DORA Digital Operational Resilience Act

ICT-related Incident Management

Part 3 of the ***DORA Deep Dive*** *Series*

Presented By:

Gerard Joyce, CTO, CalQRisk

Tuesday 26th November 2024

CalQRisk

Outline

- Introductions
- DORA Overview
- ICT-related Incident Management (What's in the Act)
- Regulatory Technical Standards (C(2024) 6901)
- Implementing Technical Standards (C(2024) 7277)
- Q&A

Who we are and what we do

- Experienced Risk & Compliance Professionals
- Members of IRM, IOB, CI (ACOI), IoD, ACCA, ISACA, ….
- We Make A Governance, Risk & Compliance Solution called CalQRisk
  - A cloud-based software solution
  - Includes a DORA-specific solution (Checklists / Register of Information report..)
- Risk Advisory Service
  - In-house / Virtual Training, Strategic Risk Alignment, Risk Management Framework development
- CalQRisk is used by 3,000+ users in regulated firms and others

  Including: Financial Services organisations and Not-For-Profit sector: Housing Associations, Charities, Sports Organisations

“

No plan survives first contact with the enemy

Helmuth von Moltke

”

DORA Overview

- A Regulation. Applies to all EU Member States
- Came into force in Jan 2023
- It becomes applicable on Jan 17th 2025
- Applies to financial entities and some of their service providers
- It’s about making the ICT systems that support financial business better
- Better in the sense that they are more secure, less likely to fail, faster to get back up and running, if they do fail.
- It harmonises and improves several guidelines that are in operation today.

DORA closes a gap by ensuring that operational resilience is not merely about financial buffers

DORA Five Pillars

- ICT Risk Management Framework - Oct 15th
- ICT Third Party Risk Management - Nov 12th
- **ICT-related Incident Management - Nov 26th Today**
- Digital Operational Resilience Testing - Dec 10th
- Information Sharing Arrangements- Jan 14th

Definitions

- ICT-related incident’ means a single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity;

ICT- related Incident Management (Act)

- **Article 10**: Detection. (mechanisms, alert thresholds, trigger response, integrity of reports)
- **Article 11:** Response and recovery. (BC policy, procedures, containment measures, communication actions, independent internal audit review, test, BIA, records of activities during disruption events
- **Article 12:** Backup policies and procedures, restoration and recovery procedures and methods (backup policies, procedures, redundant capacity, RTO, RPO, integrity of restore)
- **Article 13:** Learning and evolving (info on vulnerabilities and threats, post-incident reviews, improvements)
- **Article 14:** Communication. (Crisis communication plans, assign individual responsible for strategy implementation)

ICT- related Incident Management (Act) ctd

- **Article 17: ICT-related incident management process**.
  (detect, manage, notify, response procedure, record all incidents and cyber threats, identify root causes, prevent reoccurrence, early warning indicators, categorise, roles and responsibilities, communication plans, reporting,

- **Article 18**: **Classification of ICT-related incidents and cyber threats.**
  (clients/counterparts affected, reputation impact, duration, geographical spread, data loss, criticality of services affected, economic impact)

- **Article 19: Reporting of major ICT-related incidents and voluntary notification of significant cyber threats.**
  (initial report, inform clients without undue delay, intermediate report, updates, final report, actual impact figures)

- **Article 20**: **Harmonisation of reporting content and templates.**
  (ESA to develop RTS)

ICT-related Incident Management

The How

Regulatory Technical Standards (C(2024) 6901)

- **Article 1**: *General information to be provided in initial notifications and intermediate and final reports on major ICT-related incidents*
  - (type, FE names, ID Codes, contact details, parent, monetary impact)
- **Article 2**: *Specific information to be provided in initial notifications*
  (ref code, date/time detected, description, classification criteria, member states impacted, how discovered, origin, BCP activated?)
- **Article 3**: *Specific information to be provided in intermediate reports*
  (CA-ref code, date/time occurred, date/time activities restored, classification criteria, type, techniques used by threat actor, affected areas, affected infrastructure, impact on financial interests of clients, info on reporting to other authorities, temporary actions, indicators of compromise)
- **Article 4**: *Article Specific information to be provided in final reports*
  (root causes, date/time resolved, date/time RC addressed, resolution, direct / indirect costs/losses, financial recoveries, recurring incidents)
- **Article 5**: *Time limits for the initial notification, and for the intermediate and final reports*
  (Initial: 4 hours after classification, <24 hours from detection. Intermediate: <72 hours after initial and when activities recovered. Final: < 1 Mth after last intermediate)
- **Article 6**: Content of the voluntary notification of significant cyber threats
  (general info, date/time detected, description, potential impacts, classification criteria if threat were to materialise, status, changes, mitigation actions taken, info about notification to others, info on IoCs, other relevant info.

Regulatory Technical Standards (C(2024) 6901)

- **Article 1**: *General information to be provided in initial notifications and intermediate and final reports on major ICT-related incidents*
  - (type, FE names, ID Codes, contact details, parent, monetary impact)
- **Article 2**: *Specific information to be provided in initial notifications*
  (ref code, date/time detected, description, classification criteria, member states
- **Article 3**: *Specific information to be provided in intermediate report*
  (CA-ref code, date/time occurred, date/time activities restored, classification crit
  affected infrastructure, impact on financial interests of clients, info on reporting to oth
- **Article 4**: *Article Specific information to be provided in final reports*
  (root causes, date/time resolved, date/time RC addressed, resolution, direct / in
- **Article 5**: *Time limits for the initial notification, and for the intermed*
  (Initial: 4 hours after classification, <24 hours from detection. Intermediate: <72
  Mth after last intermediate)

Classification criteria from Commission Delegated Regulation (EI) 2024/1772

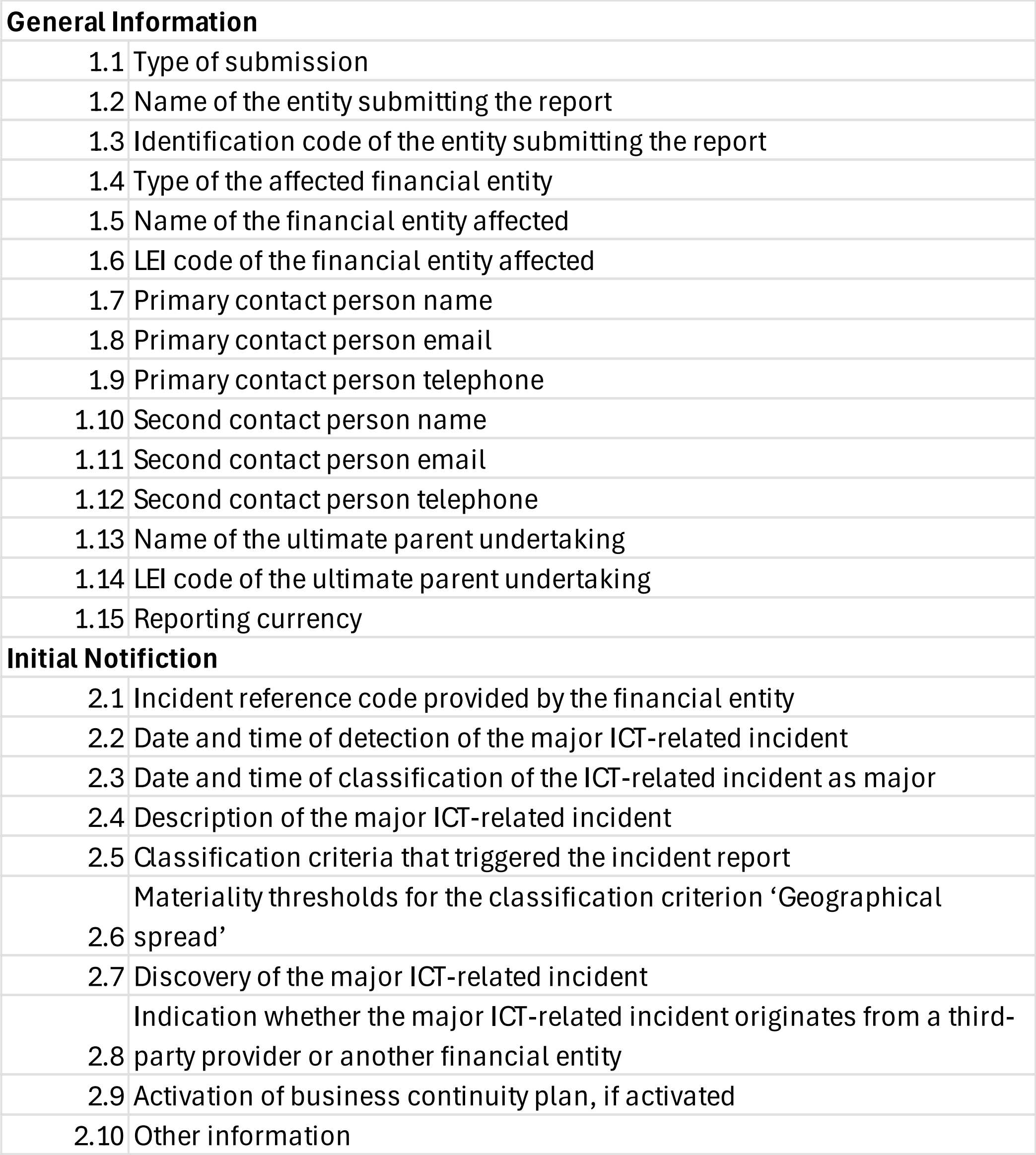
- Clients, financial counterparts and transactions
- Reputational impact
- Duration and service downtime
- Geographical spread
- Data losses
- Criticality of services affected
- Economic impact

- **Article 6**: Content of the voluntary notification of significant cyber threats
  (general info, date/time detected, description, potential impacts, classification criteria if threat were to materialise, status, changes, mitigation actions taken, info about notification to others, info on IoCs, other relevant info.

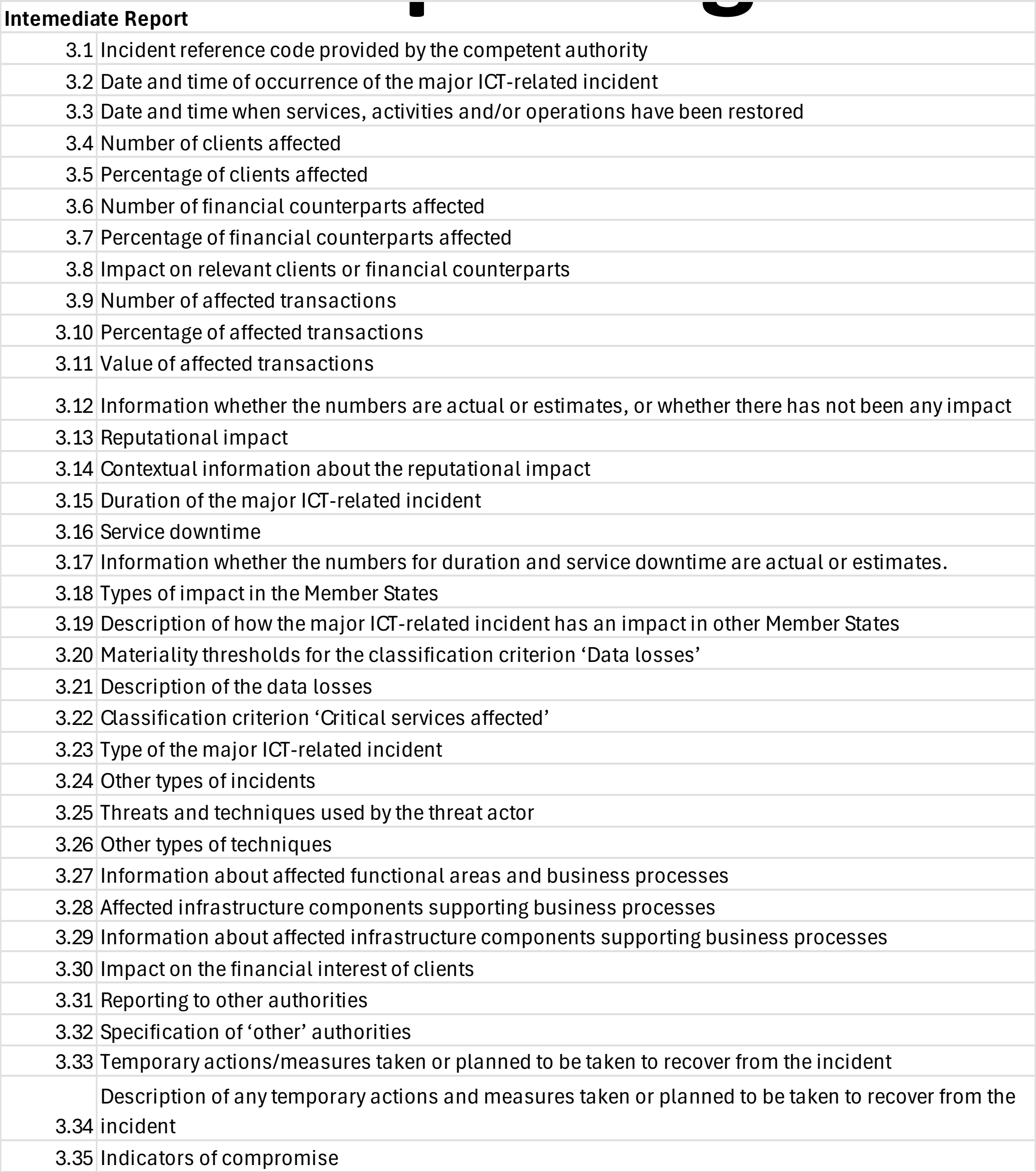
Implementing Technical Standards (C(2024) 7277)

- **Article 1**: Standard form for reporting of ICT-related major incidents
  - (See annex I)
- **Article 2**: Submission of initial notification, intermediate and final reports together
  (if all can be / are completed withing timelines specified)
- **Article 3**: Recurring incidents
  - (provide aggregated information)
- **Article 4**: Use secure channels
  - (once you are able to do so)
- **Article 5**: Reclassification of major incidents
  (by completing annex II and submitting)
- **Article 6**: Notification of outsourcing of the reporting obligation
  - (prior to first notification, as soon as arrangement concluded, name, contact details, id code, advise when cancelled)
- **Article 7**: Aggregated reporting
  (TP may aggregate where incident impacting many Fes, single Member State.)
- **Article 8:** Standard form for voluntary reporting of significant cyber threats
  - (use Annex III for reporting)

ITS for ICT-related Incident Reporting

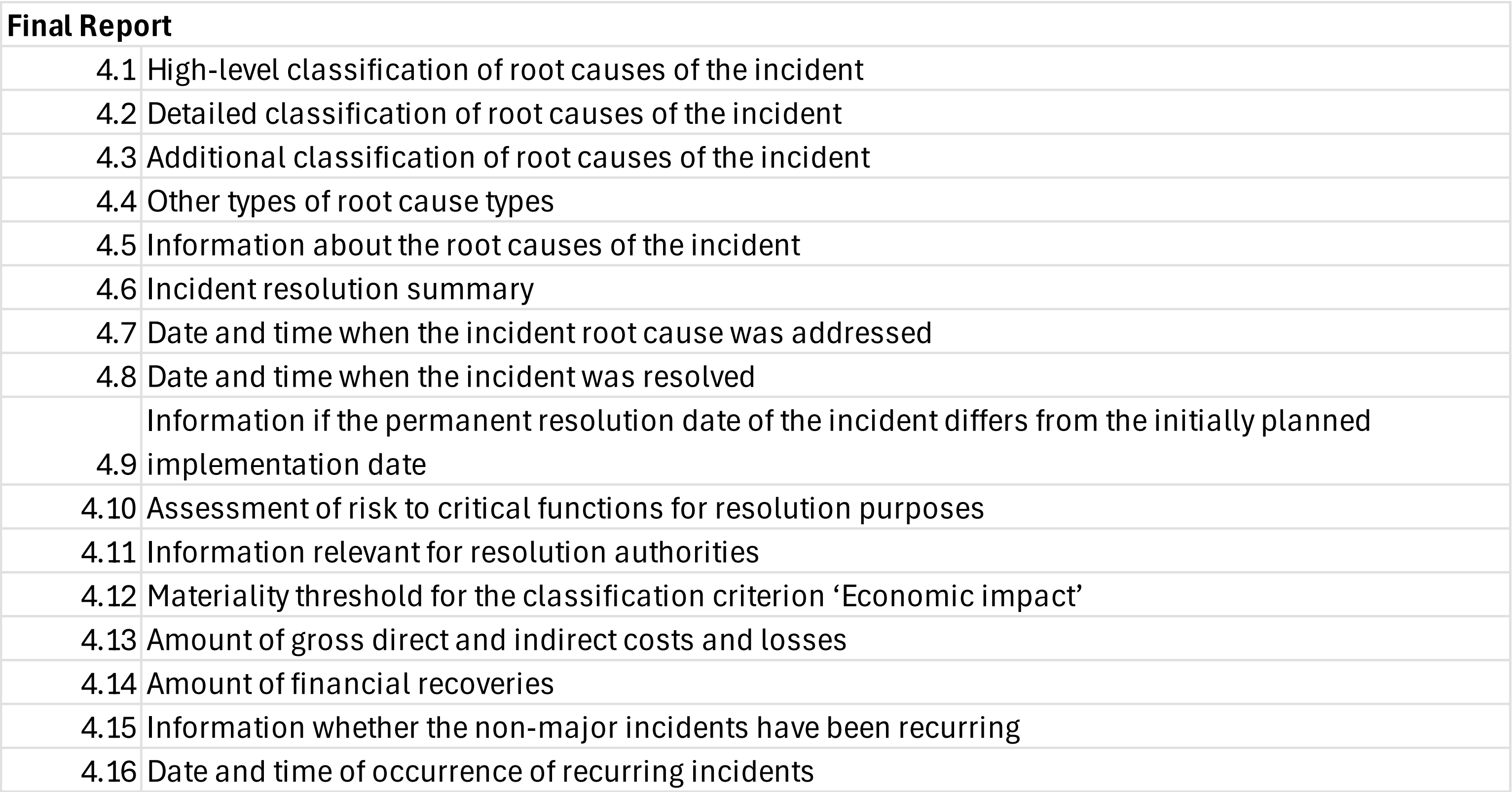


General Information	
1.1	Type of submission
1.2	Name of the entity submitting the report
1.3	Identification code of the entity submitting the report
1.4	Type of the affected financial entity
1.5	Name of the financial entity affected
1.6	LEI code of the financial entity affected
1.7	Primary contact person name
1.8	Primary contact person email
1.9	Primary contact person telephone
1.10	Second contact person name
1.11	Second contact person email
1.12	Second contact person telephone
1.13	Name of the ultimate parent undertaking
1.14	LEI code of the ultimate parent undertaking
1.15	Reporting currency
Initial Notifiction	
2.1	Incident reference code provided by the financial entity
2.2	Date and time of detection of the major ICT-related incident
2.3	Date and time of classification of the ICT-related incident as major
2.4	Description of the major ICT-related incident
2.5	Classification criteria that triggered the incident report
2.6	Materiality thresholds for the classification criterion 'Geographical spread'
2.7	Discovery of the major ICT-related incident
2.8	Indication whether the major ICT-related incident originates from a third-party provider or another financial entity
2.9	Activation of business continuity plan, if activated
2.10	Other information



Intemediate Report	
3.1	Incident reference code provided by the competent authority
3.2	Date and time of occurrence of the major ICT-related incident
3.3	Date and time when services, activities and/or operations have been restored
3.4	Number of clients affected
3.5	Percentage of clients affected
3.6	Number of financial counterparts affected
3.7	Percentage of financial counterparts affected
3.8	Impact on relevant clients or financial counterparts
3.9	Number of affected transactions
3.10	Percentage of affected transactions
3.11	Value of affected transactions
3.12	Information whether the numbers are actual or estimates, or whether there has not been any impact
3.13	Reputational impact
3.14	Contextual information about the reputational impact
3.15	Duration of the major ICT-related incident
3.16	Service downtime
3.17	Information whether the numbers for duration and service downtime are actual or estimates.
3.18	Types of impact in the Member States
3.19	Description of how the major ICT-related incident has an impact in other Member States
3.20	Materiality thresholds for the classification criterion 'Data losses'
3.21	Description of the data losses
3.22	Classification criterion 'Critical services affected'
3.23	Type of the major ICT-related incident
3.24	Other types of incidents
3.25	Threats and techniques used by the threat actor
3.26	Other types of techniques
3.27	Information about affected functional areas and business processes
3.28	Affected infrastructure components supporting business processes
3.29	Information about affected infrastructure components supporting business processes
3.30	Impact on the financial interest of clients
3.31	Reporting to other authorities
3.32	Specification of 'other' authorities
3.33	Temporary actions/measures taken or planned to be taken to recover from the incident
3.34	Description of any temporary actions and measures taken or planned to be taken to recover from the incident
3.35	Indicators of compromise

ITS for ICT-related Incident Reporting ctd



Final Report	
4.1	High-level classification of root causes of the incident
4.2	Detailed classification of root causes of the incident
4.3	Additional classification of root causes of the incident
4.4	Other types of root cause types
4.5	Information about the root causes of the incident
4.6	Incident resolution summary
4.7	Date and time when the incident root cause was addressed
4.8	Date and time when the incident was resolved
4.9	Information if the permanent resolution date of the incident differs from the initially planned implementation date
4.10	Assessment of risk to critical functions for resolution purposes
4.11	Information relevant for resolution authorities
4.12	Materiality threshold for the classification criterion ‘Economic impact’
4.13	Amount of gross direct and indirect costs and losses
4.14	Amount of financial recoveries
4.15	Information whether the non-major incidents have been recurring
4.16	Date and time of occurrence of recurring incidents

Just 76 fields !

Takeaways

- Make sure you have a robust Incident Response Plan
  - Detect, Response, Recovery, Communications
  - Have Backups
  - Do Lessons Learned
- Identify / classify “Major” incidents
  - Initial, Intermediate, Final reports (same template, increasing detail)
- Need to gather lots of information… 76 fields
- Less than 2 months to go (to Jan 17, 2025) !!

Questions ?

gerard.joyce@calqrisk.com

Linkedin.com/company/calqrisk

Twitter.com/calqrisk

CalQRisk