Cybersecurity for Senior Managers and Risk Officers
in Housing Associations

A mini Webinar from CalQRisk

CalQRisk

Manage the effect of uncertainty on objectives

18th October 2022, presented by

Gerard Joyce, CTO, CalQRisk

1

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

- Experienced Risk & Compliance Professionals

- Members of IRM, ACOI, IoD, IoB, ACCA, ISACA

- Involved in the Development of Standards

- We supply a Governance, Risk & Compliance Software Solution

- called CalQRisk

- CalQRisk is used by 200+ regulated organisations
  - Financial Services, Solicitors, Local Authorities, Universities, Schools,
  - Housing Associations, Charities, Sports Organisations..

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

- Systems are secure

- Policies and procedures are appropriate

- Staff are trained on cybersecurity risk

- There is a plan for when things go wrong

What is Cybersecurity?

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

Threat Agent · Vector · Vulnerability · Control · Technical Impact · Business Impact
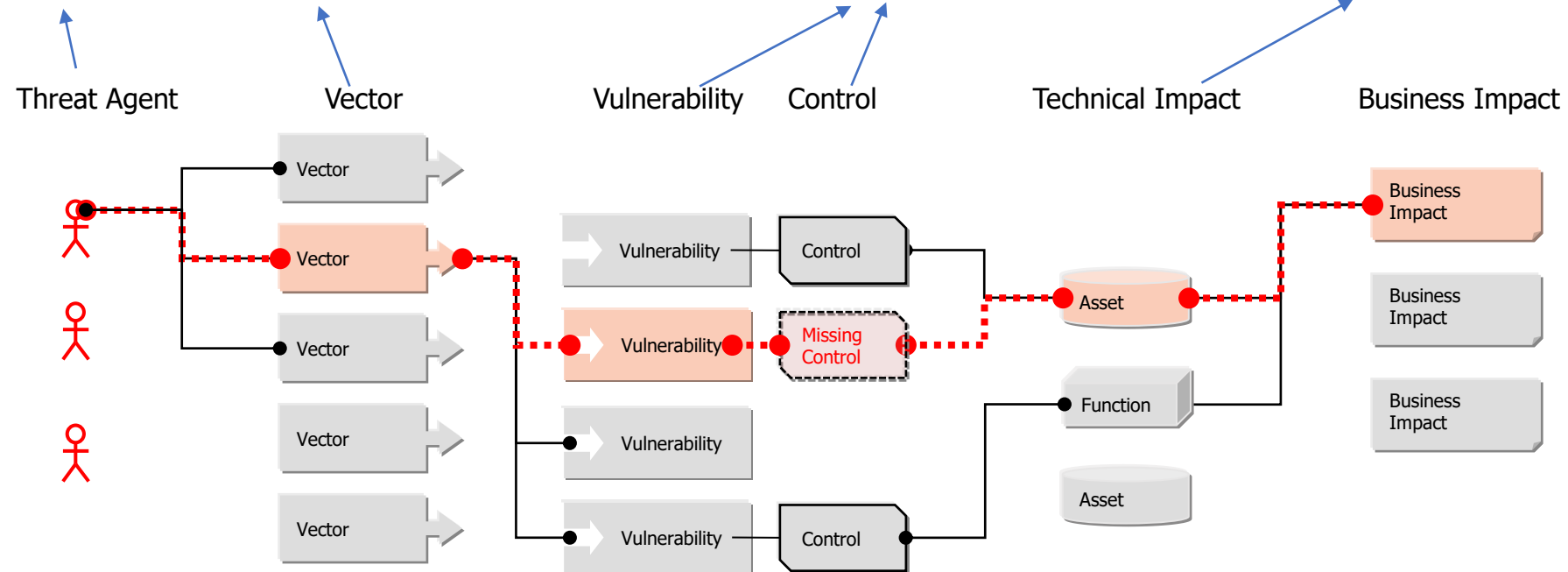
Source: Aspect Security

What are the Risks?

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

Country's largest housing association hit by cyber attack

1:20 PM BY JACK SIMPSON

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
- Social Networking
- Websites
- Wireless Hotspots
- USB Devices (Memory sticks)

Social Engineering

- Spoofing

- Phishing

- Spear Phishing

- Vishing

- Watering Hole

- Bogus Inspectors

john@Royal_Housing.net
john@Royal_Housing.net

These two are NOT the same

john@Royal_Housing.net
john@Roya**l**_Housing.net

Vulnerabilities

- Unwitting Employees

- IT System Misconfiguration

- Unpatched Flaws in Op Systems

- Mobile Devices

- Storage of Data in the Cloud

- Service Providers / Partners

Branch Office

Home

Head Office

Café

https://haveibeenpwned.com/
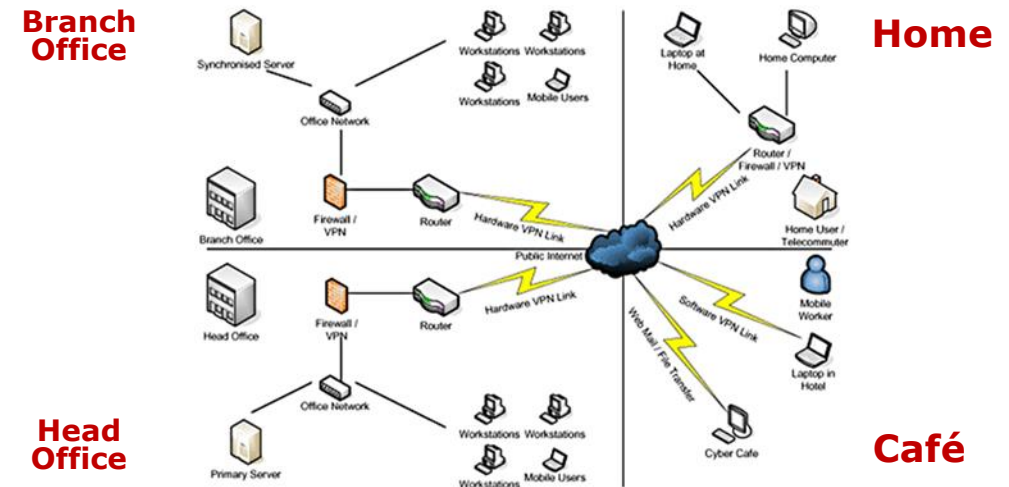
Mitigate the Risks

- 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
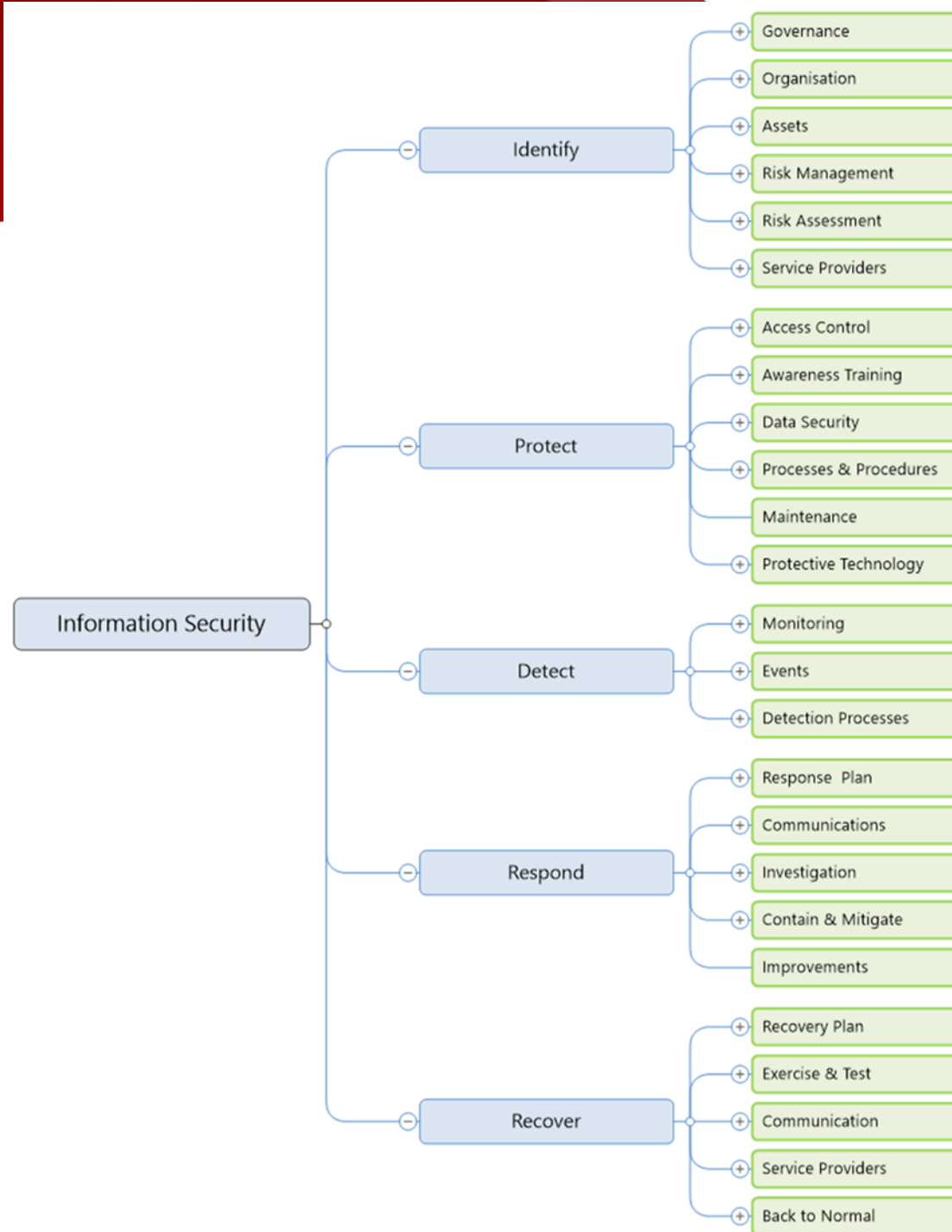
- Monitor adherence to procedures

Standards and Guidelines

- NIST Cyber Security Framework
- ISO 27001
- CIS CSC (Critical Security Controls)
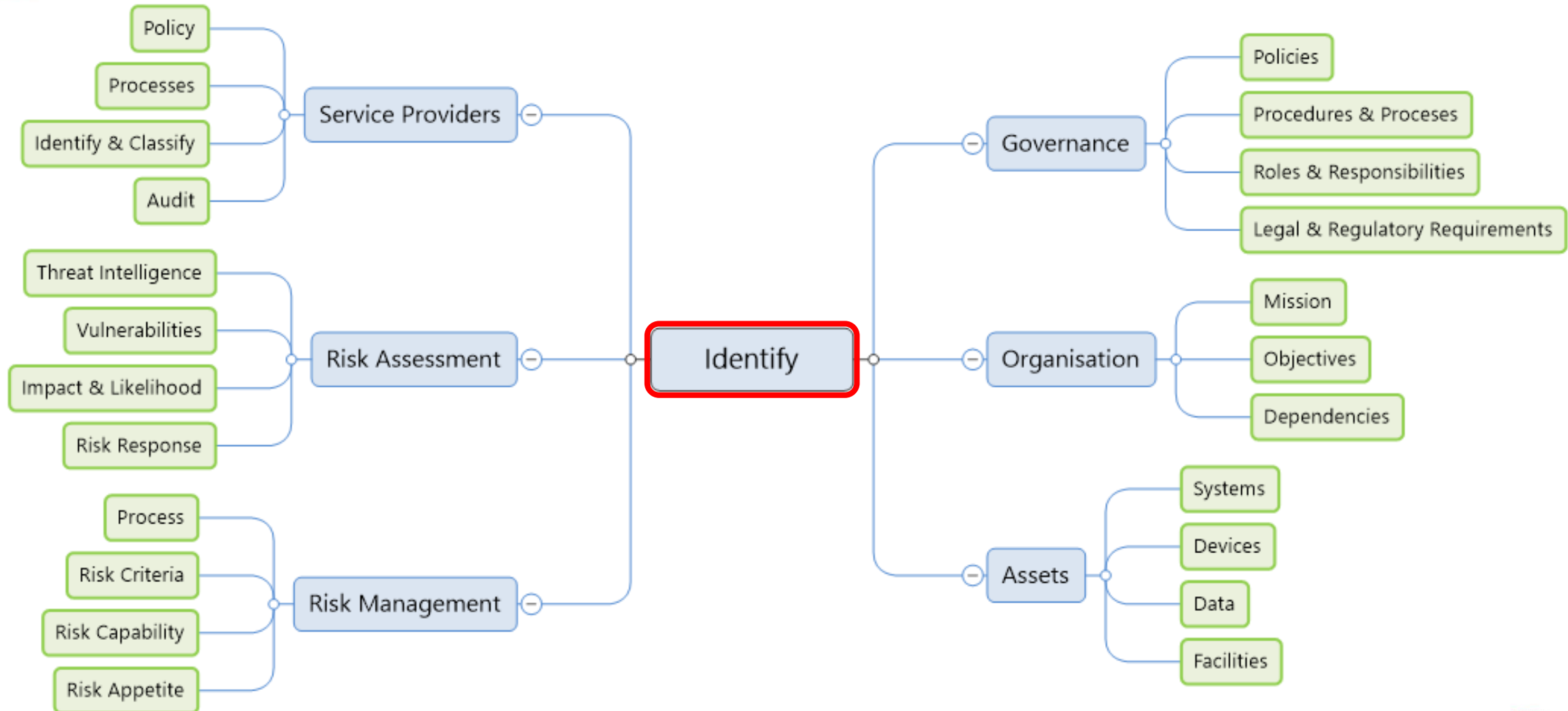- COBIT
- Cyber questionnaire (PRA)
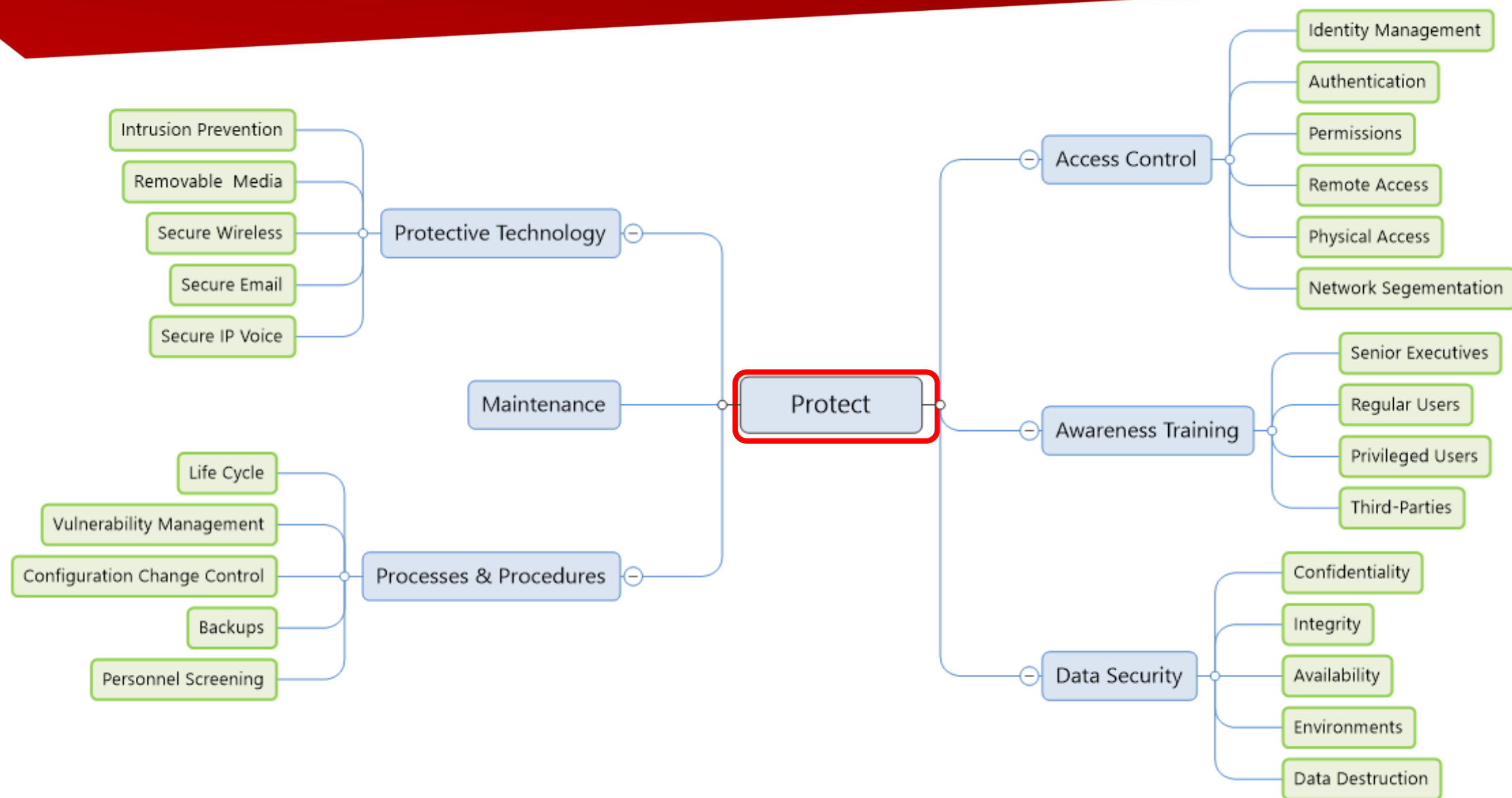
NIST Approach

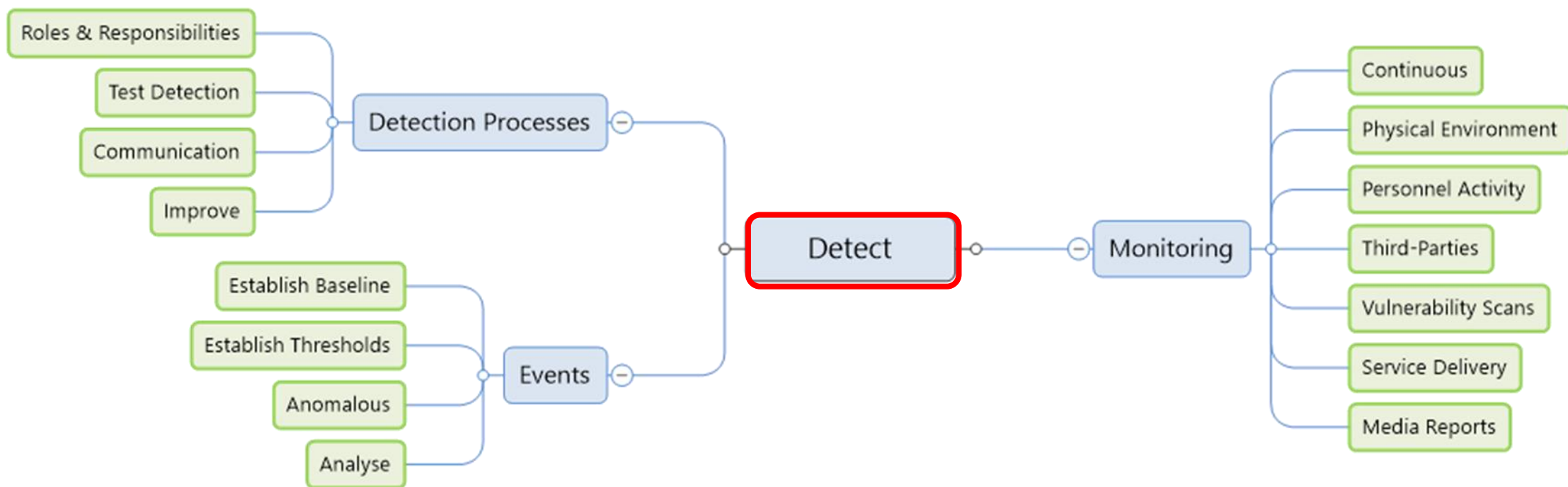**The NIST Approach**

- Identify
- Protect
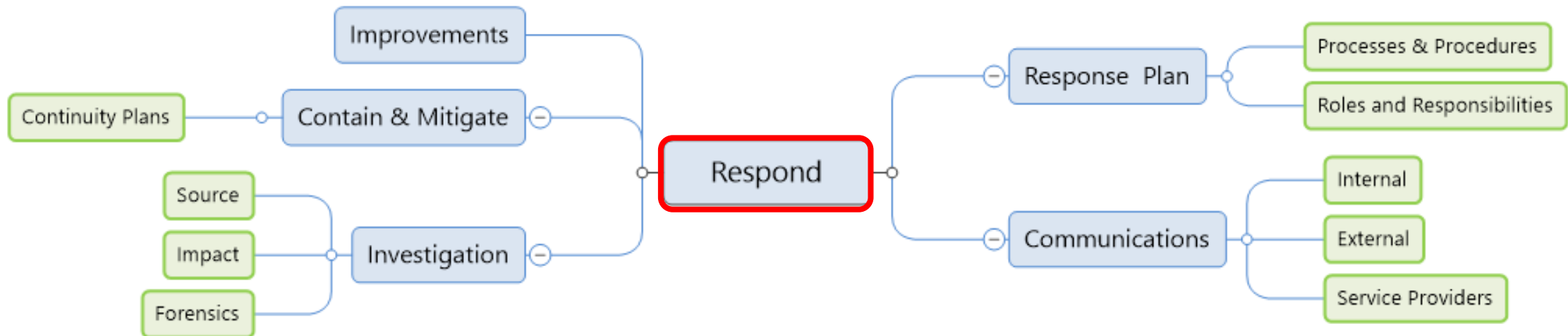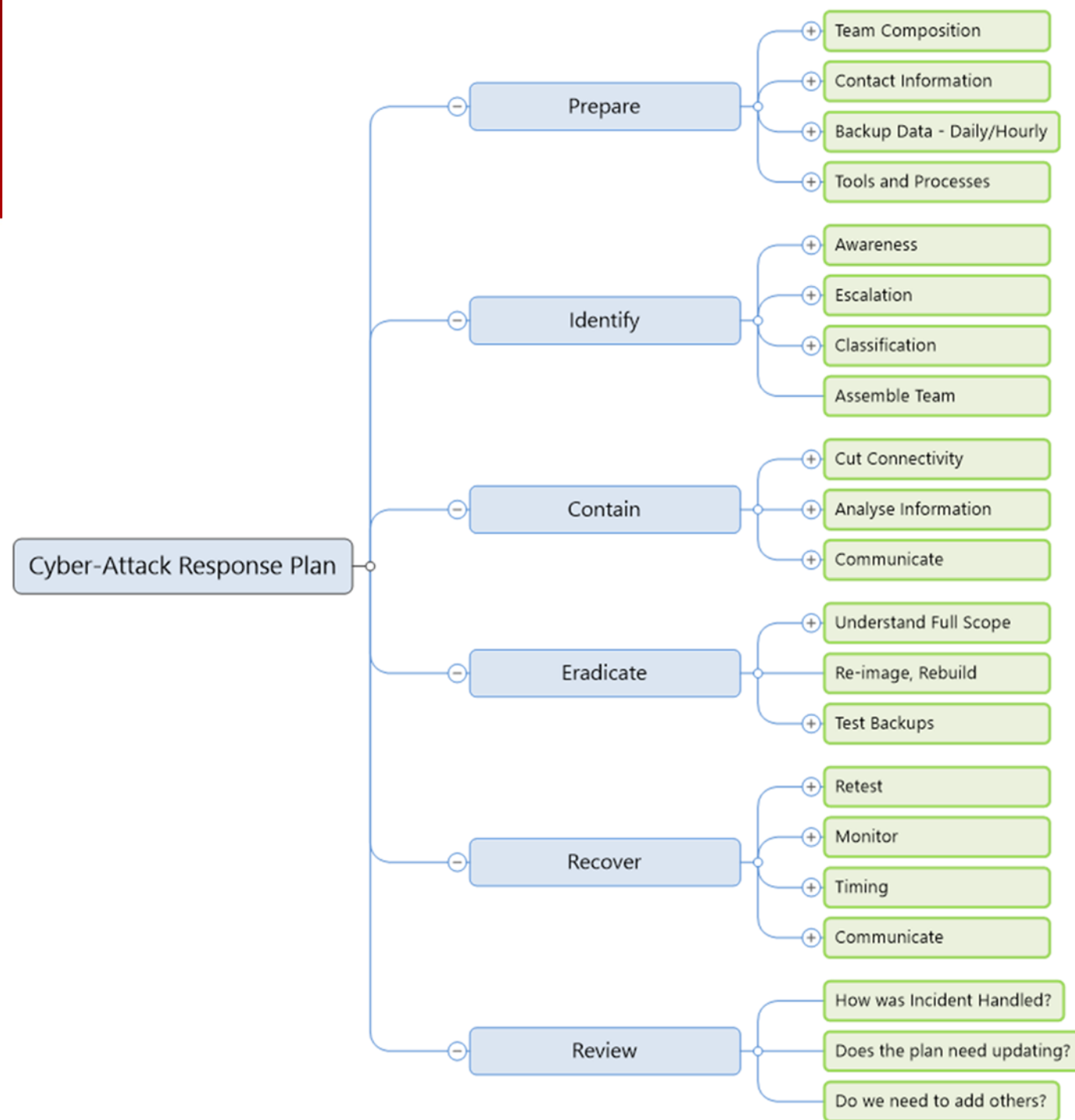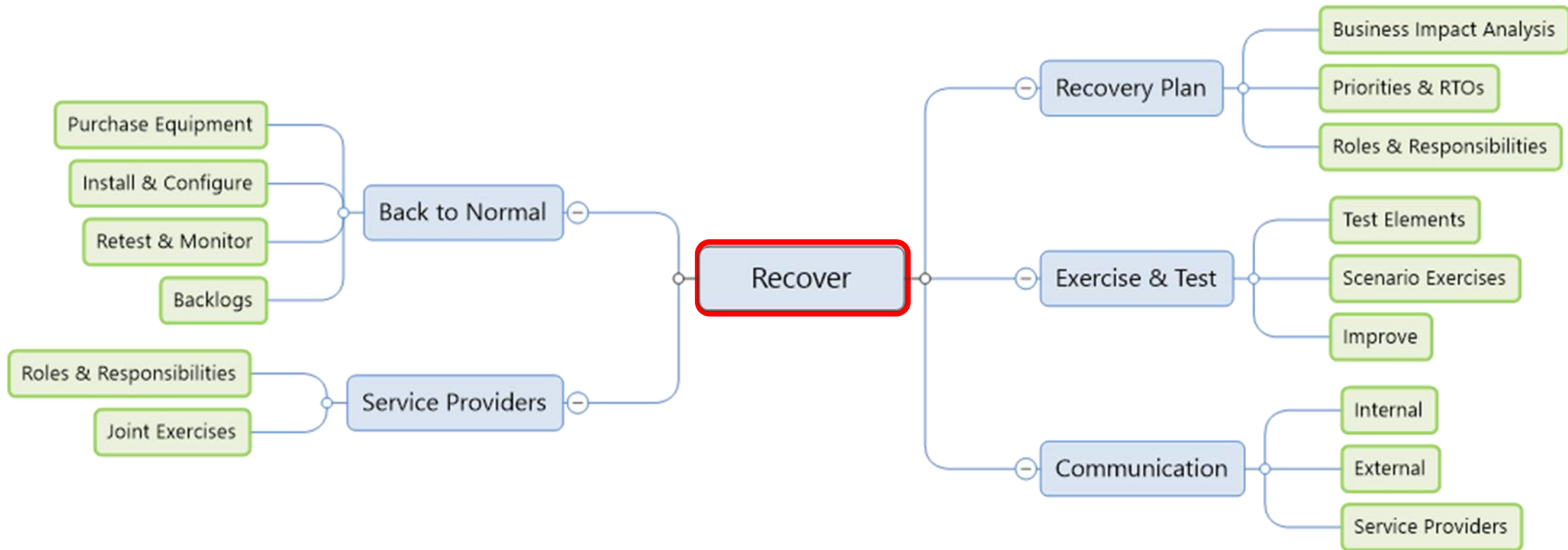- Detect
- Respond
- Recover

Identify

Protect

Respond

Response Plan

Recover

Responsibilities

4   **Oversight**
Define Objectives
Establish Structures
Provide Resources
Set Risk Appetite

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

GOVERNING BODY
Accountability to stakeholders for organizational oversight

Governing body roles: integrity, leadership, and transparency

MANAGEMENT
Actions (including managing risk) to achieve organizational objectives

INTERNAL AUDIT
Independent assurance

First line roles: Provision of products/services to clients; managing risk

Second line roles: Expertise, support, monitoring and challenge on risk-related matters

Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives

EXTERNAL ASSURANCE PROVIDERS

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

3   **Quality Control**
Independent
Adequacy and Effectiveness
Advise

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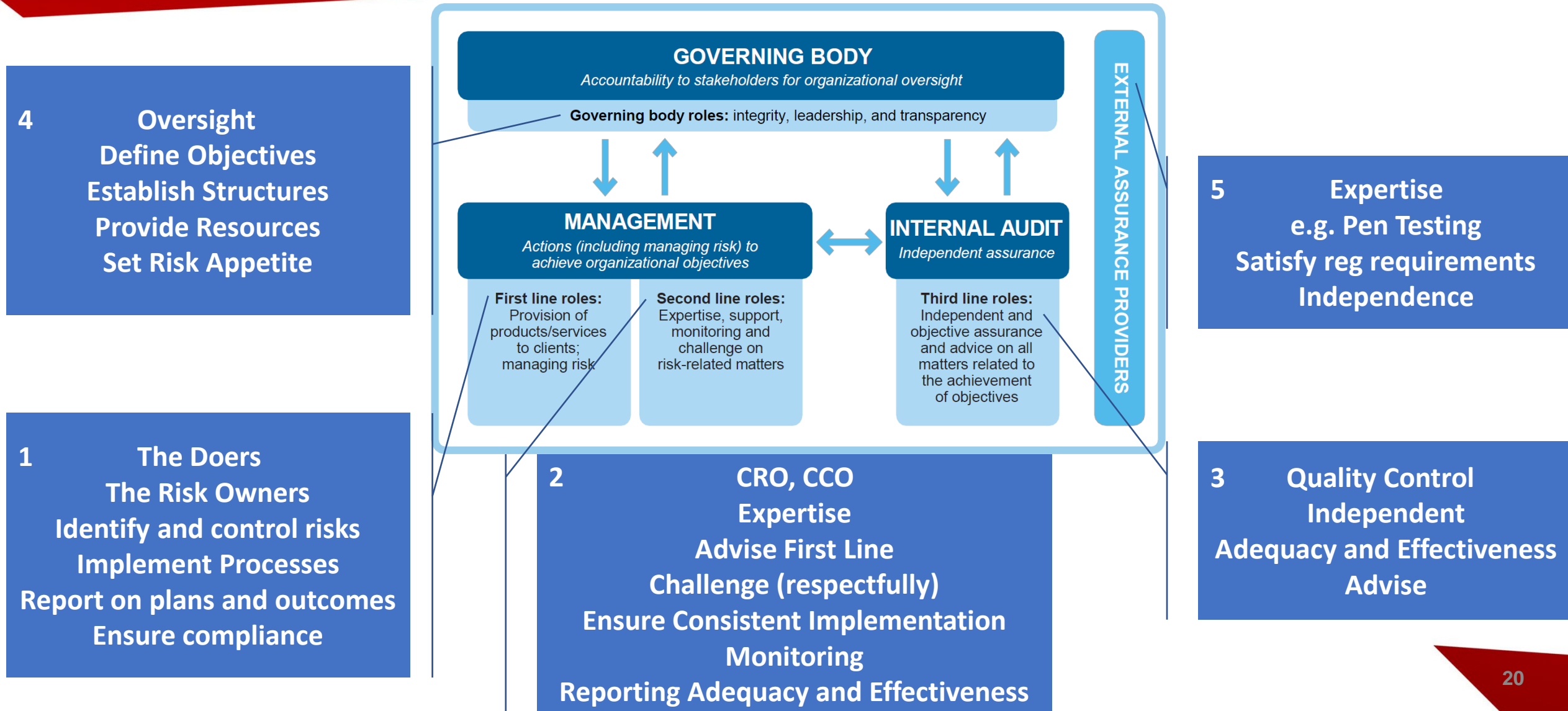**Ensure Consistent Implementation**
Monitoring
Reporting Adequacy and Effectiveness
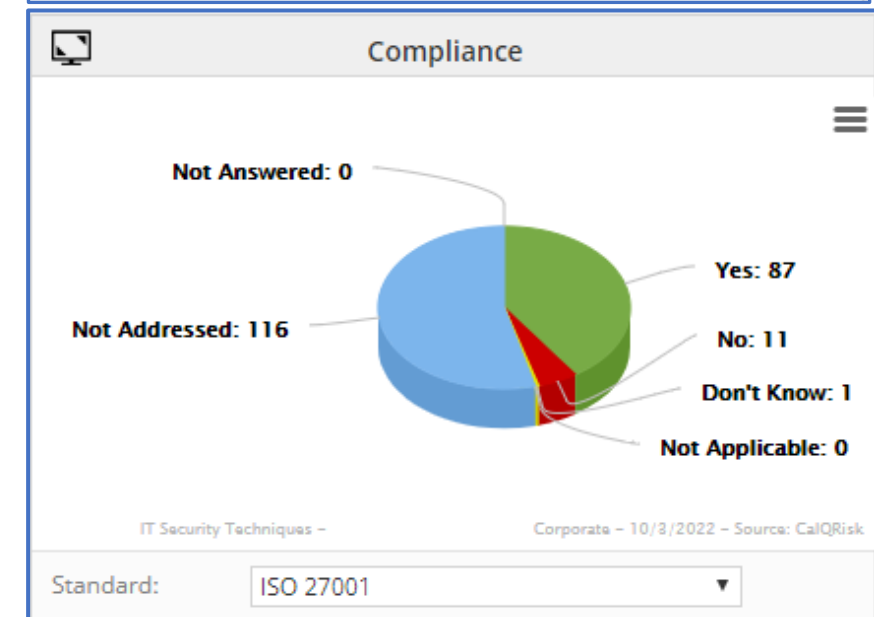
Reporting – Assuring the Boards

- ➤ What is the overall risk profile?
  - What are the Top 10 risks?
- ➤ What is threatening the Objectives?
- ➤ Are existing controls working / effective?
- ➤ Have there been any near misses / incidents?
  - Errors & Omissions, system outages, accidents, policy breaches
- ➤ Where are the gaps?
  - Confirmation of the overall compliance position
  - What is being done to address the gaps?
- ➤ Have we tested / exercised our Response Plans?
- ➤ Key Risk Indicators

Top 10 Risks

18.3	Failure to prevent unauthorised access to systems and information -
16.8	Failure to manage the prevention of money laundering through the organisation -
16	Inadequate AML Training - All Personnel
16	Failure to execute the MLRO function appropriately -
15.6	Poor recovery planning and execution post incident -
15	Inadequate governance structures for AML / CFT / FS -
14.8	Failure to ensure appropriate information security around Personal Data -
14.6	Data Processing contract / legal agreement not appropriate -
14	Overreliance on 3rd party suppliers -
13.5	Ineffective Customer Due Diligence practices - front office

Category: All | What Matters: All
Objectives: All | Standards: All

Compliance

Not Answered: 0
Not Addressed: 116
Yes: 87
No: 11
Don't Know: 1
Not Applicable: 0

IT Security Techniques – | Corporate – 10/3/2022 – Source: CalQRisk
Standard: ISO 27001

Thank You

gjoyce@calqrisk.com