# Information and Communication Technology Risk Management

*Part 1 of the **DORA Deep Dive** Series*

**Presented By**:

Gerard Joyce, CTO, CalQRisk

**Tuesday 15th October 2024**

CalQRisk

# Outline

- Introductions
- DORA Overview
- Information and Communication Technology (ICT) risk management
- Regulatory Technical Standards (2024/1774)
- 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

66

**Rules are not necessarily sacred; principles are**

***Franklin D. Roosevelt***

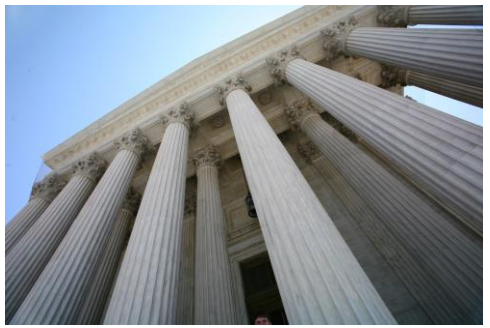
99

# 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

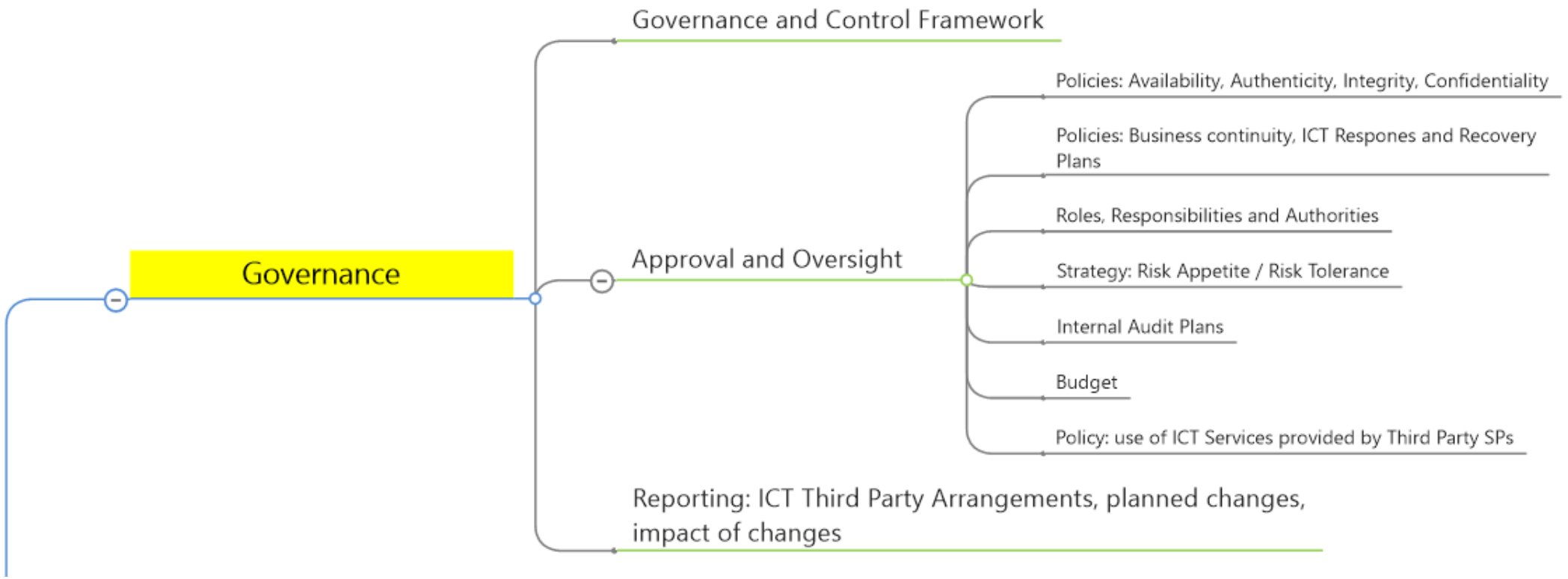


- ICT Risk Management Framework - Oct 15th Today
- ICT Third Party Risk Management - Nov 12th
- ICT-related Incident Management - Nov 26th
- Digital Operational Resilience Testing - Dec 10th
- Information Sharing Arrangements- Jan 14th

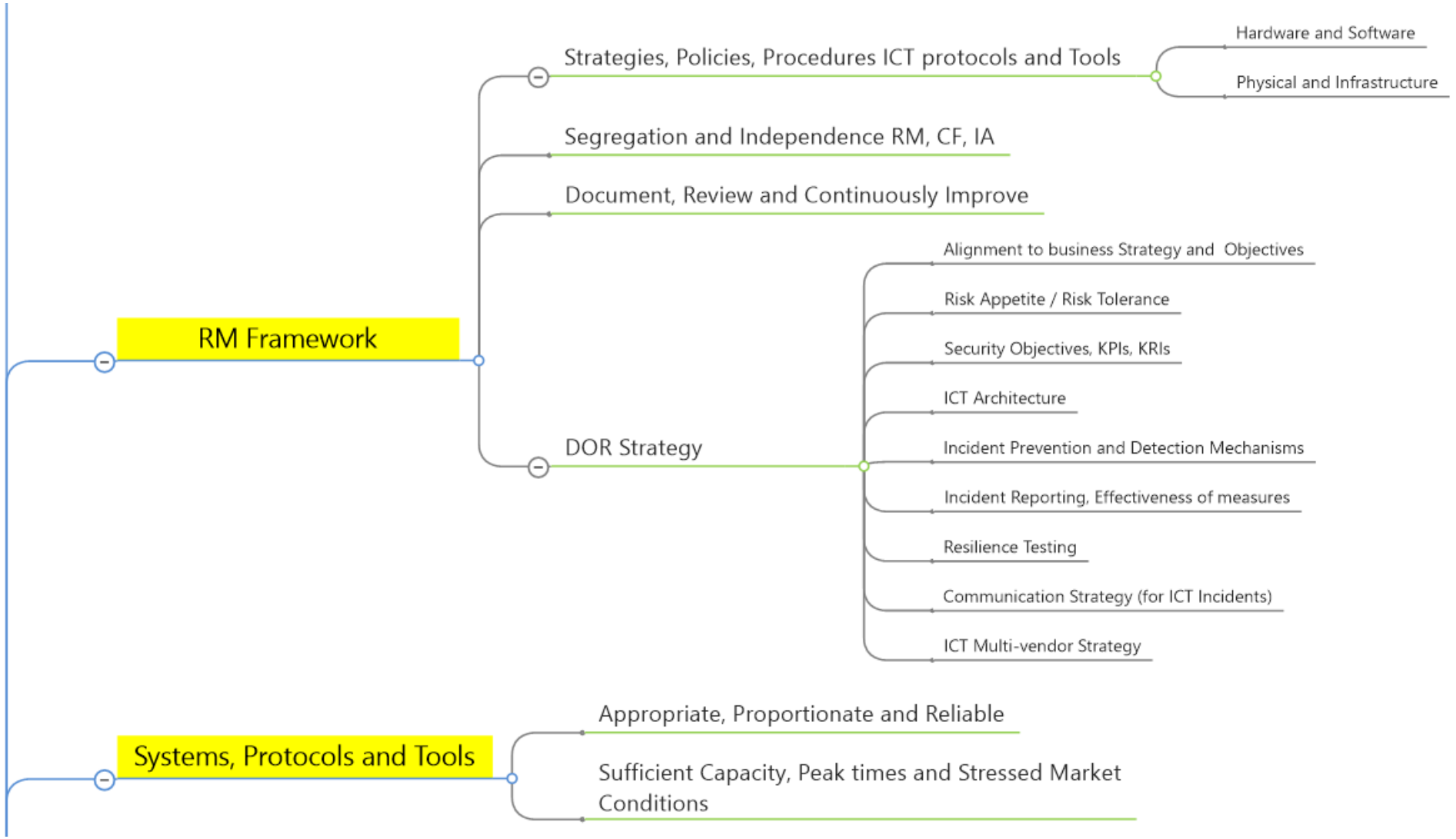
# ICT Risk Management (Ch. II)

- Article 5: Governance and organisation
- Article 6: ICT risk management framework
- Article 7: ICT systems, protocols and tools
- Article 8: Identification
- Article 9: Protection and prevention
- Article 10: Detection
- Article 11: Response and Recovery
- Article 12: Backup Policies and procedures
- Article 13: Learning and Evolving
- Article 14: Communication
- Article 15: further harmonisation of ICT risk management tools
- Article 16: Simplified ICT Risk Management Framework

# ICT Risk Management (Ch. II)

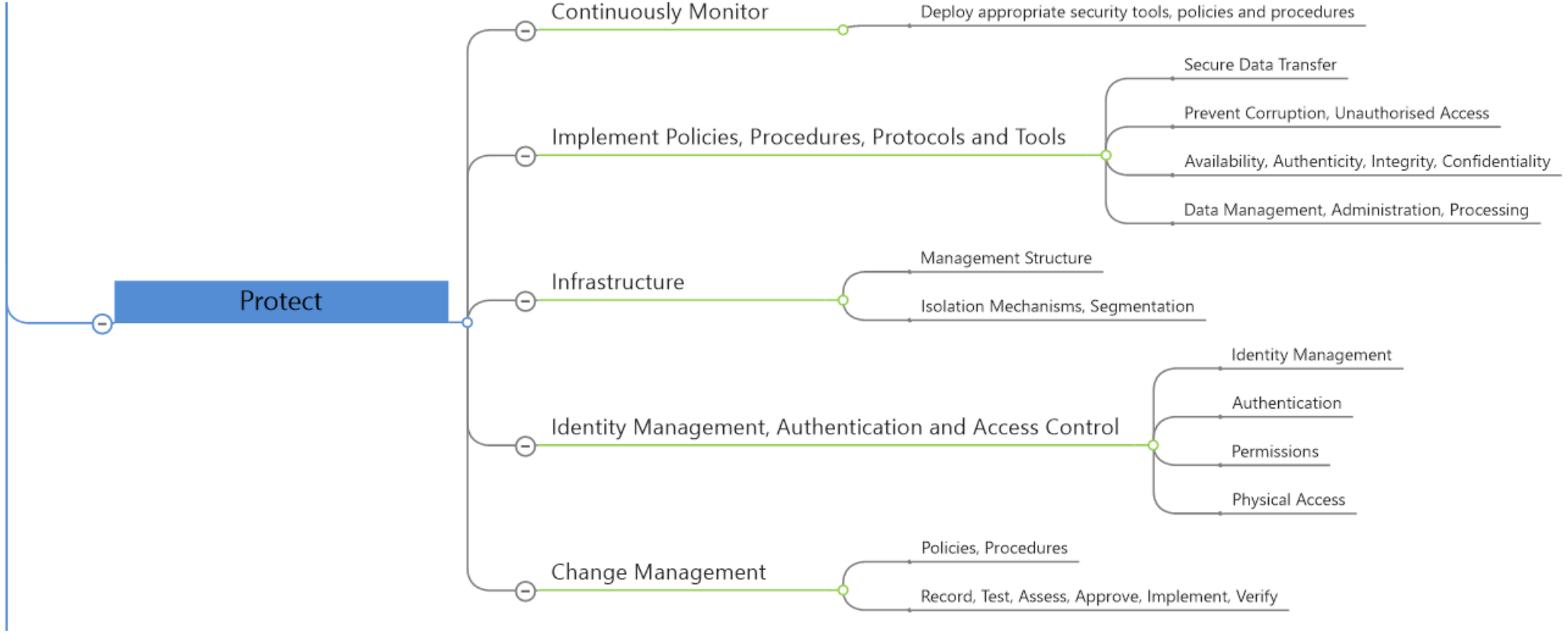


# ICT Risk Management (Ch. II)

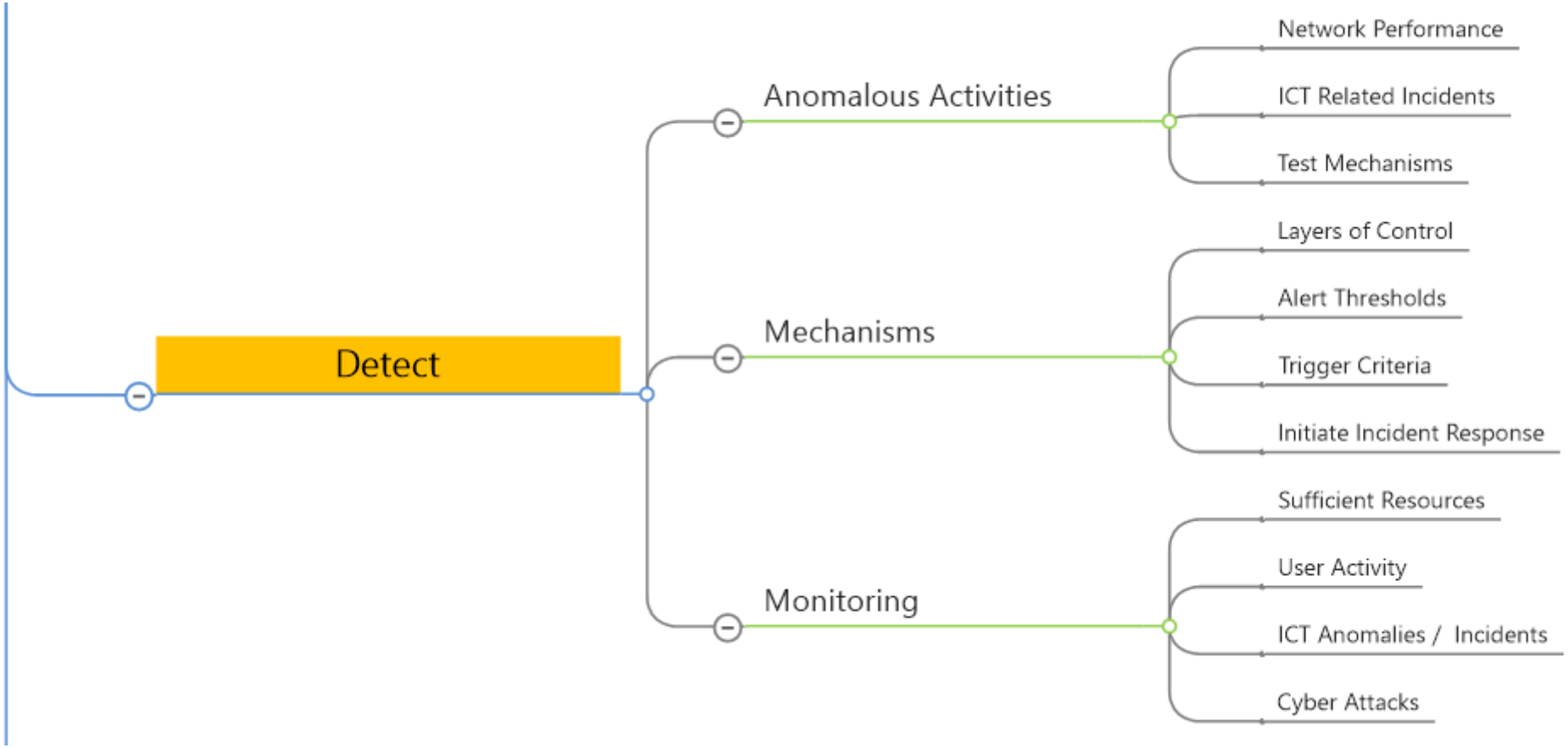


# ICT Risk Management (Ch. II)

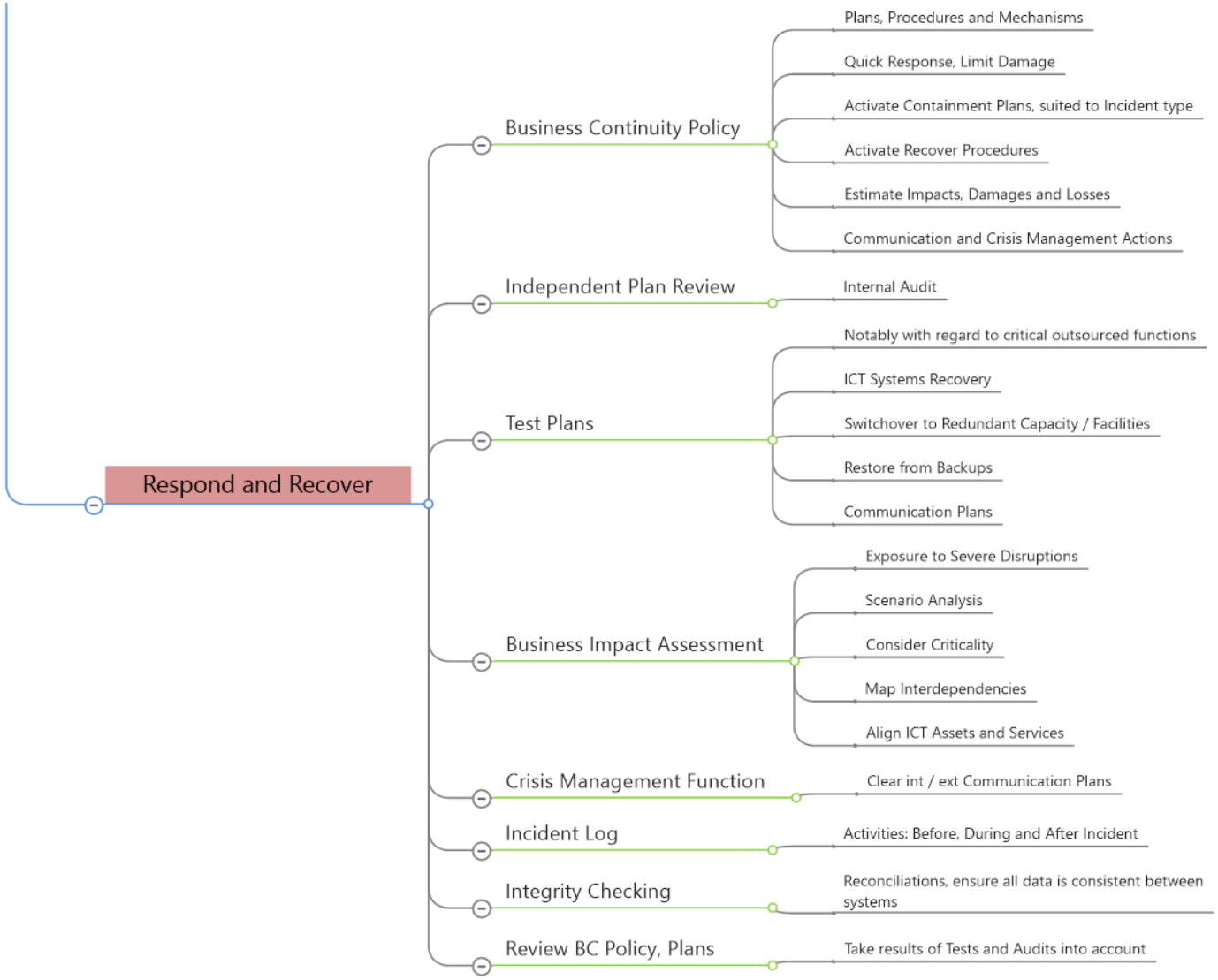
# ICT Risk Management (Ch. II)



# ICT Risk Management (Ch. II)



# ICT Risk Management (Ch. II)



# ICT Risk Management Art 12

**Backup Policies and procedures**

- Policies and Procedures, specifying scope of data covered
- Recovery Procedures
- Backup Systems: Ensure no impact on: availability, integrity, authenticity and confidentiality
- Physically and logically separate
- Redundancy, proportionate to operation
- RTO and RPO to take criticality into account and impact on market efficiency

# ICT Risk Management Art 13

**Learning and Evolving**

- Gather information on cyber threats and vulnerabilities, technological developments
- Review Incidents: Causes, Improvements
  - Response (prompt?)
  - Forensic analysis (speed, quality)
  - Escalation (effectiveness)
  - Communications
- Feed back into Risk Assessment / Plan Review
- Report annually to Management Team. (findings and recommendations)
- Awareness Training (incl. third-parties)

# ICT Risk Management Art 14

**Communication**

- Policies: for internal and external stakeholders
- Disclosure plans:  to Clients or Counterparties / Public
- Roles and Responsibilities (have at least one person responsible)

# ICT Risk Management Art 16

**Simplified ICT risk management framework… for the Exempted**

- Have and maintain a documented ICT risk management framework
- Continuously monitor the security and functioning of all ICT systems;
- Use appropriate resilient and updated ICT systems, protocols and tools
- Identify and detect anomalies in network and information systems
- Handle ICT-related incidents swiftly
- Identify key dependencies on ICT third-party service providers
- Ensure continuity of critical or important functions, through BC plans and R&R measures
- Test Plans and measures and test effectiveness of controls
- Implement changes resulting from conclusions of tests, develop awareness programme

# ICT Risk Management Art 16 ctd

**Simplified ICT risk management framework… for the Exempted**

- Review ICT risk management framework periodically and on occurrence of major incident.
- Continuously improve the framework
- Submit report on review to competent authority

# The How

# Regulatory Technical Standards (DR 2024/1774)

- Article 1 Overall risk profile and complexity (1)
- Article 2 General elements of ICT security policies, procedures, protocols, and tools (16)
- Article 3 ICT risk management (8)
- Article 4 ICT asset management policy (13)
- Article 5 ICT asset management procedure (4)
- Article 6 Encryption and cryptographic controls (7)
- Article 7 Cryptographic key management (5)
- Article 8 Policies and procedures for ICT operations (7)
- Article 9 Capacity and performance management (5)
- Article 10 Vulnerability and patch management (18)
- Article 11 Data and system security (15)
- Article 12 Logging (9)
- Article 13 Network security management (15)
- Article 14 Securing information in transit (6)
- Article 15 ICT project management (12)
- Article 16 ICT systems acquisition, development, and maintenance (17)
- Article 17 ICT change management (12)
- Article 18 Physical and environmental security (9)
- Article 19 Human Resources Policy (3)
- Article 20 Identity Management (6)

# Regulatory Technical Standards (DR 2024/1774)

- Article 21 Access Control (22)
- Article 22 ICT-related incident management policy (6)
- Article 23 Anomalous activities detection and criteria for ICT-related incidents detection and response (14)
- Article 24 Components of the ICT business continuity policy (24)
- Article 25 Testing of the ICT business continuity plan (13)
- Article 26 ICT response and recovery plans (20)
- Article 27 Format and content of the report on the review of the ICT risk management framework (16)
- Article 28 Governance and organisation (14)
- Article 29 Information security policy and measures (3)
- Article 30 Classification of information assets and ICT assets (2)
- Article 31 ICT Risk Management (9)
- Article 32 Physical and environmental security (9)
- Article 33 Access Control (9)
- Article 34 ICT operations security (10)
- Article 35 ICT Data, system and network security (9)
- Article 36 ICT security testing (3)
- Article 37 ICT systems acquisition, development, and maintenance (4)
- Article 38 ICT project and change management (2)
- Article 39 Components of the ICT business continuity plan (12)
- Article 40 Testing of business continuity plans(3)
- Article 41 Format and content of the report on the review of the simplified ICT risk management framework (10)

**Exempted Orgs**

303/ 93 Requirements

# ICT Risk Management Regulatory Technical Standards (RTS)

- Article 1 Overall risk profile and complexity (1)
- Article 2 General elements of ICT security policies, procedures, protocols, and tools (16)
- Article 3 ICT risk management (8)
- Article 4 ICT asset management policy (13)
- Article 5 ICT asset management procedure (4)
- Article 6 Encryption and cryptographic controls (7)
- Article 7 Cryptographic key management (5)
- Article 8 Policies and procedures for ICT operations (7)
- Article 9 Capacity and performance management (5)
- Article 10 Vulnerability and patch management (18)

**Example of 2 Requirements**

**2(c)** The vulnerability management procedures referred to in paragraph 1 shall verify whether:

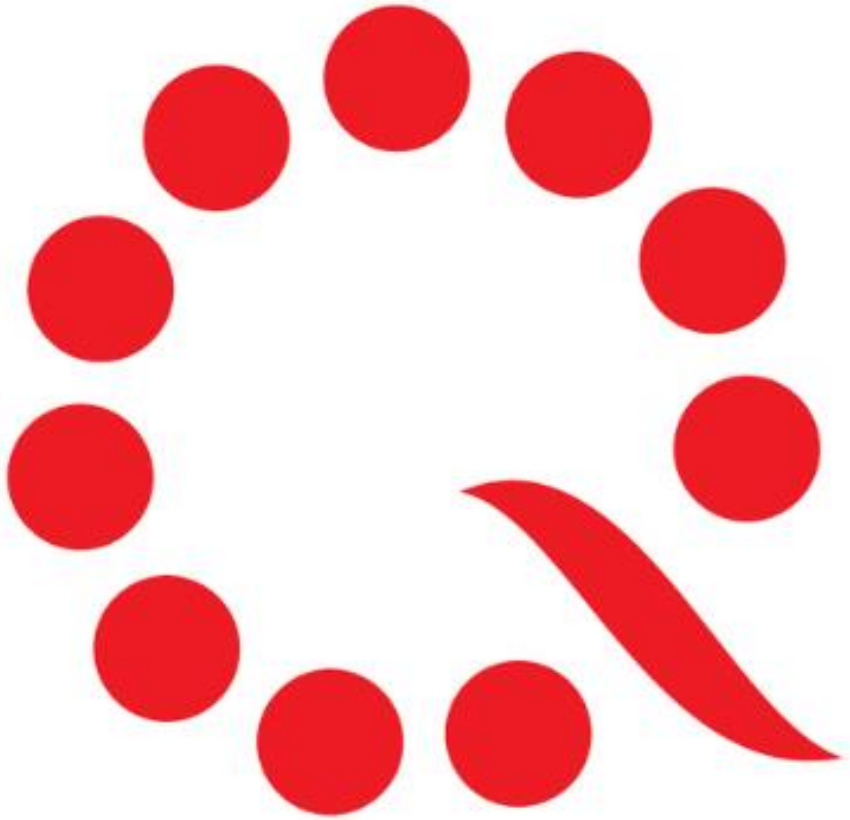
(i) ICT third-party service providers handle vulnerabilities related to the ICT services provided to the financial entity;

(ii) (ii) whether those service providers report to the financial entity at least the critical vulnerabilities and statistics and trends in a timely manner.

For the purposes of **point (c),** financial entities shall request that ICT third-party service providers investigate the relevant vulnerabilities, determine the root causes, and implement appropriate mitigating action.

# Takeaways

- It’s a lot of work, if you were starting from a blank sheet
- You should be doing most of this already
- Do a gap-analysis with current status
- Only 3 months to  go (to Jan 17 2025)



# Questions ?

gerard.joyce@calqrisk.com

Linkedin.com/company/calqrisk

**Twitter.com/calqrisk**

**CalQRisk**