KROLL

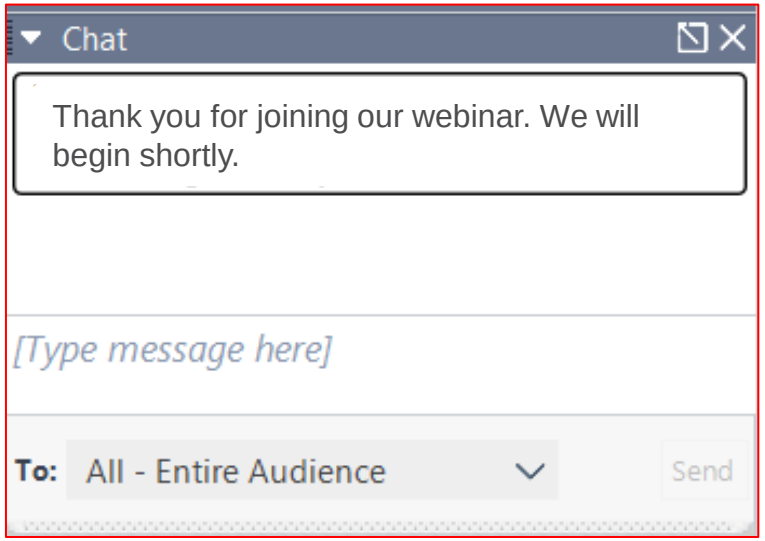
Navigating DORA Compliance: Preparing for the EU's New Digital Operational Resilience Regulation

Housekeeping

- Session is being recorded, You'll receive access to the recording in a couple days

- Ask questions via chat >

- We'll try to answer as many questions as possible



KROLL

Speaker Profiles

Hannah Rossiter
Managing Director
Financial Services Compliance and Regulation

Tiernan Connolly
Managing Director
Cyber and Data Resilience

KROLL

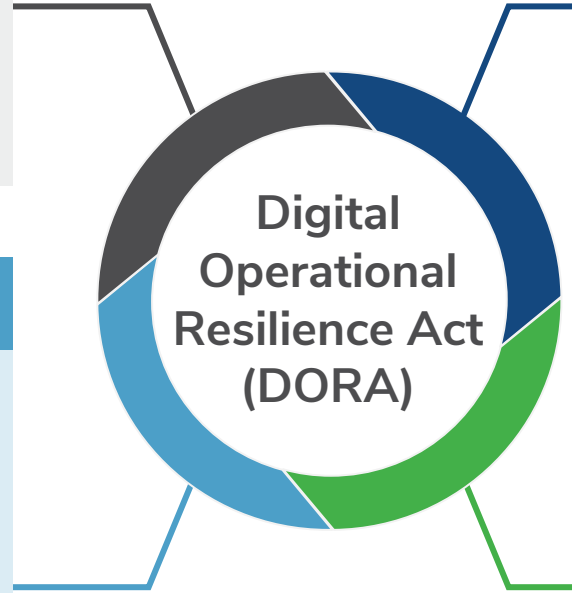
What is DORA?

Overview

A new EU legislation, designed to improve the cybersecurity and operational resilience of firms in the financial services sector. DORA applies to more than 22,000 financial entities and ICT service providers operating within the EU, as well as ICT infrastructure firms

Main Themes

- Robust and repeatable IT Risk Management Framework
- Board/Senior mgt accountability
- Third-party and Supply Chain Risk Management
- Incident Response and Incident Reporting to the regulators
- Threat Intelligence-driven Pen-testing



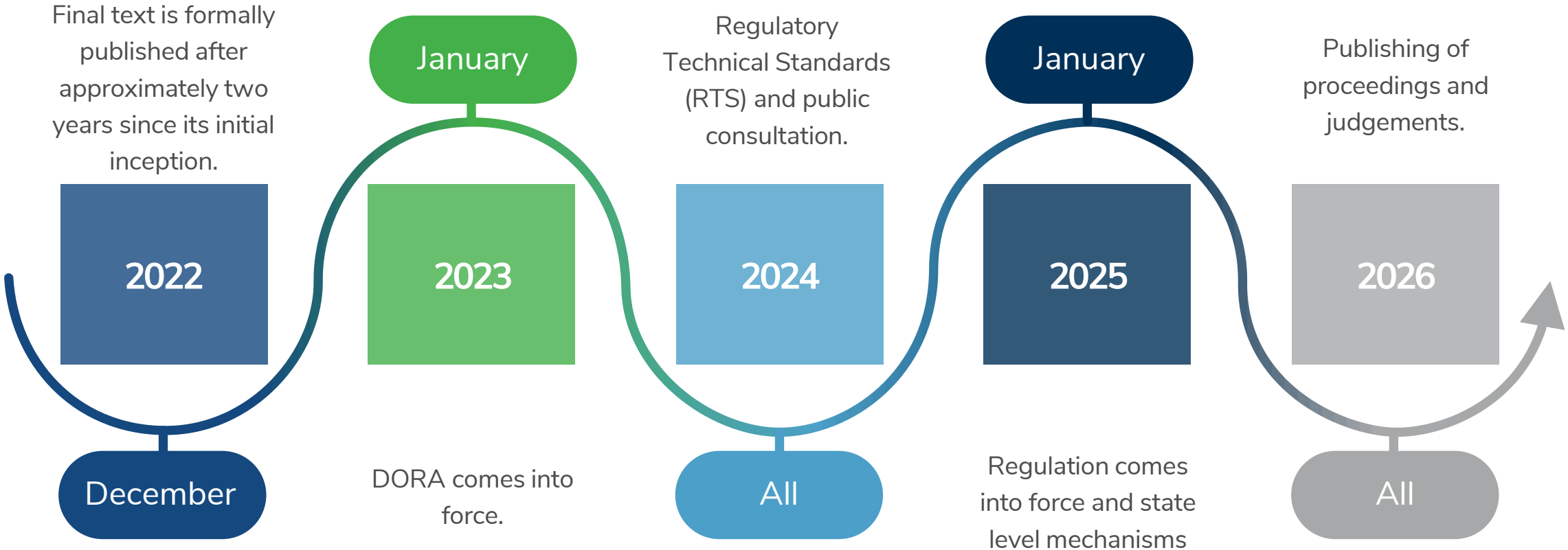
Main Objectives

- Harmonisation of ICT Risk management across EU.
- Ensuring all participants in the financial industry have the necessary
- Implementation of oversight of critical ICT service providers

Types of relevant organizations

- Credit institutions;
- Electronic money institutions
- Investment firms;
- Insurance and reinsurance undertakings;
- Asset management companies;
- Data reporting service providers;
- Credit rating agencies;
- ICT third-party service providers.

Key Timelines



Main Pillars of DORA

There are five key pillars of focus, with Business Resiliency requirements peppered throughout

How to navigate common challenges

CHALLENGE	SOLUTION
Getting stakeholder and leadership buy-in	Communicate, educate and garner support from senior stakeholders and ensure appropriate governance and reporting are in place, right up to the board
DORA requirements, especially those for Regulatory Technical Standards (RTS), can be challenging to interpret	Understand where to adapt existing controls vs more significant changes that require more resources
DORA is complex and wide-ranging	Use ”proportionality” to flexibly adhere to DORA requirements in a risk-based, business-aligned manner
Stricter controls and processes for ICT third-party risk management and oversight	Assign clear ownership and accountability for ICT third-party registers and automate register population and maintenance as much as possible

Comparing NIS2 and DORA

	NIS2	DORA
Type	**Directive** – EU Member States are responsible for implementing national laws	**Regulation** – directly applicable to financial services companies
Implementation date	October 17, 2024	January 17, 2025
Applies to	**Critical Sectors** (energy, transportation, health, space, internet etc.), MSPs, MSSPs in EU Member States	**Financial Entities** (banks, insurance, crypto, etc.) and ICT service providers in EU member states
Overlap	Part of the **broader** cybersecurity regulatory framework	**Takes precedence** where sector-specific rules apply ('Lex Specialis' exemption)
Areas of focus	Strengthening **overall** security and incident reporting requirements	**Complements NIS2** by providing specific provisions around ICT frameworks, incident response and third-party ICT contracts
Testing requirements	**Variable** depending on country	• A range of assessments and tests **every year** • Threat-led penetration testing **every three years**
Incident reporting	• An early warning within **24 hours** • An incident notification within **72 hours** • A final report within **1 month**	**Classification of 'major' incidents** and subject to the following: • An initial notification within **24 hours** • An intermediate notification within **72 hours** • A final report within **1 month**

Key Pillars

ICT Risk Management

ICT Systems, Protocols and Tools

Protection

- ✓ Implementation of sound network and infrastructure management
- ✓ Implementation of appropriate mechanisms and tools for preventive security of assets
- ✓ Administration and control of access rights
- ✓ Implementation of strong authentication mechanisms
- ✓ Implementation of controls for managing changes to assets and information systems

Detection & Reporting

- ✓ Classification of ICT supported business functions, assets and third-party service providers, with an emphasis on Critical and Important Functions (CIF)
- ✓ ICT risk assessments (cyber threats and ICT vulnerabilities)
- ✓ Implementation of several levels of control, definition of alert thresholds and criteria for triggering IT incident detection and response processes
- ✓ Regular pen-testing

Response & Recovery

- ✓ Incident management process
- ✓ Business continuity plan
- ✓ Escalation and analysis
- ✓ Implementing ICT-incident log
- ✓ Incident analysis and impact assessment
- ✓ Classification of ICT-related incidents
- ✓ Reporting of critical incidents to national authorities

Communication & Learning

- ✓ Post-incident IT reviews to identify improvements to IT operations
- ✓ Escalation of findings to the management body
- ✓ Development of IT security awareness programs for staff members
- ✓ Monitoring technological developments
- ✓ Implementation of communication plans to all stakeholders internal and external

Incident Reporting

What you need to know

Mandatory reporting of major ICT-related incidents and voluntary notification of significant cyber threats

Classification of incidents according to key pre-defined criteria and materiality thresholds for determining major ICT- related incidents;

Estimation of the aggregated costs/losses, along with other criteria, caused by major ICT related incidents

Timelines for incident reporting:

- Initial notification: 4 hours from determining the incident is major but in any event within 24 hours of detecting the incident;
- Intermediate notification within 72 hours of classifying the incident as major; and
- Final report no later than 1 month from classifying the incident as major.

Harmonisation of reporting content and templates

Types of Technical Testing Required

Multiple types of testing techniques are outlined in DORA to ensure the effectiveness of controls.

Vulnerability Scanning

Passive activity designed to detect known vulnerabilities typically unpatched systems, but also basic misconfigurations.

Typically done on a quarterly basis, however modern solutions provide ongoing scanning.

Penetration Testing

This is the next step that builds upon a vulnerability scan. It requires an attacker to attempt to exploit vulnerabilities within an environment.

To be conducted on a yearly basis or after significant IT system changes.

Threat–Led Pen Testing *aka Red Teaming*

A team will be set an objective and rules of engagement agreed. The objective could be to attempt to access a key system or dataset. Can also include a physical security element.

Periodically perform for ICT services which impact critical functions

Tabletop Exercises

An exercise where existing processes, procedures and understanding are tested.

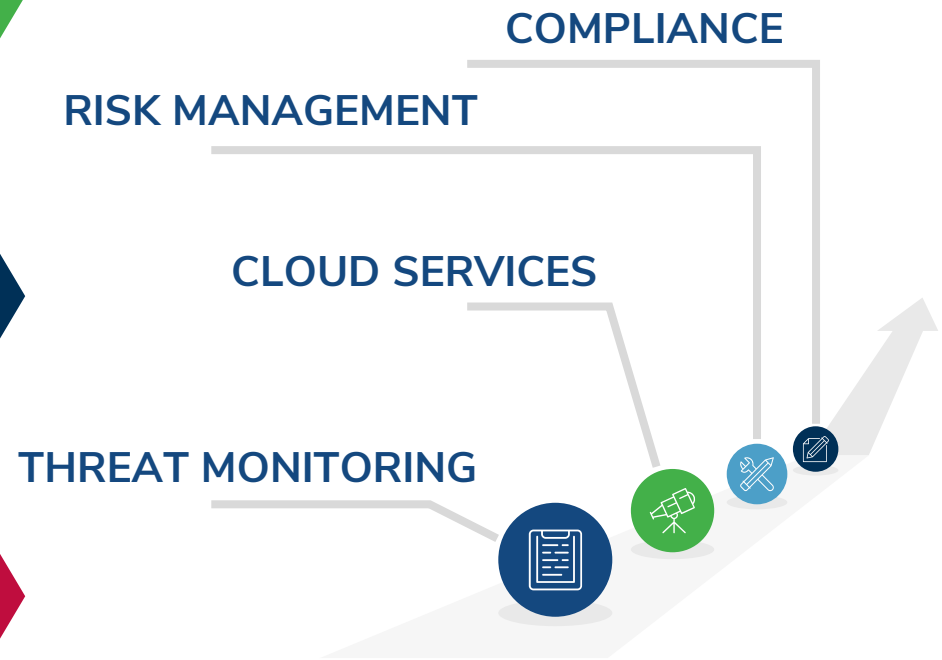
Should cover executives and technical resources.

Critical Third Parties

Certain third parties assessed as ‘critical’ to operations will require heightened controls and greater oversight

- Greater emphasis on governance, oversight and documentation
- Pre-outsourcing analysis and due diligence
- Specific contractual provisions required
- Minimum standards for information security requirements
- Exit strategies
- Access and Audit Rights

POTENTIALLY CRITICAL SERVICES

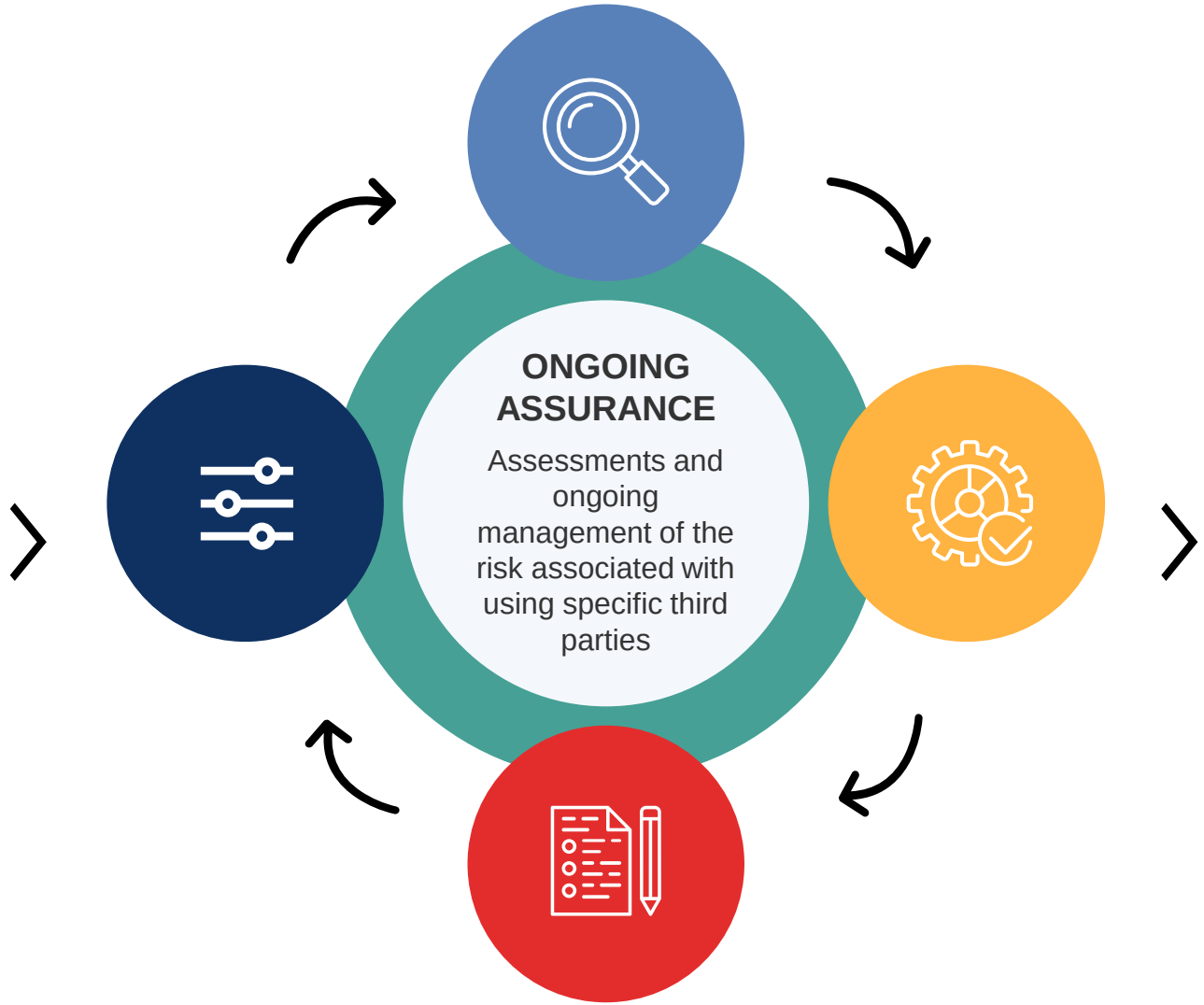


ICT Third Party Risk Management

Vendor Management Cycle

SELECTION & ONBOARDING

- Classify vendors using a risk-based approach (supplier criticality)
- Due diligence on the selected third parties before contracting
- Establishing necessary appropriate controls

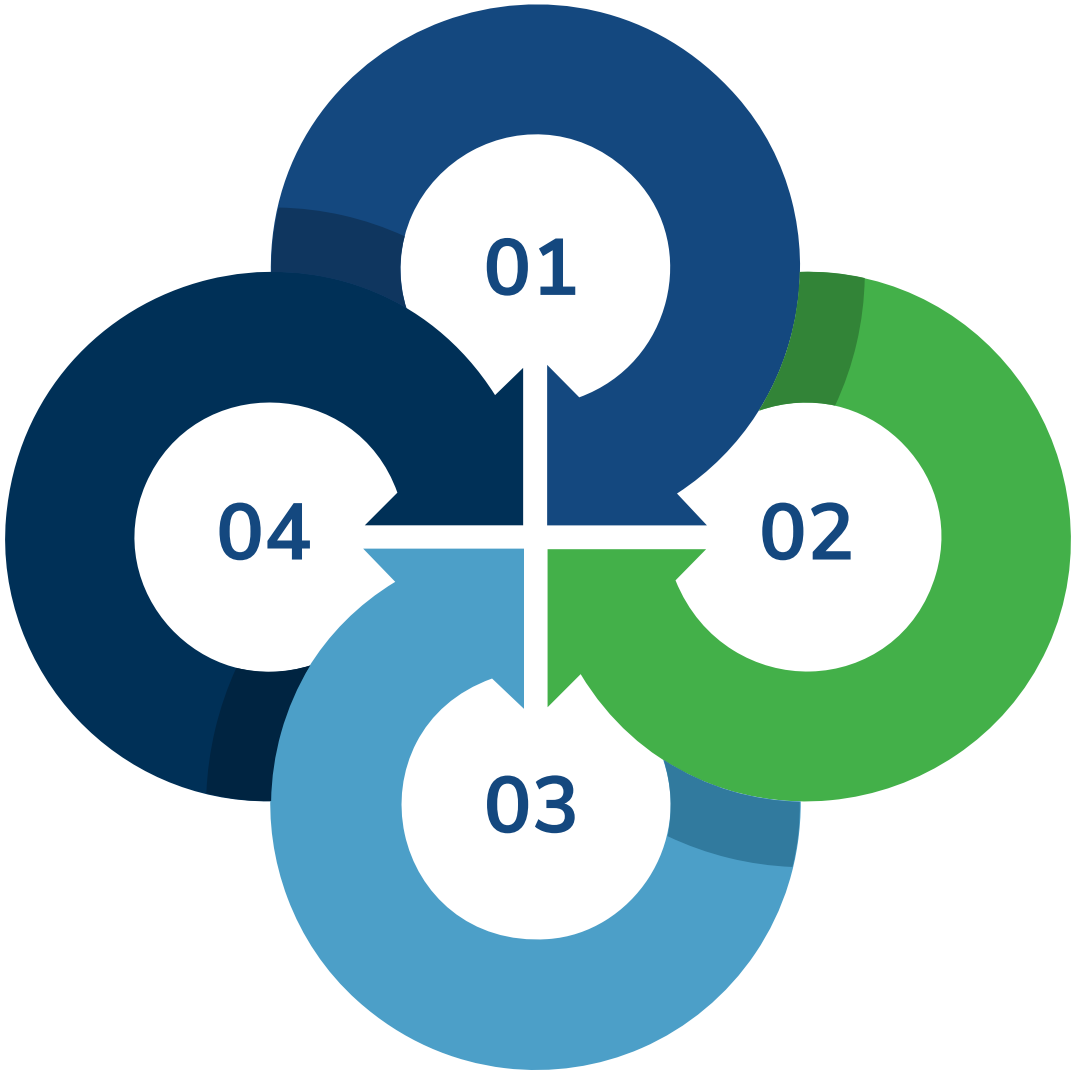


OFFBOARDING

Secure termination and offboarding of third party and company data

The Business Continuity Lifecycle

Business continuity should be a continuous activity.



UNDERSTAND

Business Impact Analysis

Risk Assessment

Objectives, products, priorities, core process, critical functions, required resources, threats and potential impact.

SOLVE

Identify potential improvements and/or investments

Improve resilience, mitigate threats, build agility, alternatives and options for recovery.

Based on cost/benefit assessment.

TEST AND REVIEW

Test program

Review cycle

Quality assessment and/or Audit

Ensure the plans and solution stay fit-for-purpose

BUILD / REBUILD

Business Continuity Plans

Create practical action plans to be used as reference during disruptions.

Proportionality

Proportionality

Simplified framework and exemptions

The Regulation provides that certain types of firms including ‘small and non-interconnected investment firms’ (as defined in the Investment Firms Prudential Regulation) will be exempt from Articles 5 to 15 of DORA but subject to a Simplified ICT Risk Management Framework.

There are also exemptions available to ‘microenterprises’ i.e. a financial entity, other than a trading venue, a central counterparty, a trade repository or a central securities depository, which employs fewer than 10 persons and has an annual turnover and/or annual balance sheet total that does not exceed 2 million EUR.

Proportionality Factors

- Size and overall risk profile,
- Nature,
- Scale and complexity of their services, activities and operations.

Regulatory Technical Standards are expected to provide greater clarity on the exact contents of the Simplified ICT Risk Management Framework.

Kroll’s DORA Services & Methodology

Kroll DORA Compliance Assessment

Key Outcomes

Understand key gaps in your maturity

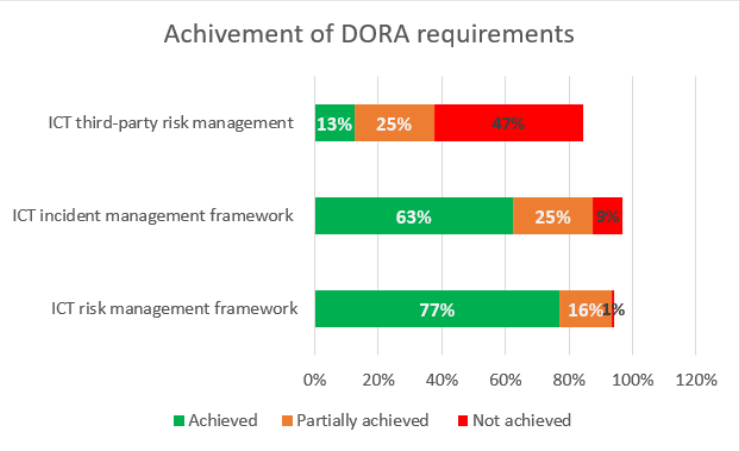
Quantitative measure of DORA compliance status highlighting key weaknesses by carrying out a gap assessment of operational resilience with DORA and draft RTS standards

Have a clear path to compliance and reducing longer term risk

Clear roadmap towards DORA compliance with priority tasks and timeframes. An action tracker is also provided with recommended owners to help stakeholders for effective project management

Implement solutions to maintain operational resiliency

With our portfolio of transformation and managed services, we can assist you with the implementation of controls, procedures, testing and services across ICT risk management, incident management, business continuity, third-party risk management, and digital resiliency testing



Our Methodology

Our 4-phased approach help organizations of all sizes address any stage of DORA maturity:

Planning

- Information gathering
- Determine type of testing required
- Tentative scheduling

Assessment

- Analysis of the core areas of operational resilience against DORA and draft RTS standards
- Clear risk rating highlighting key weaknesses

Roadmap

- Actionable tasks with effort ratings
- Reasonable timeframes for completion of individual tasks

Implementation

- Implementation of policies, procedures, assessments and managed services across all areas of operational resilience
- Development of DORA Registers

KROLL

Kroll Services aligned to DORA

DORA Pillars

1. IT Risk Management
2. IT Incident Reporting
3. Security Resiliency Tests
4. IT Third-Party Risk

Implementation

1
- ICT Risk Management Framework Development
- Policies and Procedures Library Development
- Threat Modelling
- Maturity Assessments
- Security Strategy & Roadmap Development
- Security Program Implementation
- BCP / DR

2
- Incident Mgmt Policies, Procedures & Playbooks Definition
- Incident Classification Framework/Process Definition
- MDR / Incident Response Retainer
- Tabletop Exercises

3
- Pen-Tests
- Red-Team exercises
- Compromise Assessments (BEC / Ransomware)
- Deep/Dark Web Monitoring
- Tabletop Exercises
- Vulnerability Management
- DORA/TIBER TLPT
- Threat Landscape Assessments

4
- TPRM Framework Development
- Due Dilligence Assessments
- Contractual Review/ updates
- DORA Register population support
- Critical Process/Asset Mapping

Why Kroll?

Experienced, accredited cybersecurity professionals

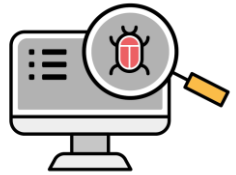
500+ skilled and certified cybersecurity consultants across the globe, experienced in not only helping clients comply with multiple regulations but staying resilient ahead of the changing landscape

Solutions across the DORA Maturity Lifecycle

Our solutions can address all aspects of DORA compliance and maturity; from assessing all possible gaps/weaknesses and advising on remediation with our consultancy expertise to implementing the right controls and providing remote managed services

Cybersecurity, Regulatory and Financial Services Risk expertise

Our experts comprise of cybersecurity, operational resilience and regulatory compliance experts with a deep understanding of relevant legislation and standards in your industry to provide real insight and value.



Fast implementation, built on previous engagements

Our experience with regulatory compliance, security program implementation, and managed risk services gives us the foundation from which to accelerate your compliance journey

Questions?

Our Locations

6,500 professionals worldwide continuing the firm's nearly 100-year history of trusted expertise.
Across **36** countries and territories worldwide.

The Americas

Atlanta
Austin
Bogota
Boston
Buenos Aires
Chicago
Dallas
Ellensburg
Hamilton
Houston
Los Angeles
Mexico City
Morristown
Nashville
New York
Philadelphia
Richardson
San Francisco
São Paulo
Seattle
Secaucus
Silicon Valley
Sunnyvale
Toronto
Washington DC

Caribbean

British Virgin Islands
Cayman Islands

Europe, Middle East and Africa

Abu Dhabi
Agrate Brianza
Amsterdam
Barcelona
Berlin
Bilbao
Birmingham
Brussels
Dubai
Dublin
Frankfurt
Gibraltar
Guernsey (CI)
Jersey (CI)
Johannesburg
Leeds
Lisbon
London
Luxembourg
Madrid
Manchester
Milan
Munich
Padua
Paris
Riyadh
Rome
TelAviv
Turin
Zurich

Asia Pacific

Bangalore
Beijing
Christchurch
Guangzhou
Hanoi
Hong Kong
Hyderabad
Jakarta
Kuala Lumpur
Manila
Mumbai
New Delhi
Shanghai
Shenzhen
Singapore
Sydney
Taipei
Tokyo

KROLL

KROLL

For more information, please contact:

Hannah Rossiter
Managing Director
Financial Services Compliance and Regulation
E: Hannah.Rossiter@Kroll.com

Tiernan Connolly
Managing Director
Strategy and Risk Consulting
E: Tiernan.Connolly@Kroll.com

About Kroll

Kroll is the world's premier provider of services and digital products related to valuation, governance, risk and transparency. We work with clients across diverse sectors in the areas of valuation, expert services, investigations, cyber security, corporate finance, restructuring, legal and business solutions, data analytics and regulatory compliance. Our firm has nearly 5,000 professionals in 30 countries and territories around the world. For more information, visit www.kroll.com.