DORA at de Volksbank

Learnings from moving from 3rd to 1st line

GLC Audit Masters

Tijs Wolffenbuttel

Lisbon – 23 May 2024

Tijs Wolffenbuttel

de volksbank

asn bank BLGwonen RegioBank SNS

4th fourth largest bank
in The Netherlands

Numbers 1, 2 and 3 of most
customer friendly
banks in the Netherlands

IT Director

Previously:
Chief Audit Executive 2013 to 2022

ABP

Largest pension fund
in The Netherlands
(for government, military, education)

One of top 10 largest pension funds
worldwide

Key Function holder Internal Audit
(parttime)

Agenda

What is the Digital Operational Resilience Act (DORA)?

Learnings from the DORA Implementation at de Volksbank

de volksbank

asn bank BLGwonen RegioBank SNS

Lessons learned from moving from 3rd to 1st line

Digital Operational Resilience Act (DORA) is applicable to?

Applicable to*

**Only limited exceptions*

How many entities?

About 22.000 Entities in the EU

- Banks
- Payment institutions & electronic money institutions
- Investment firms
- Crypto-asset service providers/issuers
- Central Counterparties (CCPs) and Central Securities Depositories (CSDs)
- Trading venues & trade repositories
- Fund managers
- Data reporting service providers
- (Re)insurance undertakings & intermediaries
- Pension funds
- Credit rating agencies (CRA’s)
- Administrators of critical benchmarks
- Crowdfunding service providers & securitisation repositories
- *ICT third-party service providers*

What is the goal of DORA?

The Digital Operational Resilience Act (DORA) is part of the EU's efforts to regulate the digital sector and enhance operational resilience, boost security requirements to reduce threats and risks from the use of ICT and improve institutions' ability to prevent and deal with ICT related incidents.

Legal basis

A regulation (and an amendment directive)

Status

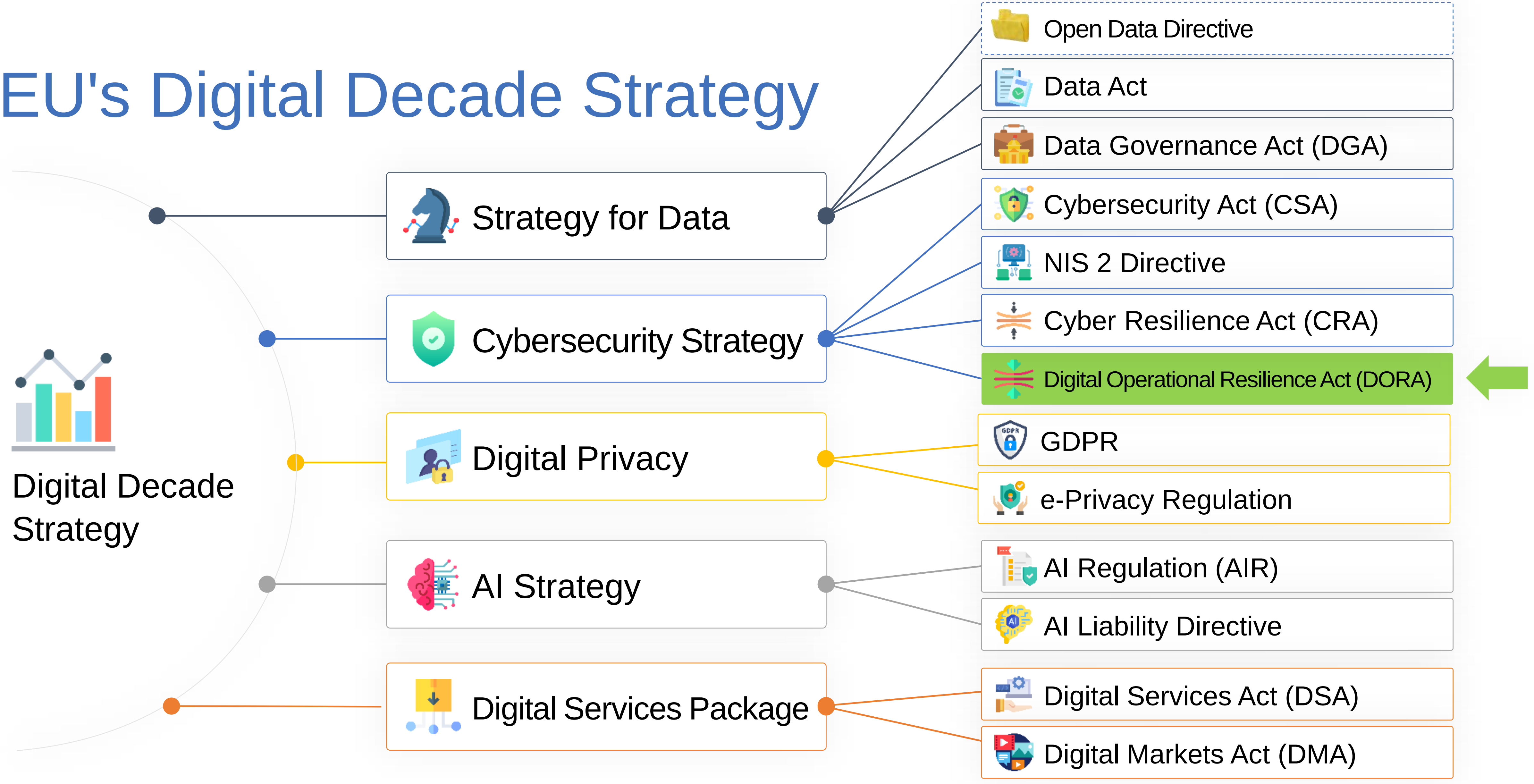
Entered into force on 16 January 2023, applicable as of 17 January 2025

Which authorities are responsible for DORA supervision?

- European Banking Authority (EBA) – supervision performed by European Central Bank (ECB)
- European Securities and Markets Authority (ESMA)
- European Insurance and Occupational Pensions Authority (EIOPA)

- And supervision performed by National Competent Authorities (NCAs)

EU's Digital Decade Strategy



Digital Decade Strategy

Strategy for Data

- Open Data Directive
- Data Act
- Data Governance Act (DGA)

Cybersecurity Strategy

- Cybersecurity Act (CSA)
- NIS 2 Directive
- Cyber Resilience Act (CRA)
- Digital Operational Resilience Act (DORA)

Digital Privacy

- GDPR
- e-Privacy Regulation

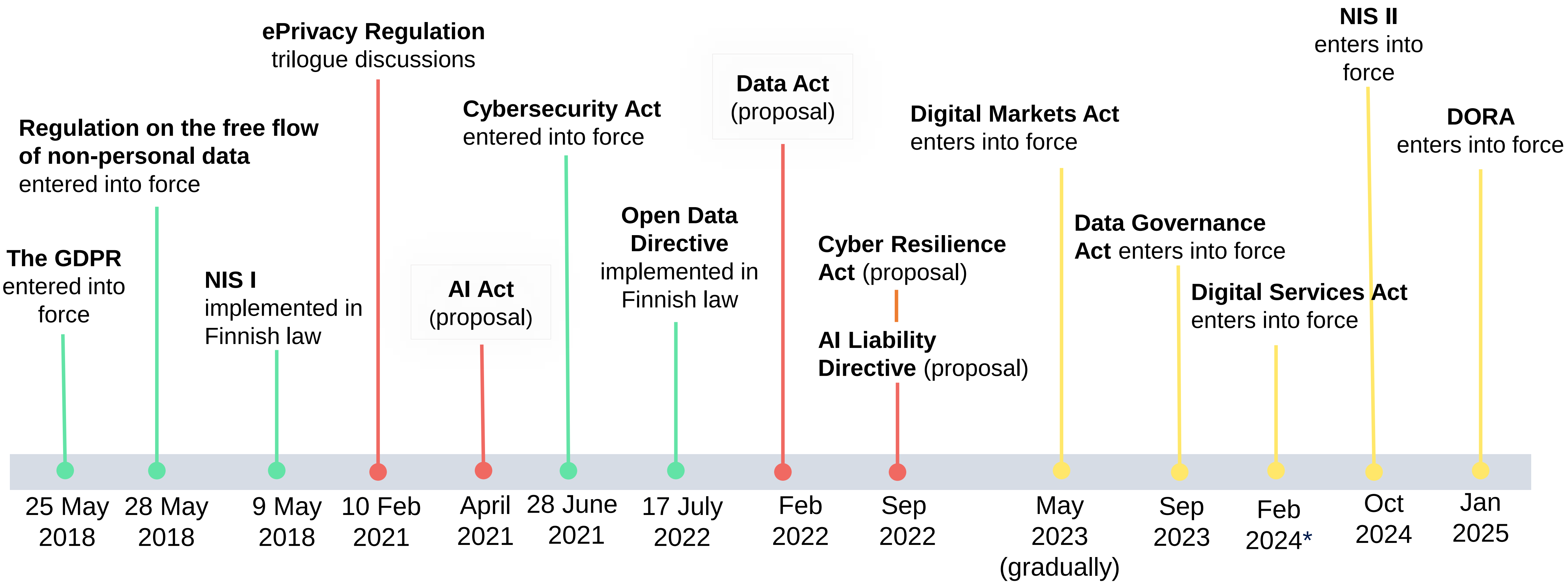
AI Strategy

- AI Regulation (AIR)
- AI Liability Directive

Digital Services Package

- Digital Services Act (DSA)
- Digital Markets Act (DMA)

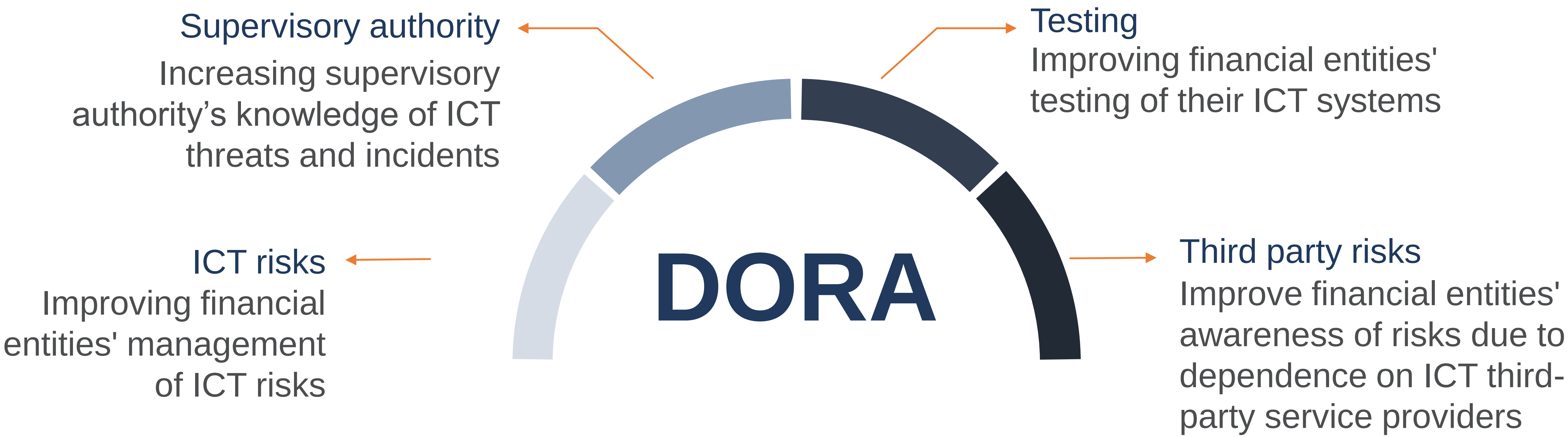
EU-rules on data and tech in constant development



- 25 May 2018 – **The GDPR** entered into force
- 28 May 2018 – **Regulation on the free flow of non-personal data** entered into force
- 9 May 2018 – **NIS I** implemented in Finnish law
- 10 Feb 2021 – **ePrivacy Regulation** trilogue discussions
- April 2021 – **AI Act** (proposal)
- 28 June 2021 – **Cybersecurity Act** entered into force
- 17 July 2022 – **Open Data Directive** implemented in Finnish law
- Feb 2022 – **Data Act** (proposal)
- Sep 2022 – **Cyber Resilience Act** (proposal); **AI Liability Directive** (proposal)
- May 2023 (gradually) – **Digital Markets Act** enters into force
- Sep 2023 – **Data Governance Act** enters into force
- Feb 2024* – **Digital Services Act** enters into force
- Oct 2024 – **NIS II** enters into force
- Jan 2025 – **DORA** enters into force

*Partially as from 16 Nov 2022

Objectives



DORA

Supervisory authority

Increasing supervisory authority’s knowledge of ICT threats and incidents

Testing

Improving financial entities' testing of their ICT systems

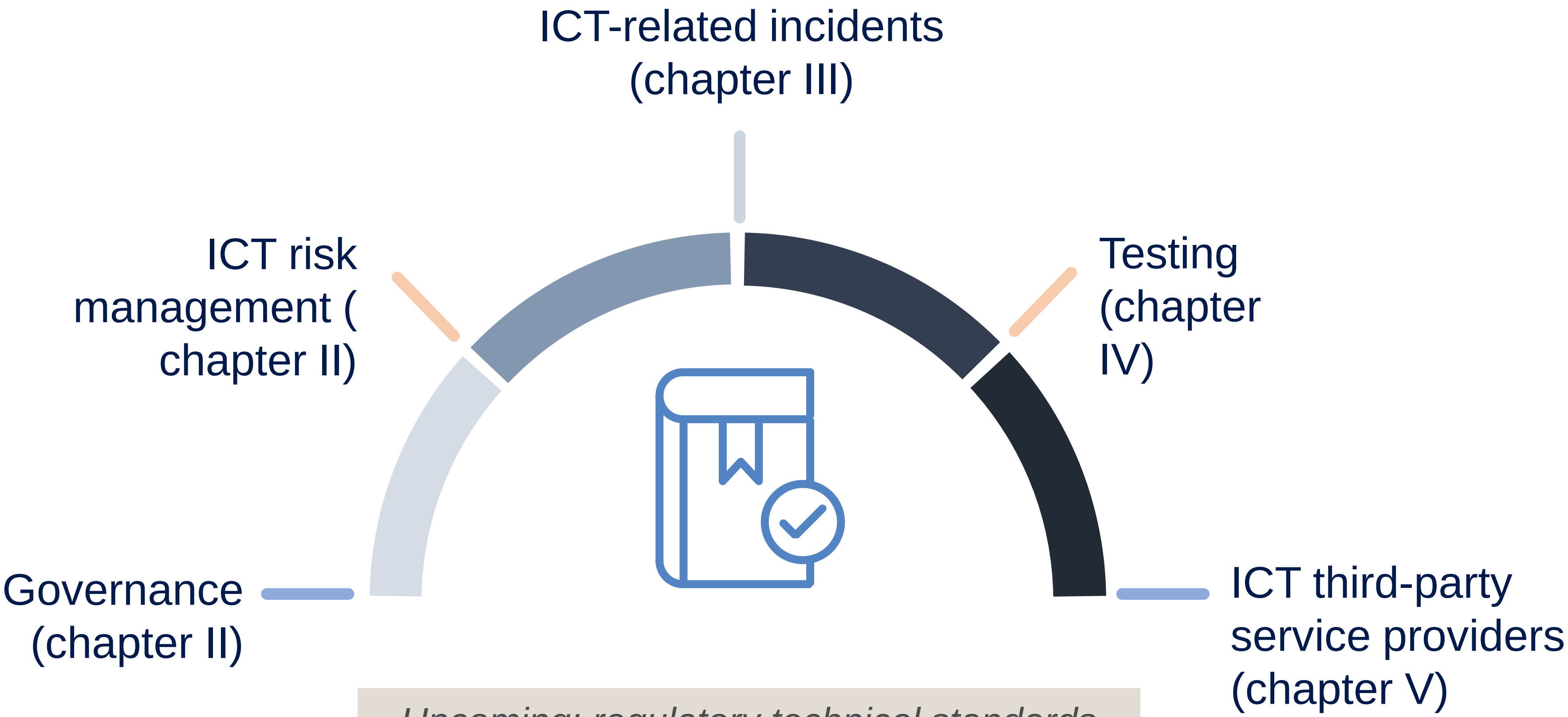
ICT risks

Improving financial entities' management of ICT risks

Third party risks

Improve financial entities' awareness of risks due to dependence on ICT third-party service providers

Requirements



Governance (chapter II)

ICT risk management (chapter II)

ICT-related incidents (chapter III)

Testing (chapter IV)

ICT third-party service providers (chapter V)

Upcoming: regulatory technical standards

Requirements: *governance*

- The management body of the financial entity shall define, approve, oversee and be accountable for the implementation of all arrangements related to the ICT risk management framework
- Members of the management body to keep knowledge on ICT risks and the impact thereof up-to-date, including through regular training
- Specific role to be established or member of senior management to be designated to monitor the (risk exposure and documentation of) arrangements for ICT services, especially those with ICT third-party service providers

Requirements: *ICT risk management*

- A sound, comprehensive and well-documented ICT risk management framework to ensure a high level of digital operational resilience
- Covering identification, protection and prevention, detection, response and recovery, learning and evolving and communication
- Up-to-date ICT systems, with enough capacity and resilience in case of stress scenarios
- Three lines of defence-model for ICT risk management
- Annual and periodic review, review after major ICT-related incident and when instructed by the supervisory authority

Requirements: *ICT-related incidents*

- Internal processes to detect, manage and notify ICT-related incidents
- All ICT-related incidents (*and* significant cyber threats) to be recorded
- Timely reporting of ‘major’ ICT-related incidents to the relevant competent authority
- Informing clients about a major ICT-related incident and significant cyber threat
- Voluntary reporting of significant cyber threats
- (Major) operational incidents and security incidents (previously PSD 2) subject to DORA’s incident framework

Requirements: *testing*

- Financial entities to establish, maintain and review a sound and comprehensive digital operational resilience testing programme
- Tests to be undertaken by independent parties, whether internal or external
- Critical systems are tested at least yearly
- Also ‘advanced’ testing: threat led penetration testing at least every three years for certain identified financial entities

Requirements: *ICT third-party service providers*

- Financial entities to adopt strategy on ICT third party risk (individual and consolidated basis)
- Financial entities to maintain a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers, distinguishing between those that cover critical or important functions and those that do not (individual and consolidated basis)
- Register is shared yearly with the competent authorities or upon their request
- Due diligence on envisaged ICT services and their providers required
- Competent authority to be informed in case of ICT services concerning critical or important functions
- Additional requirements regarding ICT third-party service providers outside the EU
- Existing and new contractual arrangements on ICT services to include specific provisions (e.g. on termination, exit or audit) – not only for outsourcing
- New oversight framework for ICT third-party service providers designated by European Supervisory Authorities (ESAs) as ‘critical’ for financial entities
- Financial entities may *not* use critical ICT third-party service providers based outside the EU that have not established an EU subsidiary within 12 months of designation
- Critical ICT-third party service provider does not have to perform services out of EU subsidiary

Final notes: *information sharing (chapter vi)*

- Financial entities may exchange amongst themselves *cyber threat* information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools, to the extent that such information and intelligence sharing:
  - takes places within ‘trusted communities’
  - is implemented through information-sharing arrangements that protect the potentially sensitive nature of the information shared (business confidentiality, protection of personal data and guidelines on competition policy)

Some other key points

Overlap between DORA and Guidelines, but differences in scope and substance

DORA goes beyond outsourcing: all ICT-related contracts in scope.

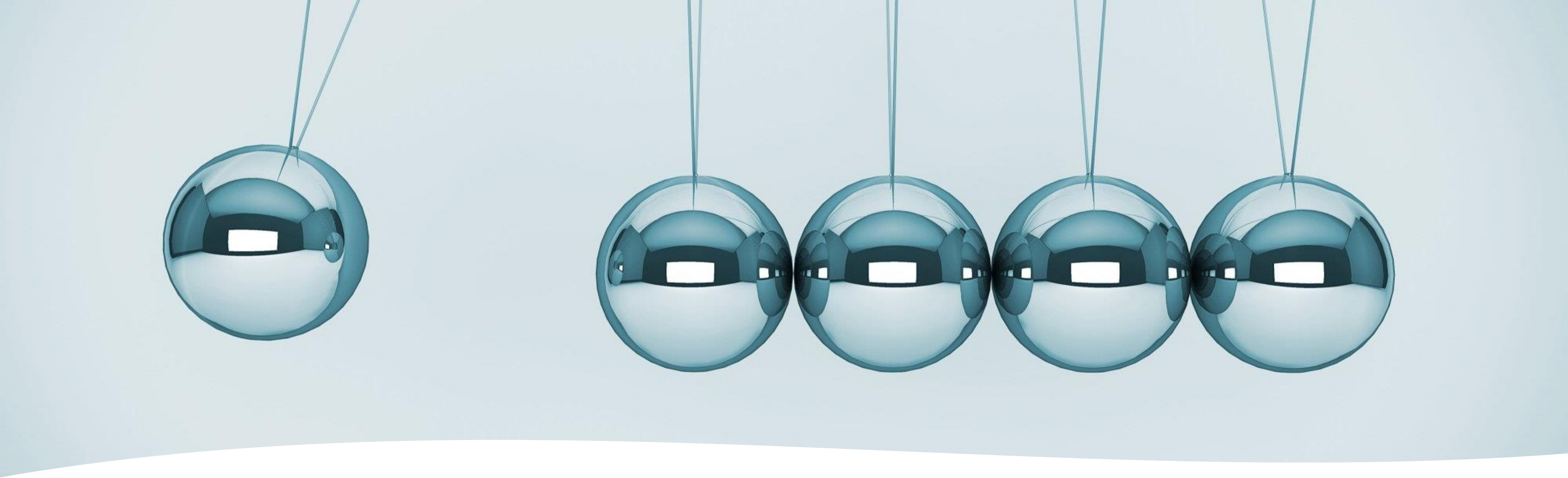
No grandfathering of existing ICT-related contacts; contracts to be repapered by 17 January 2025

Level II (RTS): Further details of requirements

Deadline for the ESAs final standards

RTS Regulatory Technical Standards

By 17 January 2024	By 17 July 2024	By 17 January 2025
RTS on procedures regarding ICT incident and cyber threat classification	RTS regarding reporting of ICT incidents	ESA report on the establishment of a central EU-hub for incident reporting
RTS on level of detail required in firms' ICT third-party provider strategies	RTS on scope and additional elements for advanced testing requirements	
RTS specifying further elements of the ICT risk management framework	RTS on key contractual provisions for subcontracting function	
RTS on the Register of Information on ICT third-party contractual arrangements	RTS on information to be provided by a CTPP to the Lead Overseer	
RTS specifying further elements of the ICT risk management framework	Delegated Act from the Commission on CTPP designation and on the oversight fees for CTPPS	
	RTS on the designation of members of a Joint Examination Team	



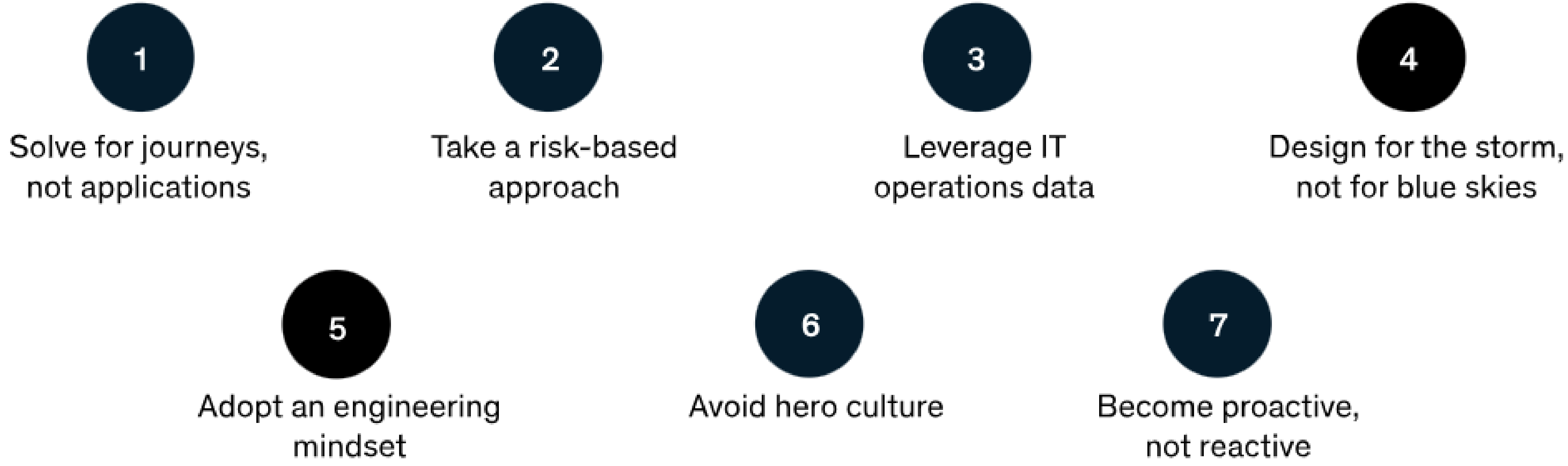
Impact of DORA

Reduce the possibility/duration of ransomware, data leakage, downtime, bad software quality at bank level → keeping the *trust level* in the bank high

More focus on:

- **Software quality** through more/better performance testing, load testing
- **Critical business functions**, instead on solely applications (complete fallback test for business functions)
- **Stakeholder management** in the incident process and (pro)active informing our customers
- **Disaster-Recovery** scenarios
- (digital) **3rd party** suppliers and the possible risks
- **Information security** (i.e. detect and response mechanisms)

What should DORA bring in our *actions* and *mindset*



1. Solve for journeys, not applications
2. Take a risk-based approach
3. Leverage IT operations data
4. Design for the storm, not for blue skies
5. Adopt an engineering mindset
6. Avoid hero culture
7. Become proactive, not reactive

Learnings from the DORA Implementation at de Volksbank

de volksbank

asn bank BLGwonen RegioBank SNS

Lessons learned on DORA implementation, but this approach can be useful for implementation of other legislation as well

1. **Start early** (sorry, too late for this lesson learned now) de Volksbank in general not so good in timely and fully implementing new regulations. Several observations in my previous role as Chief Auditor. When switching from 3rd to 1st line I wanted to do this differently.
2. **Knowledge sharing** with peers
3. **DORAThon**, perform a gap analysis with all parties involved in hackathon style: good for insights, focus and collaboration
4. Define your **critical and important functions** (this can create quite some discussion)
5. Choose an approach with **linking DORA to all relevant internal policies** and roll out work packages to all relevant departments. Our **decentral organisation** does not make quick progress, standardisation and demonstrability very easy and created some budget and staffing issues for DORA
6. Spend a lot of time to **educate and train the organisation**, especially business owners of applications
7. **Implementation of ALM/LCM (for overview), Major Incident Management and BCM application modules**
8. **Adjusting contracts with suppliers** takes a lot of time and effort: especially when there is already a backlog at Procurement: remediation on Procurement process and contracts was still ongoing
9. Make your DORA implementation really **sustainable and demonstrable. Demonstrability** often is an issue and difficult to realise
10. So therefore: **create once, use many** (for multiple assurance assignments

Finally: **Make DORA a blessing in disguise! And more to come**, because we are still implementing

Impact for de Volksbank | efforts needed to comply with DORA

		Requirements to do (85)	Requirements with low impact < 6 months realisation time (51)	Requirements with big impact > 6 months realisation time (34)
DORA pilars	**Governance**	4	1	**3**
	ICT risk management	36	22	**14**
	ICT incident reporting	9	7	**2**
	Testing digital operational resilience	16	8	**8**
	ICT third-party service providers	20	13	**7**
		85	**51**	**34**

Epic owners in relation to the DORA pillars | the expertise centres are responsible for designing and the implementation of the DORA requirements

DORA pillars

DORA scope	Departments responsible for design, policy setting & trigger for implementation
Governance	EC Risk – Kern BRT Tech, Klant & Bankieren EC HR
ICT risk management	EC Tech – Kern Security & Continuity EC Tech – Kern IT Processen EC Tech – Kern Architectuur EC Risk – Kern BRT Tech, Klant & Bankieren
ICT incident reporting	EC Tech – Kern IT Processen EC Tech – Kern Security & Continuity EC Risk – Kern BRT Tech, Klant & Bankieren EC Risk – Supervisory Office
Testing digital operational resilience	EC Tech – Kern Security & Continuity EC Tech – Kern IT Processen
ICT third-party service providers	EC Tech – Kern Security & Continuity EC Tech – Kern IT Processen EC Risk – Kern BRT Tech, Klant & Bankieren EC Risk – Supervisory Office

Examples of DORA requirements and activities | overview of requirements that de Volksbank has to comply with (from analysis performed in Q1 2023)

DORA scope

DORA makes the Volksbank organization as a whole more operationally resilient → therefore not exclusively an ICT matter

DORA applies to: 1) all internal business functions of de Volksbank and
2) all external ICT service providers that support these business functions

DORA pillars

Governance

- ❑ The Boards and senior management are involved, supervise and responsible for the realization and implementation of DORA
- ❑ The Boards and senior management keep knowledge about ICT risks and their impact up-to-date, including through regular training
- ❑ De Volksbank has an internal governance and control framework that ensures effective and prudent management of ICT risk

ICT risk management

- ❑ There is a thorough, comprehensive and well-documented ICT risk management framework→ EC Tech "From Policy to Impact!"
- ❑ ICT systems are up-to-date, with sufficient capacity and resilience in case of stress scenarios
- ❑ Annual and periodic review after major ICT-related incident, also at request of the competent authority

ICT incident reporting

- ❑ Customers are informed in a timely manner about major ICT-related incidents and significant cyber threats
- ❑ Major ICT-related incidents and cyber-threats are reported to the relevant competent authority
- ❑ (major) operational and security incidents (formerly PSD 2) are covered by DORA

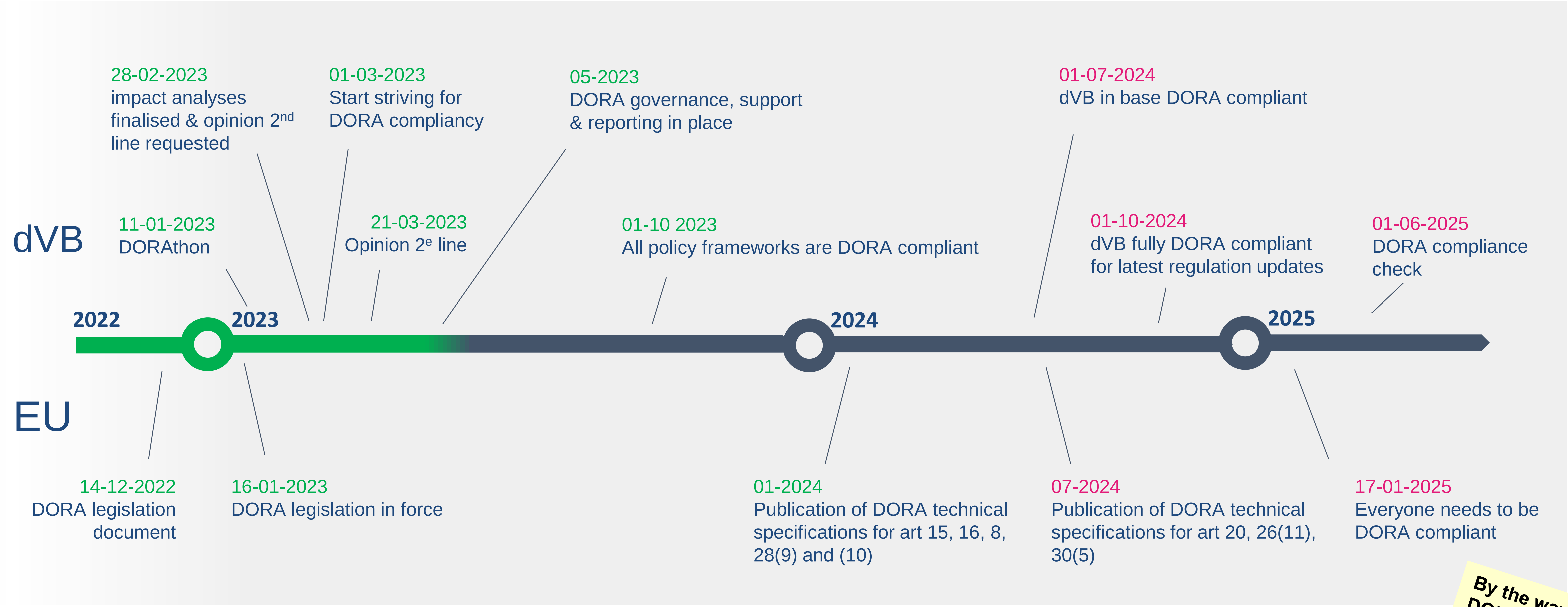
Testing digital operational resilience

- ❑ There is a comprehensive digital operational resilience testing program, critical systems are tested at least annually
- ❑ Cyber threat tests are carried out internally or externally by independent parties
- ❑ Test findings are reported and resolved

ICT third-party service providers

- ❑ All contract agreements with ICT third-party service providers contain specific DORA provisions (e.g. about termination, exit or right to audit)
- ❑ Critical ICT third-party service providers are designated by European Supervisory Authorities (ESAs)
- ❑ De Volksbank can’t have contracts with critical ICT third-party service providers from outside the EU that do not have an EU subsidiary

Roadmap | critical dates and milestones towards DORA compliancy



28-02-2023
impact analyses finalised & opinion 2nd line requested

01-03-2023
Start striving for DORA compliancy

05-2023
DORA governance, support & reporting in place

01-07-2024
dVB in base DORA compliant

11-01-2023
DORAthon

21-03-2023
Opinion 2e line

01-10 2023
All policy frameworks are DORA compliant

01-10-2024
dVB fully DORA compliant for latest regulation updates

01-06-2025
DORA compliance check

14-12-2022
DORA legislation document

16-01-2023
DORA legislation in force

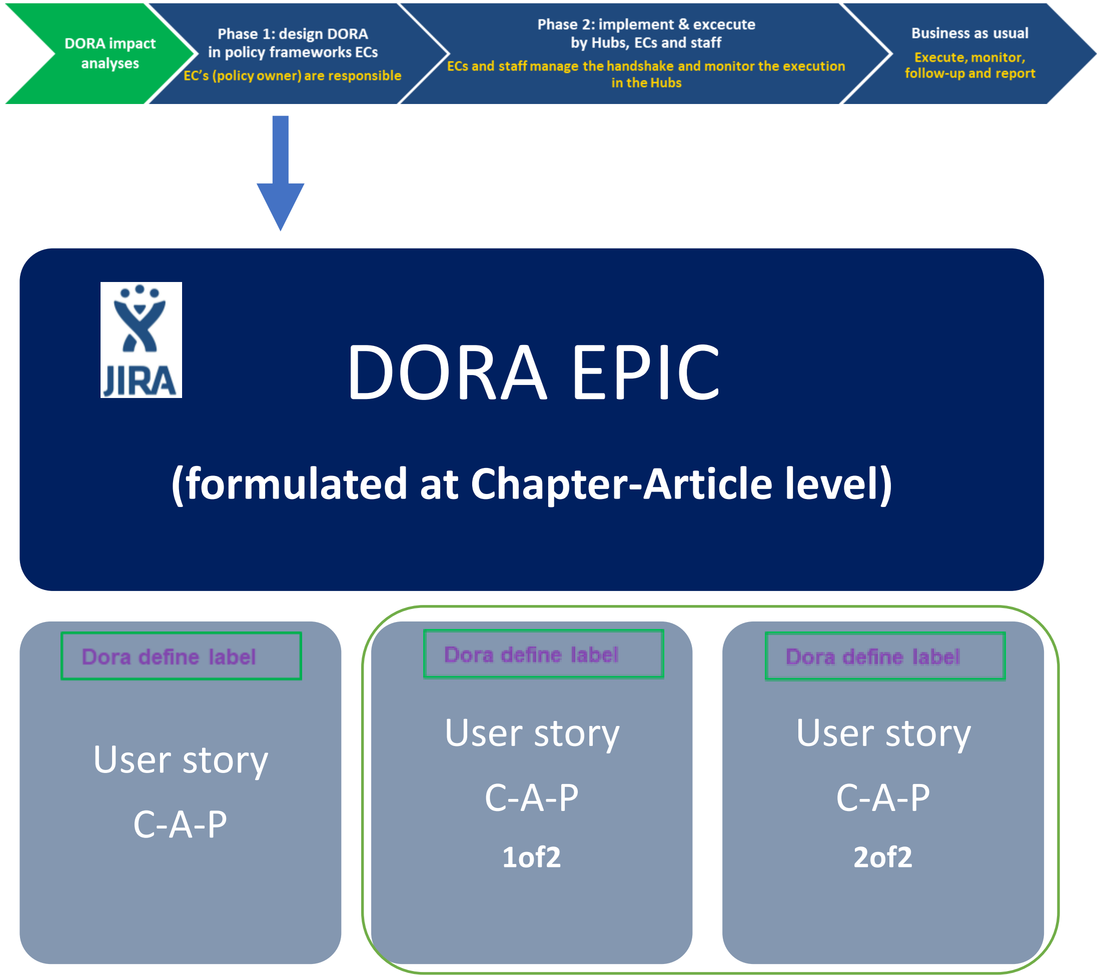
01-2024
Publication of DORA technical specifications for art 15, 16, 8, 28(9) and (10)

07-2024
Publication of DORA technical specifications for art 20, 26(11), 30(5)

17-01-2025
Everyone needs to be DORA compliant

By the way. DORA will not stop…

Way of working for phase 1 | Agile tooling JIRA is used for DORA work distribution and progress tracking. EPICS are defined as Chapter-Article and User Stories on paragraph level



DORA impact analyses

Phase 1: design DORA in policy frameworks ECs

EC's (policy owner) are responsible

Phase 2: implement & excecute by Hubs, ECs and staff

ECs and staff manage the handshake and monitor the execution in the Hubs

Business as usual

Execute, monitor, follow-up and report

DORA EPIC

(formulated at Chapter-Article level)

Dora define label

User story

C-A-P

Dora define label

User story

C-A-P

1of2

Dora define label

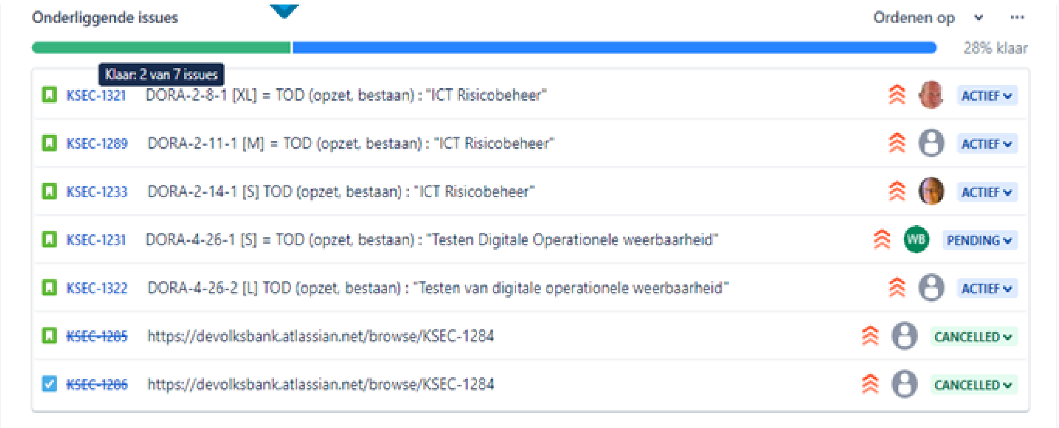
User story

C-A-P

2of2

Weekly progression monitoring

1. **Qualitative** in weekly progression dialogs (status, progress, impediments)
2. **Quantitative** in Jira via progress on finished user stories (i.e. by filtering on Dora define label)



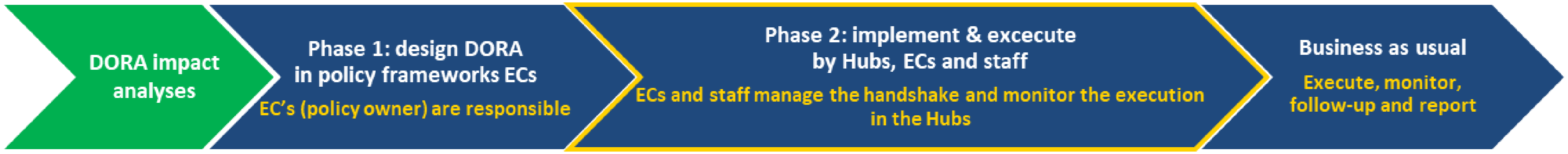
Onderliggende issues — Ordenen op ⌄ ···

28% klaar

Klaar: 2 van 7 issues

KSEC-1321	DORA-2-8-1 [XL] = TOD (opzet, bestaan) : "ICT Risicobeheer"	ACTIEF ⌄
KSEC-1289	DORA-2-11-1 [M] = TOD (opzet, bestaan) : "ICT Risicobeheer"	ACTIEF ⌄
KSEC-1233	DORA-2-14-1 [S] TOD (opzet, bestaan) : "ICT Risicobeheer"	ACTIEF ⌄
KSEC-1231	DORA-4-26-1 [S] = TOD (opzet, bestaan) : "Testen Digitale Operationele weerbaarheid"	WB PENDING ⌄
KSEC-1322	DORA-4-26-2 [L] TOD (opzet, bestaan) : "Testen van digitale operationele weerbaarheid"	ACTIEF ⌄
~~KSEC-1285~~	https://devolksbank.atlassian.net/browse/KSEC-1284	CANCELLED ⌄
☑ ~~KSEC-1286~~	https://devolksbank.atlassian.net/browse/KSEC-1284	CANCELLED ⌄

Phase 2 | Implementation | ECs make logical work items to be implemented by Hubs or ECs



DORA impact analyses

Phase 1: design DORA in policy frameworks ECs

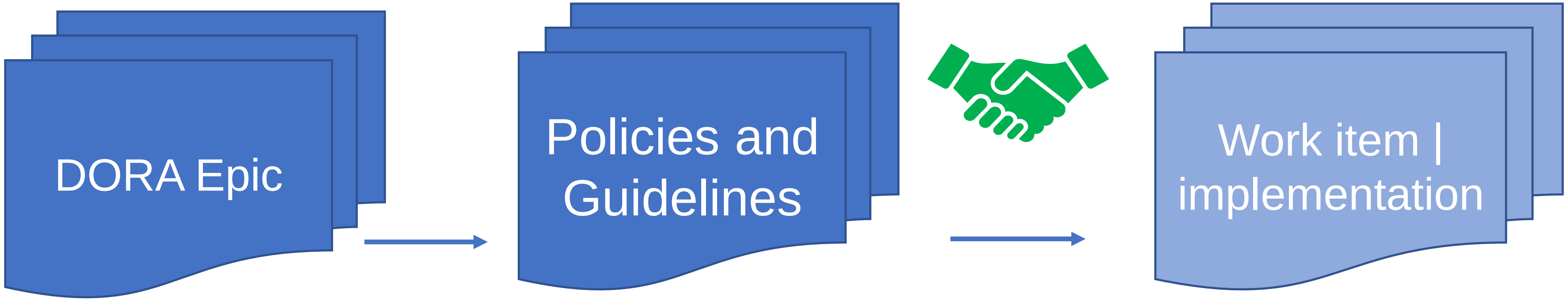
EC's (policy owner) are responsible

Phase 2: implement & excecute by Hubs, ECs and staff

ECs and staff manage the handshake and monitor the execution in the Hubs

Business as usual

Execute, monitor, follow-up and report

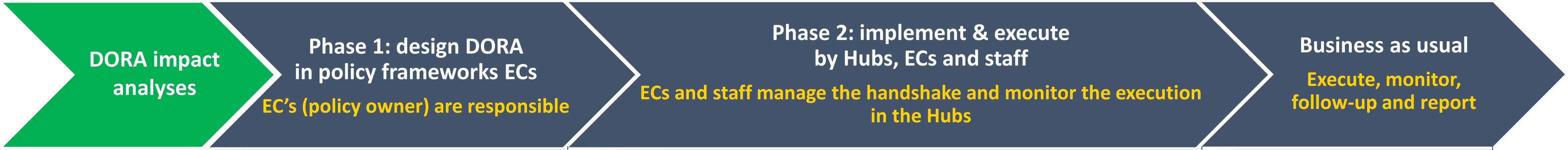


DORA Epic

Policies and Guidelines

Work item | implementation

Approach and priorities | the DORA roadmap consists of two phases 1) policy definition and 2) policy implementation. Priorities are set for phase 1



DORA impact analyses

Phase 1: design DORA in policy frameworks ECs

EC's (policy owner) are responsible

Phase 2: implement & execute by Hubs, ECs and staff

ECs and staff manage the handshake and monitor the execution in the Hubs

Business as usual

Execute, monitor, follow-up and report

Central | creation of new and adjusted policy frameworks

1

Urgency on 3rd party | ECs start with the pilar *ICT third party service providers.*

Big chunks | *high impacted requirements* with an implementation period between 6 months a 1 year.

Smaller pieces | Then the *last requirement* with an implementation period 6 months at maximum.

Target date is at the end of Q3 2023 all the requirements are integrated with the policy frameworks.

Decentral | implementation is done by all the Hubs

Logical and efficient work packages will be "handed over" for implementation. Where ECs and staff support Hubs in adjusting their way of working.

The **complexity and interconnections** between the DORA requirement is high. Therefore, we use **de Volksbank way of working** (RACI) to distribute the new and or adjusted tasks and responsibilities. This can be new for some departments.

Business as usual

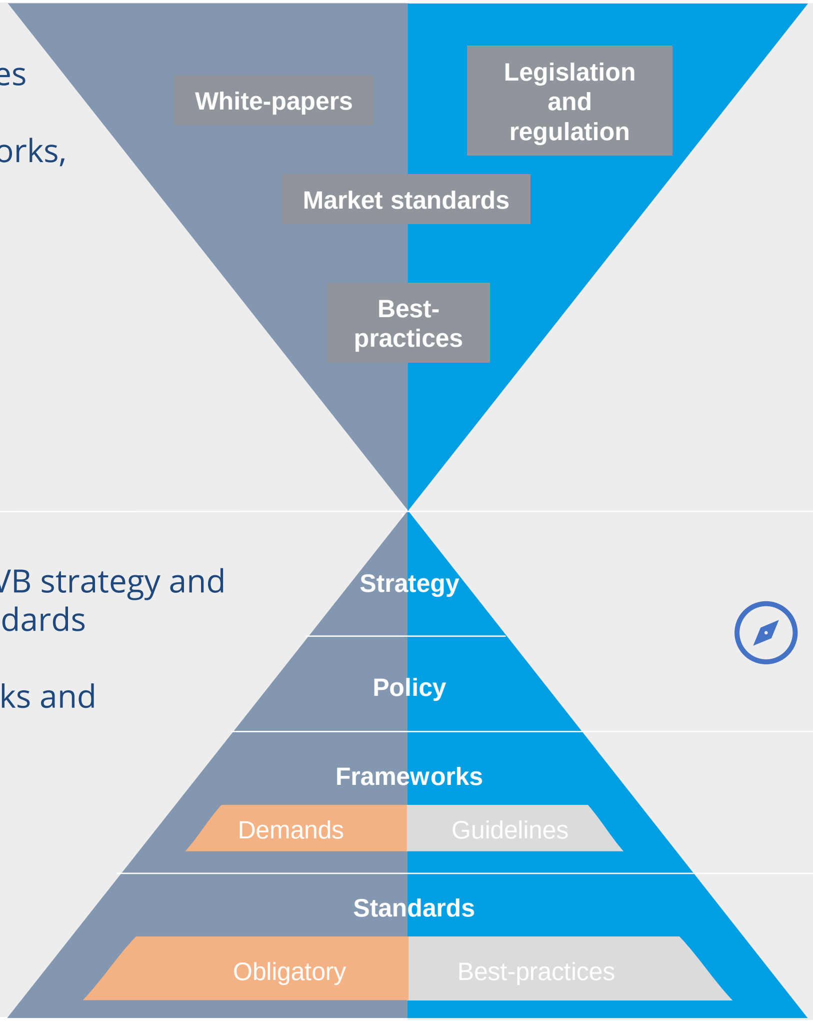
In the 2nd half of 2024 all the DORA requirements are integrated within the policy framework (processes included) and executed by Hubs.

The existing monitoring, follow-up and reporting for compliance to the standards from EC Risk and EC Compliance will be used

First priority on 3rd party requirements ready to be implemented

IT Systems Risk | from legislation/regulation, best practices and market standards – to policy, frameworks and execution

External
Legislation and regulation, best-practices
And market standards are input
for the IT (risk) strategy, policy, frameworks,
Implementation and execution



White-papers

Legislation and regulation

Market standards

Best-practices

Strategy

Policy

Frameworks

Demands

Guidelines

Standards

Obligatory

Best-practices

DNB/ECB/EBA Guidelines
DORA, Privacy
NOREA, OWASP
COBIT, NIST,
IT4IT, CCM,
CIS, etc...

Internal
From concrete (risk) targets linked to dVB strategy and
external legislation/regulation and standards

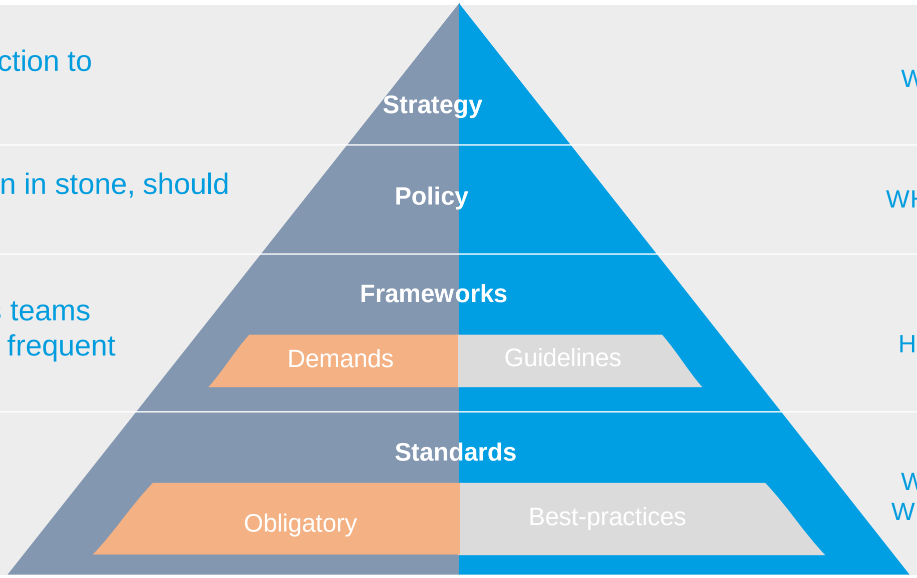
To understandable appliable frameworks and
Standards for BizDevOps teams

RP IT Systems Risk

Procedures & controls

Tools & instructions

From policy to impact | clear and consistent structure, facilitating effective execution combined with reporting and risk acceptance



			TARGET GROUP
Translation of the de Volksbank strategy and connection to risk & security for customer and regulator	Strategy	WHY	Hubs, EC's, Regulators
The (risk) goals to realise this strategy. Static, written in stone, should stay stable for several years.	Policy	WHAT	Hubs, EC's, Risk, Regulators
Translation of policies to frameworks for BizDevOps teams to meet/use to help reaching policy goals. Dynamic, frequent adaptation depending on threats and regulation.	Frameworks	HOW	Product Owners, Engineers, Risk
Concrete tools for BizDevOps teams to live up to the goals with obligatory standards and/or best-practices. Easy to find and self-explaining	Standards	WITH WHAT	Engineers

Define	Implement	Execution by Hubs, ECs, Staff departments	Monitor, follow-up and report	Risk registration
Design polies with BizDevOps teams and Platform Hub	Implementation with BizDevOps teams and Platform Hub	Execution by BizDevOps teams	Hubs, ECs, Staff departments, EC's regulate and escalate	Transparency & in control

Lessons learned from moving from 3rd to 1st line

Lessons learned from my move from 3rd to 1st line

Chief Audit Executive

33 operational and IT auditors

April 2022

IT Director

750 - 1000 IT engineers, architects, process & security specialists, managers, etc.

Lessons learned from my move from 3rd to 1st line

1. **High over reporting** on issues is useful for the executive and supervisory boards but often not sufficient for creating full impact in the business: I was already aware of many issues but they were much more severe and structural than as seen from an audit point of view
2. **How really visible in the organization are you and your team?** Looking at Audit from this role, Audit is even less visible than I thought!
3. **Too much auditing by emailing and videoconferencing**: do you than actually see what is happening? Data analytics including process mining is one of the things to get better insights into what is actually happening.
4. Although already fully aware of the need to do this: still spend more time on **root cause analysis** (7 times why) Really understand how busy first line management is and why things are not seen, not prioritized, not done.
5. Often: **do not make use of second line insights and work too much**: too often they were way to far from seeing and understanding what is really happening in the business, especially when looking at non-financial risks.
6. **Knowing the capabilities of audit staff** helps to better ask for support from them and / or pointing out useful audits and audit scopes. Help the business better understand what the audit department is capable of (don't expect this to be known info)
7. Finally, what I already said when I was heading the audit department and is to my opinion still applicable: the more you dare to cooperate with 1st and 2nd line the more added value you can deliver, **do not be too afraid of losing independence**: almost all auditors tend to have a very good GPS to remain independent, and just provide the right training to keep those GPS calibrated.
8. **It's really hard work in the first line, give them some slack and understanding sometimes!**