Pearson

C-MRiC.ORG
Centre for Multidisciplinary Research, Innovation and Collaboration

Focusing on the Recovery Aspects of Cyber Resilience

Dr Cyril Onwubiko[1, 2]

[1]Director, Enterprise Security Architecture, Pearson Plc

[2]Founder, **Centre for Multidisciplinary Research, Innovation & Collaboration (C-MRiC)**

@DrCyrilOnwubiko

Cyber Physical Social Systems

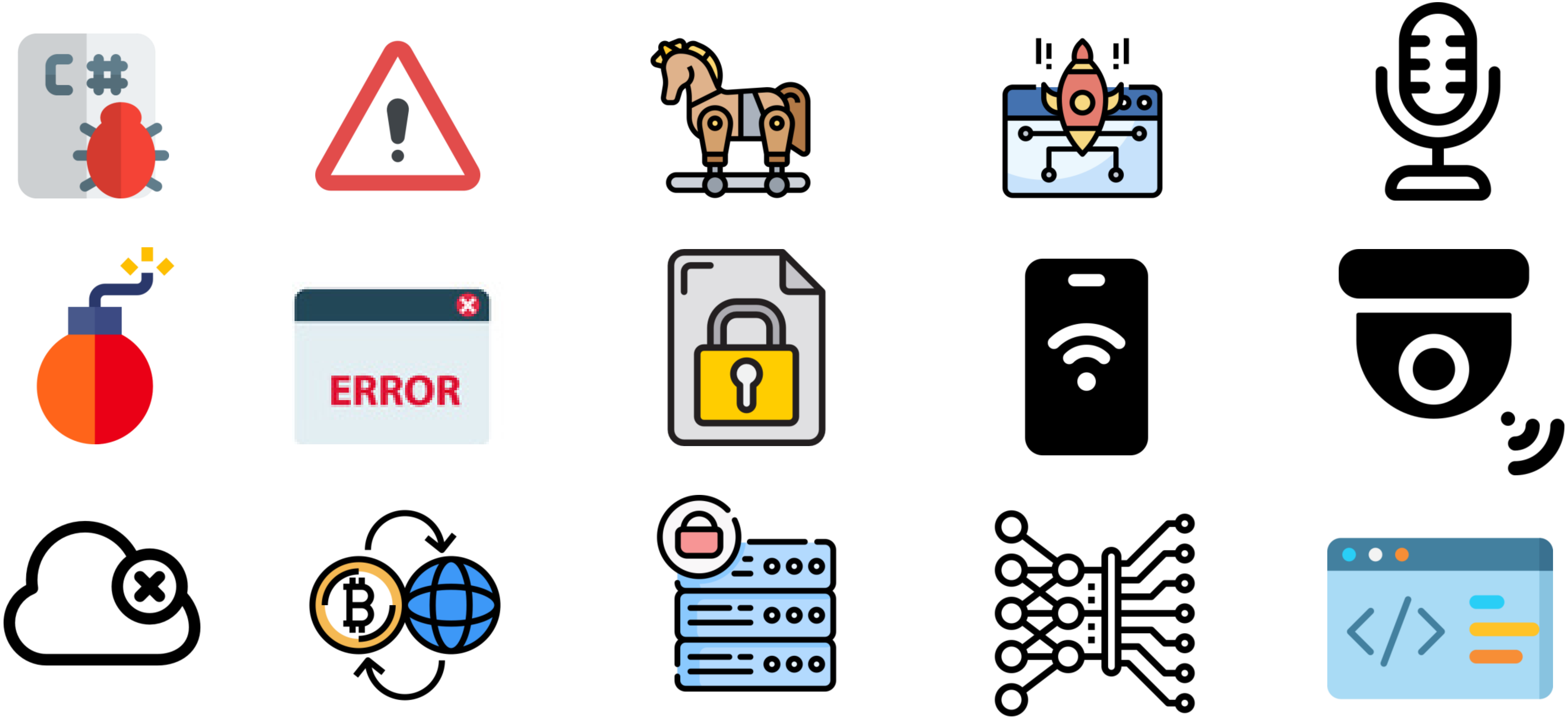
“If anything can go wrong, it will ….”

Murphy’s Law

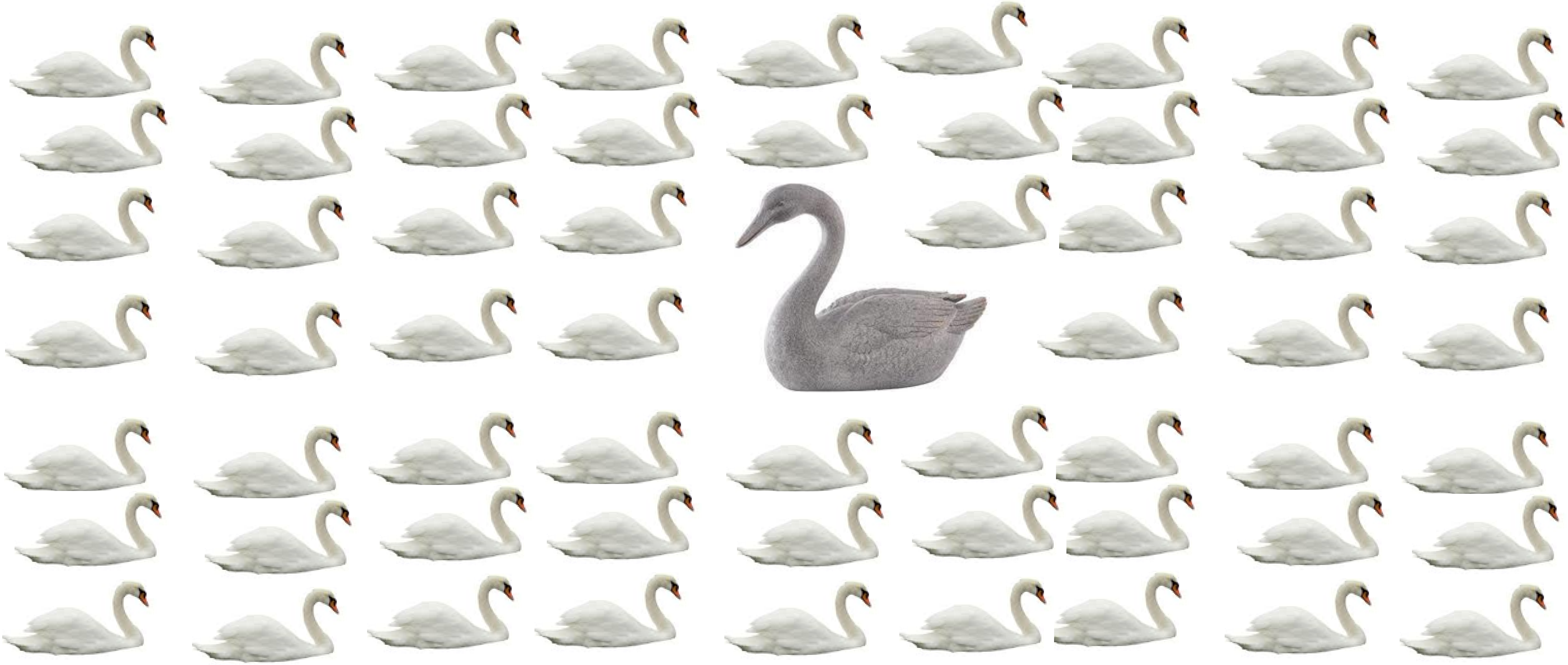
Tesla Cybertruck

On Friday 22 November 2019, Elon Musk unveiled Tesla Cybertruck in Hawthorne, California.

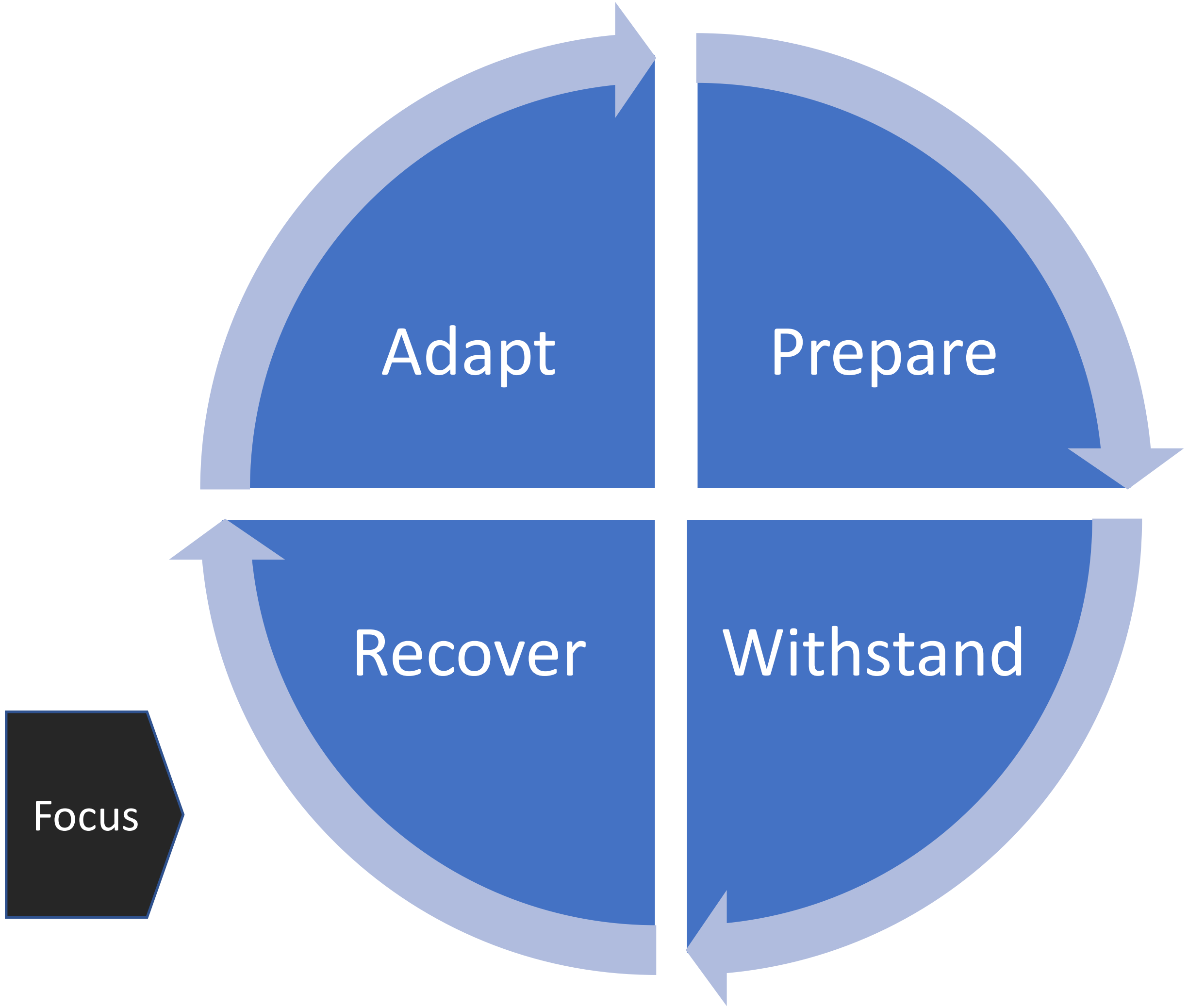
Errors / Failures / Attacks / Breaches / Incidents



Grey Swan

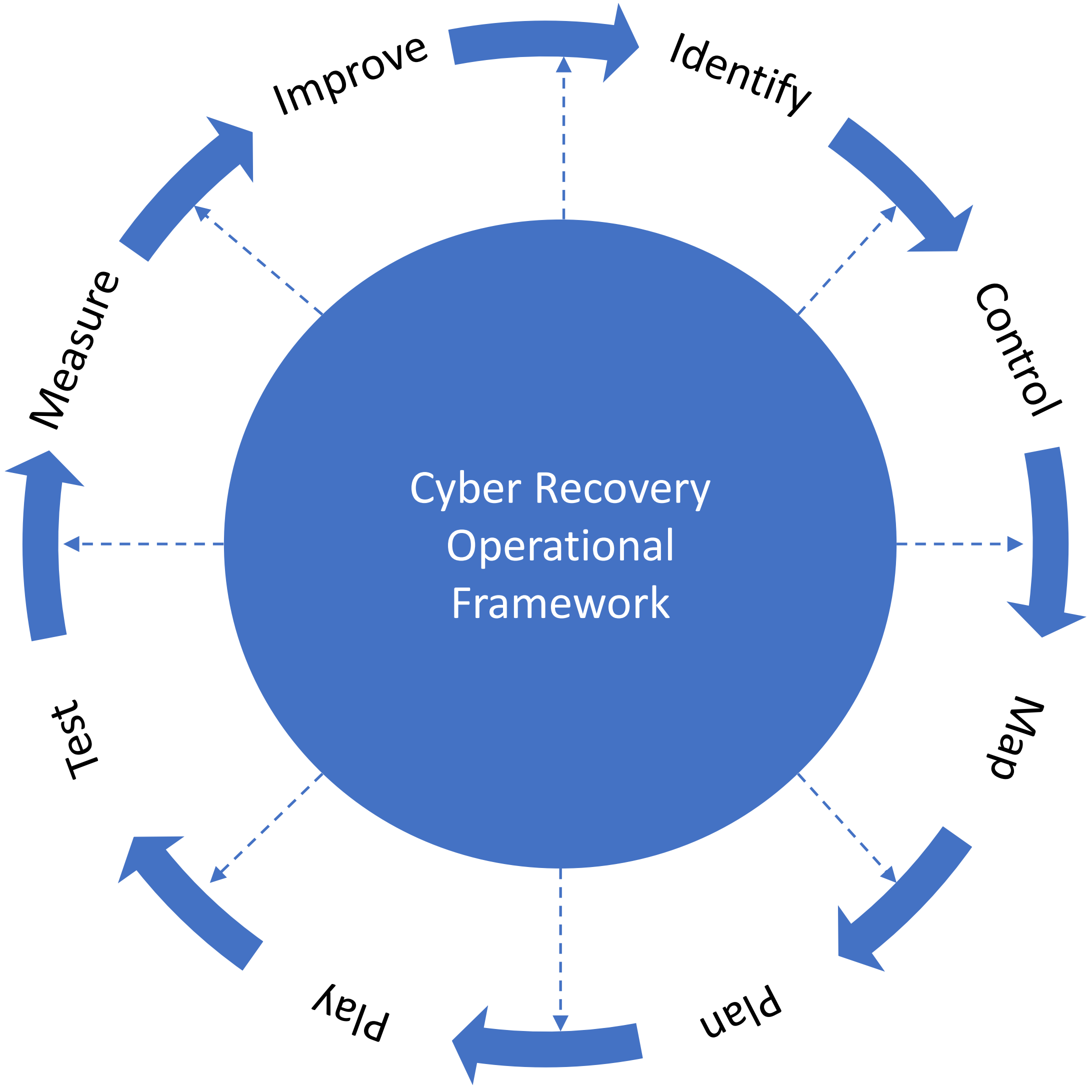


Cyber Resilience

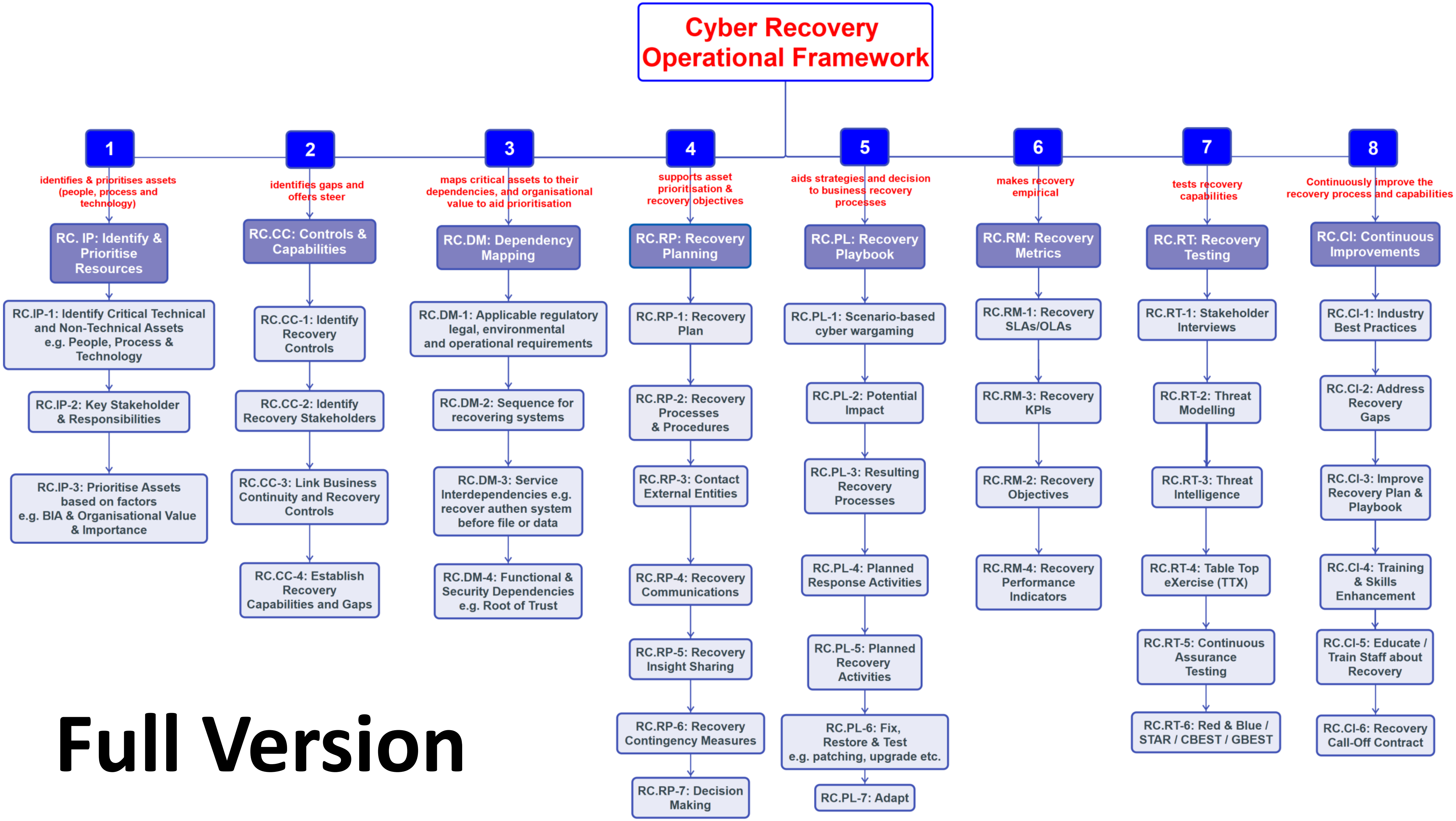


Introducing our

Cyber Recovery Operational Framework©



Cyber Recovery Operational Framework



1 identifies & prioritises assets (people, process and technology)

RC. IP: Identify & Prioritise Resources

- RC.IP-1: Identify Critical Technical and Non-Technical Assets e.g. People, Process & Technology
- RC.IP-2: Key Stakeholder & Responsibilities
- RC.IP-3: Prioritise Assets based on factors e.g. BIA & Organisational Value & Importance

2 identifies gaps and offers steer

RC.CC: Controls & Capabilities

- RC.CC-1: Identify Recovery Controls
- RC.CC-2: Identify Recovery Stakeholders
- RC.CC-3: Link Business Continuity and Recovery Controls
- RC.CC-4: Establish Recovery Capabilities and Gaps

3 maps critical assets to their dependencies, and organisational value to aid prioritisation

RC.DM: Dependency Mapping

- RC.DM-1: Applicable regulatory legal, environmental and operational requirements
- RC.DM-2: Sequence for recovering systems
- RC.DM-3: Service Interdependencies e.g. recover authen system before file or data
- RC.DM-4: Functional & Security Dependencies e.g. Root of Trust

4 supports asset prioritisation & recovery objectives

RC.RP: Recovery Planning

- RC.RP-1: Recovery Plan
- RC.RP-2: Recovery Processes & Procedures
- RC.RP-3: Contact External Entities
- RC.RP-4: Recovery Communications
- RC.RP-5: Recovery Insight Sharing
- RC.RP-6: Recovery Contingency Measures
- RC.RP-7: Decision Making

5 aids strategies and decision to business recovery processes

RC.PL: Recovery Playbook

- RC.PL-1: Scenario-based cyber wargaming
- RC.PL-2: Potential Impact
- RC.PL-3: Resulting Recovery Processes
- RC.PL-4: Planned Response Activities
- RC.PL-5: Planned Recovery Activities
- RC.PL-6: Fix, Restore & Test e.g. patching, upgrade etc.
- RC.PL-7: Adapt

6 makes recovery empirical

RC.RM: Recovery Metrics

- RC.RM-1: Recovery SLAs/OLAs
- RC.RM-3: Recovery KPIs
- RC.RM-2: Recovery Objectives
- RC.RM-4: Recovery Performance Indicators

7 tests recovery capabilities

RC.RT: Recovery Testing

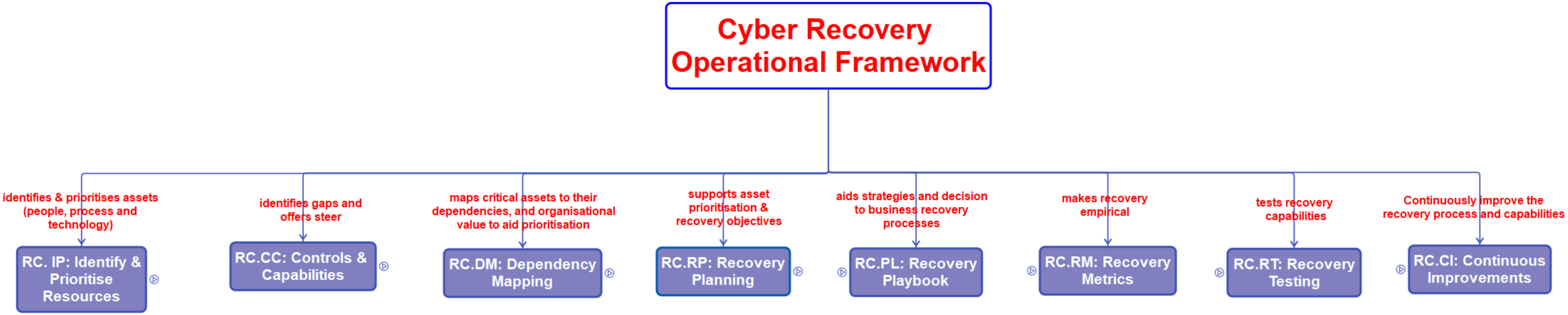
- RC.RT-1: Stakeholder Interviews
- RC.RT-2: Threat Modelling
- RC.RT-3: Threat Intelligence
- RC.RT-4: Table Top eXercise (TTX)
- RC.RT-5: Continuous Assurance Testing
- RC.RT-6: Red & Blue / STAR / CBEST / GBEST

8 Continuously improve the recovery process and capabilities

RC.CI: Continuous Improvements

- RC.CI-1: Industry Best Practices
- RC.CI-2: Address Recovery Gaps
- RC.CI-3: Improve Recovery Plan & Playbook
- RC.CI-4: Training & Skills Enhancement
- RC.CI-5: Educate / Train Staff about Recovery
- RC.CI-6: Recovery Call-Off Contract

Full Version



Cyber Recovery Operational Framework

identifies & prioritises assets (people, process and technology)

RC. IP: Identify & Prioritise Resources

identifies gaps and offers steer

RC.CC: Controls & Capabilities

maps critical assets to their dependencies, and organisational value to aid prioritisation

RC.DM: Dependency Mapping

supports asset prioritisation & recovery objectives

RC.RP: Recovery Planning

aids strategies and decision to business recovery processes

RC.PL: Recovery Playbook

makes recovery empirical

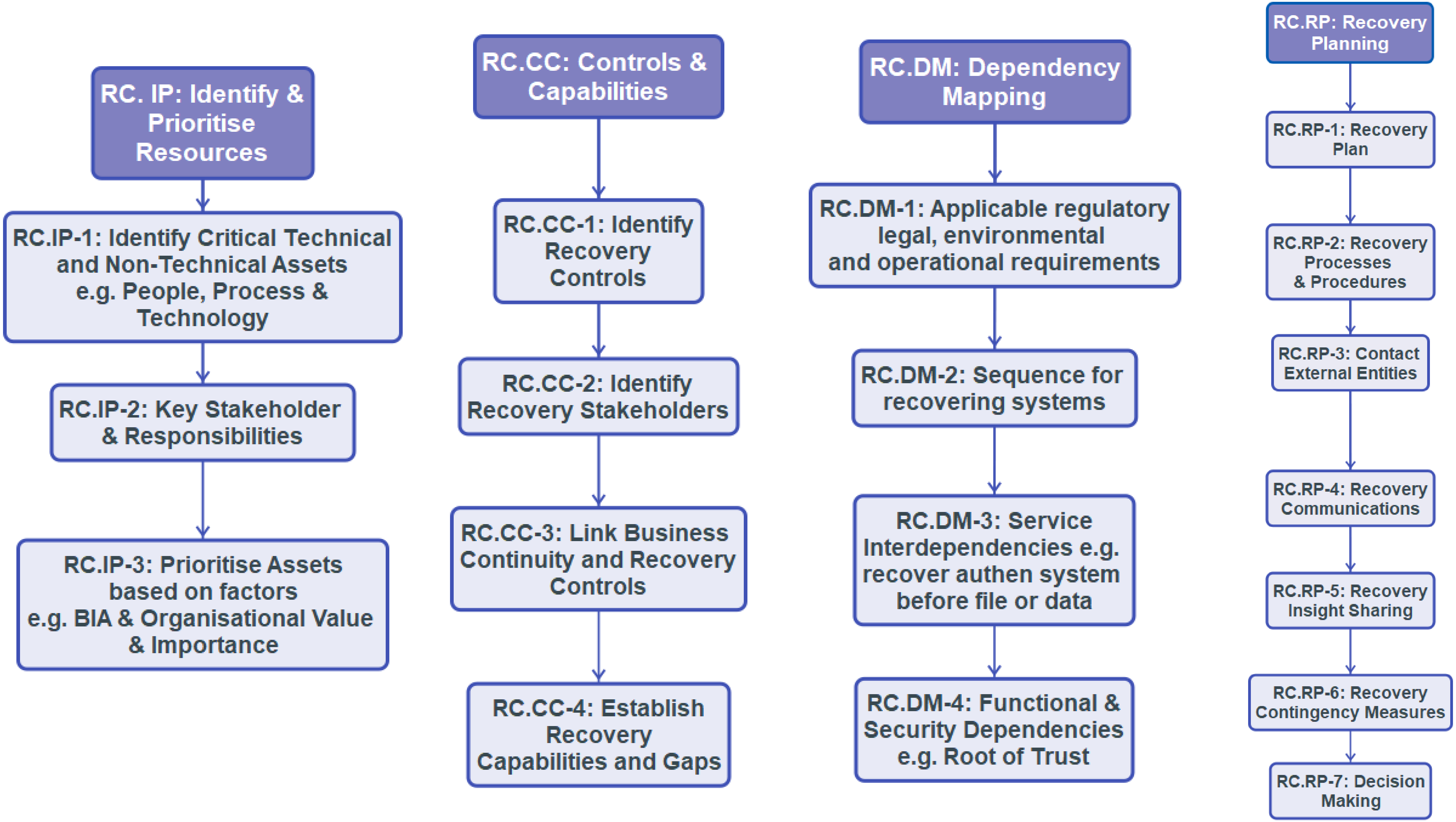
RC.RM: Recovery Metrics

tests recovery capabilities

RC.RT: Recovery Testing

Continuously improve the recovery process and capabilities

RC.CI: Continuous Improvements



RC. IP: Identify & Prioritise Resources

RC.IP-1: Identify Critical Technical and Non-Technical Assets e.g. People, Process & Technology

RC.IP-2: Key Stakeholder & Responsibilities

RC.IP-3: Prioritise Assets based on factors e.g. BIA & Organisational Value & Importance

RC.CC: Controls & Capabilities

RC.CC-1: Identify Recovery Controls

RC.CC-2: Identify Recovery Stakeholders

RC.CC-3: Link Business Continuity and Recovery Controls

RC.CC-4: Establish Recovery Capabilities and Gaps

RC.DM: Dependency Mapping

RC.DM-1: Applicable regulatory legal, environmental and operational requirements

RC.DM-2: Sequence for recovering systems

RC.DM-3: Service Interdependencies e.g. recover authen system before file or data

RC.DM-4: Functional & Security Dependencies e.g. Root of Trust

RC.RP: Recovery Planning

RC.RP-1: Recovery Plan

RC.RP-2: Recovery Processes & Procedures

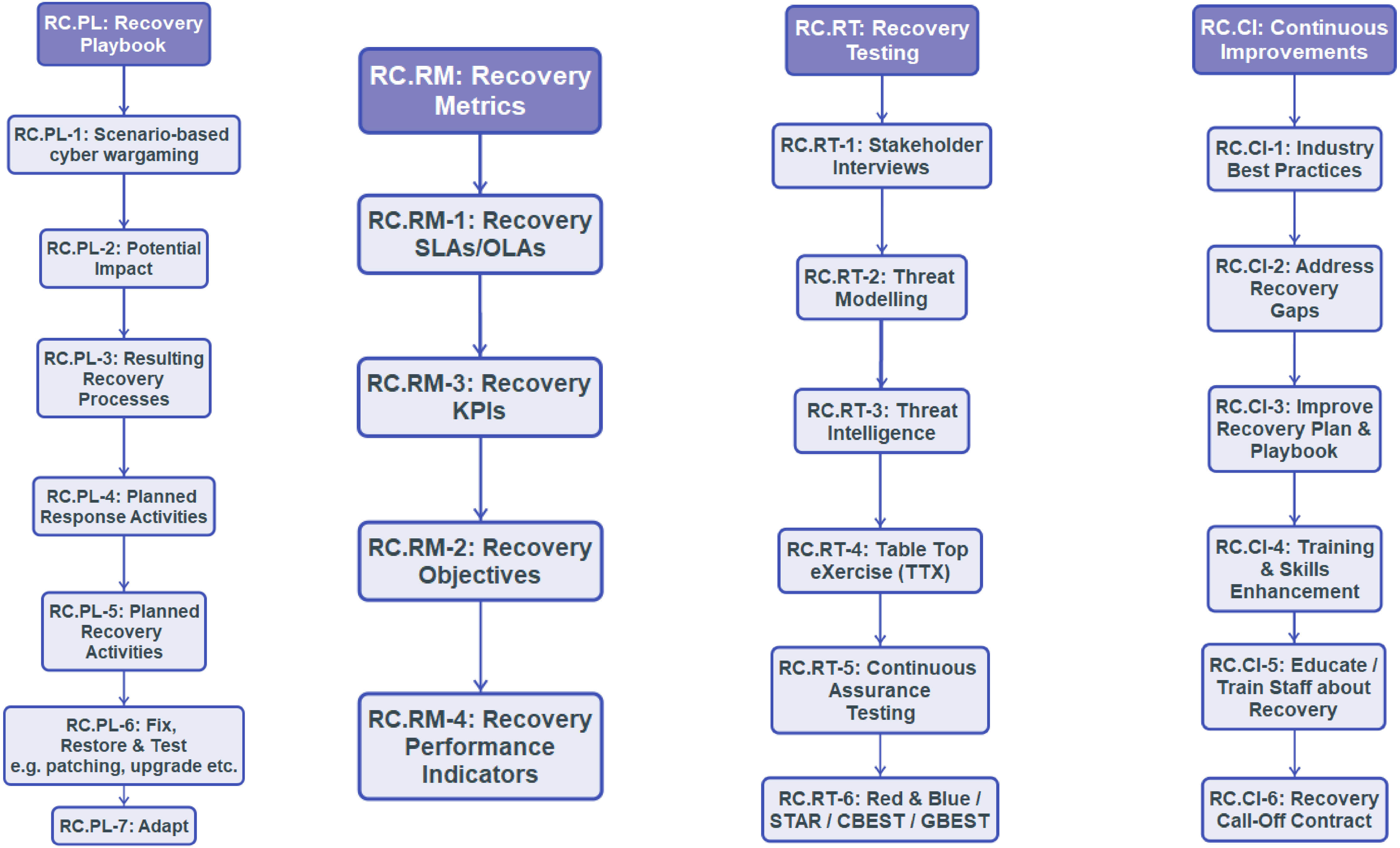
RC.RP-3: Contact External Entities

RC.RP-4: Recovery Communications

RC.RP-5: Recovery Insight Sharing

RC.RP-6: Recovery Contingency Measures

RC.RP-7: Decision Making



RC.PL: Recovery Playbook

- RC.PL-1: Scenario-based cyber wargaming
- RC.PL-2: Potential Impact
- RC.PL-3: Resulting Recovery Processes
- RC.PL-4: Planned Response Activities
- RC.PL-5: Planned Recovery Activities
- RC.PL-6: Fix, Restore & Test e.g. patching, upgrade etc.
- RC.PL-7: Adapt

RC.RM: Recovery Metrics

- RC.RM-1: Recovery SLAs/OLAs
- RC.RM-3: Recovery KPIs
- RC.RM-2: Recovery Objectives
- RC.RM-4: Recovery Performance Indicators

RC.RT: Recovery Testing

- RC.RT-1: Stakeholder Interviews
- RC.RT-2: Threat Modelling
- RC.RT-3: Threat Intelligence
- RC.RT-4: Table Top eXercise (TTX)
- RC.RT-5: Continuous Assurance Testing
- RC.RT-6: Red & Blue / STAR / CBEST / GBEST

RC.CI: Continuous Improvements

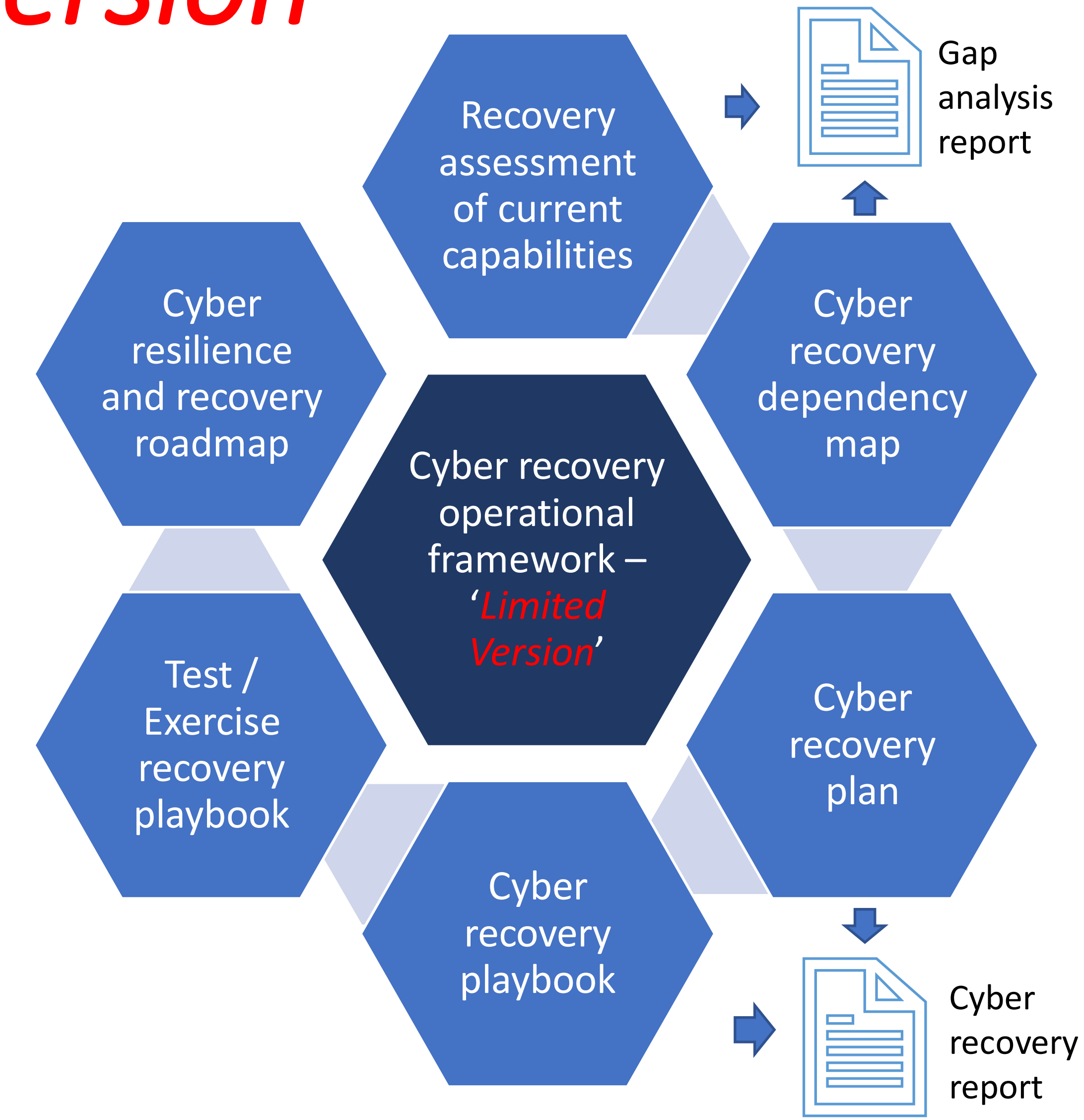
- RC.CI-1: Industry Best Practices
- RC.CI-2: Address Recovery Gaps
- RC.CI-3: Improve Recovery Plan & Playbook
- RC.CI-4: Training & Skills Enhancement
- RC.CI-5: Educate / Train Staff about Recovery
- RC.CI-6: Recovery Call-Off Contract

Cyber Recovery Framework

Limited Version

- We recognise not every organisation has the resources to create and develop every aspect of the framework.

- The *Limited Version* is how best to scale down the implementation of the framework so that it is not onerous to an organisation. We do not recommend this approach, but it's better than nothing!



Cyber recovery operational framework – '*Limited Version*'

Recovery assessment of current capabilities

Gap analysis report

Cyber recovery dependency map

Cyber recovery plan

Cyber recovery report

Cyber recovery playbook

Test / Exercise recovery playbook

Cyber resilience and recovery roadmap

Conclusion

- Cyber recovery prepares an organisation to be **efficient** and **effective in resilience**.
- Resilience cannot be achieved purely on the basis of ***withstanding intrusion***, ***attack or harm***. At some point, the ability to withstand or absorb cyber incident will fail, just as it did with Cybertruck, and then it is our ability to recover from the incident that will underpin the survivability of the organisation.
- Cyber recovery is a **journey**, not an endpoint, tool or an appliance that an organisation can procure. It is a continuous set of activities that require time, funding and senior management commitment to be successful.
- Cyber recovery must be **adaptive**. It should continuously evolve over time. As new TTPs are utilised for cyber-attacks, so our recovery controls, capabilities, processes and playbooks should be adapted.
- Cyber recovery controls, processes, playbooks, runbooks, and cyber COOP should be regularly **tested and exercised**.
- **Staff training**, upskilling and collaboration with external recovery parties should be as regular as possible. All these together make recovery a successful journey.

Thank You!

Q&A