Security Compliance & Certification

Miranda Chilvers (DNB)
Petre (AIVD)
Dirk Jan van den Heuvel (Secura)

Secura

Introduction

- Security is hard to define
- Security is hard to measure
- However, we all want to rely on it …
- We want all (basic) aspects to be covered
- To do better than average
- Cyber criminals not to get access too easy

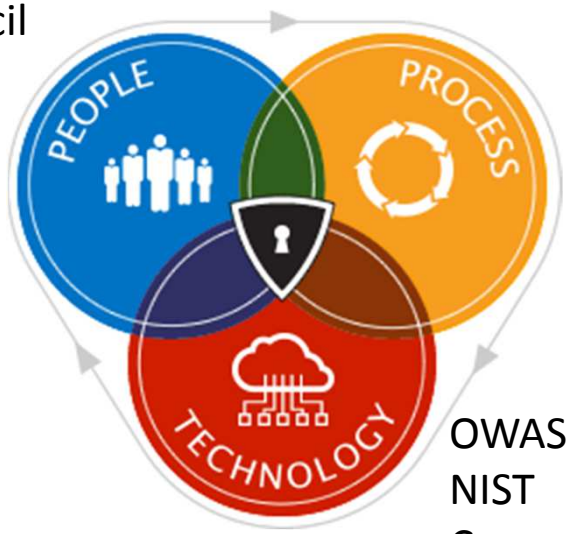
→We need to go from reactive to proactive

→To build confidence we need standards, compliance framework, certification schemes & benchmarking

Secura

Standards & Certification

SANS/ISACA/ISC2
PECB/EC Council
Offensive Sec./
CREST
…..



ISO 27.001
Cyber Essentials
NIST CSF
NEN 7510
BIR / BIG / BIWA
…..

OWASP
NIST
Common Criteria / BSPA
FIPS / PCI
IEC 62443
…..

- Who defines the standard?
- Who defines the compliance program?
- Who runs the program?
- How to stimulate compliance?

→ Many different ways

Secura

Three examples

1. Miranda Chilvers (DNB) Guideline for Cloud Service Providers by EBA
2. Petr (AIVD) about the Baseline Security Product Assessment (BSPA) Scheme
3. Dirk Jan van den Heuvel about the EU Cyber Security Act and the ECSO Meta-Scheme

Secura

Guideline for Cloud Service Providers by EBA

Miranda Chilvers (DNB)

Secura

Cloud computing new style
- EBA recommendations -

Miranda Chilvers

DeNederlandscheBank
EUROSYSTEEM

Introduction & agenda

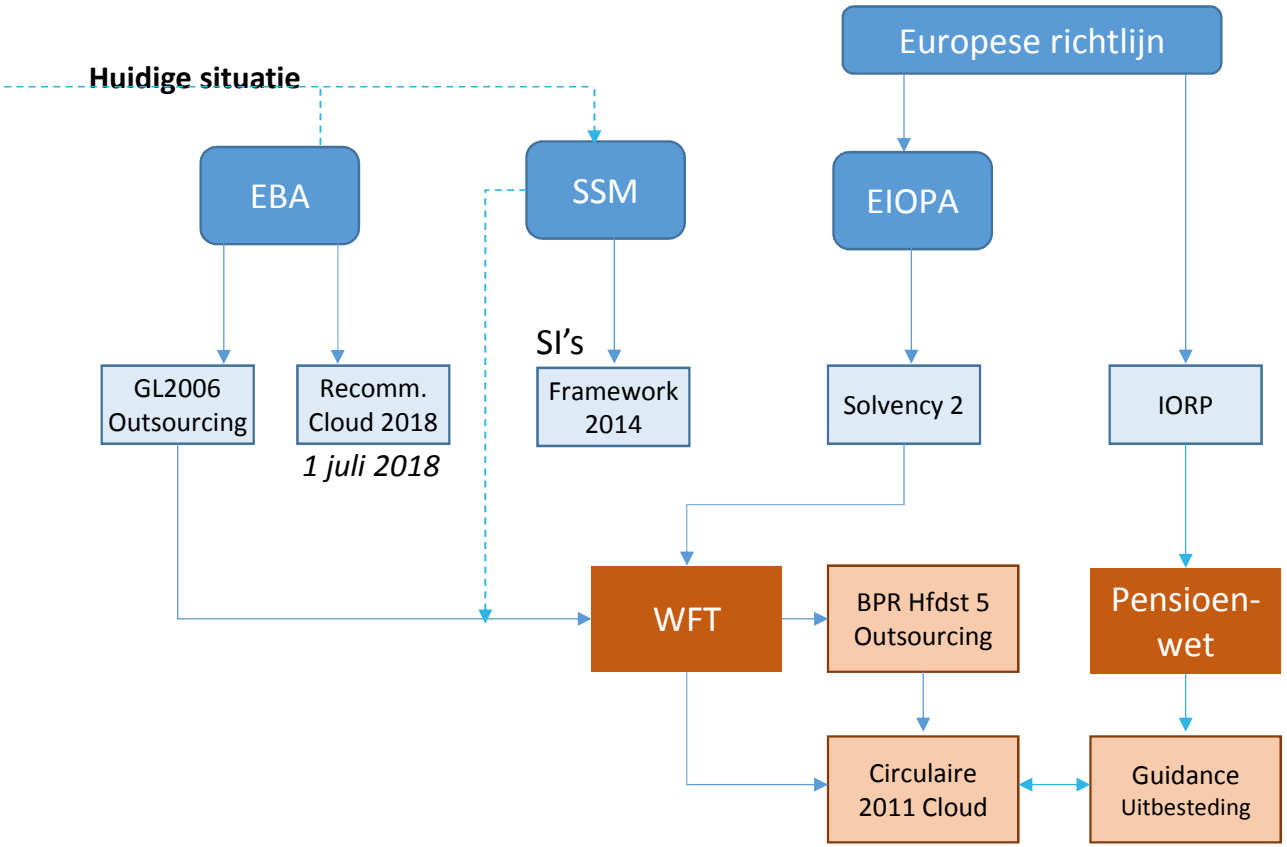
Introduction

- Miranda Chilvers – Senior Supervisor / Expert outsourcing

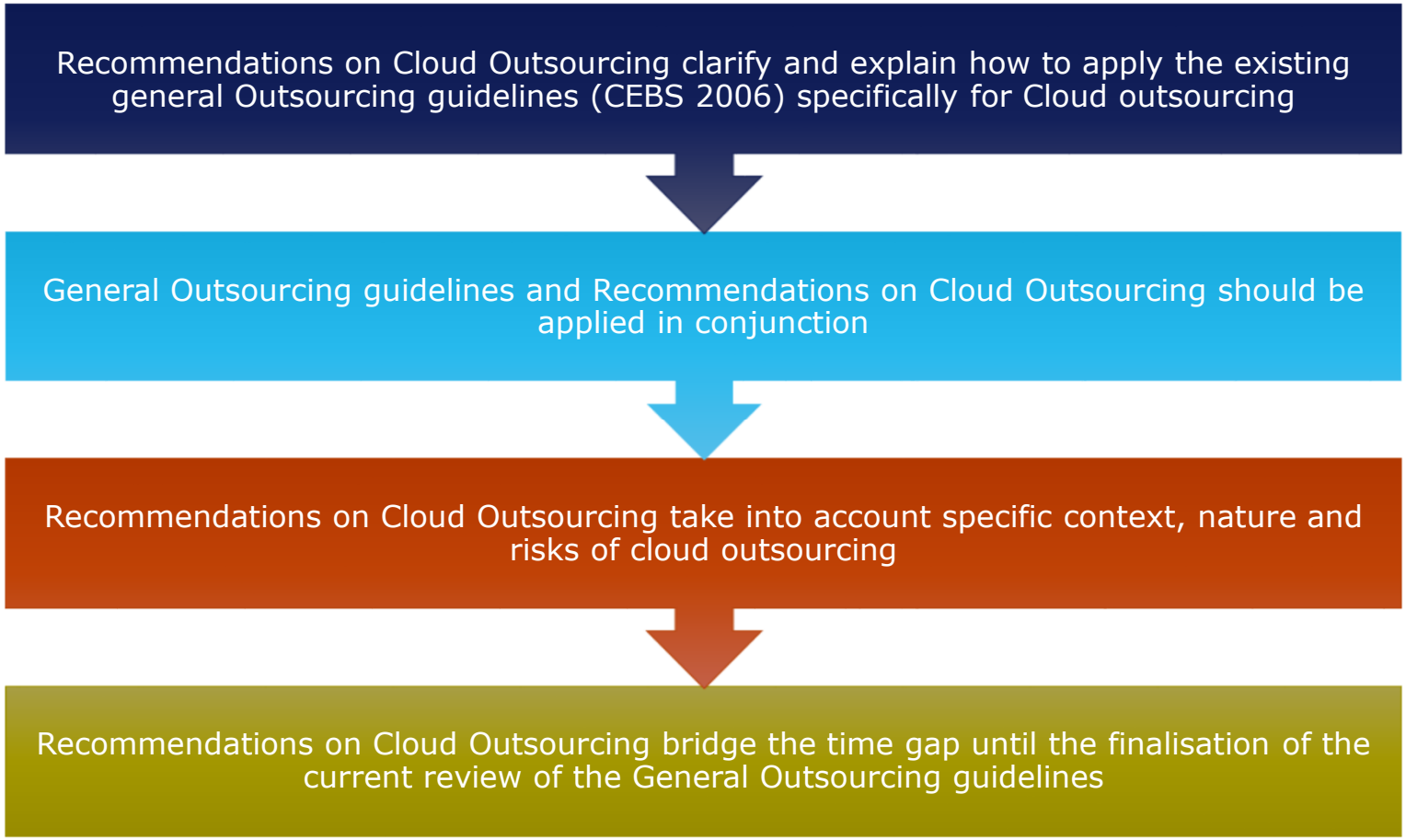
Agenda:

- Legal framework
- Cloud computing
  - Why recommendation on cloud computing
  - Outline recommendation cloud computing
- Digital Loket Toezicht (DLT) Outsourcing

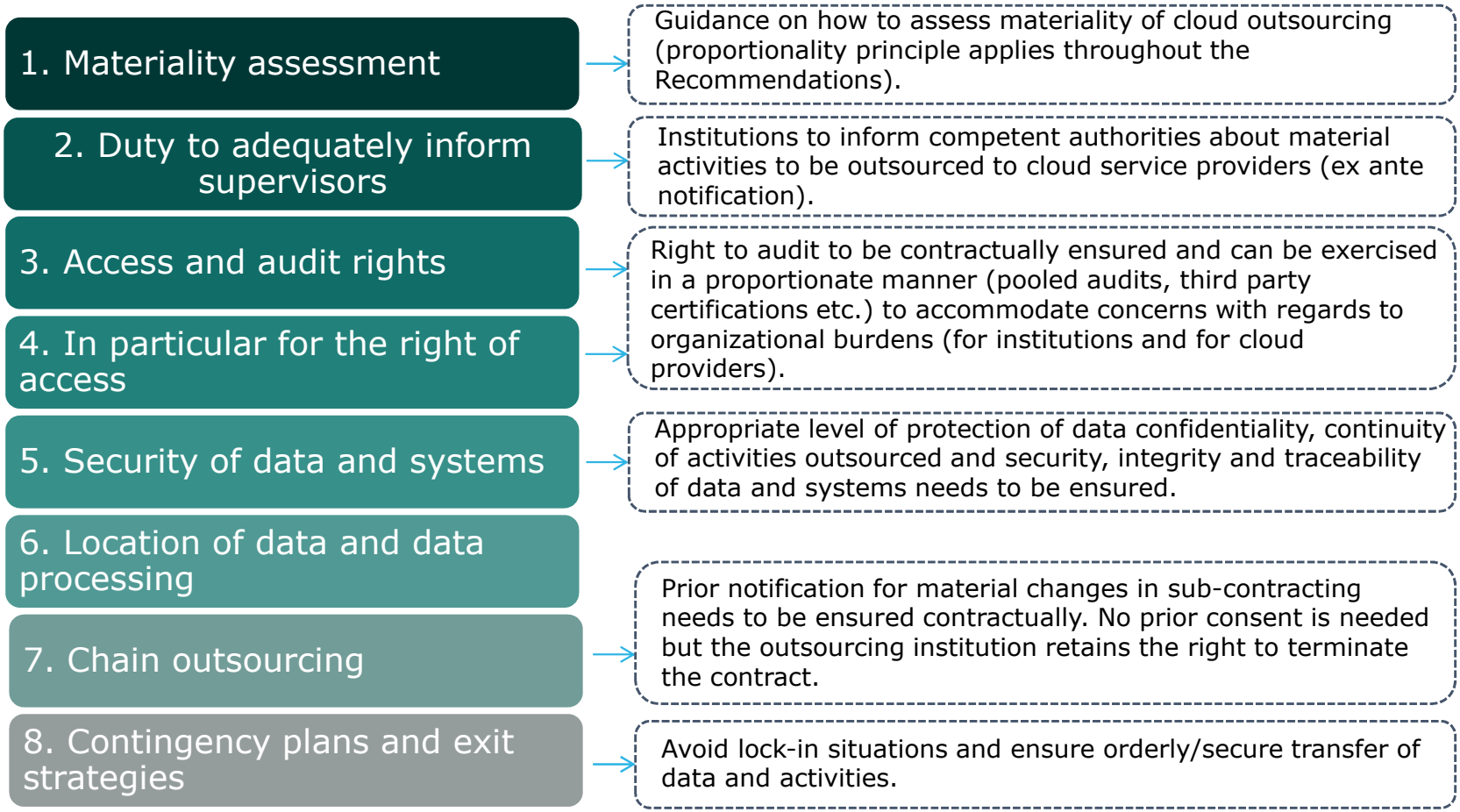
Legal framework



Link with general Outsourcing Guidelines



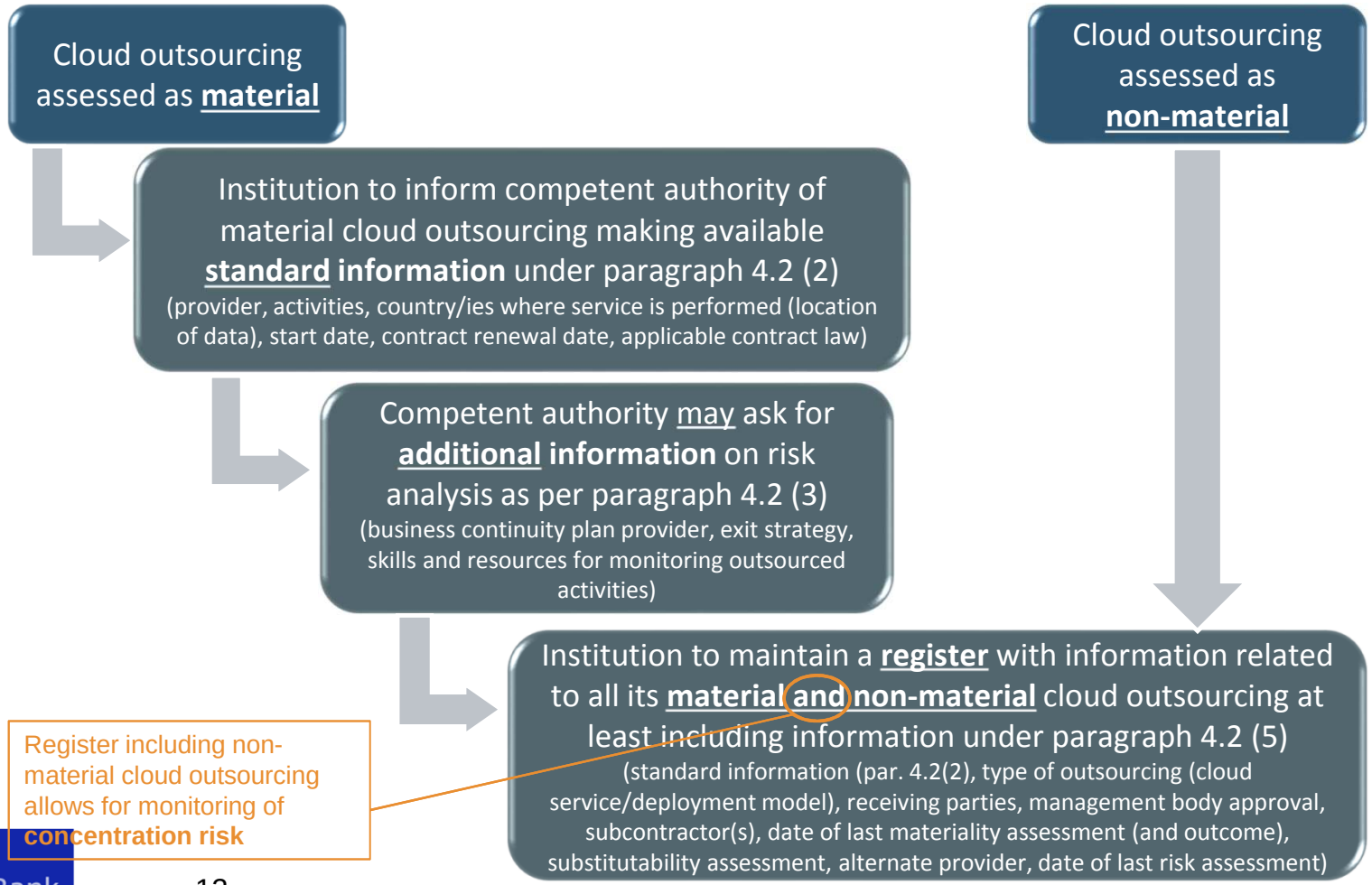
Outline of the EBA Recommendations on cloud (1-7-2018)



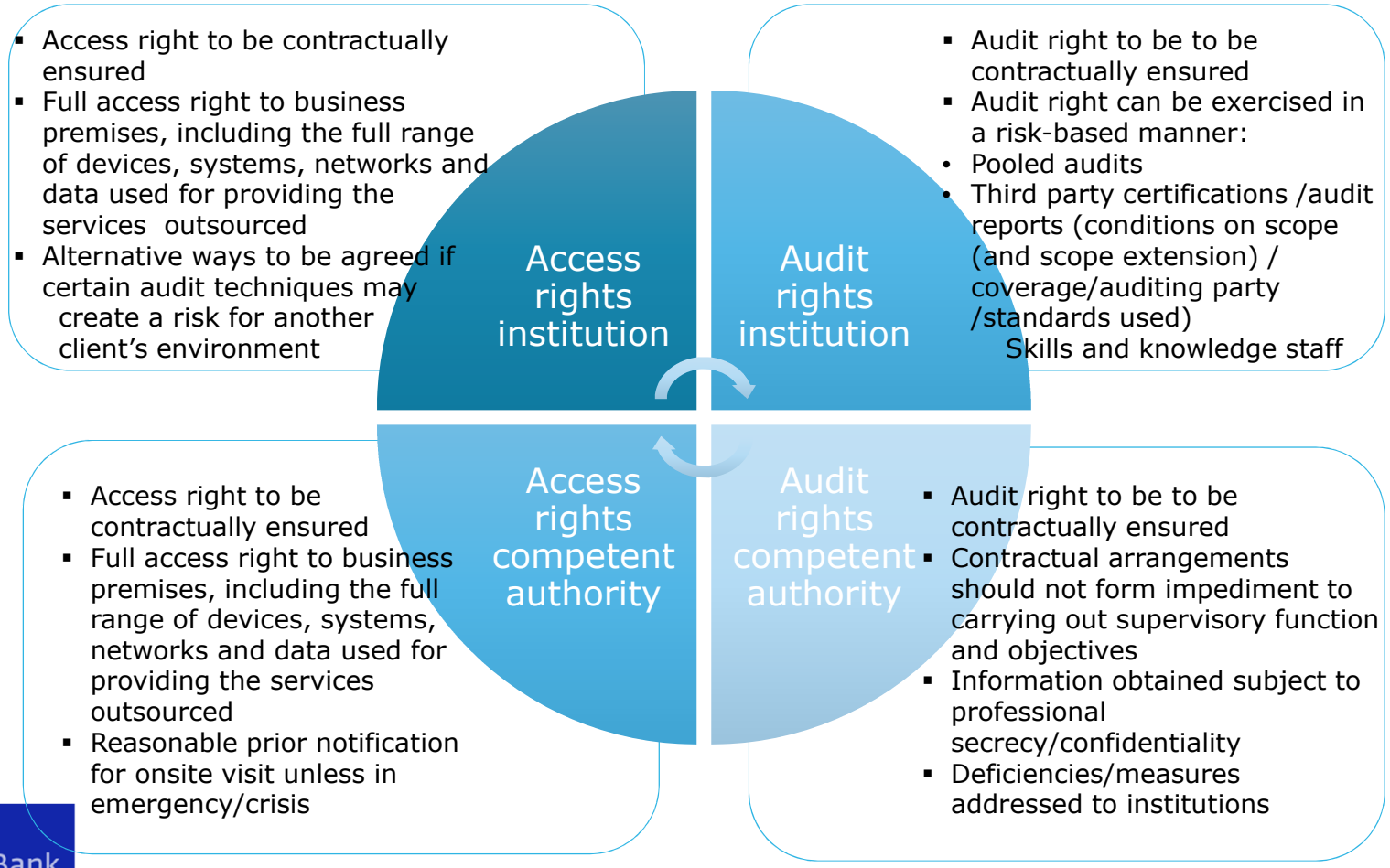
Materiality assessment

General Outsourcing Guidelines (CEBS 2006) **Criteria for assessment of materiality outsourcing**	Recommendations on cloud outsourcing **Criteria for assessment of materiality cloud outsourcing**
▪ Any weakness or failure in the provision of the activities could have a significant effect on the institution's ability to meet its regulatory responsibilities and/or to continue in business (**business continuation**); ▪ Activities requiring a licence from the supervisory authority (**licensed activities**); ▪ Activities having a significant impact on institution's **risk management**; ▪ The management of risks related to these activities.	▪ Criticality and inherent risk profile of activities, i.e. activities that are critical to the **business continuity/viability** of the institution and its obligations to customers; ▪ Direct **operational impact of outages**, and related legal and reputational risks; ▪ Impact of any disruption of the activities on **revenue prospects**; ▪ Potential impact of a **confidentiality breach or failure of data integrity** on the institution and its customers.

Duty to adequately inform supervisors



3) Access and audit rights



4) Security of data and systems

Prior to cloud outsourcing

- Identify and classify activities, processes and related data and systems as to sensitivity and required protection.
- Risk-based selection of activities, processes and related data and systems considered for cloud outsourcing.
- Define appropriate level of protection of data confidentiality, continuity of activities outsourced, and integrity and traceability of data and systems.
- Consider specific measures where necessary for data in transit, data in memory and data at rest (such as the use of encryption technologies and appropriate key management architecture).

Written agreement

- Put in place a written agreement with the cloud service provider which includes obligations with regards to security and protection of data.

During cloud outsourcing

- Monitor the performance of activities and security measures, including incidents on an ongoing basis, and take corrective measures if necessary.

5) Location of data and data processing

Institutions to adopt a risk-based approach to data and data processing locations

Assessment of countries where cloud services are provided should consider:

- Potential **risk impacts**, legal risks and compliance issues
- Potential **oversight limitations** (risks to effective supervision by competent authority)
- Wider **political and security stability** of the jurisdictions
- **Laws in force** in the jurisdictions (including data protection laws)
- Law enforcement provisions in the jurisdictions (including insolvency law in case of cloud service provider failure)

Institutions should ensure that these risks are kept within acceptable limits commensurate with the materiality of the outsourced activity.

6) Chain outsourcing

- Institution to take account of the risks associated with chain outsourcing.
- Institution to specify in outsourcing agreement:
  - any types of activities that are excluded from potential subcontracting;
  - cloud service provider retains full responsibility and oversight of subcontracted services;
  - cloud service provider to inform institution of any planned significant changes to subcontracting or subcontracted services named in the initial agreement.
- Institution to review and monitor the performance of the overall service on an ongoing basis (regardless of whether they are performed by the cloud service provider or subcontractors).

- **Prior notification by the cloud service provider** of planned significant changes in sub-contracting (including notification period) needs to be contractually ensured.
- **No prior consent from the institution** is required to changes in sub-contracting, but the institution should retain the right to terminate the contract if the planned changes will have an adverse effect on the risk assessment of the agreed services.

7) Contingency plans and exit strategies

Outsourcing institution should have contingency plan and exit strategy in place to ensure business continuity and avoid lock in situations.

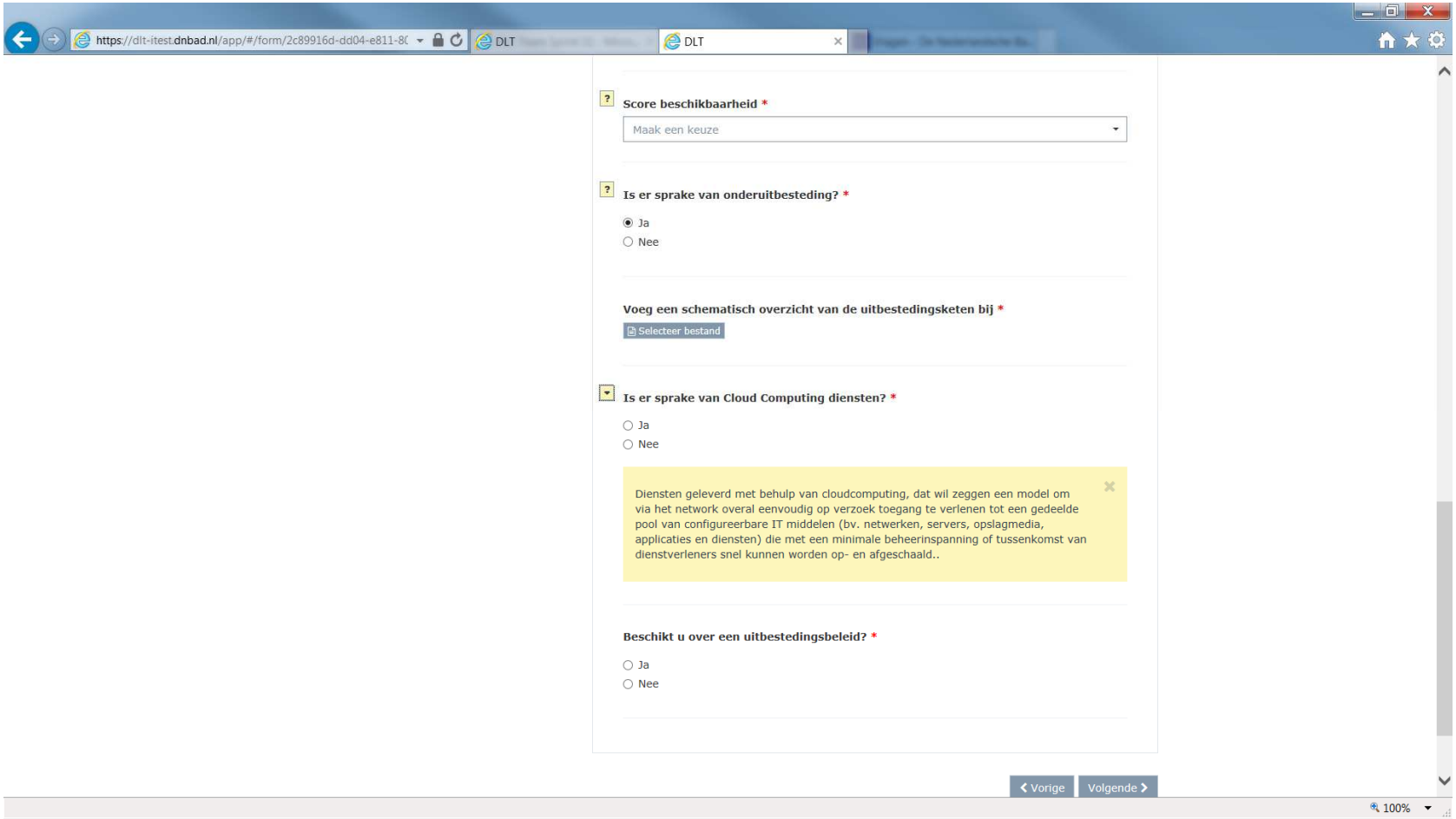
Contingency plan

- Institution should plan and implement **arrangements to maintain the continuity of its business** in the event that the provision of services by the cloud service provider fails or deteriorates to an unacceptable degree.
- Institution to develop **key risk indicators** to identify unacceptable level of services, and include indicators that can trigger the exit plan in their ongoing monitoring/oversight of the services.

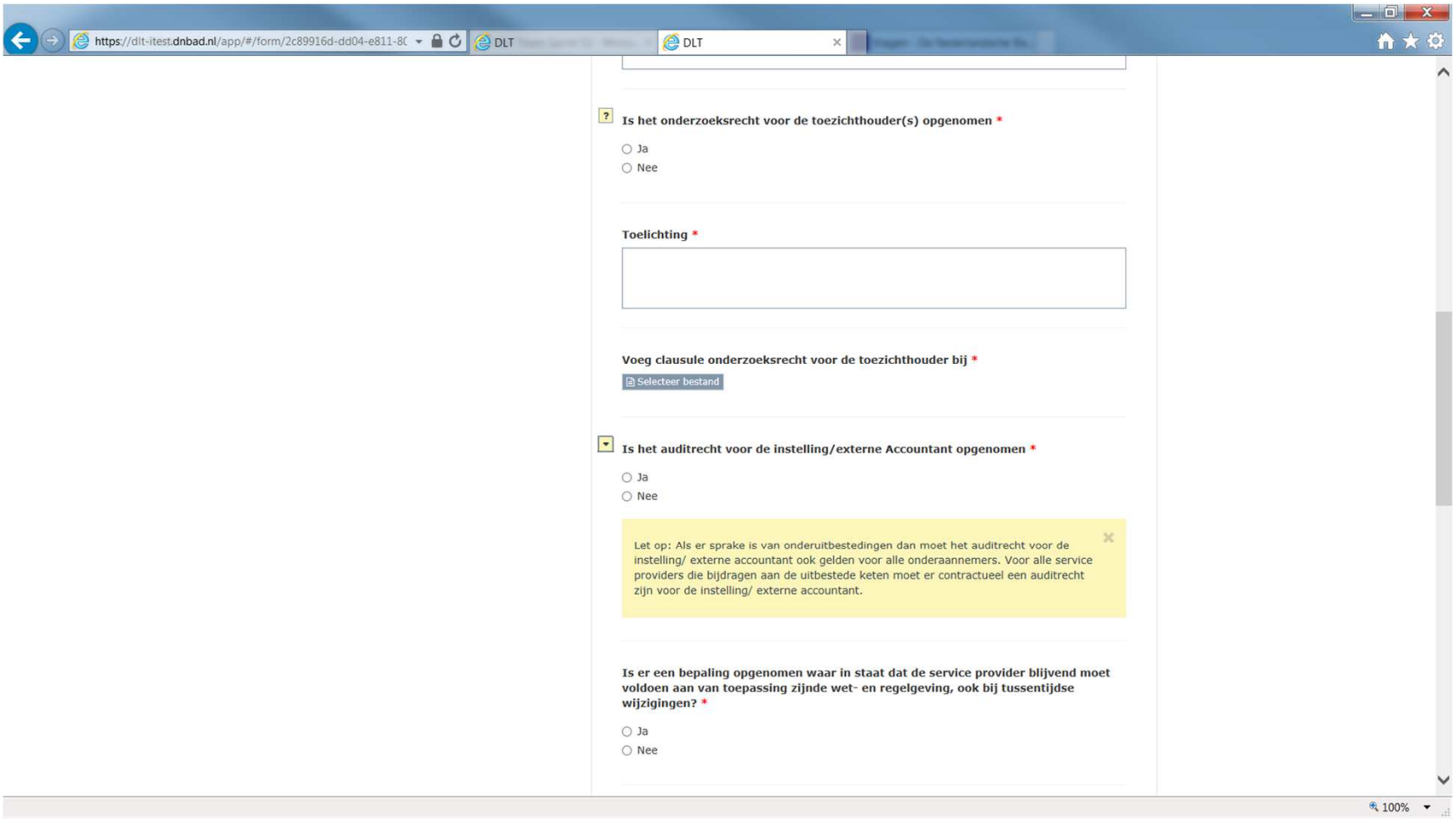
Exit strategy

- Outsourcing contract should include:
  - a **termination and exit management clause**;
  - An obligation on the cloud service provider to sufficiently support the orderly transfer of the activity to another service provider or to the outsourcing institution in case of exit.
- Institution should develop clear **exit strategy and plans** to ensure smooth exit of cloud outsourcing arrangements if needed without undue disruption to its provision of services.
  - Exit plans to be comprehensive, documented and sufficiently tested where appropriate;
  - Identify alternative solutions and transition plans (including success criteria, required resources, assigned roles and responsibilities, time needed for exit/transfer)

Digital portal supervison - Outsourcing



Digital portal supervison - Outsourcing



Email m.j.chilvers-van.der.kruk@dnb.nl

Baseline Security Product Assessment (BSPA) Scheme

Petr (AIVD)

Secura

EU Cybersecurity Act & ECSO Meta-Scheme

Dirk Jan van den Heuvel

Secura

Need for standards & certification

- NIS Directive July 2016 → National NIS (NIB) laws by now
  - Critical Infrastructures
  - CSIRTs
  - appropriate and proportionate technical and organisational measures to avoid cyber crime
  - Role Supervisory & Regulatory bodies (per industry)
- IoT (in)security
- Medical Device Directive
- Automotive Type Approval Process
-

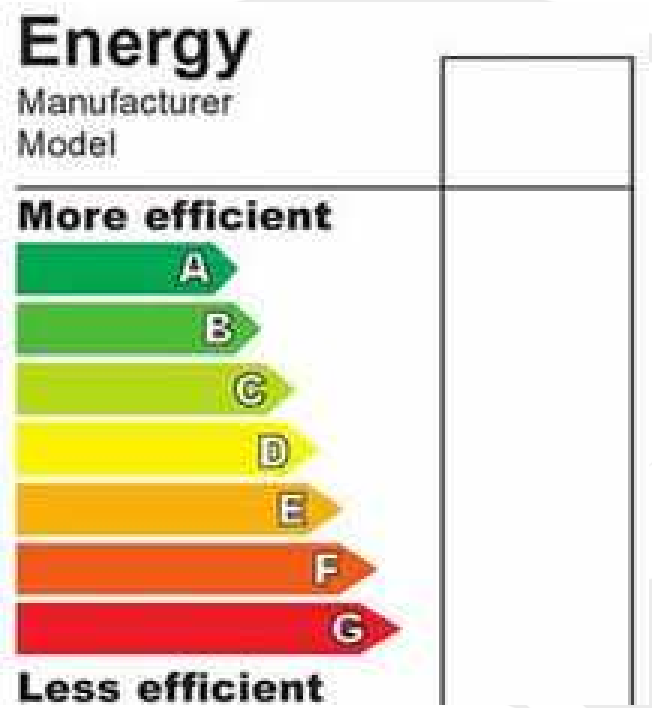
EU Cybersecurity Act

- EU Cybersecurity Act expected by the end of 2018 to
  - Arrange a stronger mandate for ENISA
    - Permanent Role (policy)
    - Operational Tasks (e.g. CERT-EU)
    - Central Role in European cybersecurity certification
  - Allow a EU Cybersecurity Certification Framework to be developed
- In collaboration with national accreditation bodies
- To allow cross-recognition
- To stimulate pan-European schemes (per industry)

Secura

ECSO Meta-scheme

- European Cyber Security Organisation (ECSO)
- Public-Private Partnership
- Answer to the EU Cyber Security Act
- Wish is to set-up a meta scheme like for Energy Efficiency
- Various levels per domain/industry



Secura

Levels in the ECSO meta-scheme

Levels of assurance in the Cybersecurity Act	Levels of assurance from the ECSO's meta-scheme (alternative naming)	Body performing the evaluation
High	A^g	National (governmental) body
	A	3rd party evaluation facility (lab)
Substantial	B	
Basic	C^i	
	C^s	Self-evaluation

Secura

Status

- Meta-scheme is under development. More than 150 companies participate
- Split in
  - Products
  - Services
  - Organisations
- Pilots to be expected in 2019

Secura

Relevance

As Secura we expect (towards the future) cyber security to be governed (more) by standards, compliance frameworks and certification in order to:

- Provide guidance and directions in fast changing landscape
- communicate and proof security and quality level
  - Common ground
  - Comparability
  - Repeatability
  - Marketing/Branding
- Provide Market Access
- Improve confidence level in security

Secura

FOLLOW US ON

Secura