Commvault®

Improving Operational Resiliency

NIS2 / DORA – Regulatory Landscape

Data is everywhere

(And harder to protect than ever before)

89% of companies are multi-cloud[1]

50% of enterprise-critical data will be outside a company's cloud[2]

60% of companies lack complete visibility into where data reside[3]

1. Flexera State of the Cloud Report 2023, 2.Gartner 12 Data and Analytics Trends to Keep on Your Radar,
3. 5th Annual Nutanix Enterprise Cloud Index

How do threats impact your business?

In Finance Organisations, downtime costs:

$15,000 per minute
$21.6M per day
$151.2M per week

How are these threats impacting the other challenges your business is facing?

- Complexity of distributed data
- Doing more with less
- Compliance demands
- Protecting brand experience

Directive on measures for a high common level of cybersecurity (NIS2)

What is it?

NIS2 (Regulation 2022/2555) sets out a ne rules to ensure stronger cybersecurity in EU.

It aims to build cybersecurity capabilities across EU, mitigate threats to network and information systems used to provide essential services in key sectors and ensure the continuity of such services when facing incidents.

Applies to:
NIS - Healthcare, Transport, FSI, Digital Infrastructure, Water supply, Energy, DSPs
+ NIS2 - Medium Enterprises and up (50-250 employees), Electronic communications network/services providers, Networking services platforms, data center services, Waste & Water, Manufacturing of critical products, Postal and Courier services, Food, Public Administration.

What's the impact?

Under NIS2 entities will need to step up efforts aimed at:

- accountability,
- supply chain cybersecurity,
- handling and crisis management,
- vulnerability handling and disclosure,
- policies and procedures to assess the effectiveness of cybersecurity risk management measures,
- basic computer hygiene practices and cybersecurity training,
- the effective use of cryptography,
- Human resource security,
- access control policies
- asset management

Timelines

Entry in force:
January 16th 2023

Transposition to local law

Date of transposition:
October 17th, 2024

2023

2024

2024

NIS2 - Key Pillars and Objectives

Governance

Role of the management bodies

Approve & oversee

Liability

Training

ICT risk management measures

Technical, operational, organizational

Appropriate & proportional

Incidents

CSIRT

Early warning (<24h)

Notification (<72h)

Final report (1 month)

Certifications

MS & EU Commission may impose req on certain products/services

Standardization

=> ENISA

Other

Voluntary framework for vulnerability disclosures

COMMVAULT PERSPECTIVE

RISK

Improve data security and lower your risk profile by proactively locating, securing and protecting critical data assets

READINESS

Ensure resilience with advanced preparedness, early visibility of threats, automated validation and continual recovery testing

RECOVERY

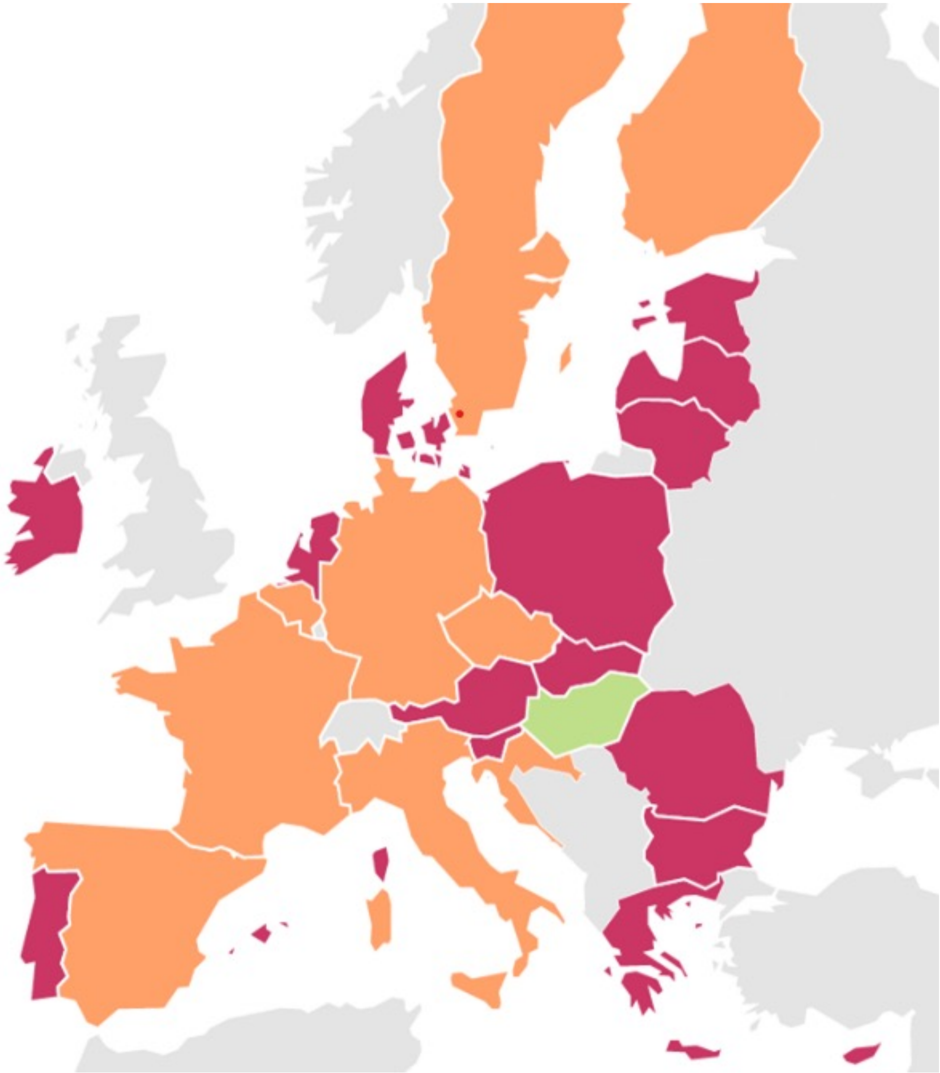
Ensure rapid recovery with the flexibility to recover from anywhere to anywhere at scale

Transposing NIS2

POLAND

Relevant legislative developements
No developments
Most likely amendment to: Ustawa o krajowym systemie cyberbezpieczeństwa (uKSC)

Dates to watch!
Member States must establish a list of essential and important entities and entities providing domain name registration services by April 17th, 2025.



Credits: NIS2 tracker – Bird&Bird NISD 2 Tracker - Bird & Bird (twobirds.com)

Digital Operational Resilience Act (DORA)

What is it?

DORA (Regulation 2022/2554) sets out a new ICT Risk Management Framework for Financial Sector (FS) in EU.

It aims to consolidate and upgrade ICT risk requirements throughout FS with particular focus on digital resilience components.

Includes requirements for ICT Vendors.

Applies to EU based FS entities with other countries following (e.g. UK – Bank of England, PRA, FCA).

What's the impact?

Under DORA FS entities will need to step up efforts aimed at:

Evidencing the current digital operational resilience status and understanding the potential impact of any disruptions

Setting out clear information security objectives

Ensuring comprehensive capabilities and mechanisms in place to enable effective ICT risk management

Reassessing relations with ICT vendors

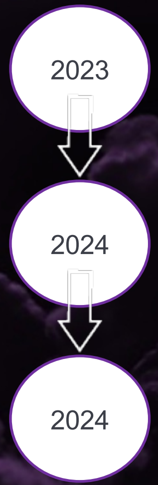
Sanctions – administrative & criminal penalties to be defined by EU Member States.

Timelines

Entry in force:
January 17th, 2023

Technical Standards defined and issued

Date of effect:
January 17th 2025



DORA - Key Pillars and Objectives

ICT risk management framework

Sound, comprehensive & documented

ICT systems, protocols, tools

Appropriate

Reliable

Sufficient capacity

Technologically resilient

Key contractual provisions

ICT risk management measures

Technical, operational, organizational

Other

Incident reporting

Vulnerability disclosure

TLPT

COMMVAULT PERSPECTIVE

RISK

Improve data security and lower your risk profile by proactively locating, securing and protecting critical data assets

READINESS

Ensure resilience with advanced preparedness, early visibility of threats, automated validation and continual recovery testing

RECOVERY

Ensure rapid recovery with the flexibility to recover from anywhere to anywhere at scale

DORA – Delegated acts - consultations

European Supervisory Authorities

eba European Banking Authority

eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

1st batch

- RTS on ICT risk management framework and RTS on simplified ICT risk management framework
- RTS on criteria for the classification of ICT-related incidents
- ITS to establish the templates for the register of information
- RTS to specify the policy on ICT services performed by ICT third-party providers

2nd batch

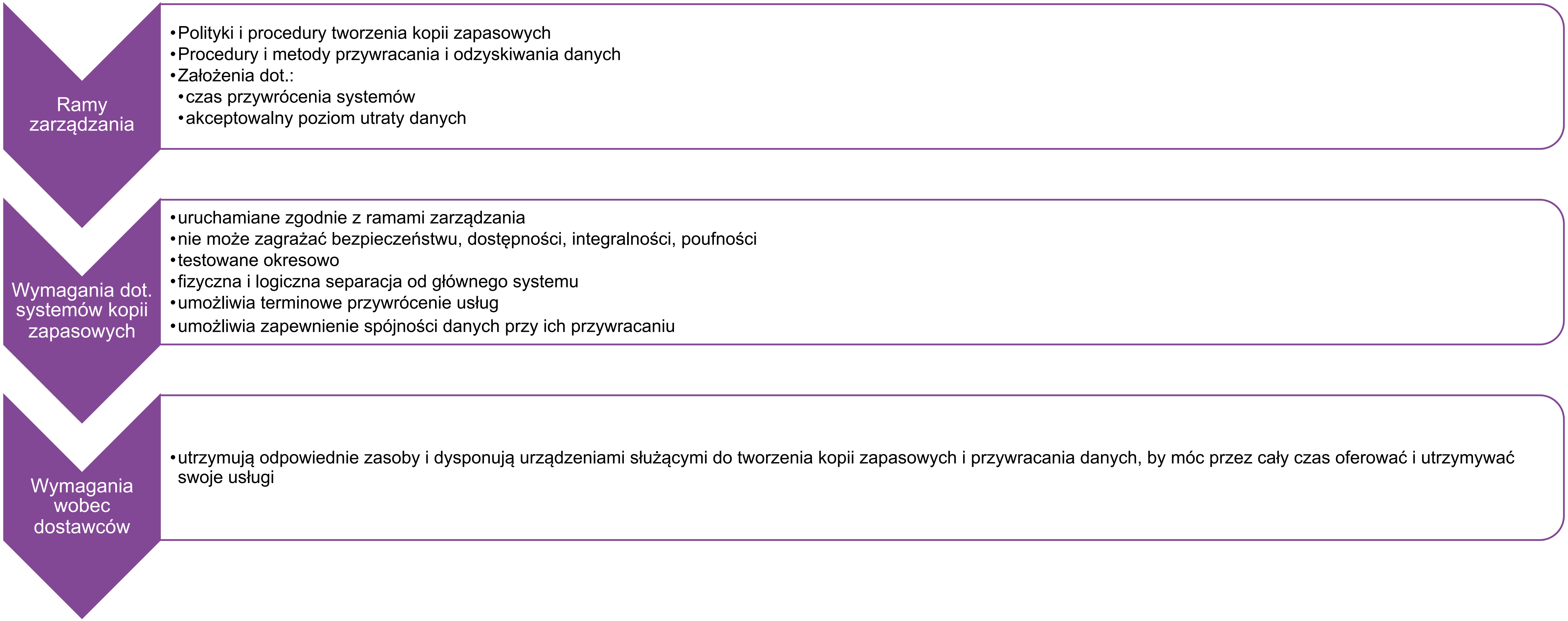
- RTS and ITS on content, timelines and templates on incident reporting
- GL on aggregated costs and losses from major incidents
- RTS on subcontracting of critical or important functions
- RTS on oversight harmonisation
- GL on oversight cooperation between ESAs and competent authorities
- RTS on threat-led penetration testing (TLPT)

March 4th, 2024

Commvault

Sample requirement (DORA)

ART. 12 DORA - BACKUP POLICIES AND PROCEDURES, RESTORATION AND RECOVERY PROCEDURES AND METHODS



Ramy zarządzania

- Polityki i procedury tworzenia kopii zapasowych
- Procedury i metody przywracania i odzyskiwania danych
- Założenia dot.:
  - czas przywrócenia systemów
  - akceptowalny poziom utraty danych

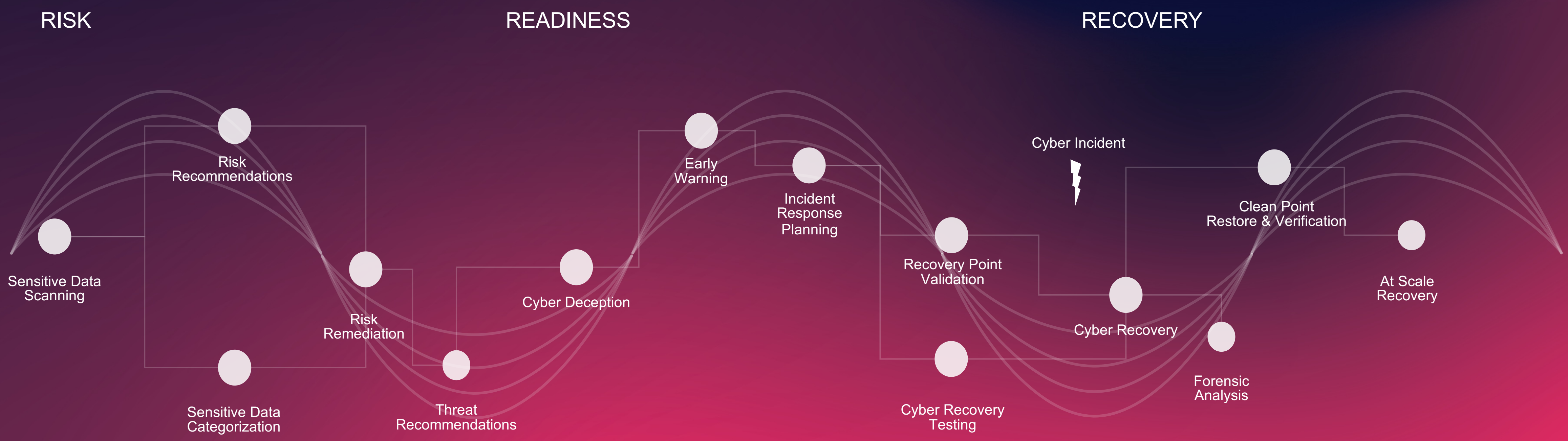
Wymagania dot. systemów kopii zapasowych

- uruchamiane zgodnie z ramami zarządzania
- nie może zagrażać bezpieczeństwu, dostępności, integralności, poufności
- testowane okresowo
- fizyczna i logiczna separacja od głównego systemu
- umożliwia terminowe przywrócenie usług
- umożliwia zapewnienie spójności danych przy ich przywracaniu

Wymagania wobec dostawców

- utrzymują odpowiednie zasoby i dysponują urządzeniami służącymi do tworzenia kopii zapasowych i przywracania danych, by móc przez cały czas oferować i utrzymywać swoje usługi

Closing the DORA Regulation GAP with Commvault



Commvault

Summary

How does Commvault help with DORA regulation?

- Identify Critical information assets to reduce risk, minimize the impact of data loss
- Early warning of suspicious activities, integrated into existing security ecosystem
- Secure, Zero-trust, air-gapped Cyber Resilience Recovery platform for any workload
- Reduced complexity and cost of clean recovery and recovery testing
- Cross workload, cloud and hypervisor portability to provide an exit strategy

COMMVAULT PERSPECTIVE

RISK

Improve data security and lower your risk profile by proactively locating, securing and protecting critical data assets

READINESS

Ensure resilience with advanced preparedness, early visibility of threats, automated validation and continual recovery testing

RECOVERY

Ensure rapid recovery with the flexibility to recover from anywhere to anywhere at scale

Next Steps

1

Book a workshop with Commvault to discuss how Commvault can help with Dora

2

Minutes to Meltdown, tabletop exercise workshop coming soon

3

Executive briefing for readout and cyber resilience vision roadmap

Further Reading

- Contact Commvault to arrange a Resiliency Workshop to understand more on Dora from a cross functional perspective
- Review Commvault Blog on Data Privacy Regulations
- Review Commvault Cybersecurity solutions
- Review whitepaper on Operational Readiness
- Review whitepaper on Strengthening Ransomware Protection with Data Isolation