Security Audit Framework for Management in the Enterprise

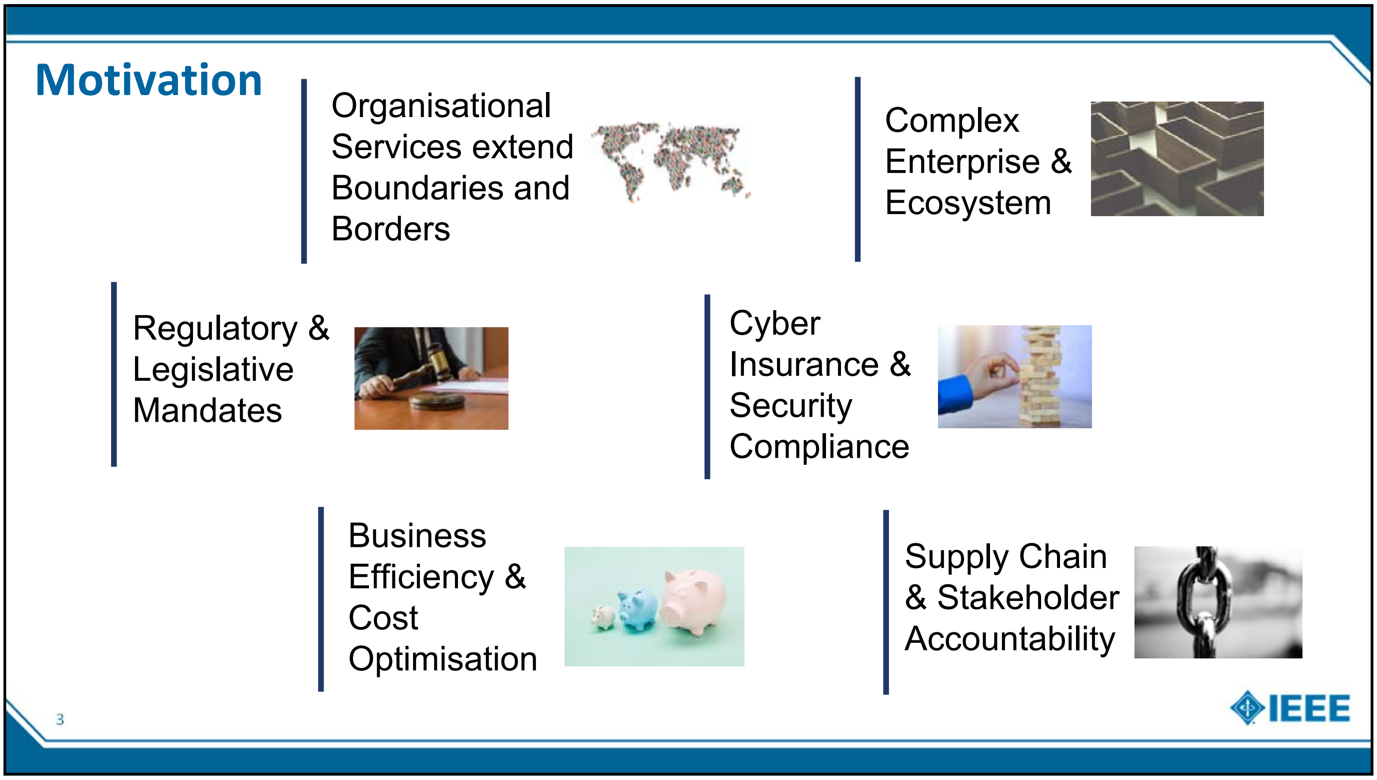
IEEE Distinguished Lecture Series – IEEE Computer Society, Silicon Valley, USA

Dr Cyril Onwubiko
DVP & Board of Governors - IEEE CS

IEEE Computer Society, Silicon Valley, USA
December 7, 2021 @16:00 – 17:15 GMT

IEEE
Advancing Technology for Humanity

Security Audit has become a **complex business undertaken**, yet extremely essential for **business resilience**.



Motivation

Organisational Services extend Boundaries and Borders

Complex Enterprise & Ecosystem

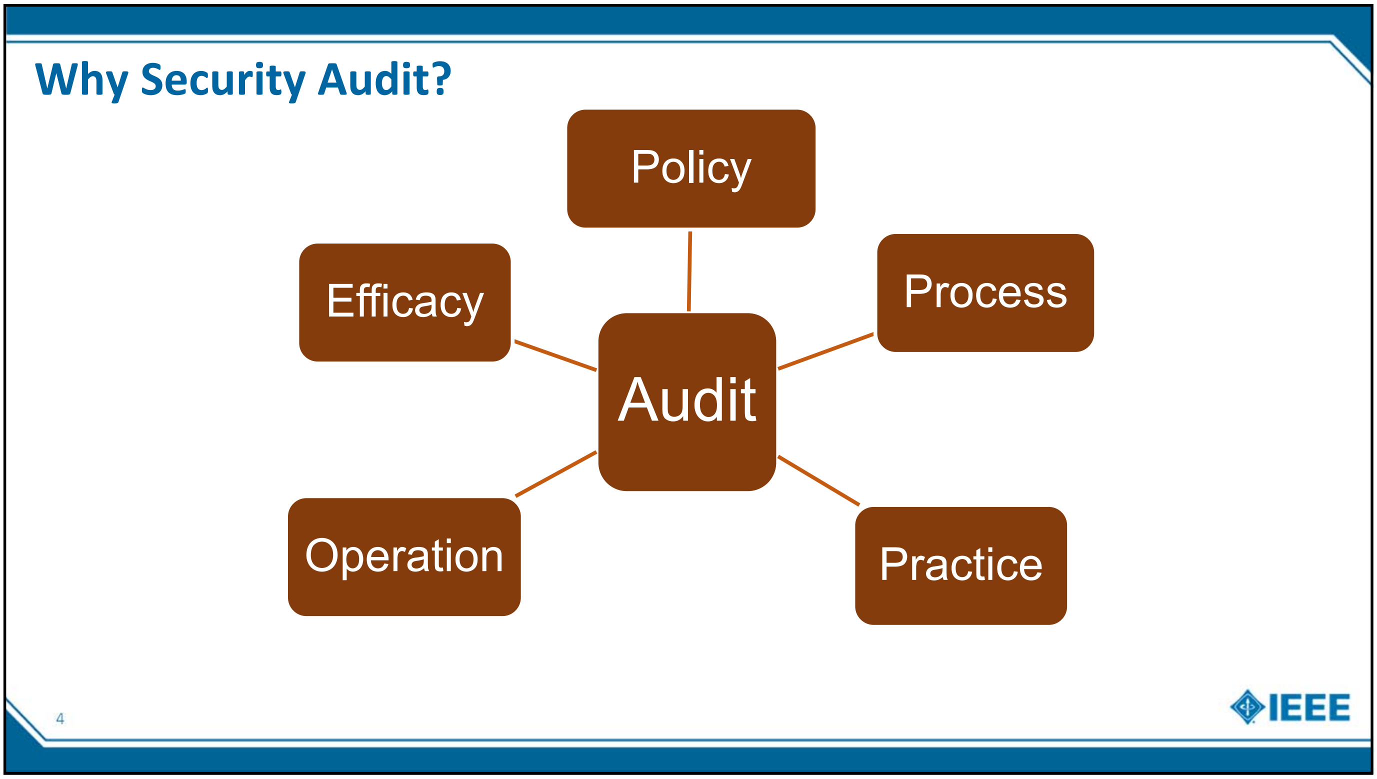
Regulatory & Legislative Mandates

Cyber Insurance & Security Compliance

Business Efficiency & Cost Optimisation

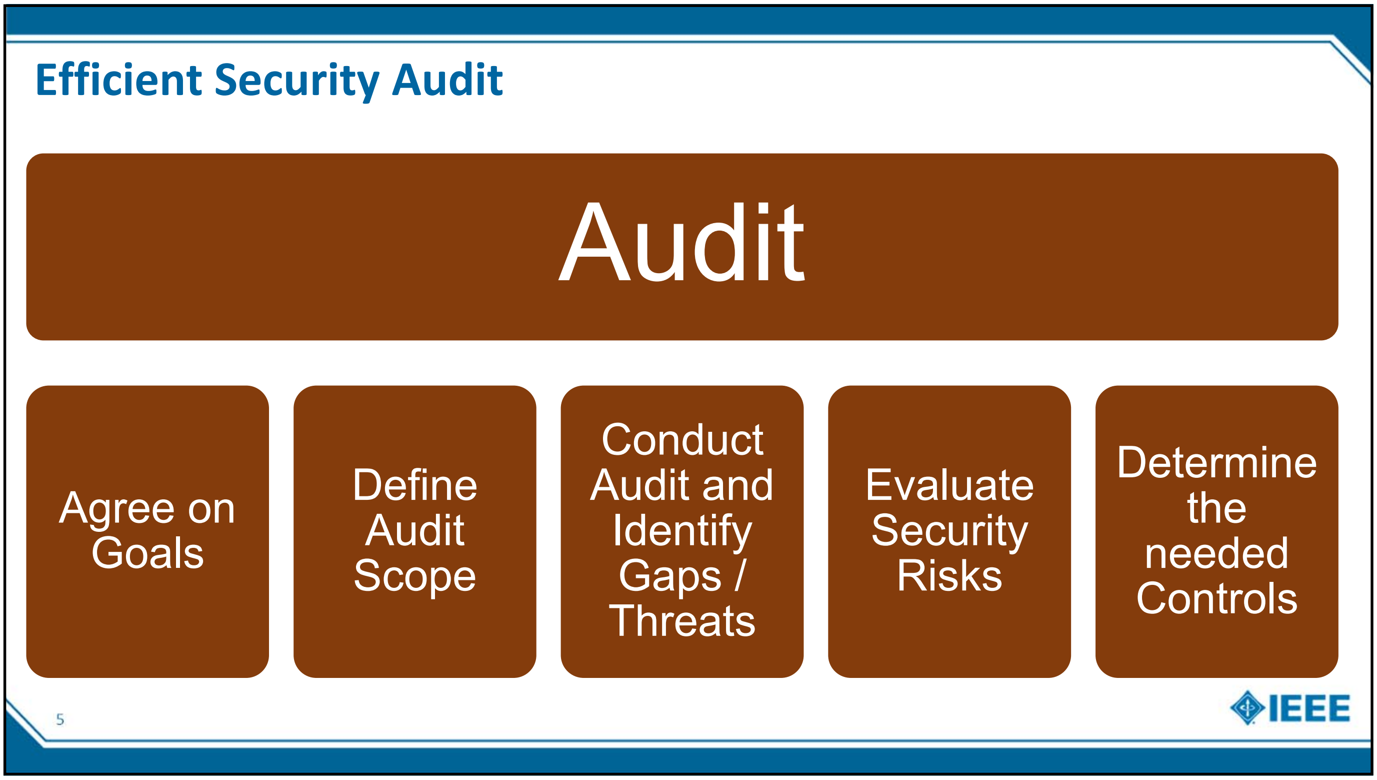
Supply Chain & Stakeholder Accountability

3



Why Security Audit?

4



Efficient Security Audit

Audit

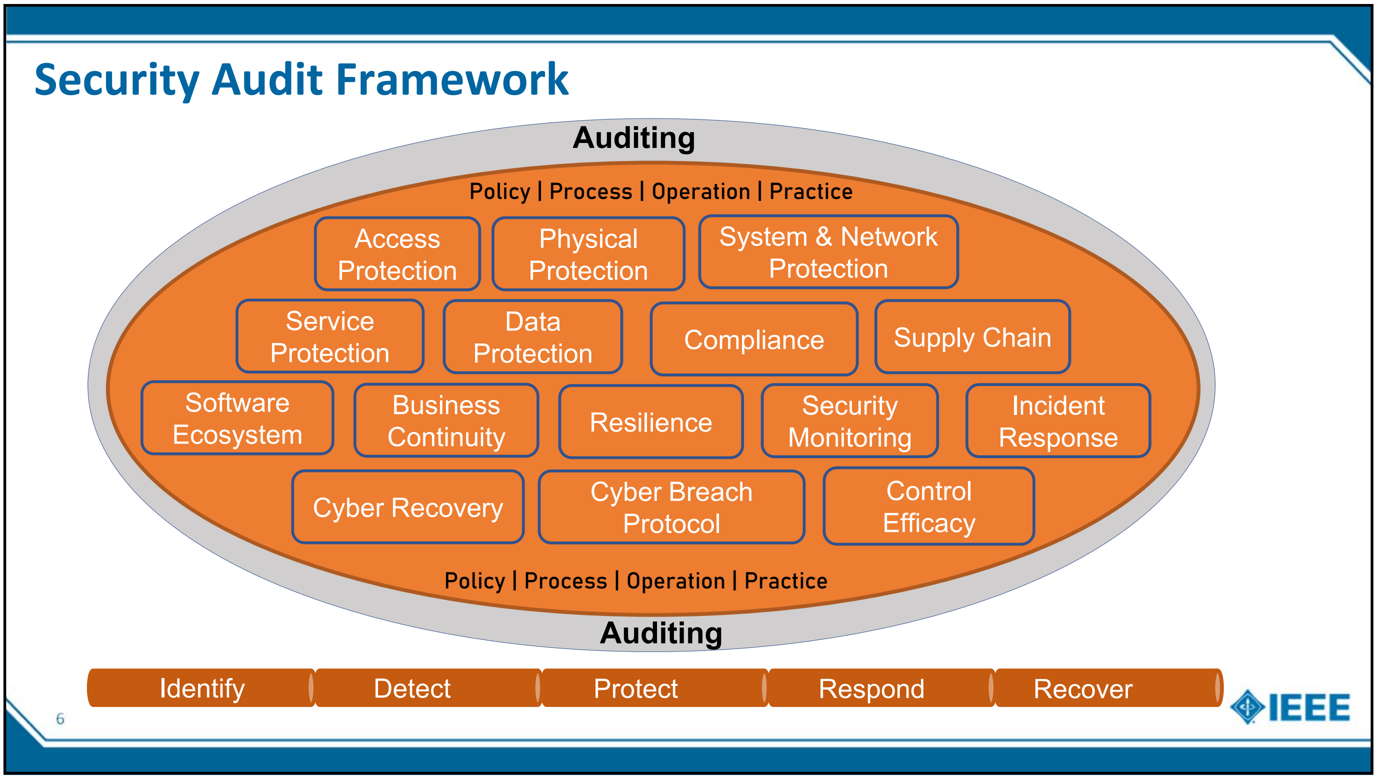
Agree on Goals

Define Audit Scope

Conduct Audit and Identify Gaps / Threats

Evaluate Security Risks

Determine the needed Controls



Security Audit Framework

Auditing

Policy | Process | Operation | Practice

Access Protection

Physical Protection

System & Network Protection

Service Protection

Data Protection

Compliance

Supply Chain

Software Ecosystem

Business Continuity

Resilience

Security Monitoring

Incident Response

Cyber Recovery

Cyber Breach Protocol

Control Efficacy

Policy | Process | Operation | Practice

Auditing

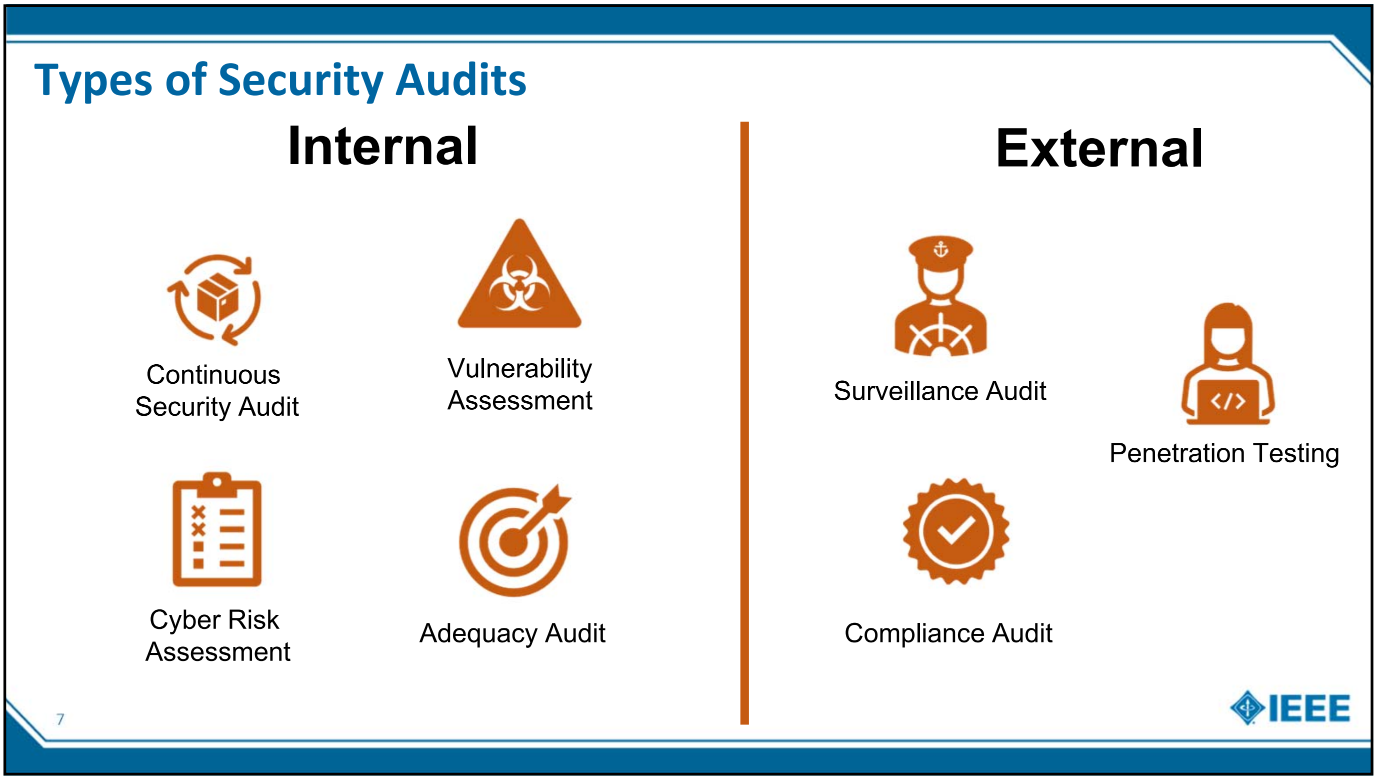
Identify

Detect

Protect

Respond

Recover



Types of Security Audits

Internal

- Continuous Security Audit
- Vulnerability Assessment
- Cyber Risk Assessment
- Adequacy Audit

External

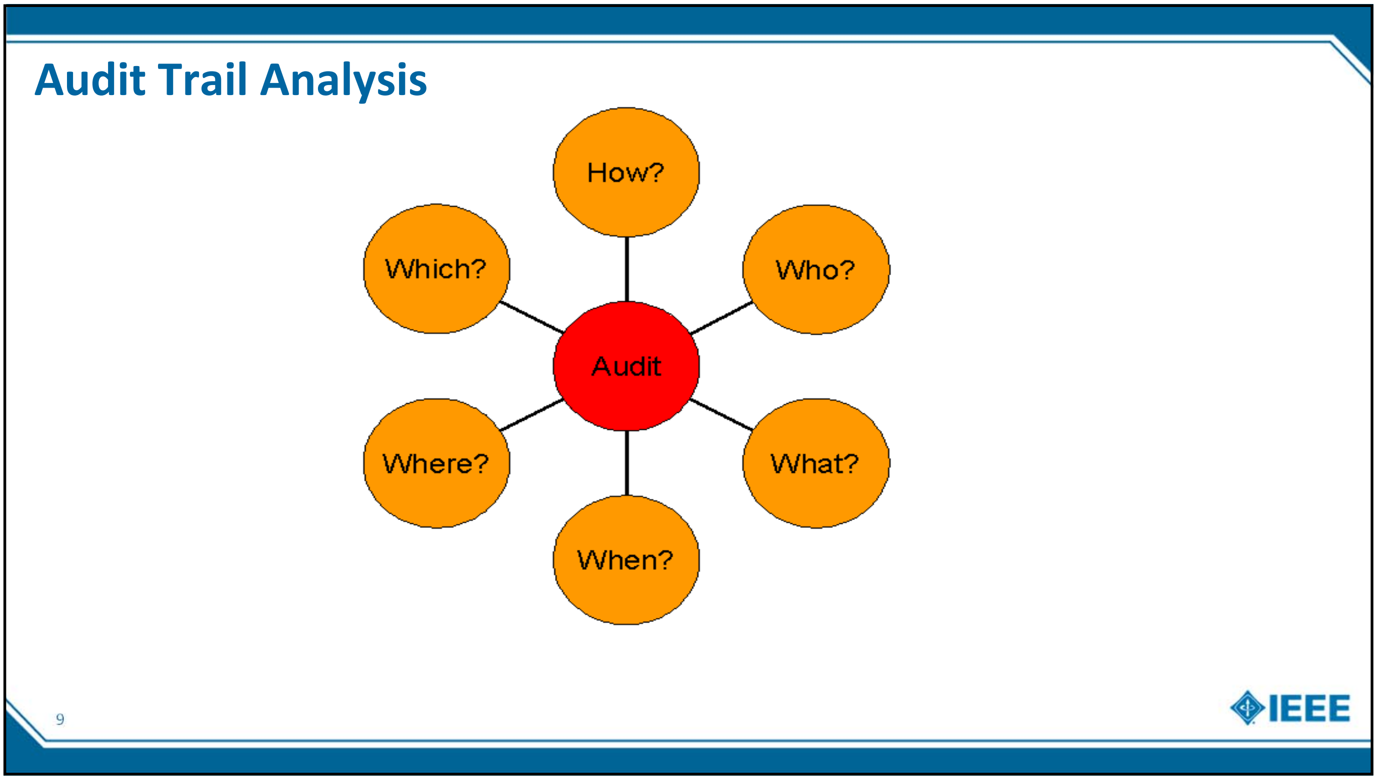
- Surveillance Audit
- Penetration Testing
- Compliance Audit

7

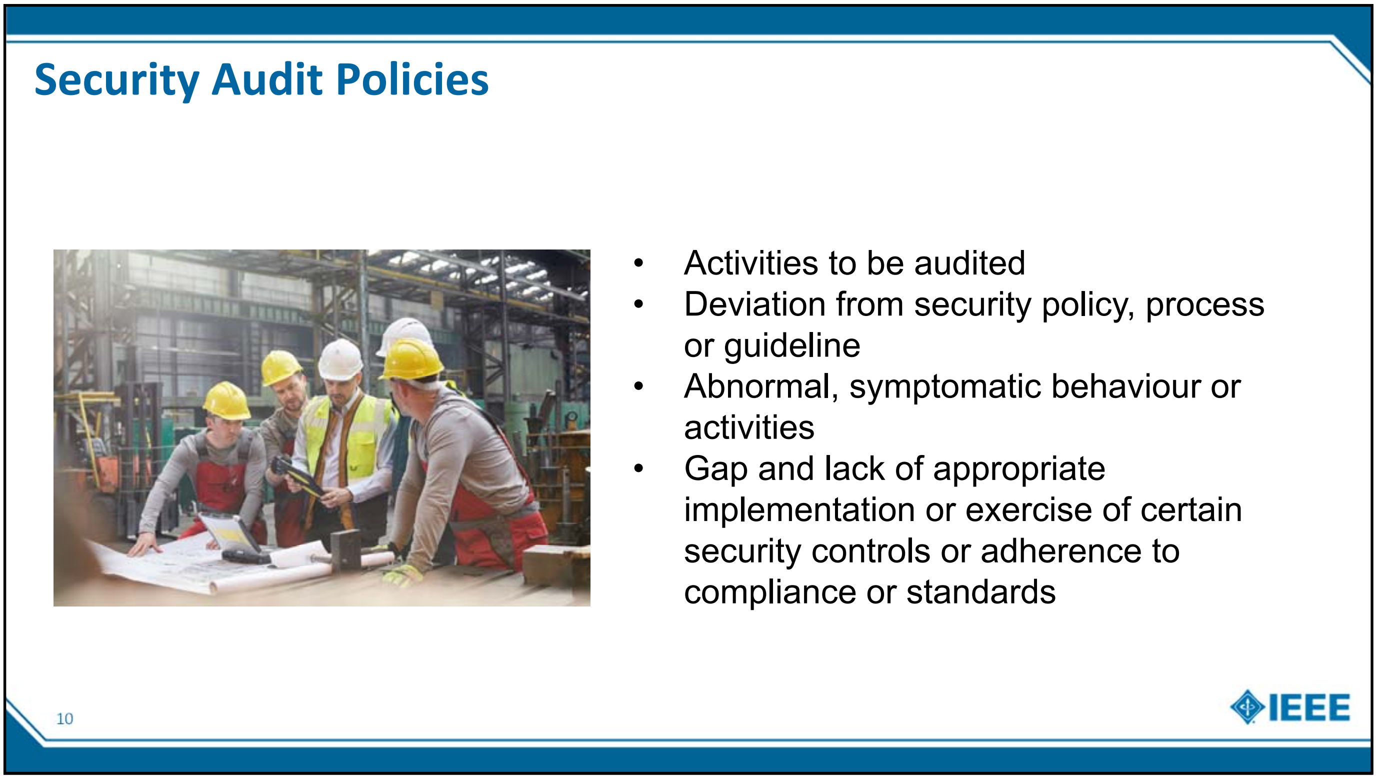
Security Audit, Compliance and Standards

- PCI DSS
- GLBA
- HIPPA
- SOX
- FISMA
- ISO 27001/2
- COBIT
- California Security Breach Information Act
- GDPR

8

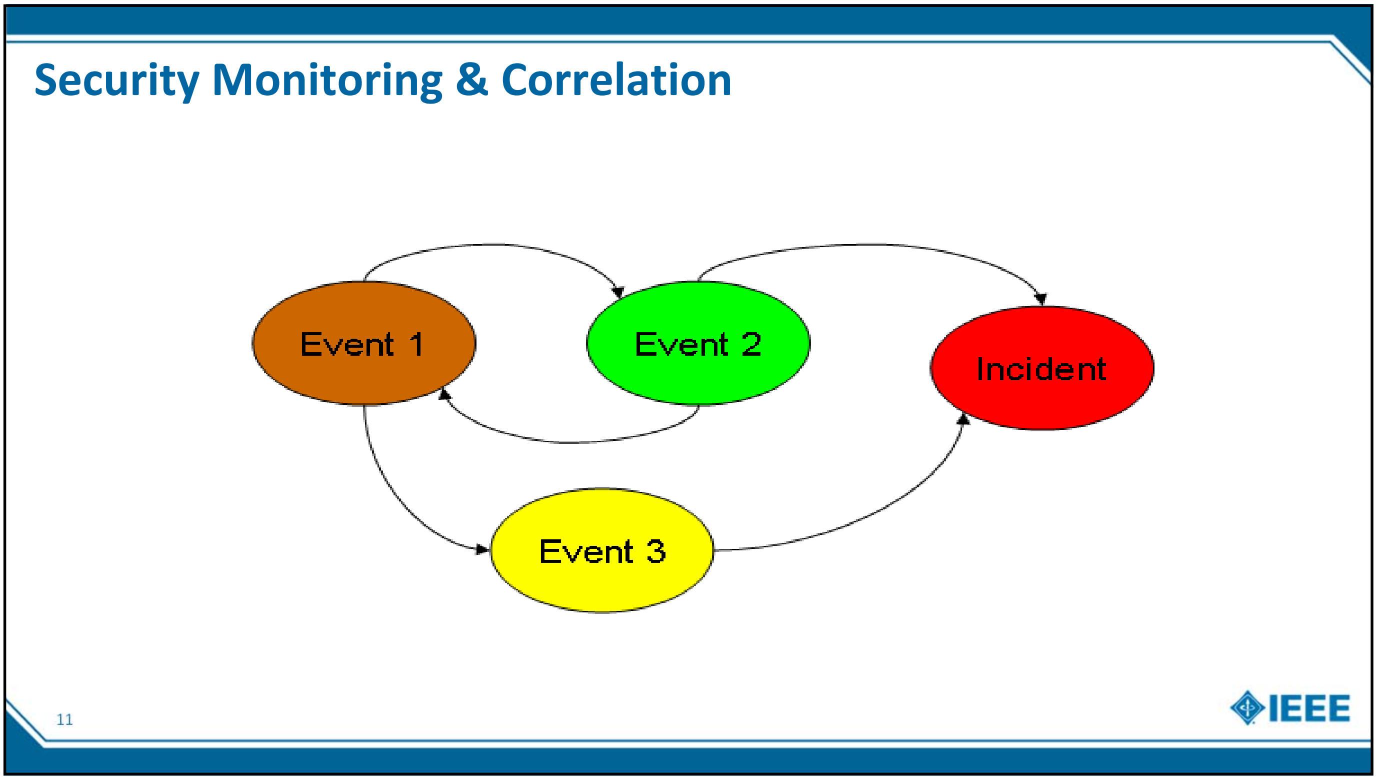


Audit Trail Analysis



Security Audit Policies

- Activities to be audited
- Deviation from security policy, process or guideline
- Abnormal, symptomatic behaviour or activities
- Gap and lack of appropriate implementation or exercise of certain security controls or adherence to compliance or standards



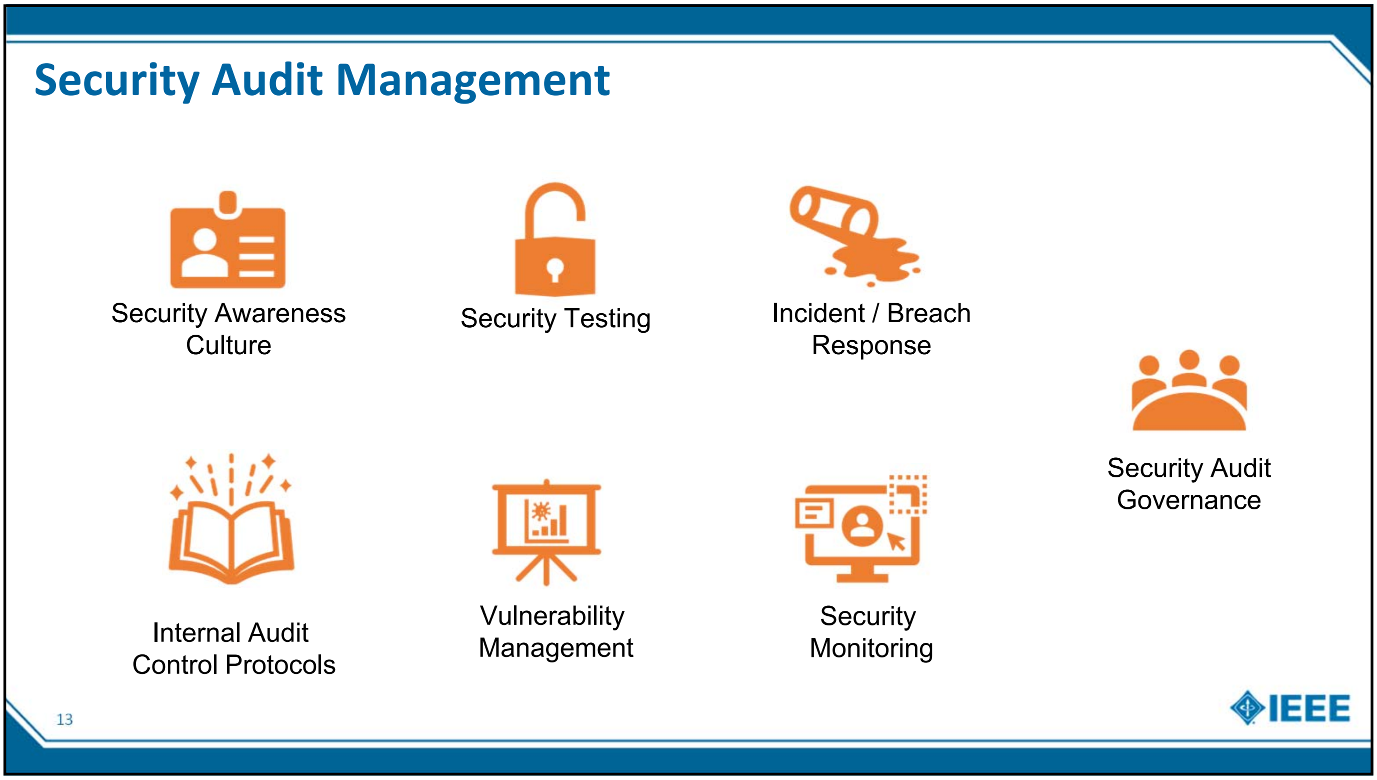
Security Monitoring & Correlation

11

Controls Effectiveness & Efficacy

- Controls effectiveness & efficacy
- Maintenance and operation
- Gaps
- Cost optimisation and residual risk

12



Security Audit Management

Security Awareness Culture

Security Testing

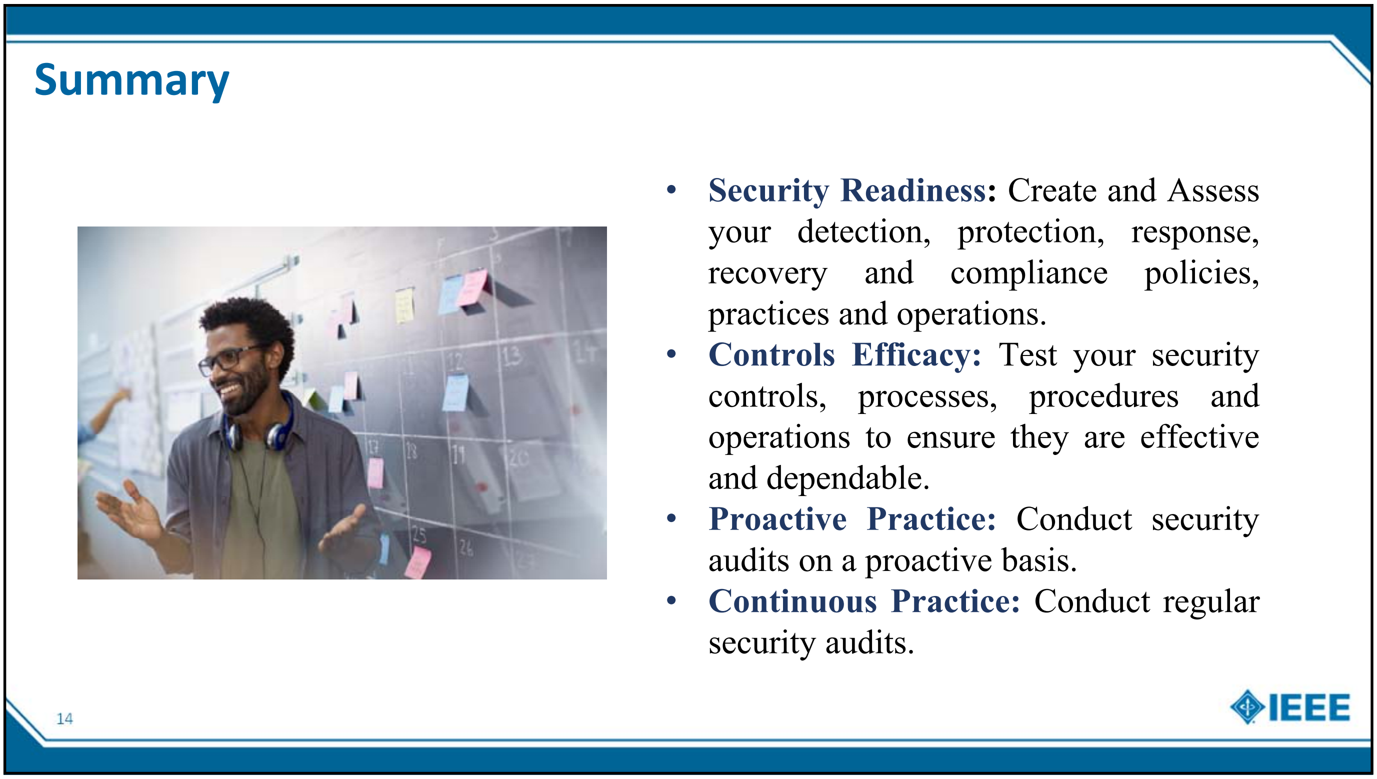
Incident / Breach Response

Security Audit Governance

Internal Audit Control Protocols

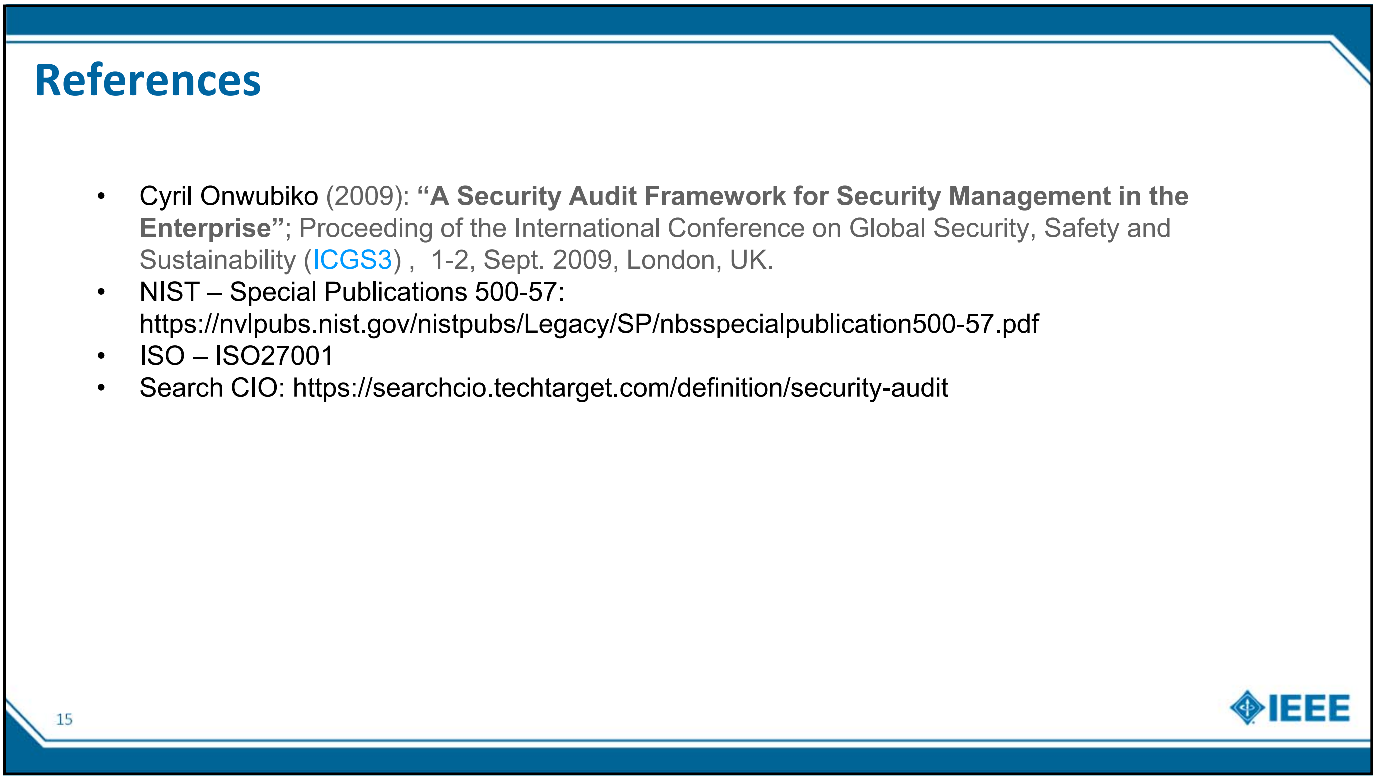
Vulnerability Management

Security Monitoring



Summary

- **Security Readiness:** Create and Assess your detection, protection, response, recovery and compliance policies, practices and operations.
- **Controls Efficacy:** Test your security controls, processes, procedures and operations to ensure they are effective and dependable.
- **Proactive Practice:** Conduct security audits on a proactive basis.
- **Continuous Practice:** Conduct regular security audits.



References

- Cyril Onwubiko (2009): **“A Security Audit Framework for Security Management in the Enterprise”**; Proceeding of the International Conference on Global Security, Safety and Sustainability (ICGS3) , 1-2, Sept. 2009, London, UK.
- NIST – Special Publications 500-57: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nbsspecialpublication500-57.pdf
- ISO – ISO27001
- Search CIO: https://searchcio.techtarget.com/definition/security-audit

15

Cyber Science 2022 Conference, Cardiff, Wales, United Kingdom

Deadline for call for papers is **February 28, 2022**

Cyber Science 2022

Pioneering research and innovation in Cyber Situational Awareness

www.c-mric.com/conferences

20-21 June

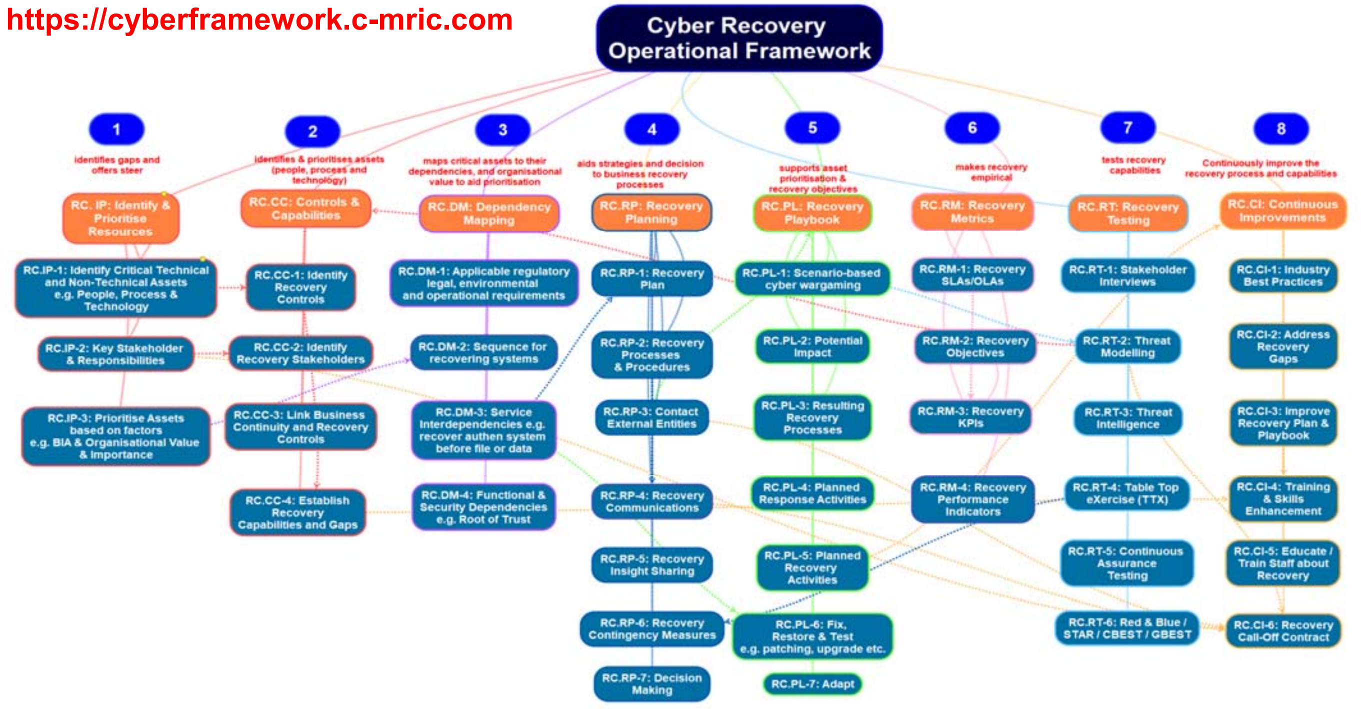
https://c-mric.org

Cardiff Metropolitan University
Prifysgol Metropolitan Caerdydd
IEEE Advancing Technology for Humanity
C-MRiC.ORG Centre for Multidisciplinary Research, Innovation and Collaboration

16

https://c-mric.org

https://cyberframework.c-mric.com



Cyber Recovery Operational Framework

1 – identifies gaps and offers steer

- 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 & prioritises assets (people, process and technology)

- 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 – aids strategies and decision to business recovery processes

- 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 – supports asset prioritisation & recovery objectives

- 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-2: Recovery Objectives
- RC.RM-3: Recovery KPIs
- 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

https://cyberframework.c-mric.com