dijst@dnb.nl