Fundamentals of Cybersecurity for Senior Managers and Risk Officers

CalQRisk

Manage the effect of uncertainty on objectives

15th March 2022, presented by

Gerard Joyce, CTO, CalQRisk

Outline

- Introduction – Who we are
- What is Cybersecurity
- What are the Risks
- Standards and Guidelines
- Elements of Cybersecurity
- The NIST Approach - Identify, Protect, Detect, Respond, Recover
- Risk Management and Senior Manager's responsibilities
- Reporting to and Assuring the Board

Introduction - CalQRisk

CalQRisk
Manage the effect of uncertainty on objectives

CalQRisk is an Integrated Governance, Risk & Compliance Software Solution

- CalQRisk is used by 200+ regulated organisations

CalQRisk: the Company

- Experienced Risk & Compliance Professionals
- Members of IRM, ACOI, IoB, IoD, ACCA, ISACA
- Involved in the Development of Standards

Recently published a White Paper on Risk Management and Resilience

"There are only two types of companies: Those that have been hacked, and those that will be.“

FBI Director Robert Mueller

- **The UN reported a 600% increase in malicious emails during the pandemic**
- **Cybercrime will cost the world $>10 trillion annually by 2025**

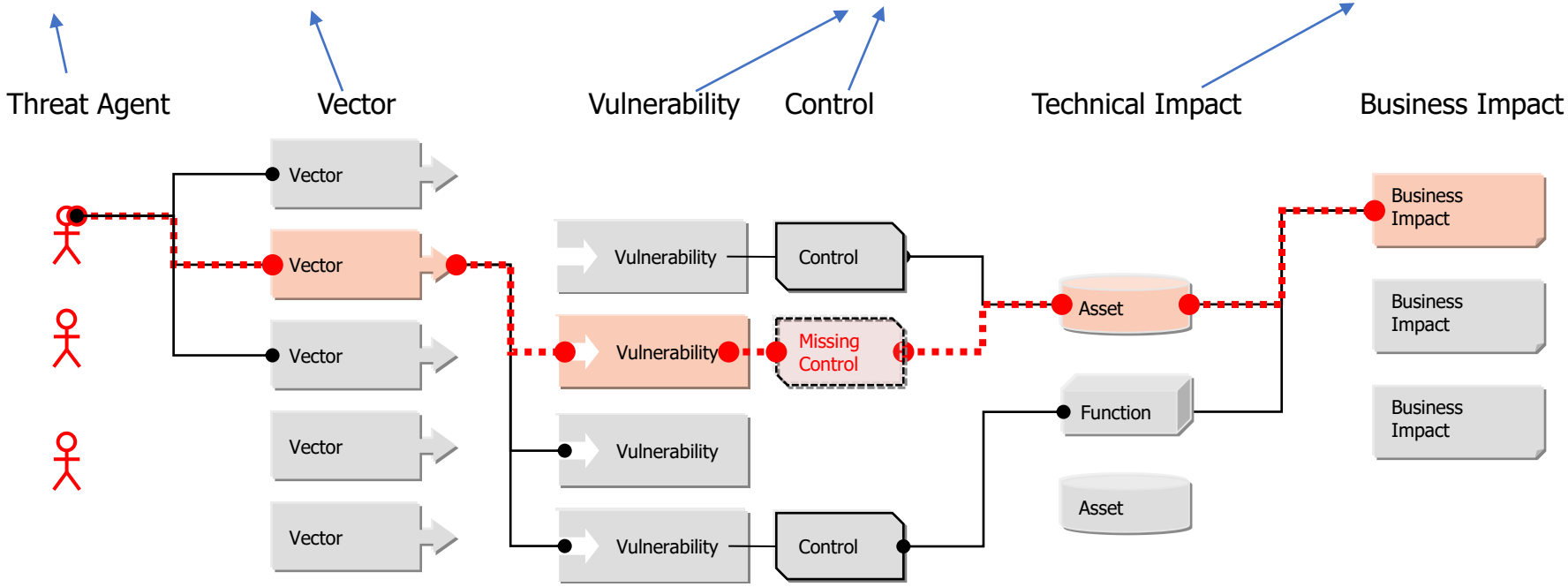
Stakeholder Expectations

- Cyber risks are understood and prioritised
- IT capability matches organisational ambitions
- Policies and procedures are appropriate
- Staff are trained on cybersecurity risk
- Systems are secure
- There is a plan for when things go wrong

What is Cybersecurity?

CalRisk
Manage the effect of uncertainty on objectives

Criminal sends **Email** with link to malware that **evades detection** and allows **access to Server**



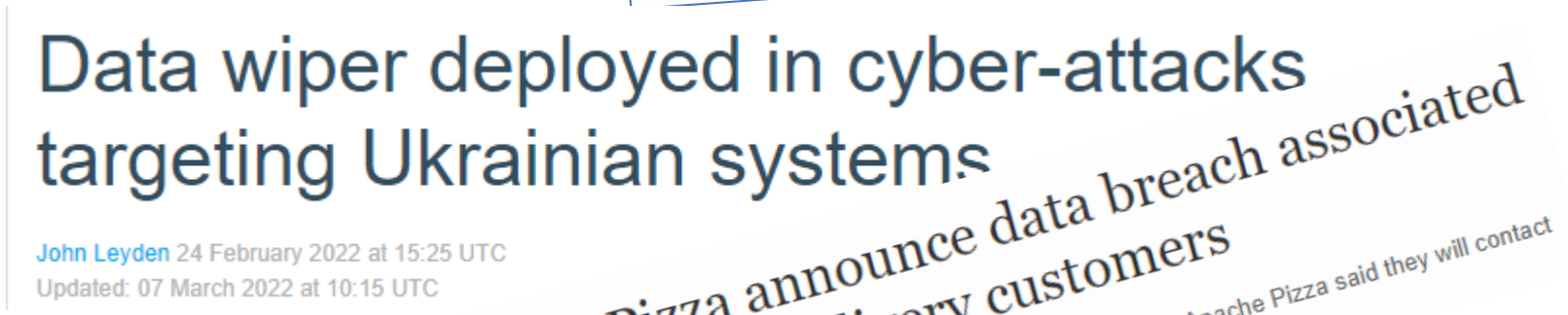
Source: Aspect Security

What are the Risks?

- Data Breach
- Loss of Assets
- Data Altered
- Extortion
- Spyware
- Identity Theft
- Distributed Denial of Service (DDoS)


'Sophisticated' cyber attack hits major academy chain

[redacted] says ransomware attack will have a 'significant impact' on its academies

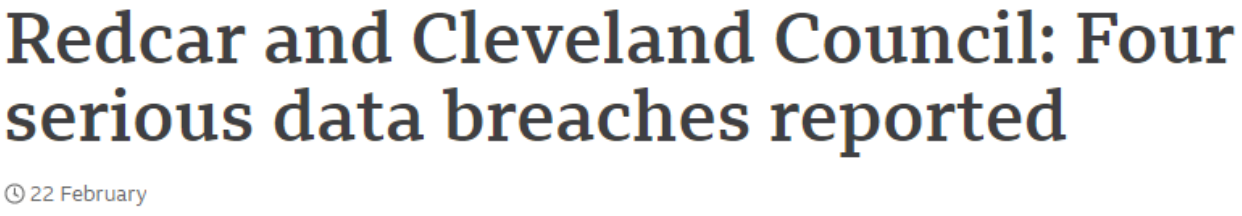

Data wiper deployed in cyber-attacks targeting Ukrainian systems

John Leyden 24 February 2022 at 15:25 UTC
Updated: 07 March 2022 at 10:15 UTC

Apache Pizza announce data breach associated with details of delivery customers

The Data Protection Commission has been notified of the breach and Apache Pizza said they will contact gardaí.


Samsung Confirms Massive Galaxy Hack After 190GB Data Torrent Shared Via Telegram


Redcar and Cleveland Council: Four serious data breaches reported

22 February

Attack Techniques

- Email, links, attachments
- Social Engineering
- Websites
- Wireless Hotspots
- Social Networking
- USB Devices (Memory sticks)

Social Engineering

- Spoofing
- Phishing
- Spear Phishing
- Vishing
- Watering Hole
- Bogus Inspectors

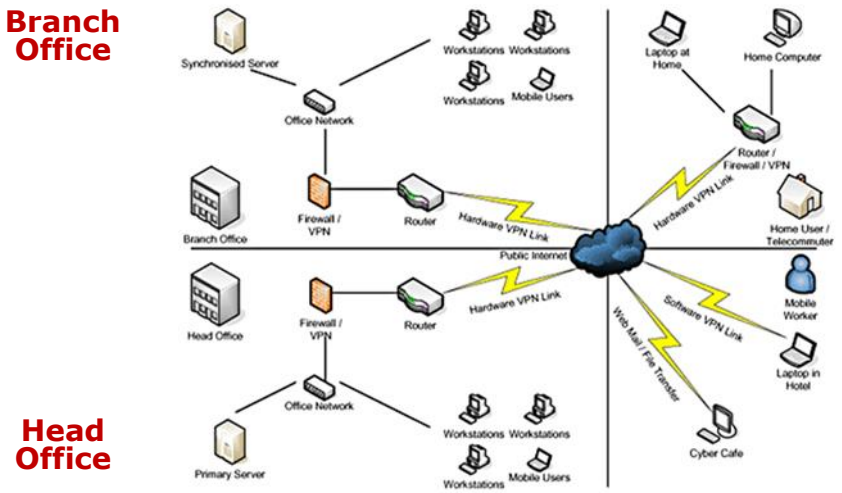
john@ABC_School.net
john@ABC_School.net

These two are NOT the same

john@ABC_School.net
john@ABC_SchooI.net

Vulnerabilities

- Unwitting Employees
- IT System Misconfiguration
- Unpatched Flaws in Op Systems
- Mobile Devices
- Storage of Data in the Cloud
- Service Providers / Partners



https://haveibeenpwned.com/

Mitigate the Risks

CalRisk
Manage the effect of uncertainty on objectives

- Enforce your information security policy
  - Classify data according to sensitivity
  - Encrypt sensitive data in transit / at rest
  - Manage the use of personal devices / Prevent
  - Require strong passwords / changing of passwords / two-factor authentication
- Train employees to recognise suspicious activity
  - Departure from agreed protocol / instructions
- Conduct Due Diligence on partners you rely on
- Document your procedures and stick to them
- Monitor adherence to procedures

Standards and Guidelines

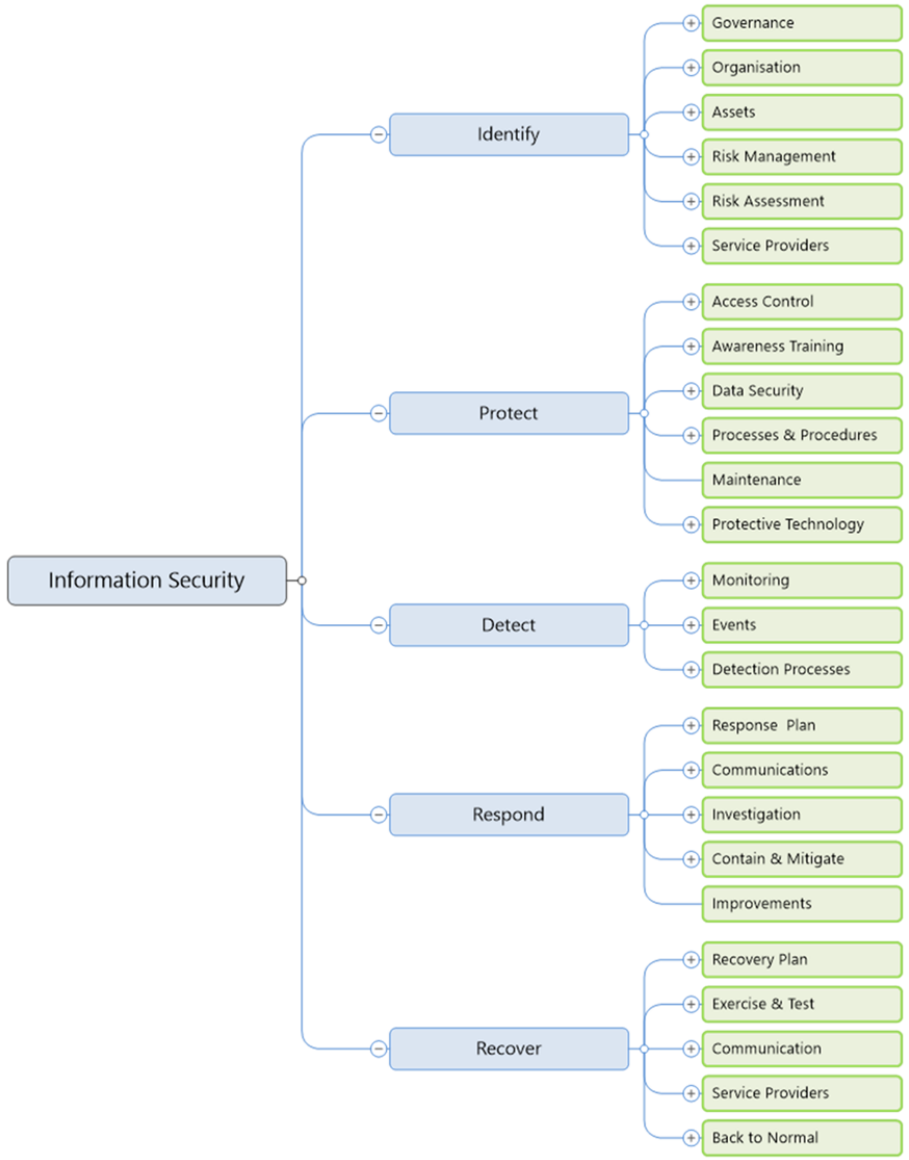
- NIST Cyber Security Framework
- ISO 27001
- CIS CSC (Critical Security Controls)
- COBIT
- Cyber questionnaire (PRA)
- CBI Cross Industry Guidance (2016)

Elements of Cybersecurity

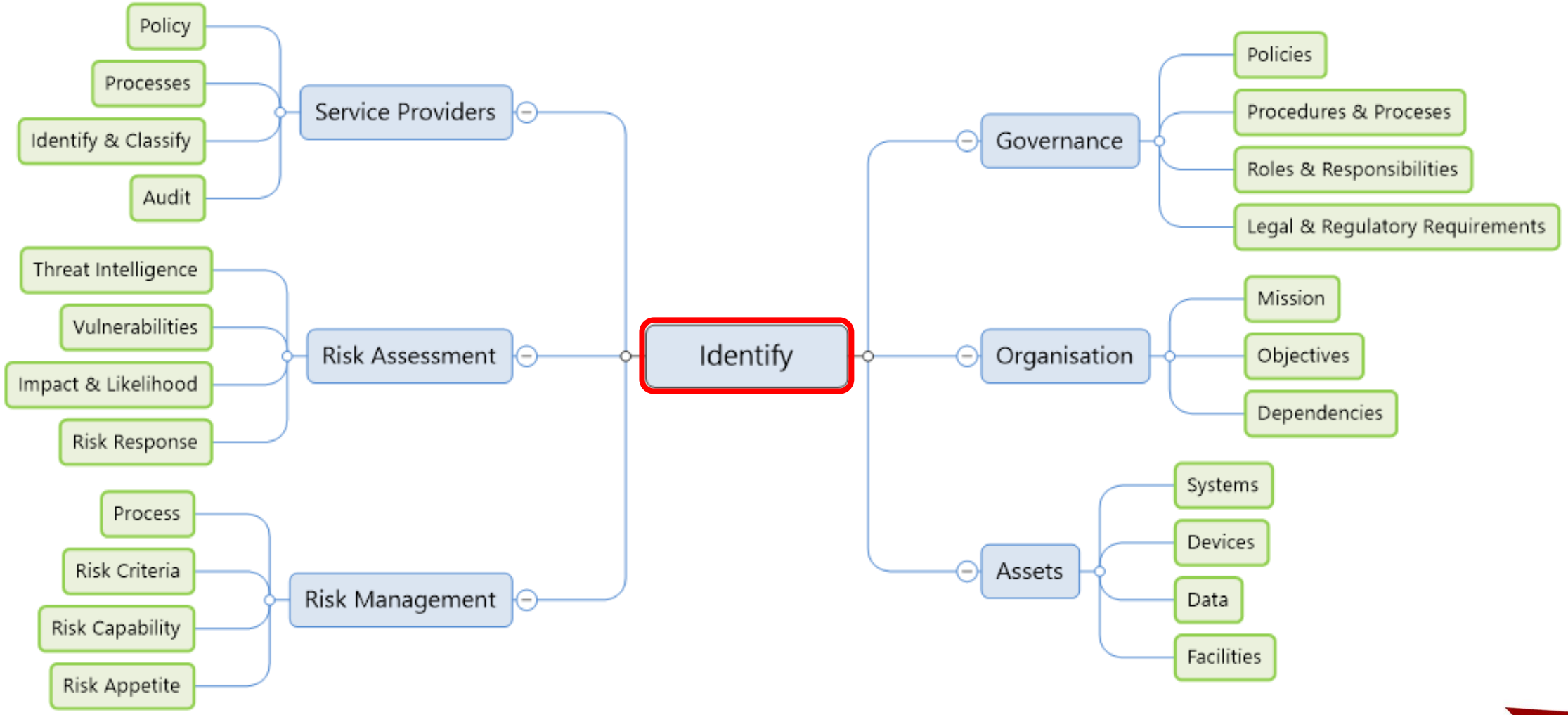
CalRisk
Manage the effect of uncertainty on objectives

The NIST Approach

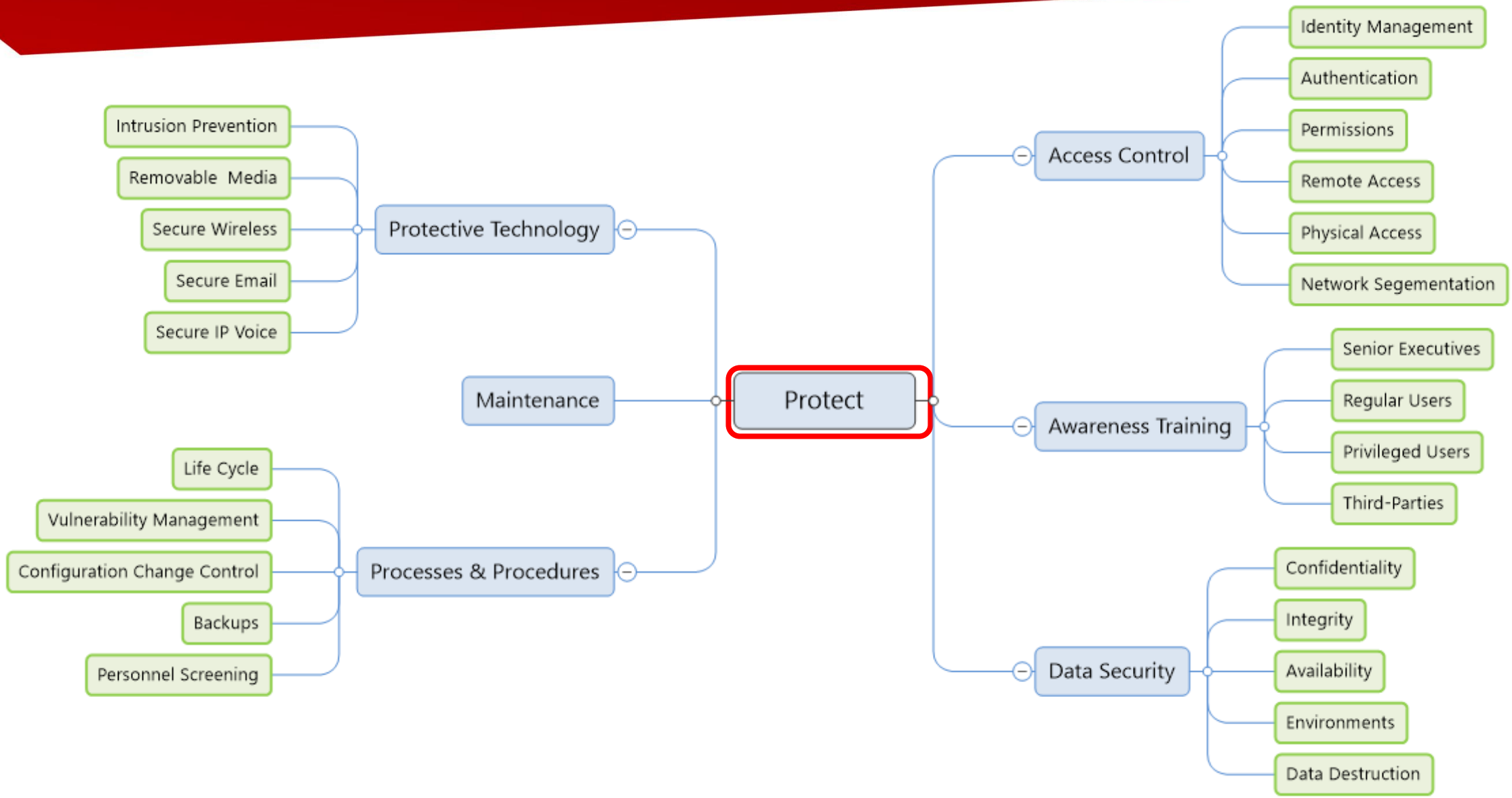
1. Identify
2. Protect
3. Detect
4. Respond
5. Recover



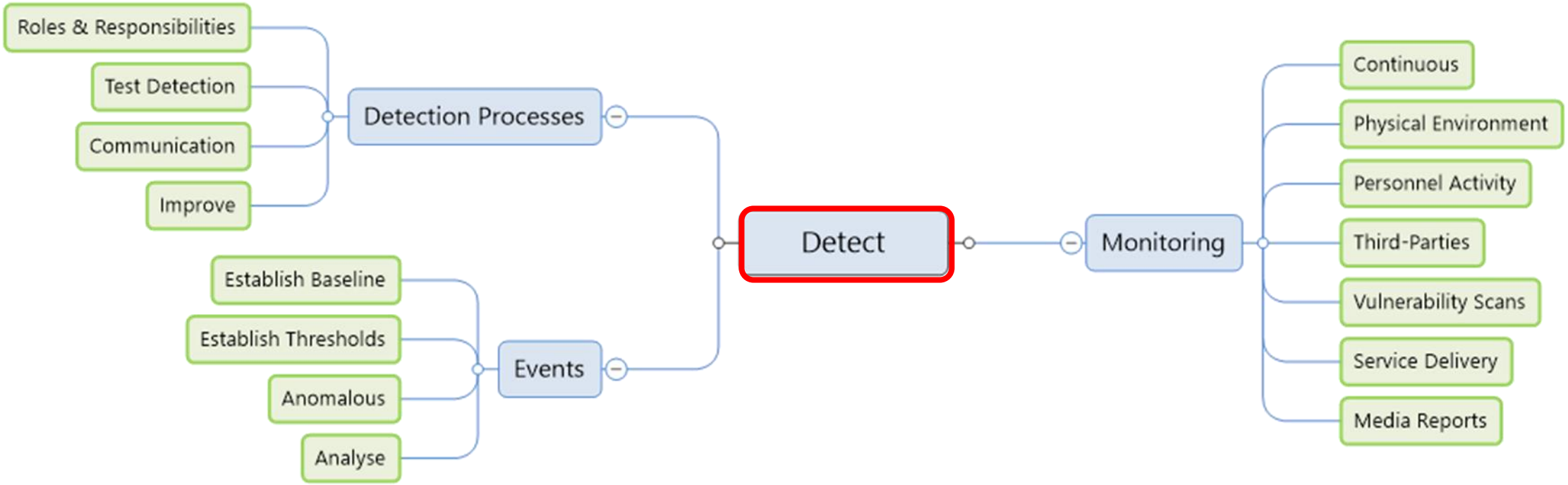
1. Identify


Identify
Service Providers
Policy
Processes
Identify & Classify
Audit
Risk Assessment
Threat Intelligence
Vulnerabilities
Impact & Likelihood
Risk Response
Risk Management
Process
Risk Criteria
Risk Capability
Risk Appetite
Governance
Policies
Procedures & Proceses
Roles & Responsibilities
Legal & Regulatory Requirements
Organisation
Mission
Objectives
Dependencies
Assets
Systems
Devices
Data
Facilities

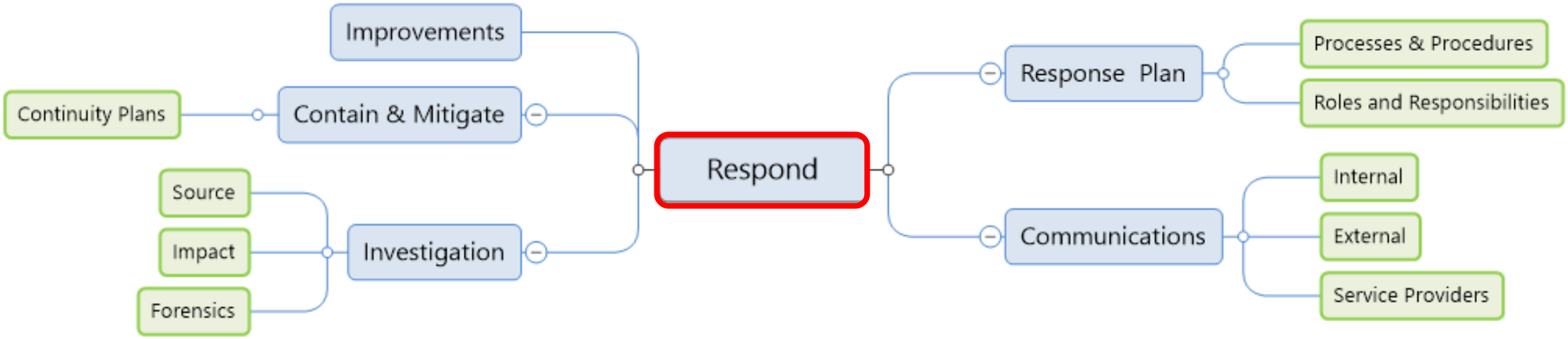
2. Protect


Protect
Protective Technology
Intrusion Prevention
Removable Media
Secure Wireless
Secure Email
Secure IP Voice
Maintenance
Processes & Procedures
Life Cycle
Vulnerability Management
Configuration Change Control
Backups
Personnel Screening
Access Control
Identity Management
Authentication
Permissions
Remote Access
Physical Access
Network Segementation
Awareness Training
Senior Executives
Regular Users
Privileged Users
Third-Parties
Data Security
Confidentiality
Integrity
Availability
Environments
Data Destruction

3. Detect

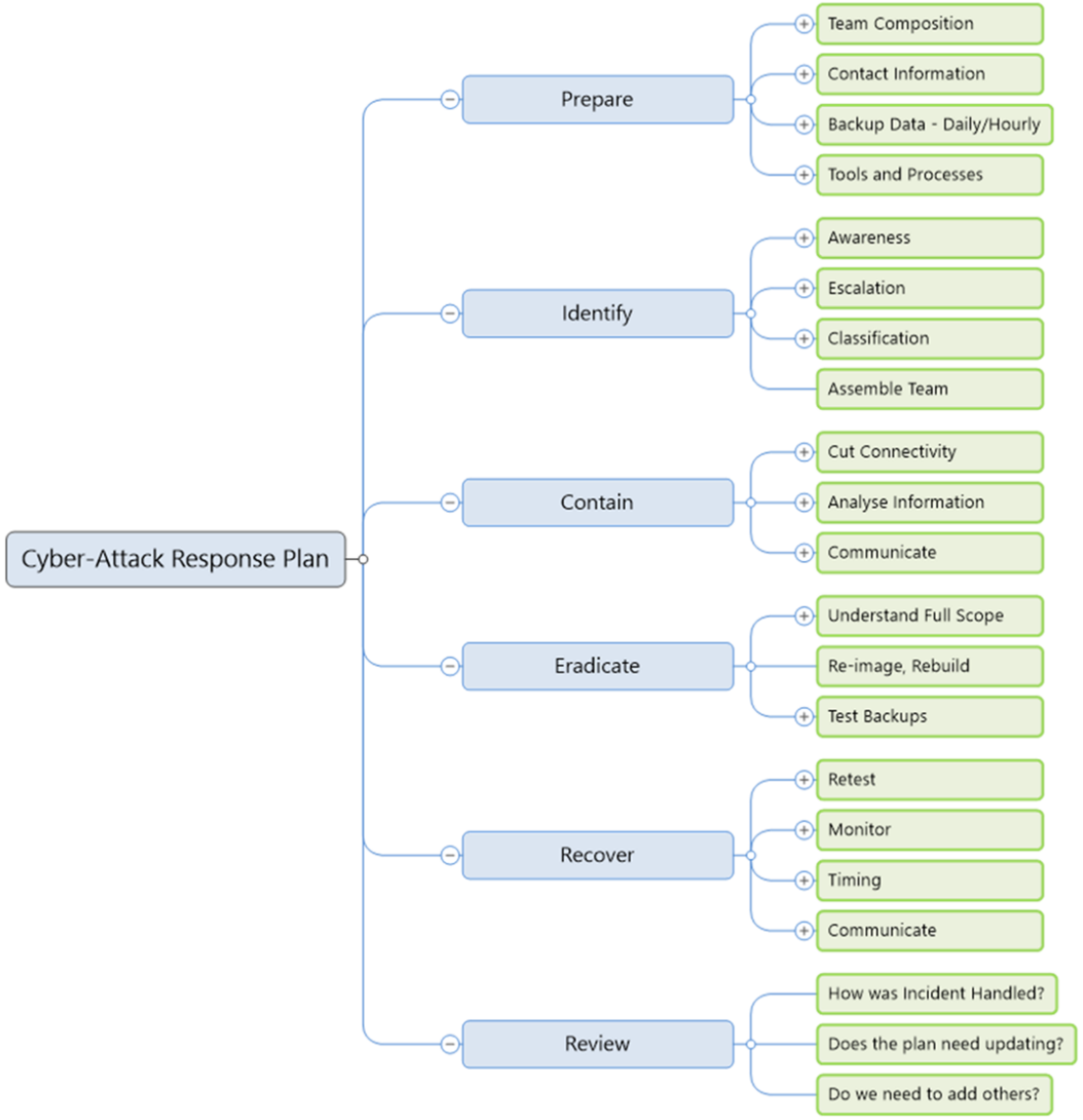

Roles & Responsibilities
Test Detection
Communication
Improve
Detection Processes
Establish Baseline
Establish Thresholds
Anomalous
Analyse
Events
Detect
Monitoring
Continuous
Physical Environment
Personnel Activity
Third-Parties
Vulnerability Scans
Service Delivery
Media Reports

4. Respond

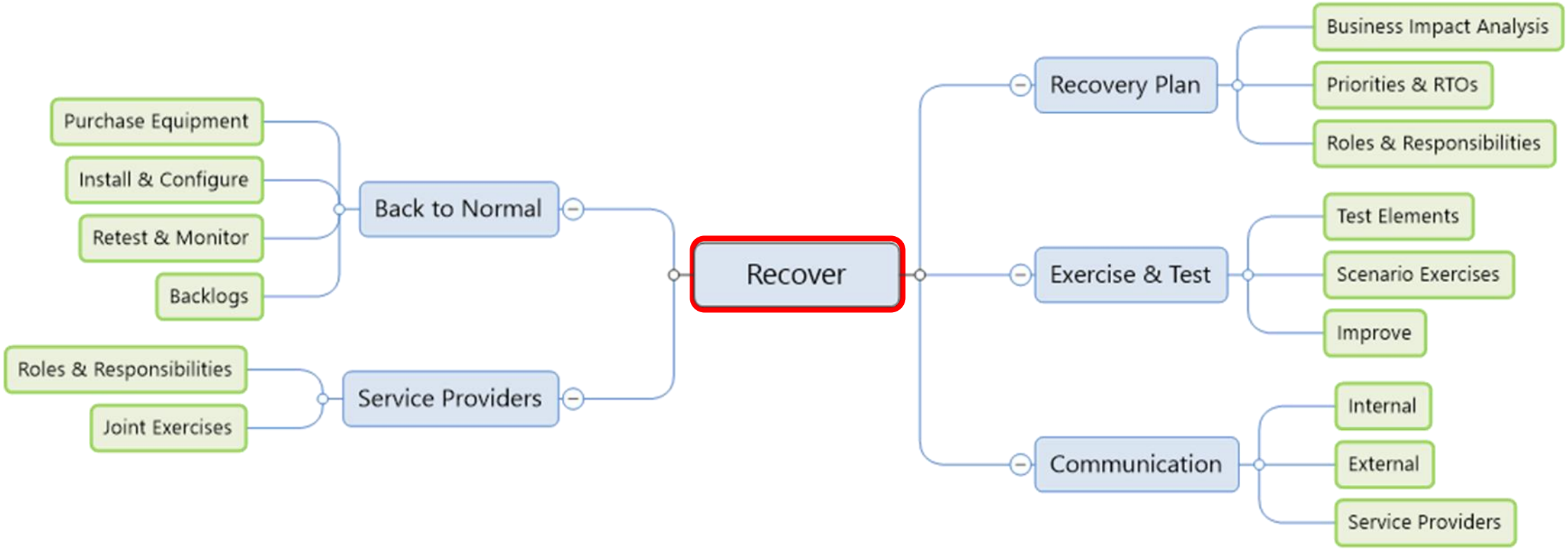

Respond
Improvements
Contain & Mitigate
Continuity Plans
Investigation
Source
Impact
Forensics
Response Plan
Processes & Procedures
Roles and Responsibilities
Communications
Internal
External
Service Providers

Response Plan

CalRisk
Manage the effect of uncertainty on objectives



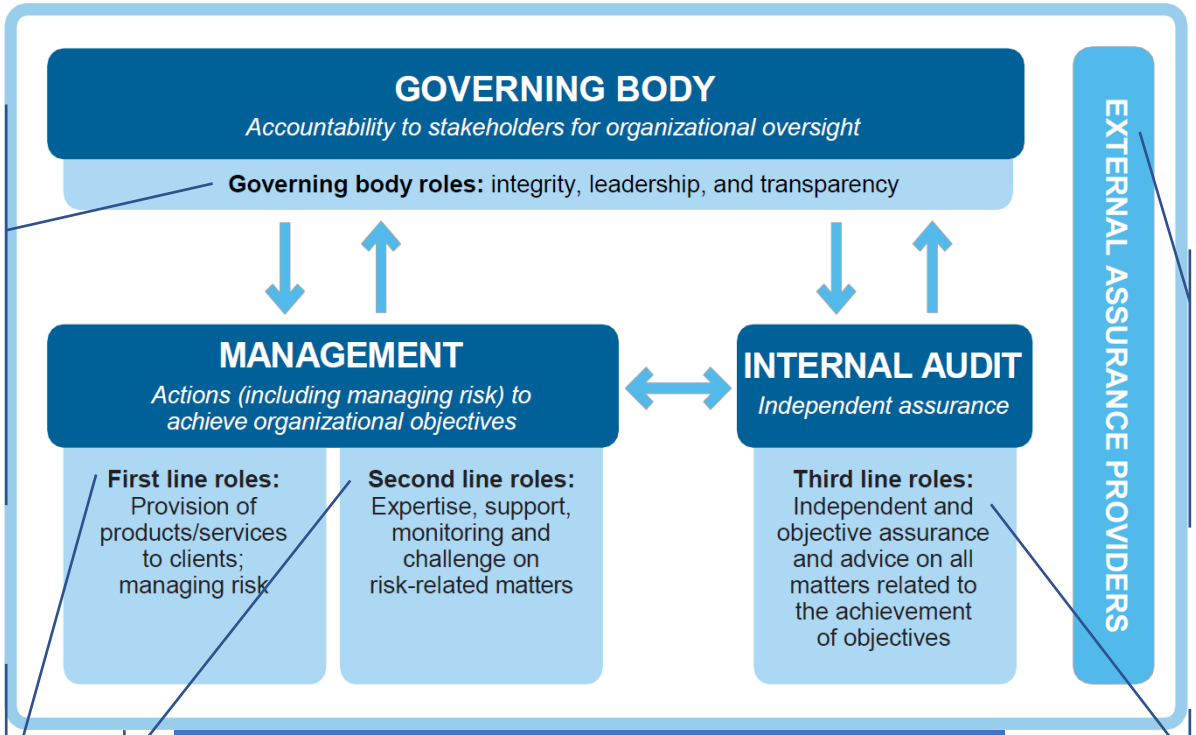
5. Recover


Recover
Back to Normal
Purchase Equipment
Install & Configure
Retest & Monitor
Backlogs
Service Providers
Roles & Responsibilities
Joint Exercises
Recovery Plan
Business Impact Analysis
Priorities & RTOs
Roles & Responsibilities
Exercise & Test
Test Elements
Scenario Exercises
Improve
Communication
Internal
External
Service Providers

Responsibilities

Cal Risk
Manage the effect of uncertainty on objectives

4 Oversight
Define Objectives
Establish Structures
Provide Resources
Set Risk Appetite
Establishes Internal Audit



5 Expertise
e.g. Pen Testing
Satisfy reg requirements
Independence

1 The Doers
The Risk Owners
Identify and control risks
Implement Processes
Report on plans and outcomes
Ensure compliance

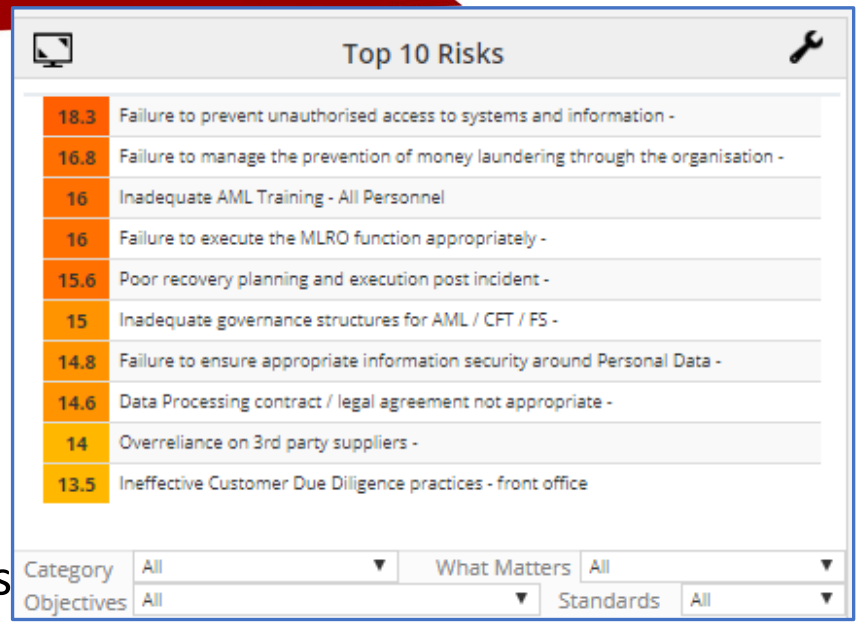
2 CRO, CCO
Expertise
Advise First Line
Challenge (respectfully)
Ensure Consistent Implementation
Monitoring
Reporting Adequacy and Effectiveness

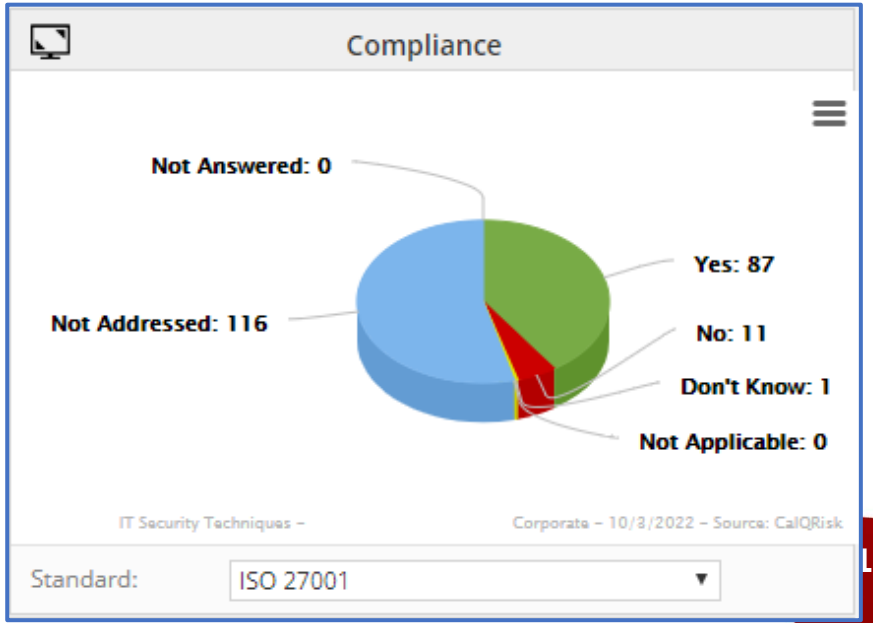
3 Quality Control
Independent
Adequacy and Effectiveness
Advise

Reporting - what Boards should know

CalQRisk
Manage the effect of uncertainty on objectives

1. What is the overall risk profile?
   - What are the Top 10 risks?
2. What is threatening the Objectives?
3. Are existing controls working / effective?
4. Have there been any near misses / incidents?
   - Errors & Omissions, system outages, accidents, policy breaches
5. Where are the gaps?
   - Confirmation of the overall compliance position
   - What is being done to address the gaps?
6. Have we tested / exercised our Response Plans?
7. Key Risk Indicators
   - Types: Exposure, Stress, Causal, Failure
   - Breaches of Risk Appetite rules





Q & A

Thank You

gjoyce@calqrisk.com