



DORA Experiences Event

An event by the NOREA DORA Taskforce

14/05/2025

Program of the day

- ❖ 14.30 Walk-in (with drinks)
- ❖ 14:45 Opening by Rene Zendijk
- ❖ 15.00 DORA Taskforce product launch - Sandeep Gangaram Panday
- ❖ 15.20 Speaker I - DNB Marcel Verhoeven
- ❖ 15.50 Speaker II - Achmea Martijn de Laat & Christopher Nield
- ❖ 16.20 Break
- ❖ 16.35 Speaker III – CM.com Anjeni Bedi
- ❖ 17.05 Panel moderated by Shairesh Algoe
- ❖ ~ 17.45 Closing with drinks & dinner (BBQ)

NOREA DORA Taskforce



Otto Hulst
Beleidsadviseur
Pensioenfederatie



Marvin Kruin
ZZP IT auditor



Nico Mossel
CISO
Bunq



Ibrahim Dogan
ZZP IT auditor
BNG Bank



Jeroen van Bommel
Risk manager
PME Pensioenfonds



Rico Zundert
CISO
Argenta



Dirk-Jan Knaapen
Manager IT
TVM verzekeringen



Danny Bos
Senior manager
Eraneos



Christopher Nield
Senior Risk manager
Achmea & DUFAS



Shairesh Algoe
CISO
Quantum Foundation



Arno Kroese
Director
KPMG



Jeremy Oschmann
Customer Director
Schuberg Philis



Jesper de Boer
Director IT Audit &
Assurance
Deloitte



René Zendijk
Head Internal Audit
Scildon



Shankar Sahtie
Consultant
Securesult



**Sandeep Gangaram
Panday**
Trust Officer
Schuberg Philis



Wilfred Hanekamp
IT auditor / Partner
Afier



Yvonne Telleman
Consultant
Argis



Rob Imming
ZZP
DigiNovus



Ali Karaagac
ZZP IT auditor
BNG Bank



Harry Boersen
Consultant
Ayvens



Jacco Jacobs
Director
Norea

SPEECH

A race we cannot afford to lose: cybersecurity in an age of geopolitical tensions



'To keep financial institutions and the financial system safe, resilience against cyberattacks has become just as important as holding sufficient capital and liquidity.', said Steven Maijoor at the ISDA Annual General Meeting in Amsterdam today. In his speech he talked about the cyber threat against the financial industry, and market infrastructures in particular.

Published: 14 May 2025



To keep financial institutions and the financial system safe, resilience against cyberattacks has become just as important as holding sufficient capital and liquidity. So we need to do whatever we can to further boost it. Both in terms of detection and recovery. And we need to work together. Governments, banks, market infrastructures, supervisors, telecom, energy and other vital players in the outsourcing chain. Because this is a race we cannot afford to lose.



DORA in Control

A Practical Guide to Achieve Enhanced Digital Operational Resilience

A study report by NOREA

Authors:

S. Gangaram Panday – Schuberg Philis

J. Oschmann – Schuberg Philis

© 2024 NOREA, All rights reserved

PO box 242, 2130 AE Hoofddorp

Phone: +31 (0) 88 4960 380

The Netherlands

e-mail: norea@norea.nl



DORA in Control

A Practical Guide to Achieve Enhanced Digital Operational Resilience

A study report by NOREA

Authors:

S. Gangaram Panday – Schuberg Philis

J. Oschmann – Schuberg Philis

©2024 NOREA, All rights reserved

PO box 242, 2130 AE Hoofddorp

Phone: +31 (0) 88 4960 380

The Netherlands

e-mail: norea@norea.nl

DORA in Control

Key features



Accessible language



Actionable controls



DNB maturity model



Progress tracking



DNB58 mapping

DORA Simplified

Governance and Risk Management

1. Management responsibilities
2. Risk management framework
3. Risk assessments
4. (Internal) ICT audit

Operational Management

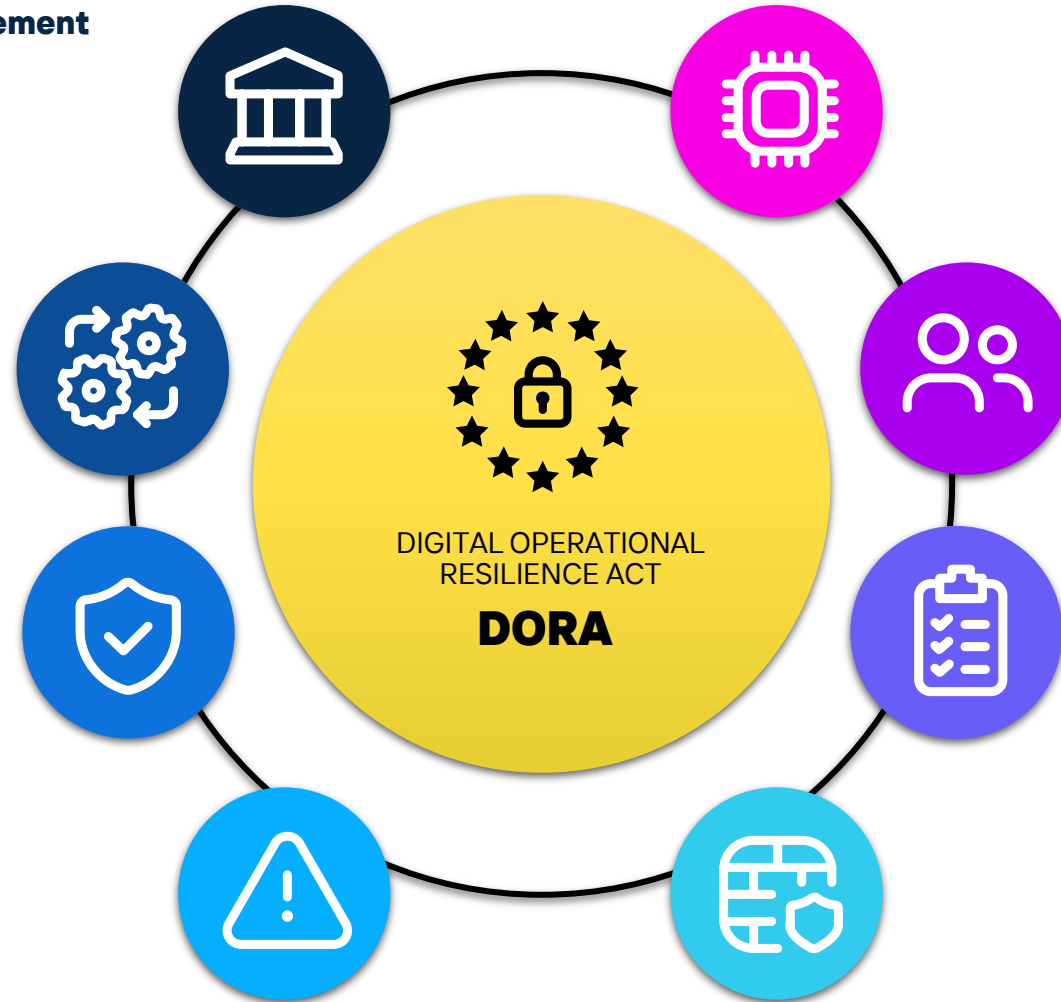
5. Asset management
6. Change management
7. ICT operations

Continuity Management

8. Backup management
9. Response & recovery

Incident Management

10. Incident classification
11. Incident management



Software and Systems Development

12. Acquisition, development, and maintenance
13. Project management

Third-party Risk Management

14. Third-party due diligence and selection
15. Third-party (standard) contract management
16. Third-party (critical) contract management
17. Third-party risk management
18. Subcontracting management

Resilience Testing

19. Digital operation resilience testing
20. Threat-led penetration testing

Security Management

21. Architectural and network security
22. Security monitoring & log management
23. Data and (legacy) system security
24. Encryption and cryptography
25. Identity and access management
26. Physical and environmental security
27. Security awareness
28. Vulnerability and patch management



Progress Dashboard

DORA Domains:	Code:	Sub-domain ID:	Sub-domain:	Control ID	Control:	Control description:	DORA Level 1 and 2 Articles:
Governance and Risk Management	GRM	1	Management Responsibilities	1.1	Governance of ICT risk	The Management body shall take ultimate responsibility for effectively managing all ICT risks of the financial entity. As such, the management body periodically (e.g. annually) reviews and approves: - Policies related to the availability, authenticity, integrity, and confidentiality of data, including the policy on arrangements with ICT third-party service providers (see control 2.1). - The roles, responsibilities and governance arrangements for ICT risk management (including those related to ICT third-party arrangements), including the continuous monitoring thereof. - the policy on arrangements with ICT third-party service providers and stays informed about third-party arrangements, services provided, planned material changes regarding third-party service providers, and understand the impact of these changes on critical and important functions of the entity (including risk assessment results).	5.1 5.2 5.3 5.4 6.8 13.4 13.7
Governance and Risk Management	GRM	1	Management Responsibilities	1.2	Knowledge of the Management Body	The Management body shall ensure that it is kept up to date with sufficient knowledge and skills to understand and assess ICT risks and operations (e.g. through periodic trainings).	
Governance and Risk Management	GRM	1	Management Responsibilities	1.3	Digital Operational Resilience Strategy	The Management body shall set and approve the digital operational resilience strategy and periodically update when needed. The digital operational resilience strategy must: - Set out how the risk management framework will be implemented. - Elaborate on the alignment between the risk management framework and the business strategy and objectives. - Establish the ICT risk tolerance level (based on risk appetite) and the impact tolerance level for ICT disruptions. - Include clear security objectives, including Key Performance Indicators (KPIs) and risk metrics. - Elaborate on the ICT reference architecture and any changes needed to reach specific business objectives. - Outline the mechanisms in place to detect ICT-related incidents - Contain evidence to prove the current digital operational resilience situation (e.g. based on the number of major ICT-related incidents and the effectiveness of preventive measures. - Contain how the digital operational resilience testing is implemented (see controls under 19 and 20). - Outline the communication strategy in case of incidents (see 11.3) The Management body shall allocate and review the budget required for resources to fulfill the digital operational resilience needs of the entity. Ensure monitoring is arranged on the effectiveness of the implementation of the digital operational resilience.	
Governance and Risk Management	GRM	1	Management Responsibilities	1.4	Business Continuity Oversight	The Management body reviews and approves periodically (e.g. annually) the ICT business continuity policy and the ICT response and recovery plans.	
Governance and Risk Management	GRM	1	Management Responsibilities	1.5	Audit Plan Approval and Review	The Management body reviews and approves periodically (e.g. annually) internal ICT audit plans, ICT audits, and material modifications to the audits.	

DORA in Control Framework

DORA in Control is endorsed by:

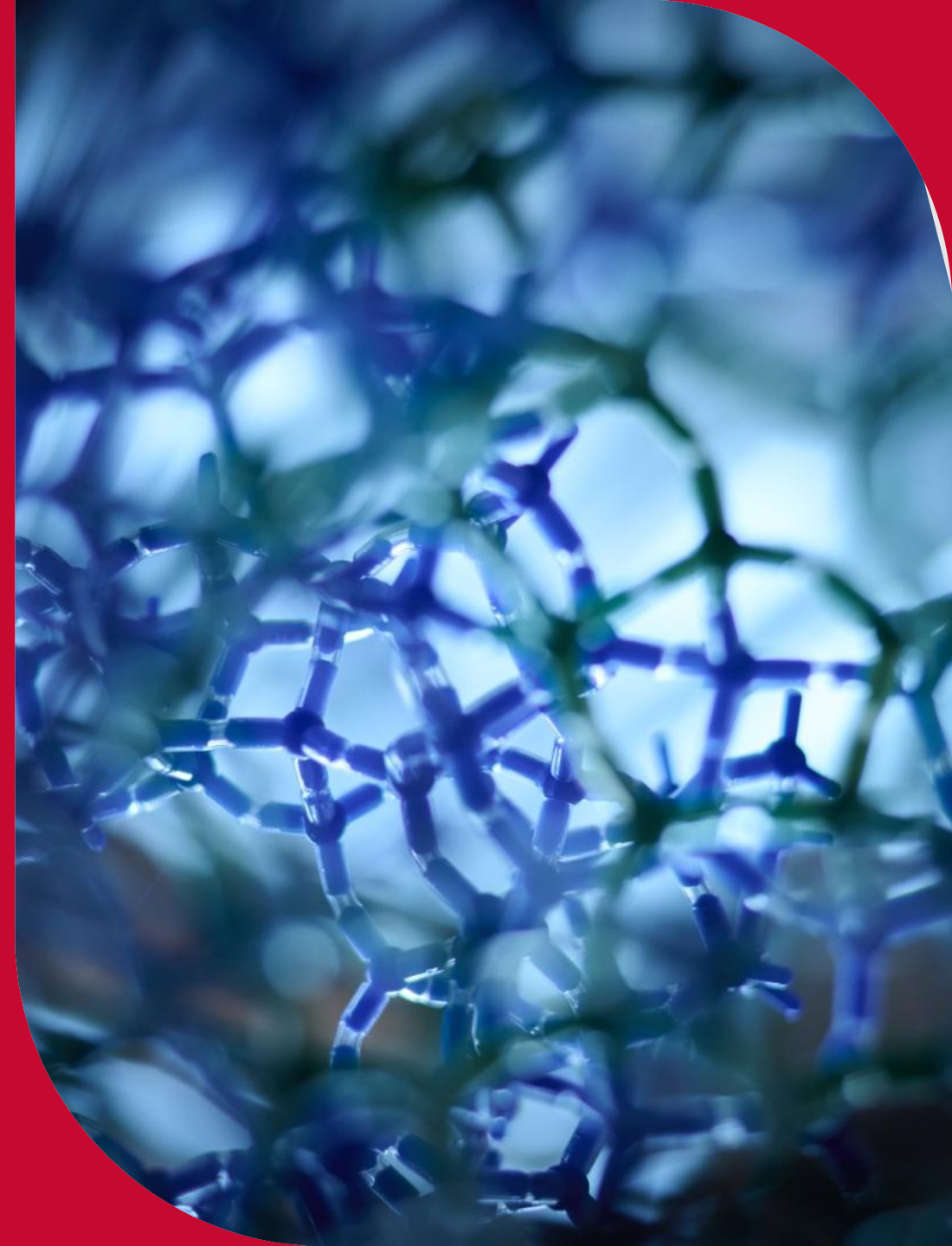


VERBOND VAN VERZEKERAARS



DORA Control Framework V3.1

- DORA Control framework becoming more and more a market standard
- 8400 downloads
- Followers on LinkedIn from 40+ countries
- We received some feedback from users for improvements



DORA Control Framework V3.1

Since publication of the framework in October 2024, the following standards changed:

RTS/ITS	Impact on the controls	Changed controls
RTS on content, timelines, and templates on incident reporting	No	N/A
ITS Major incident Reporting	No	N/A
RTS Threat-led penetration testing	Yes	Control 20.2
ITS Register of information	No	N/A
RTS Subcontracting	Yes	Controls: 16.3, 18.1, 18.2, 18.3

DORA Control Framework V3.1

- Additionally, based on feedback we changed 11 other controls
- In total 16 controls have changed
- No new controls have been added
- Detailed change log is included

16.2	Contractual Clauses	Secure rights for continuous performance monitoring, including unrestricted rights to access, inspection, and audit. This encompasses alternative assurance levels, cooperation with regulator inspections, and full disclosure of audit scope, procedures, and frequency. Include a mandatory transition period upon termination, allowing the service provider to continue services during migration, affording the entity time to transition to another provider or in-house solutions based on service complexity. Mandate the implementation and testing of business contingency plans and the establishment of a security management system by the service provider. Require the service provider's participation in the entity's (advanced) testing program (TLPT), where required.	Secure rights for continuous performance monitoring, including unrestricted rights to access, inspection, and audit. This encompasses alternative assurance levels, cooperation with regulator inspections, and full disclosure of audit scope, procedures, and frequency. Include a mandatory transition period upon termination, allowing the service provider to continue services during migration, affording the entity time to transition to another provider or in-house solutions based on service complexity. Mandate the implementation and testing of business contingency plans and the establishment of a security management system by the service provider. <i>When negotiating contractual arrangements, consider the use of standard contractual clauses developed by public authorities for specific services.</i> Require the service provider's participation in the entity's (advanced) testing program (TLPT), where required. <i>Where participation of an ICT third-party service provider in TLPT may adversely impact services or data confidentiality for customers outside the scope of DORA, it may be agreed in writing to perform a pooled TLPT.</i>
16.3	Third-party Critical Subcontracting Management	Delineate critical and important ICT services in contracts with third-party ICT service providers, specifying conditions for subcontracting. Require continual monitoring of subcontracted services supporting critical functions to ensure compliance with contractual obligations. Detail monitoring and reporting responsibilities of the third-party service provider to the financial entity, including risk assessments related to subcontractor locations and data ownership. Mandate incident response and business continuity plans for subcontractors, along with adherence to specified service levels and security standards. <i>Ensure subcontractors grant the same audit and access rights to the financial entity as the primary service provider.</i> Retain termination rights for the financial entity in cases of unauthorized subcontracting or failure to meet agreed-upon service levels. Implement changes relative to contractual agreements as soon as possible and document the planned timeline for the implementation.	Delineate critical and important ICT services in contracts with third-party ICT service providers, specifying conditions for subcontracting. Require continual monitoring of subcontracted services supporting critical functions to ensure compliance with contractual obligations. Detail monitoring and reporting responsibilities of the third-party service provider to the financial entity, including risk assessments related to subcontractor locations and data ownership. Mandate incident response and business continuity plans for subcontractors, along with adherence to specified service levels and security standards. Ensure subcontractors grant the same audit and access rights to the financial entity as the primary service provider. Retain termination rights for the financial entity in cases of unauthorized subcontracting or failure to meet agreed-upon service levels. Implement changes relative to contractual agreements as soon as possible and document the planned timeline for the implementation.

Download DORA Framework v3.1 here:



www.norea.nl/dora

NEW: BOARDROOM TRAINING GUIDELINE
New publication:

DORA BOARDROOM training
guideline



Guideline DORA Boardroom training

A guideline by NOREA



Guideline DORA Boardroom training

A guideline by NOREA

Key features



Accessible language



Actionable
objectives



DORA requirement
clarified



Build on DORA
control framework



NIS2 included

Domain	Knowledge objectives	Responsibility objectives	Mapping to practical questions for improved boardroom dialogue based on the factsheet from the NCSC ⁵ and CSR ⁶	Typically the responsibility of the management body?
1. Governance & Risk Management	<ul style="list-style-type: none"> Understand the collective and individual role and accountability of the Management Body members Being able to contribute to the definition of the organization's risk appetite and risk tolerance level Understanding the organisation's critical functions and their dependency on ICT services Understanding the organisation's ICT risk management framework and the risk cycle (plan, do, check and act) Understand the expectations of the Digital Operational Resilience Strategy (DORA or NIS2 specific) or IT security strategy 	<ul style="list-style-type: none"> Carry out the management body responsibility for digital resilience and updating the ICT risk framework taking into account the organization's environment (e.g. increased threats or geopolitical developments) Oversee the resilience of most critical ICT and the mitigation of the cyber security risks of the organization within the risk appetite Understand the Internal Audit year plan and specifically, the prioritization and added value of the audits in relation to the key IT risks Oversee compliance with regulatory cyber requirements (DORA or NIS2 specific) or IT security strategy. 	<p>NCSC:</p> <ul style="list-style-type: none"> What are the most pressing issues I need to focus on? What do you need to ensure that management allocates sufficient people and resources to achieve the objectives? What mechanism is in place within the organization to secure the cybersecurity strategy and approval of policies around risk management by management? With what frequency is cybersecurity on the agenda to ensure that there is sufficient progress on this topic? What is the role and task of the CISO when it joins board meetings? As a board member, what do I need to know to gain sufficient insight into this organization's cybersecurity risks? Are risk assessments carried out, if so, what are the main issues and outcomes of the risk assessments carried out? 	Yes

Domain	Knowledge objectives	Responsibility objectives	Mapping to practical questions for improved boardroom dialogue based on the factsheet from the NCSC ⁵ and CSR ⁶	Typically the responsibility of the management body?
	<ul style="list-style-type: none"> Understanding the different types of back-up and recovery strategies 			
4.Incident management	<ul style="list-style-type: none"> Understanding the key aspects of the incident management policy and escalation paths. Understanding classification and reporting of incidents Knowing the most important stakeholders and their roles in the event of a major incident. 	<ul style="list-style-type: none"> Knowing the DORA and NIS2 specific major incident reporting timelines (if relevant also SEC) Knowing how to report major incidents to the supervisory authorities in the different regions Capacity to lead the technical incident response and participate in the strategic response to major incidents 	CSR: <ul style="list-style-type: none"> Do we have an incident response plan? Are we, as a company and as the board, (sufficiently) insured against cyber risks? 	No
5.Software and systems development	<ul style="list-style-type: none"> Understanding the key aspects of the software and systems development policy 	<ul style="list-style-type: none"> Understanding most critical aspects regarding testing systems Understanding how well the required tests are performing 	N/A	No
6.Third-party Risk management	<ul style="list-style-type: none"> Understanding the third-party risk management process incl. supplier management and understand that third party risk must be managed as an integral component of ICT risk and ICT risk management framework Understanding key contractual agreements such as e.g. exit strategy, unrestricted rights of access, inspection and audit and notice periods and reporting obligations of the TPP 	<ul style="list-style-type: none"> Knowing the critical third-party providers of the institution and oversee their periodic evaluation whether the strategy still fits Knowing the impact of changes in the chain of critical subcontractors Knowing the level of compliance to the required security and contractual requirements of the critical third-party providers of the institution Having insight in involvement of the critical third-party providers of 	NCSC: <ul style="list-style-type: none"> Which third parties do we use? CSR: <ul style="list-style-type: none"> Do we know the dependencies of ICT suppliers and do we control the involved risks? 	Yes

Boardroom training guideline available here:



www.norea.nl/dora

Roadmap




Milestone II **DORA Taskforce**

NOREA
Incident Classification Tool

Release date:
28-10-2024

NOREA
DE BUREAUCRANIE VAN IT-AUDITORS



Milestone III **DORA Taskforce**

NOREA
Exit Plan Template

Release date:
11-12-2024

NOREA
DE BUREAUCRANIE VAN IT-AUDITORS



Milestone IV **DORA Taskforce**

NOREA
Boardroom Training Guidelines

Release date:
14-05-2025

NOREA
DE BUREAUCRANIE VAN IT-AUDITORS



Milestone V **DORA Taskforce**

NOREA
Business Continuity Guidelines

To be released:
~06 - 2025

NOREA
DE BUREAUCRANIE VAN IT-AUDITORS



Milestone VI **DORA Taskforce**

NOREA
Proportionality assessment

To be released:
~2025

NOREA
DE BUREAUCRANIE VAN IT-AUDITORS

DORA Experiences Event

14 mei 2025

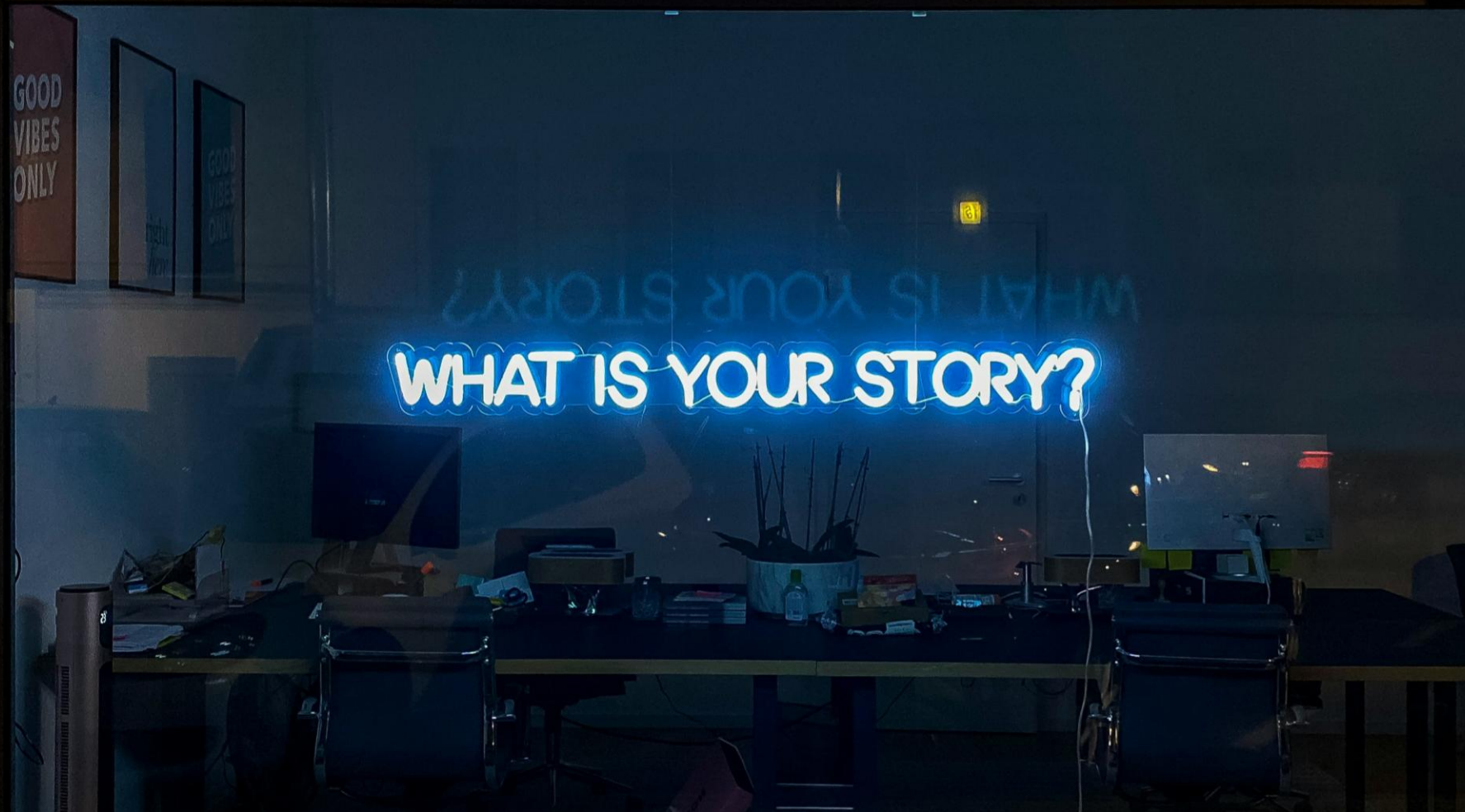
Martijn de Laat

Christopher Nield



We do not have a monopoly of wisdom

We're not going to tell how it should be done – only how Achmea has done its implementation



Today we will share our experiences

To ensure a complete picture, we will do this together



Martijn de Laat
Group Information Security
Officer



Christopher Nield
Program manager DORA ODV

Roadmap

There will be time for questions at the end of the presentation



Setting the scene



Achmea consists of a group of labels and companies

Woven into the fabric of Dutch homes and our financial sector

HAGELONIE

FBTO

achmea 

Mortgages

 INTERAMERICAN
PART OF ACHMEA


Interpolis.
Glashelder

achmea 

Real Estate

achmea 

Farm Insurance

 **avéro** | achmea

 **Zilveren
Kruis**

achmea 

Investment Management


eurocross
assistance

achmea 

Pensioenservices

De Friesland

 EUREKO
SIGORTA


**Centraal
Beheer**


Union
P o i s t o v ň a

achmea 

Bank

inshared 

achmea 

Profile:

We are a financial service provider
by and for customers

Ambition:

Achmea creates sustainable value for
its customers, employees and company
and society at large

Mission

Together we solve major social issues
in the domains:



Bringing
healthcare closer



Smart mobility



Carefree living
& working



Income for today
and tomorrow

Building blocks

1.

Large
customer
base

2.

Skilled
employees

3.

Strong
partner-
ships

4.

Expertise
in data
& digital

5.

Outstanding
financial
position

achmea 

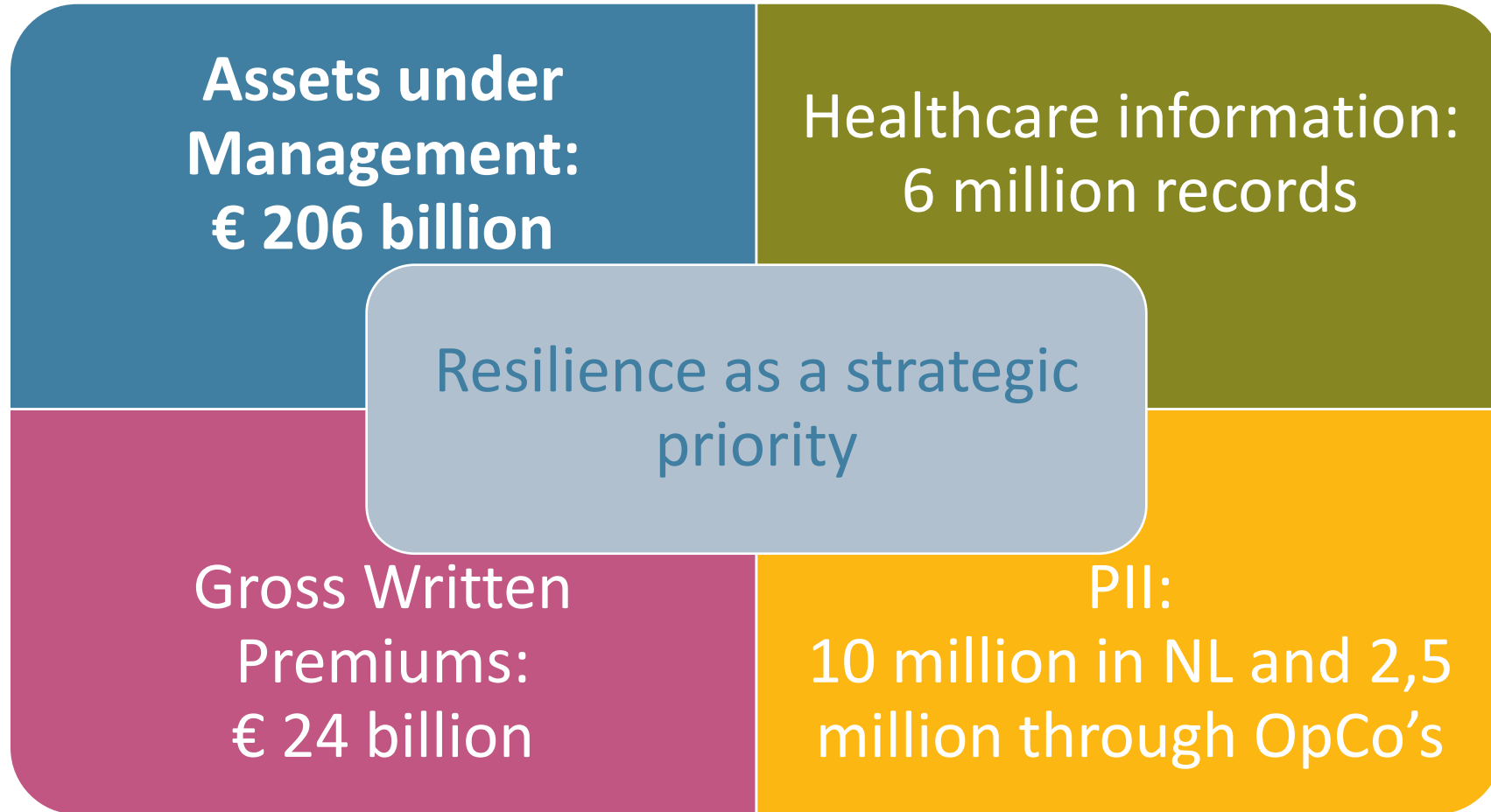

Interpolis.
Glashelder

 Zilveren
Kruis


Centraal
Beheer


Achmea takes her responsibility

A high level of resilience is required, not least because of our interwovenness in homes and lives



Strategy



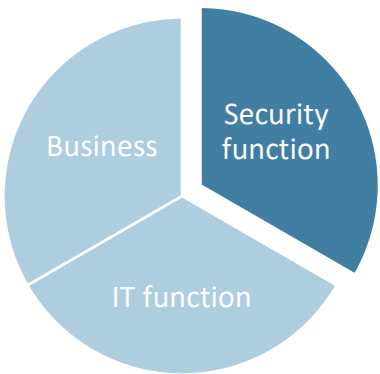
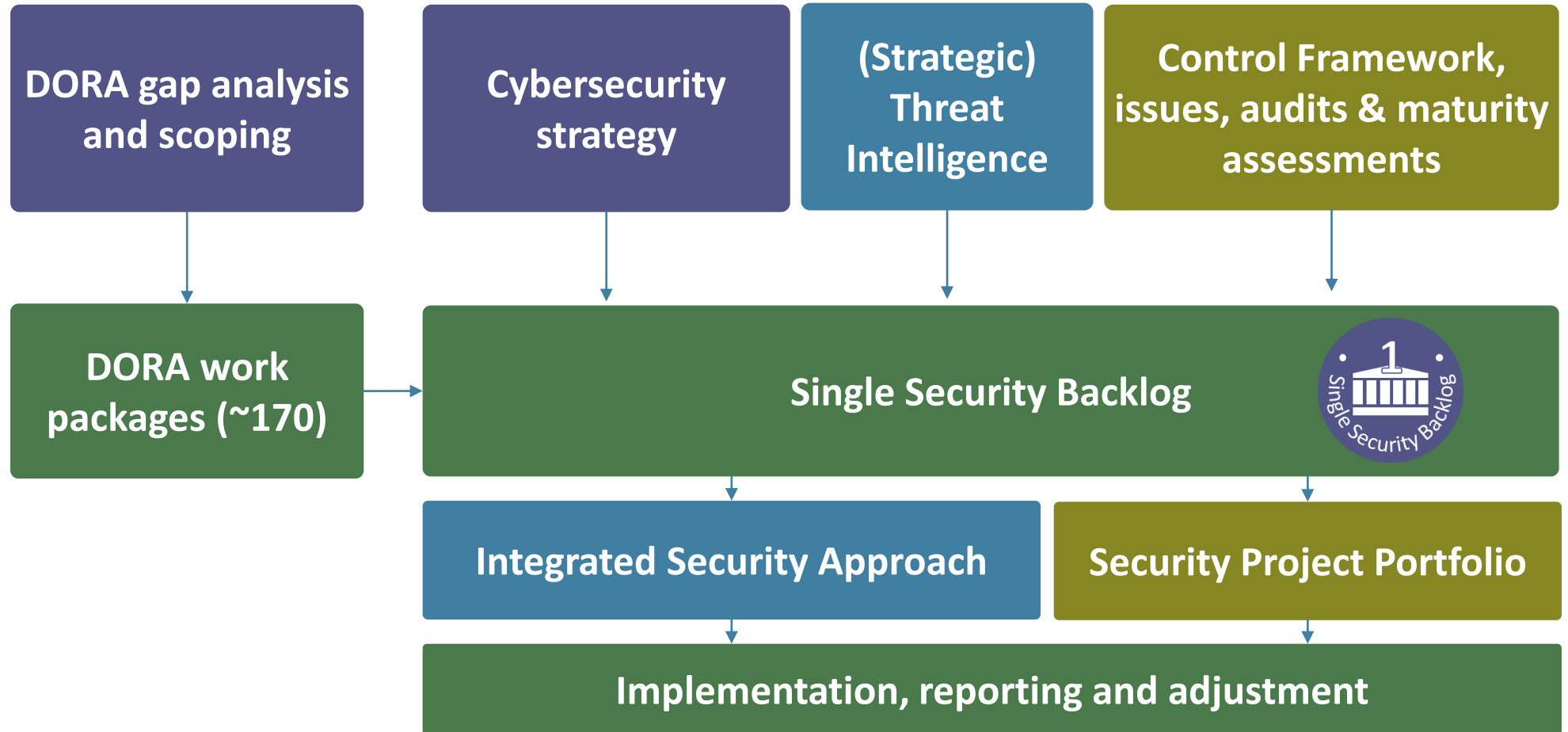


Achmea's challenge is to maintain balance between demonstrable compliance with the DORA and focussing on actual resilience

To achieve this, we reuse existing solutions and governance to implement the DORA

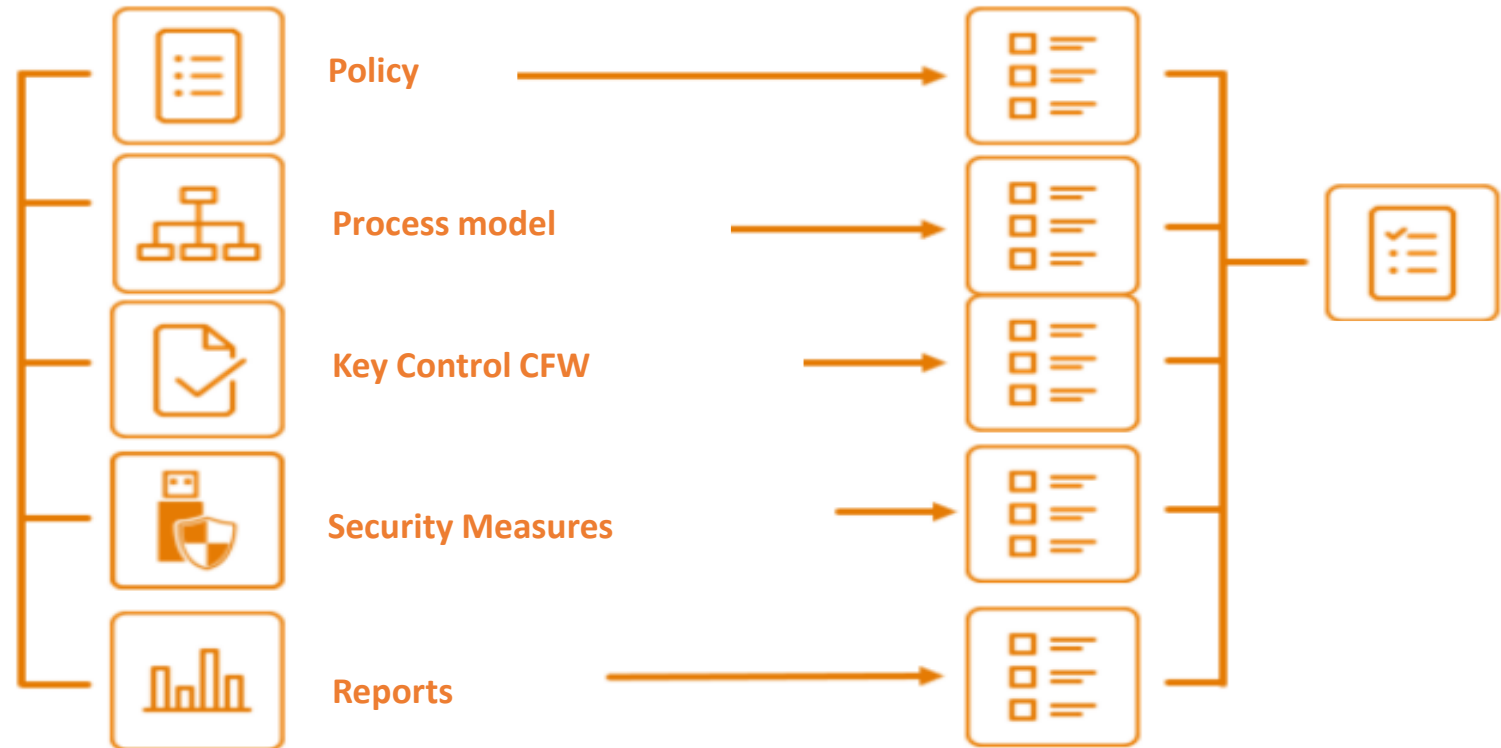
How do you eat an elephant?

Through a cascade of strategy, goals and work packages (and cutlery)



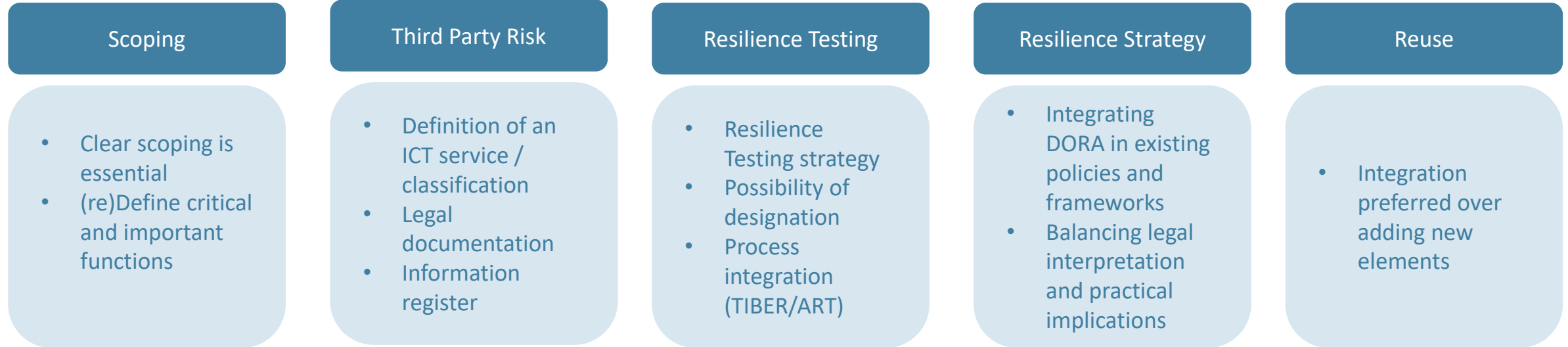
How did we conduct the Gap Analysis?

All articles from DORA have been checked against impact on five topics



Focal points of our DORA implementation

Strategic accents to clarify priority and way of working



Execution

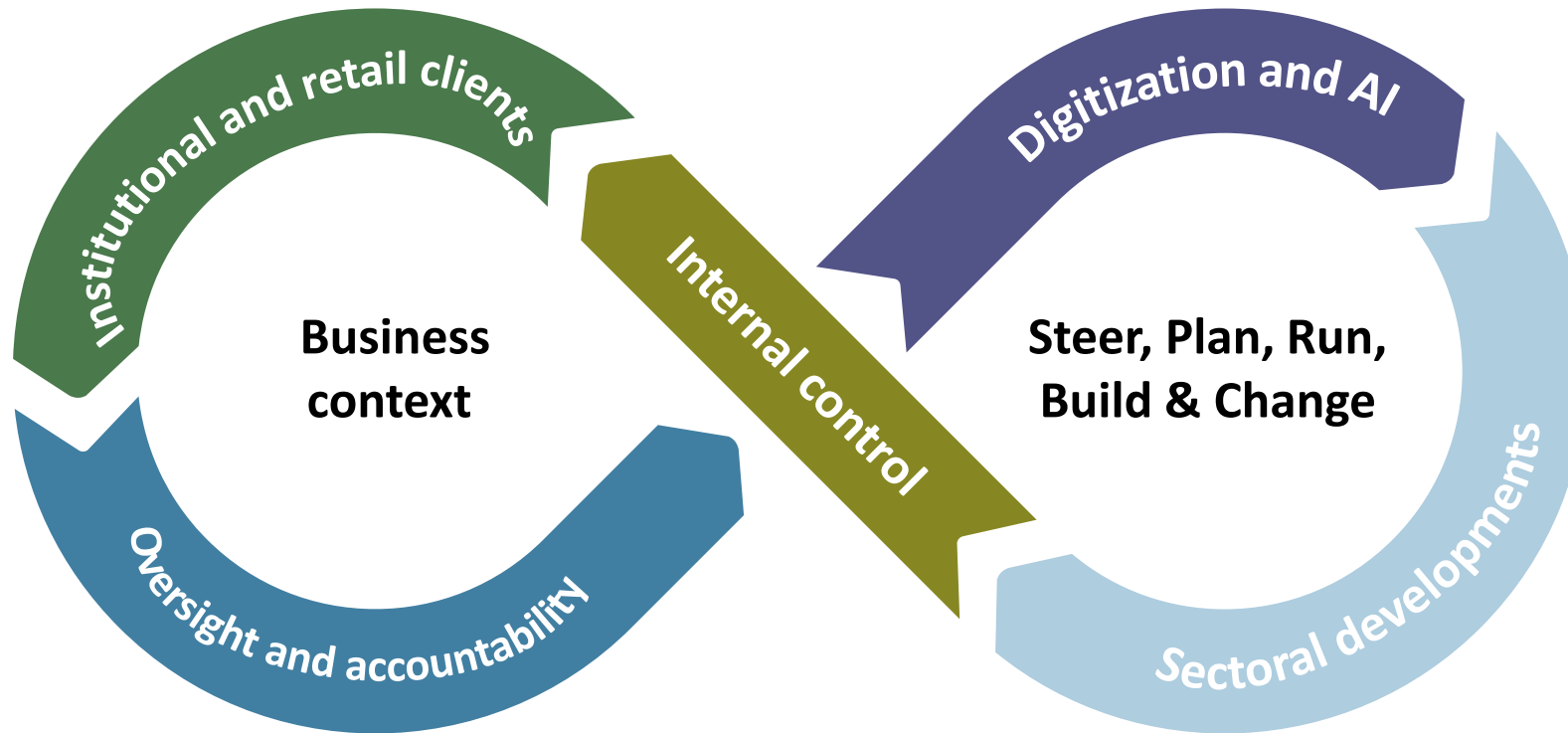




Start with the end in mind
Whilst maintaining agility

DORA is interwoven in all aspects of operations

Achmea isn't an IT company, but DORA requires attention across the board



DORA demands attention from non-IT teams

DORA has impact with regards to commercial choices and propositions

Institutional clients impose additional demands

Transforming requirements into local results

Achmea consists of a diverse set of financial entities

Aligning differing business context with one way of working

- Credit institution
- Managers of alternative investment funds
- Investment firms
- Insurance undertakings
 - Life insurance
 - Pension insurance
 - Health insurance
- Pensions
 - Premiepensioeninstelling
 - Pensioenuitvoerder



Generic

One gap analysis
Cascade gap to package
One way of working
Board reporting
Involvement 2nd and 3rd line



Bespoke results

Col functions
w.r.t. other laws
(Wtp)

Major data
providers outside
of EER

(a.o.) Mortgage
funds DORA
exempt

Scoping FE-2-FE

Different levels of
maturity

Rule vs. principle
based

Differing legal frameworks

Retail and / or institutional
clients

Integrating strength as both an opportunity and a threat

No add-on and high reuse, however DORA implementation becomes less explicit

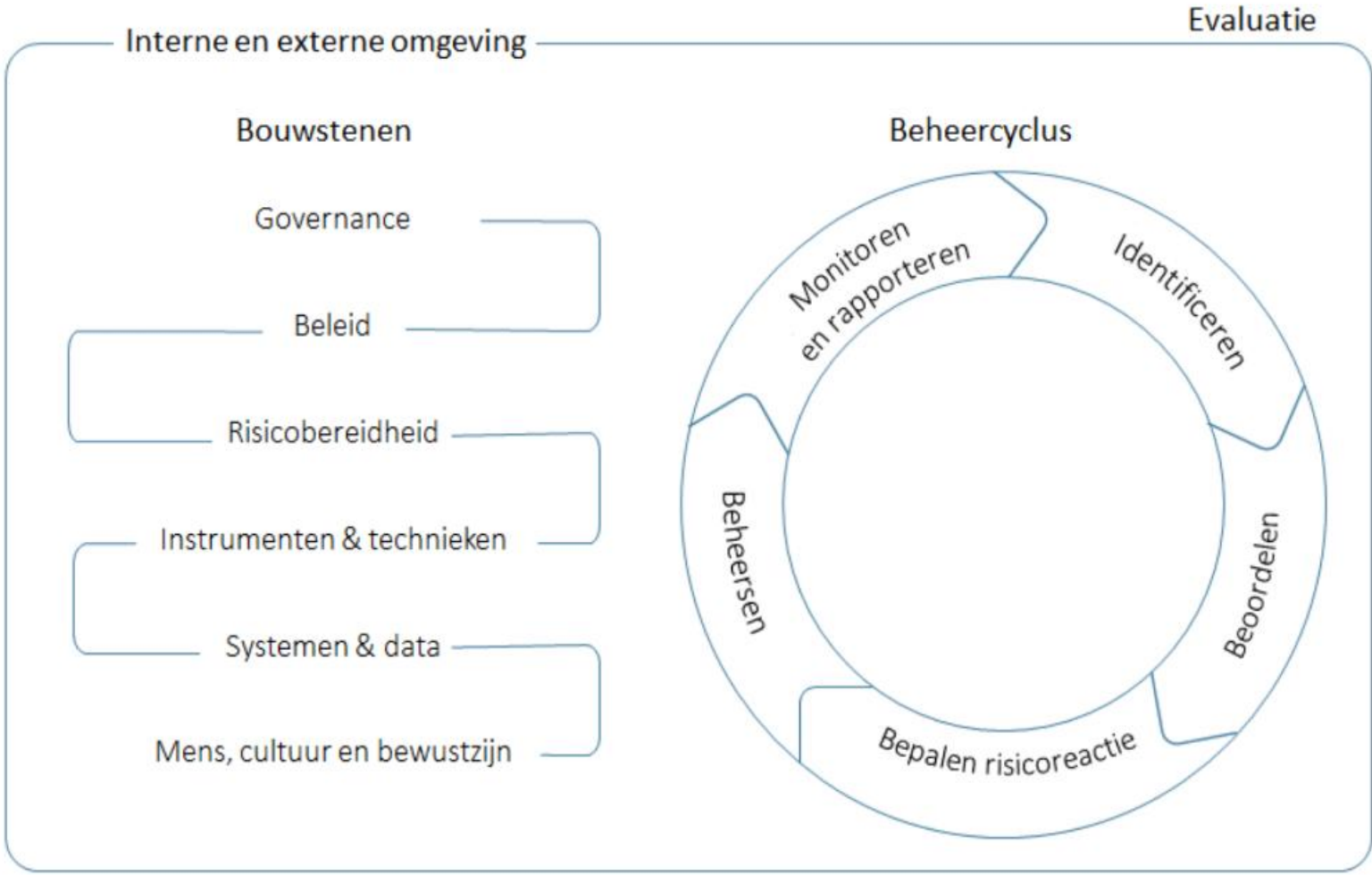


IGRC beleid

Integrated Governance, Risk en Compliance systeem



Colofon
Versie: 1.1
Status: Definitief
Datum: 18-02-2025
Classificatie: Intern



Trust the process

Focus on the best way of implementation, not the most visible

Policy

- ESA
- Outsourcing
- DORT
- Incident management
- BCM
- Information security

Process

- Major incident process
- Security monitoring
- 55 IT processes assessed

Governance

- New board requirements
- Assessing existing charters

Technology

- Toolchain incident management
- Additional security monitoring
- Additional MFA
- Ransomware, TLPT & PQC

People

- Security awareness
- Education, training and communication
- Legal liability

Integrating DORA into
business as usual




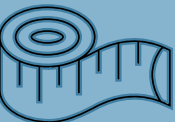
Additional challenge is
how to maintain an
**integrated system with a
reproducible trail to its
components to ensure
demonstrable compliance**

Lessons learned



What did we learn?

We can be (and are) very proud of what our colleagues have achieved

	Challenge	Where the magic happens	Lesson learned	CSF
	Differing opinions on the 'how' of DORA compliance. Width, depth, ...	Cocreation with clients and partners; garner support and avoid surprises. Proactive communication to clarify uncertainties	Open mindedness	
	DORA's scope is broad with high impact regarding cost of control. Col-functions as framework and risk	Aligning with legal definitions objectifies discussion and increases harmonisation	Insight in process, IT- and contract landscape. Risk based	
	Short implementation timeline and a long internal focus before starting	Forging ahead to maintain dialogue with clients, suppliers, colleagues and overseers	Daring to make choices	
	Tension between a generic way of working and specific requirements, specifically handshakes	Necessary additional governance to ensure alignment legal frameworks and business context on generic way of working	Committing and delivering	

Thank you for your attention

Questions?



DORA Experiences Payment Institutions (PI's)



14 May 2025



Intro



Anjeni (Pancham) Bedi ✓

Executive Board Member Payments CM.com | Compliance | Lid RvT
Kunst Centraal | SER Topvrouwen

The Randstad, Netherlands · [Contact info](#)

CM.com Dutch technology company specialized in services for conversational commerce

Enhance customer engagement

Founded in 1999 by Jeroen van Glabbeek & Gilbert Gooijers

Breda based but global presence



VBIN Verenigde Betaal Instellingen Nederland

Represent the interests of the Dutch Payments Institutions & pursue an even level playing field



Maurice Jongmans
Chair VBIN
CEO Online Payment
Platform B.V.



Alexander Verhoeven
Board VBIN
Head of Compliance &
Risk Intersolve Payments
B.V.



André Reumerman
Treasury VBIN
CFO Buckaroo B.V.



Anjeni Bedi
Board VBIN
Exec. Board Member
CMP B.V.



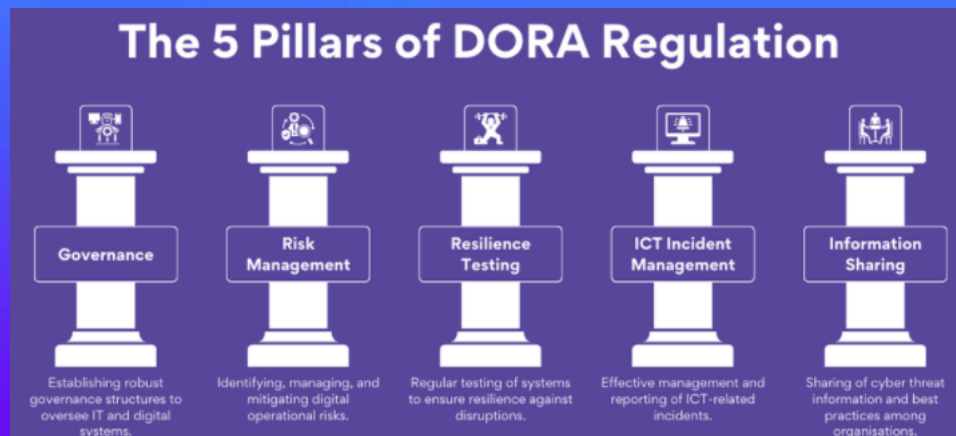
VBIN Verenigde Betaal Instellingen Nederland Selection of our Members





DORA...the beginning

1. Early alignment with other VBIN members on key topics from DORA
2. VBIN provided a platform for discussion with members, key experts, DNB and other interest groups
3. DNB facilitated events to discuss key topics
4. Many events around DORA



Source: Metomic



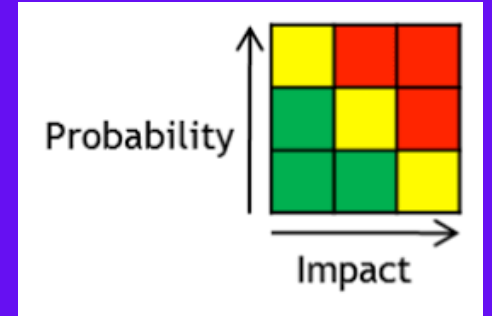


Challenges in DORA implementation



Challenges in implementing DORA

A) Risk Based Approach Focus on integrity risks



RISK APPETITE

Challenges in implementing DORA

B) A wide variety of PI's in the Fin-ecosystem

Services - What do payment institutions do?

Processing credit transfers and direct debits

Issuing and acquiring payment cards

Providing mobile payments or online payment gateways

Operating payment accounts (excl. deposit accounts)

Technical role – *How does the technical infrastructure look like?*

Payment Service Provider (PSP)

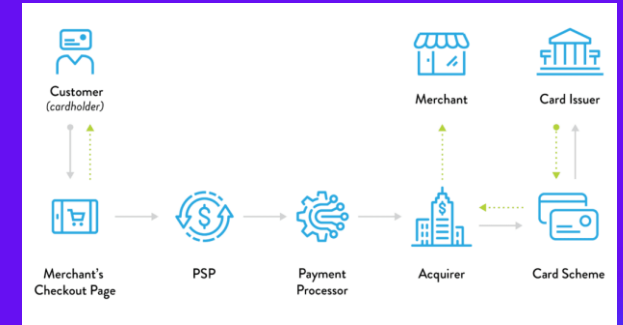
Role: PSPs facilitate the connection between merchants and acquiring banks, providing technology for processing payments, but they do not hold merchant accounts.

Acquirer

Role: Acquirers are banks or financial institutions that manage merchant accounts, process card transactions, and settle funds to merchants.

Payment Facilitator (PFAC)

Role: PFACs, or PayFacs, are similar to acquirers but they aggregate multiple sub-merchants under a single master merchant account. They onboard sub-merchants, handle underwriting, and facilitate payment processing on their behalf.



Priority Commerce

Challenges in implementing DORA

Special attention for specific roles for payment institutions in the Fin-ecosystem and DORA adherence

Function	Regulated under DORA	Direct ICT Risk Management	Incident Reporting	Subject to TLPT	Third-Party Risk
PSP	✓ Yes	✓ Full	✓ Yes	✓ Possible	✓ Yes
Acquirer	✓ Yes	✓ Full + Merchant Risk	✓ Yes	✓ Possible	✓ Yes
PFAC (regulated)	✓ Yes	✓ Full	✓ Yes	✓ Possible	✓ Yes
PFAC (unregulated)	✗ No	⚠ Limited via Acquirer	⚠ Indirect	✗ No	✓ Subject to Oversight

Challenges in implementing DORA

C) Overhaul ICT risk mgt



- Fragmented or legacy systems
- Aligning all departments and processes under a single ICT risk framework can be complex and costly
- Compliance fatigue due to overlapping NIS2, PCI- DSS, GDPR, and DORA audits
- Insufficient internal policies



- OneTrust platform to streamline policy mapping & audit workflows
- Vanta generating & tracking compliance documents and embedded review/approval process
- Apply mapping to different frameworks instead of separate documents
- Build audit-ready documentation via Confluence
- Store test results, policies and evidence in centralized repositories

Challenges in implementing DORA



D) Top management alignment



“The management body is accountable for defining, approving, overseeing, and implementing all arrangements related to the ICT risk management framework.”

Not only sponsorship but actual involvement!



Management reports including KRI's and KPI's to report on operational resilience

*VBIN -> early involvement of top management in VBIN discussion platforms
Improve training content for executive board members as well as for Supervisory Board
Members/Non -executive board members*

Challenges in implementing DORA

E) Third Party Risk management



- Raise the bar in terms of third-party risk management!
- Integrate steps in purchasing processes -> including specific clauses in contracts & follow up on (performance) evaluation
- More collaboration with suppliers in the area of testing
- Defining exit strategies -> is this workable?
- Renegotiating existing vendor contracts to include DORA clauses, ensuring service continuity and compliance across the chains



- RiskRecon to increase visibility in the chain of vendors and related exposure
- Tooling to simplify onboarding of third party with a structured risk assessment scoring

Challenges in implementing DORA



F) Incident management & reporting



- Insufficient forensic readiness for post-incident investigations
- Difficulty tracking & reporting minor ICT incidents and near misses
- Multi discipline approach often weak and/or misalignment exist
- Focus on remediation/damage control rather than gathering datapoints for reporting
- Even datapoints cannot be retrieved easily/centrally



- Implementation of Velociraptor for endpoint visibility, forensic collections and knowledge on chain of custody procedures
- Use of Jira for automated logging and classification
- RCA guiding in steering in operational resilience -> multiple occurrences of an incident with a similar cause, need focus to solve the underlying problem
- Use of the NOREA incident classification tooling

Challenges in implementing DORA



E) Testing



- Lacking a strategic vision on this topic
- No structured process for scenario-based resilience testing (as required under DORA)
- Tests are often managed in silo's (vulnerability tests, penetration tests, business continuity tests...)
- Critical functions and dependencies are not properly in scope
- Not always internal expertise present to conduct the testing
- Lack of traceable resilience testing history
- Difficulty with alignment with ICT third party providers on testing obligation & necessity



- Tabletop Exercise tools to simulate a crisis and collaborate with a third party consultancy
- Adoption of Jira and Confluence to manage test results and evidence collection
- Clear roles, responsibilities and accountability, including PR role!
- Re-assess test strategy and practice what you preach!

Challenges in implementing DORA



F) Intragroup ICT outsourcing



- Lack of formal SLAs or contracts with intragroup providers, relying on informal governance or implied cooperation
 - * Due diligence obligations must be met
 - * Formal contracts with all required clauses are mandatory
- Drafting compliant contracts internally can be politically and operationally sensitive
- Intragroup arrangements can create systemic risk within a group, & oversight may be weaker than with external vendors
- Intragroup services not considered as "outsourcing" for reporting purposes -> non-compliance
- Difficult to implement realistic exit strategies due to shared infrastructure or group-level dependencies

Challenges in implementing DORA



F) Intragroup ICT outsourcing



- Development group-wide DORA outsourcing policy including intragroup arrangements
- Internal provider = “third party” for compliance purposes—apply same vetting, oversight, & contractual controls
- Standardized intragroup outsourcing contract templates with DORA-required clauses
- Maintenance of a central register of all intragroup ICT dependencies & assess concentration risk regularly
- Implement business continuity & resilience plans specifically for central ICT hubs or shared service centers
- KPI's and regular performance reporting to monitor intragroup ICT delivery
- Draft plausible exit strategies, even if complete disengagement is unlikely
- Gap analysis between existing intragroup arrangements and DORA requirements.
- Run training programs for internal service providers to understand their regulatory obligations.
- Implement a DORA compliance dashboard that flags gaps or outdated contracts



***25 Years at
the Forefront
of Innovation.***

Anjeni.Pancham@cm.com

Info@vbin.com

[Anjeni Bedi | LinkedIn](#)