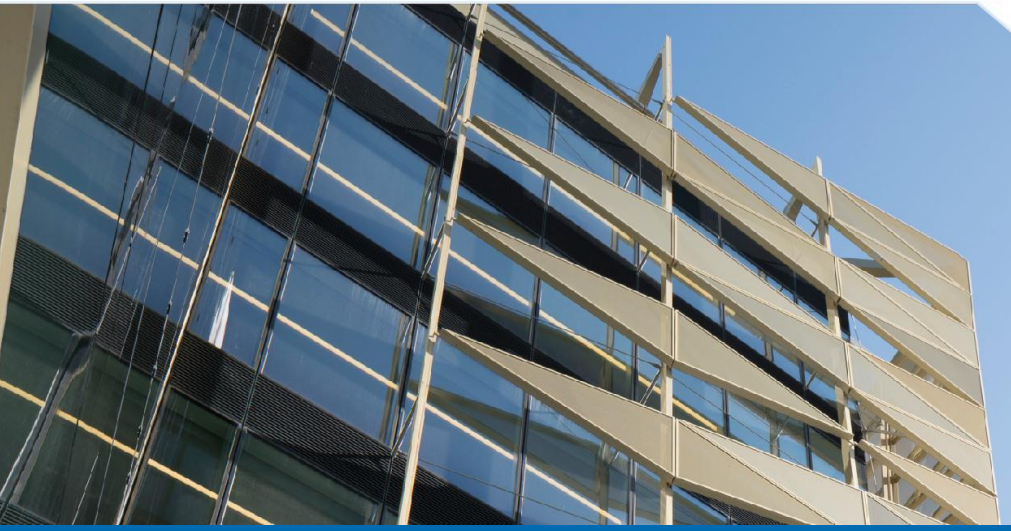
Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

DORA



Digital Operational Resilience Act (DORA)
Industry Briefing
6 November 2024

Opening Speech by Gerry Cross

Director of Financial Regulation - Policy and Risk at Central Bank of Ireland

Overview of the key pillars of DORA by Joern Dobberstein

Policy Manager at Central Bank of Ireland

What is the Digital Operational Resilience Act (DORA)?

Objective of DORA

- DORA is a directly applicable EU regulation to establish a comprehensive framework on **digital operational resilience for EU financial entities**
- Establishes **uniform requirements concerning the security of network and information systems** supporting the business processes of financial entities
- Applies to a **wide number of financial entities**, amongst others, to credit and payment institutions, insurance companies, investment firms, and crypto-asset service providers
- Imposes **obligations** on how **financial entities manage ICT-related risks**
- Imposes additional **obligations on the supervisory competent authorities, including oversight of critical ICT third party providers,** with an impact on the supervision of ICT-related risks
- Contributes to **regulatory harmonisation**

European Supervisory Authorities (ESAs)

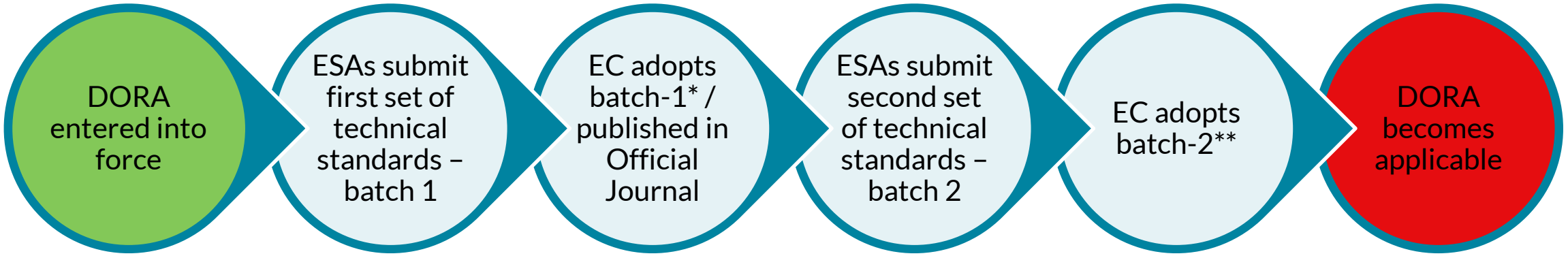
EBA EUROPEAN BANKING AUTHORITY

eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

DORA's timelines

DORA's timelines –continued



- Still awaiting European Commission (EC) adoption:

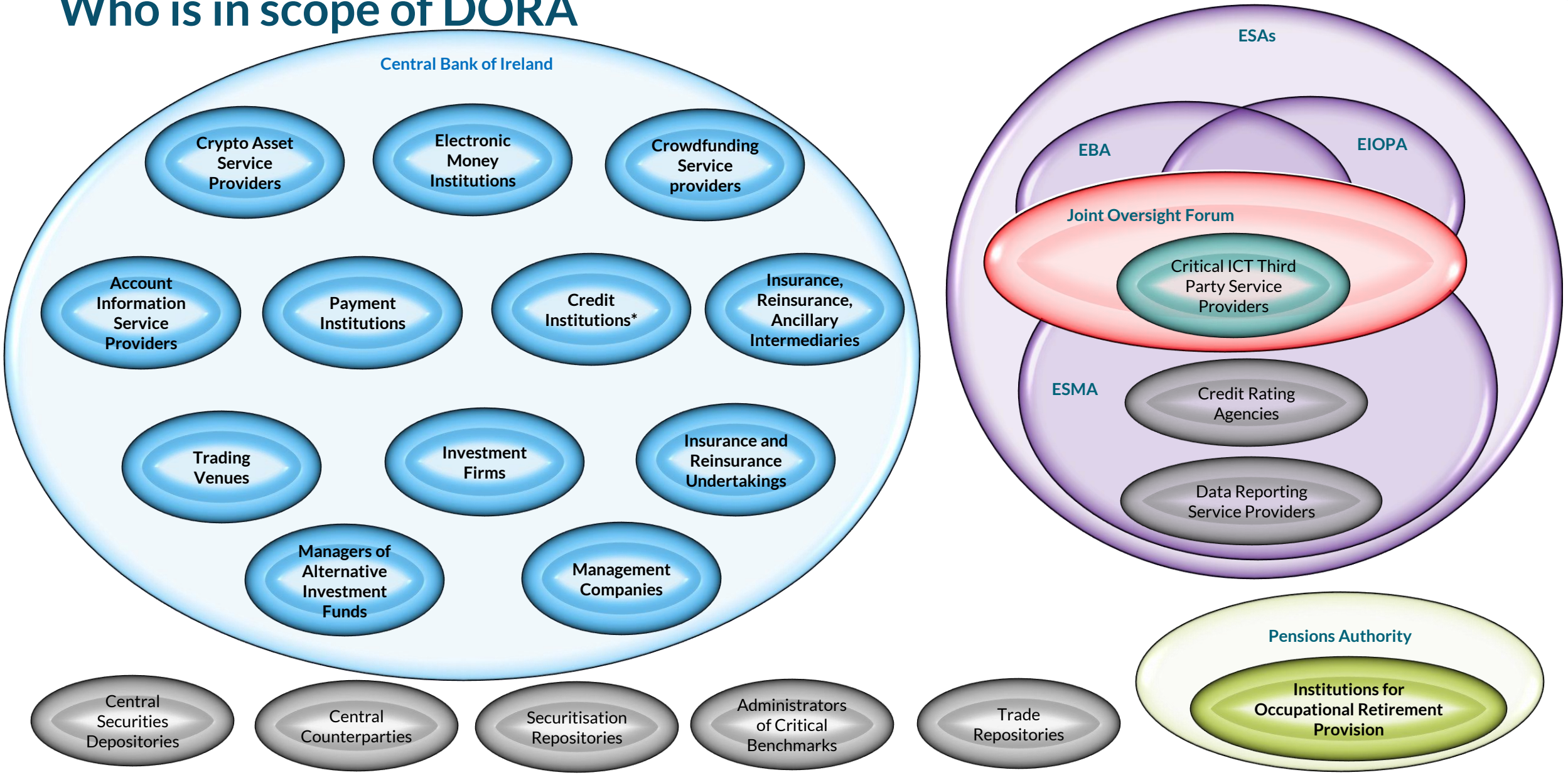
* Implementing Technical Standards (ITS) on the Register of Information

** Regulatory Technical Standards (RTS) on subcontracting; RTS on threat-led penetration testing; RTS on Joint Examination teams

- Currently under 3 month European Parliament (EP) scrutiny:

** RTS on content and time limits for major ICT-related incident reporting;
RTS on harmonisation on oversight

Who is in scope of DORA



None of the financial entity types marked in grey are currently authorised in Ireland
*SI Credit Institutions are supervised by the ECB

What are the key pillars of DORA?

Collaboration & Cooperation

Articles 45-49

Voluntary exchange of information between financial entities and cross sector cyber related crisis management exercises

ICT Risk Management

2x RTS

Articles 5-16

In summary:

- **Responsibility resides with the management body of the financial entity**
- **ICT risk management integral part of enterprise risk management**
- **Technical requirements:**
- Identify, protect, detect,
- response and recover.

ICT–related incident management

2x RTS / 1x ITS

Articles 17-23

In summary:

- **Requirements and processes for identifying, managing and reporting of all ICT incidents**
- **Classification of ICT incidents and cyber threats**
- **Reporting of major ICT incidents and voluntary notification of cyber threats**

Digital operational resilience testing

1x RTS

Articles 24-27

In summary:

- **Basic testing for all financial entities, incl.** vulnerability scans, performance tests, code reviews, etc.
- **Advanced TLPT testing in accordance with the TIBER-EU framework**

Managing of ICT third–party risk

3x RTS / 1x ITS

Articles 28-44

In summary:

- **Requirements and processes for ICT third-part risk management, incl. a register of information and min. contract requirements**
- **Oversight Framework for Union critical ICT Third-party providers (CTPP) through ESAs**

A focus on the expectations of Financial Entities in relation to: ICT risk management and ICT outsourcing by Helen Murphy

IT Risk Inspector at Central Bank of Ireland

DORA – Areas in Focus for Financial Entities

DORA Level 1 Regulation	• Chapter II – ICT Risk Management • Chapter IV – Digital Operational Resilience Testing • Chapter V – Managing ICT Third Party Risk
DORA Level 2 texts	• RTS on ICT Risk Management Framework (RMF) and Simplified ICT RMF • RTS on Policy on ICT Third Party Services • ITS on Register of Information • RTS on Subcontracting

ICT Risk Management

Mind-set/Approach

- **Good risk management**
  - Build on what you have
  - Integrate and embed into existing ICT Risk Management framework *(policies, procedures, monitoring & oversight)*
  - Strengthen existing controls and practices
  - Ensure residual risks are tolerable risks
  - **Include a Digital Operational Resilience Strategy**
  - **Annual Report on review of the ICT RMF**

New

- **Proactive**
  - Identify gaps with DORA requirements and close them
  - Keep up and evolve with the changing environment, identifying vulnerabilities and threats
  - Policies, procedures, protocols and tools need to remain relevant
- **Proportionality**
  - Risk based controls (e.g. cryptographic controls) and mitigants
  - Simplified ICT Risk Management
- **Information sharing**
  - Timely communication and sharing of information

Building on the Fundamentals

Governance

Roles and Responsibilities, details of expectations of the management body, informative reporting to the management body etc.

Core Operations

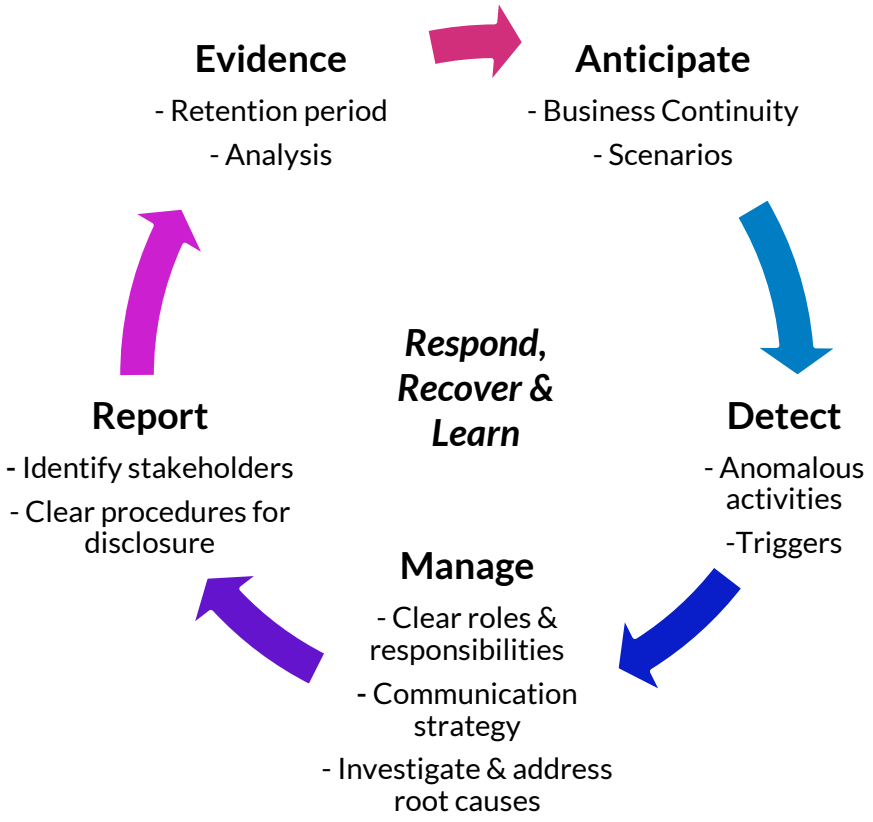
ICT Assets (whole lifecycle), Data, Networks, Software, Legacy systems

Change Management and Oversight

Oversight by the management body, controls to minimize disruption such as the use of test environments and having contingency or “fall back” plans in place

Digital Operational Resilience

Strategy



Testing

DORA requires:

- **Comprehensive Test Programme** to be established as part of the ICT risk management framework.
- At least **yearly** Digital Operational Resilience testing, by **independent parties**, on a risk-based approach.

Different types of testing, depending on the nature, size, complexity of services, activities and operations may include:

- Vulnerability assessment and scanning;
- Penetration testing;
- Open Source analyses; and
- Source code testing, among others.

ICT Third Party Risk Management

Strategy and policies

DORA requirements to have:

- A **Strategy on ICT Third Party Risk in place.** ICT **intra-group service providers**, should be considered as ICT third-party service providers.
- A **Policy** on the Use of ICT services supporting **critical** or **important** functions provided by ICT third party service providers (TPPs). This should cover the full lifecycle of the outsourcing arrangements. Policies are to be applied in a consistent and coherent way within group entities.
- A **Methodology** for determining which ICT services support critical or important functions.

Governance

Ultimate responsibility for the control and monitoring of ICT risk management rests with the management body.

Establish a Role or **designate a member** of **senior management**, responsible for monitoring the relevant contractual arrangements.

Appropriate **reporting** to the management body should be put in place.

Subcontracting

The RTS on subcontracting covers contractual requirements between Financial Entities and TPPs, and TPPs and subcontractors.

Principle focus - to be able to **identify and monitor performance of subcontractors supporting critical and important functions**. This should be reported in the register of information.

ESAs Dry run of the Collection of Register of Information

Participation

- 31 Financial Entities regulated by the Central Bank of Ireland participated

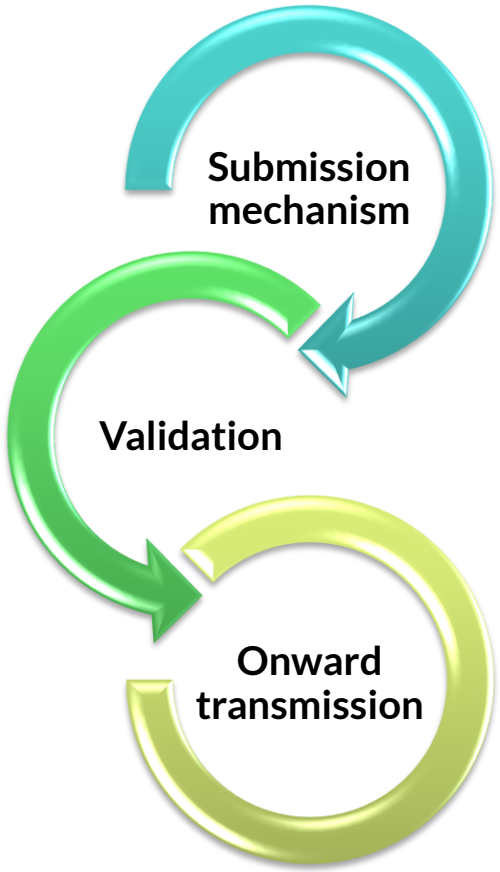
Insights

- **Overall, Data Quality was poor**
- This was across all financial entities not just ones relevant to the Central Bank of Ireland
- **A very low number of financial entities had no Data Quality issues**
- The most common issues observed were:
  - Duplicate values found on key variables
  - Mandatory field value missing
  - Invalid LEI code
  - Invalid value for LISTCURRENCY and LISTBINARY
  - Mandatory field values missing; and
  - Invalid date

Feedback and next steps

- Individual feedback files have been shared with participating financial entities where received from ESAs
- ESAs will hold a workshop in December to go through observed issues from the dry run

Process for collection of the Registers of Information



- **Submission mechanism:** Financial entities will be assigned the Register as a return on the Central Bank of Ireland portal, in the same manner as many other returns currently submitted.
- **Validation:** Automated validation checks will be performed when the file is submitted, based on the ESAs taxonomy. If the file does not pass these checks, it will need to be updated and resubmitted.
- **Onward Transmission:** In addition to the automated validation, supervisors will have the opportunity to perform some additional validation before the file is transmitted onwards to the ESAs.
- **Timing:**
  - 2025: As it currently stands, financial entities should be prepared to submit the registers to the Central Bank of Ireland in the first week of April 2025.
  - 2026 onwards: Our current understanding is that Financial entities will need to submit their Registers of Information to the Central Bank of Ireland, by early March each year.

A focus on the expectations of Financial Entities in relation to: Major Incident and Cyber Threat Reporting & Response by Eoghan Horkan

Senior Manager Crisis Preparedness and Operational Resilience at Central Bank of Ireland

Major ICT-related Incident and Significant Cyber Threat reporting

DORA introduces harmonised cross sectoral Major ICT-related Incident and Significant Cyber Threat reporting to ensure individual financial entities have a clear view of the incidents and threats they are experiencing and authorities are positioned to respond to risks and threats. Focus today is on the reporting requirements rather than overall incident management processes.

Major ICT-related Incidents

Clearly defined reporting timelines:

- Initial report – within 4 hours
- Intermediate report – within 72 hours
- Final report – within 1 month

Information is outlined in the ITS, with mandatory fields and information required increasing with each subsequent report

Information provided will inform supervisory response, including at an EU level if the incident has a widespread impact

Significant Cyber Threats

Notification of significant cyber threats is voluntary

Information requested is outlined in the ITS and aims to provide detailed and relevant information to support review

Requested information is less structured than the major incident report and will inform supervisory response

Voluntary reports can also be made to the Computer Security Incident Response Team in the National Cyber Security Centre

Operational considerations for Major ICT-related Incident and Significant Cyber Threat reporting

DORA introduces a number of new or enhanced operational and system changes that financial entities need to be aware of and prepared for

Current reporting

DORA reduces the reporting burden for financial entities with **existing incident reporting**. For others, there will be an initial impact but DORA will also raise ICT incident detection, reporting and response maturity

Central Bank portal

Central Bank portal that is used for regulatory reporting will be the system used to for DORA reporting, which will appear as two new return types for financial entities

Template

In line with the DORA aim of **harmonising incident reporting**, the templates developed by the ESAs will be used for Major Incident and Cyber Threat reports

Guidance

Operational guidance to **support incident and cyber threat reporting** will be provided to financial entities. Technical and supervisory support will be available through normal channels, similar to other Central Bank returns and reports.

Major ICT-related Incident and Significant Cyber Threat reporting

Financial entities will log on to the Central Bank Portal to report major incidents and cyber threats using reporting templates developed by the ESAs

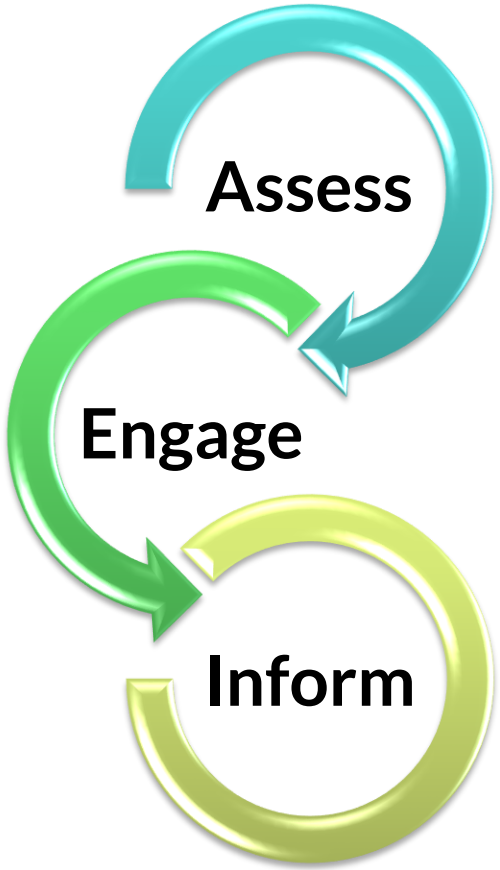
Central Bank Portal

- Central Bank Portal to upload major incident and cyber threat reports
- Straightforward and user friendly approach
- Reports will appear as two new return types
- Users will select the relevant type of report (major incident/cyber threat) and upload completed template
- System validation of the template will occur
- Users will receive confirmation of acceptance or an error message (on screen and email) outlining issues in report

Reporting templates

- Use the ESA template for reporting
- Developed by ESAs over the last number of months and public consultation on ITS
- Excel file with drop downs and validation within the file itself
- Additional validation in line with RTS and ITS when Excel file is uploaded to ensure data quality
- Final RTS and ITS were adopted on 23 October

Central Bank's response to Major Incident and Significant Cyber Threat reports



- **Assess:**
  - Assessment will be conducted by supervisory staff and supporting SME teams
  - Assessment will consider impact on the financial entity or entities, consumers and the wider financial system where multiple entities are affected.
- **Engage:**
  - Our response, including supervisory engagement, will be informed by the severity, nature and impact of incident/threat
  - We may follow up with supervisory actions as required after the incident
- **Inform:**
  - We will inform relevant ESAs and other authorities as required under DORA
  - We will engage with other authorities, where required, to support a co-ordinated response to any national or EU incidents.

Central Bank Expectations

Ensure readiness to meet reporting requirements on 17 January 2025. Focus on accurate and timely reporting. Ensure you are open and engaged with the Central Bank.

Preparedness

We expect financial entities to implement an ICT incident management process to **detect, manage and to notify** stakeholders of ICT incidents including identifying their root causes

Reporting

We expect financial entities to report major incidents **within the timelines** and in line with the expectations in the RTS/ITS

Engagement

Financial entities are expected to engage with the Central Bank on major incidents in a **proactive and transparent** manner. Allows regulator assess if wider systemic risks are present

Continuous development

We expect entities to implement a system of **continuous improvement** with respect to incident management, incorporating lessons learned into Business Continuity Plans and wider risk management plans

Panel discussion and Q&A engagement session with attendees

Panel Discussion & Q&A

- **Moderator**
  - **Gavin Curran** - Head of Securities & Markets Supervision at Central Bank of Ireland

- **Panel members**
  1. **Lisa O' Mahony** - Head of Governance & Operational Resilience at Central Bank of Ireland
  2. **Joern Dobberstein** - Policy Manager at Central Bank of Ireland
  3. **Aoife Langford** – Head of Financial Crisis Preparedness and Management at Central Bank of Ireland
  4. **Andrea Vetrone** - Senior Expert and Head of the Digital Operational Resilience act (DORA) implementation at EIOPA

Banc Ceannais na hÉireann
Central Bank of Ireland

Eurosystem