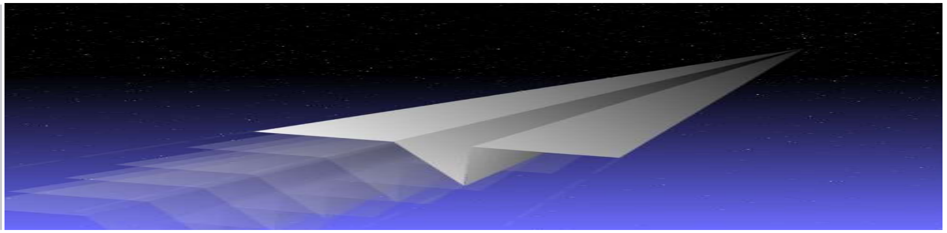
DEVELOP CAPABILITY

Cyber Security and the importance of your security posture



Bal Matu C.Eng MIET CQP FCQI CISA CEH ECSA CPSA

28 March 2024

bal@DevelopCapability.co.uk

www.DevelopCapability.co.uk

Bal Matu

- www.DevelopCapability.co.uk – Cyber Essentials Certification Body/ISO 27001 Consultancy
  - Cyber Essentials Plus Certification Body and Auditor
  - TickITplus Accredited Training Provider
  - ISMS Consultant and ISO 27001 Lead Auditor Training Provider

  - Background
    - 6 yrs - Graduate Engineer to Head of Design Assurance (Defence)
    - 2 yrs Quality Manager (Defence)
    - 2 yrs – Auditor/Consultant/Trainer for an Accredited Certification Body
    - 30+ yrs – Auditor/Consultant/Trainer (Contract)
    - IRCA Registered Lead Auditor since 1992
    - TickIT*plus*/ISO20000-1/ISO27001/ISO22301/TISAX Lead Auditor
    - World Lottery Association Security Control Standard (WLA – SCS) Lead Auditor
    - EC-Council Certified Ethical Hacker (CEH) and Certified Security Analyst (Practical) (ECSA)
    - CREST Registered Penetration Tester

Structure

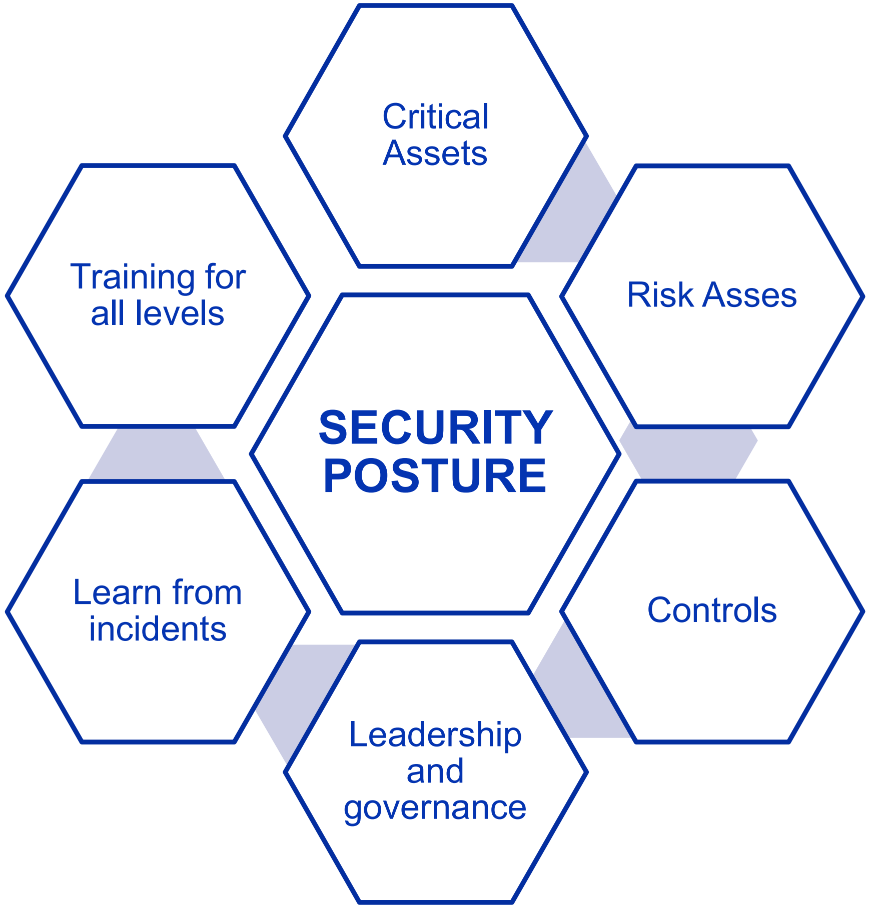
- Part 1 – Introduction and why a good security posture is important
- Part 2 – Security Frameworks – Examples and how they work
- Part 3 –How to use the Frameworks and also create a good security posture (Scenario)
- Part 4 – Summary

Part 1

INTRODUCTION

Why should we optimise our Security Posture?

- A good Security Posture will address
- Not only the
  - technical aspects of information security
- but also the
  - physical, cultural and behavioural aspects
- and demonstrate
  - effective leadership and governance



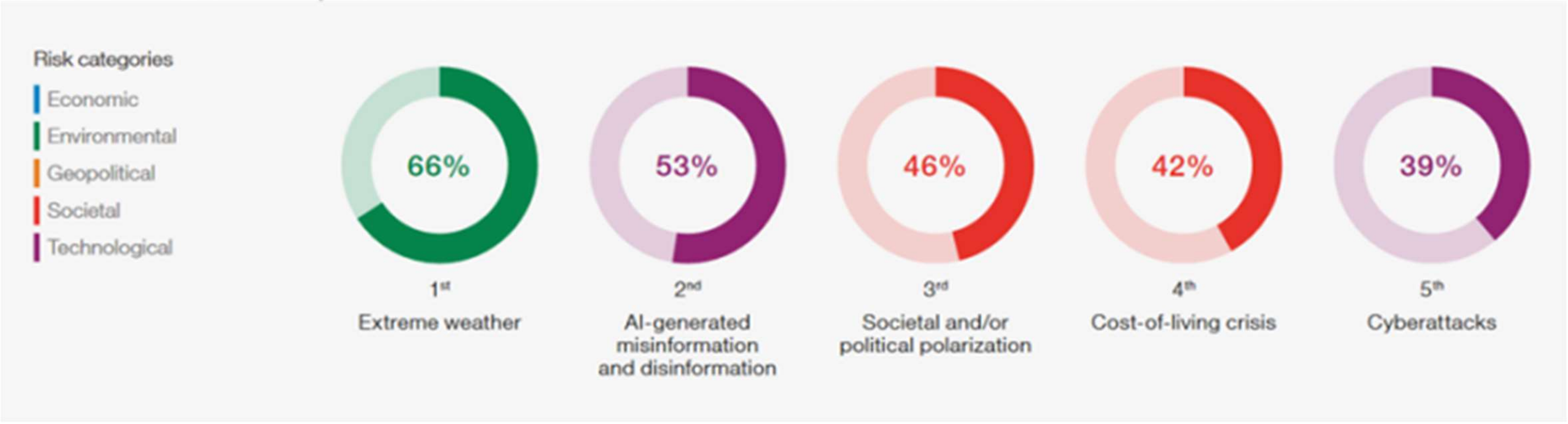
World Economic Forum (WEF) – 2024 Global Risk Report

- 39% of respondents believe cyberattacks present a material crisis on a global scale in 2024

FIGURE B

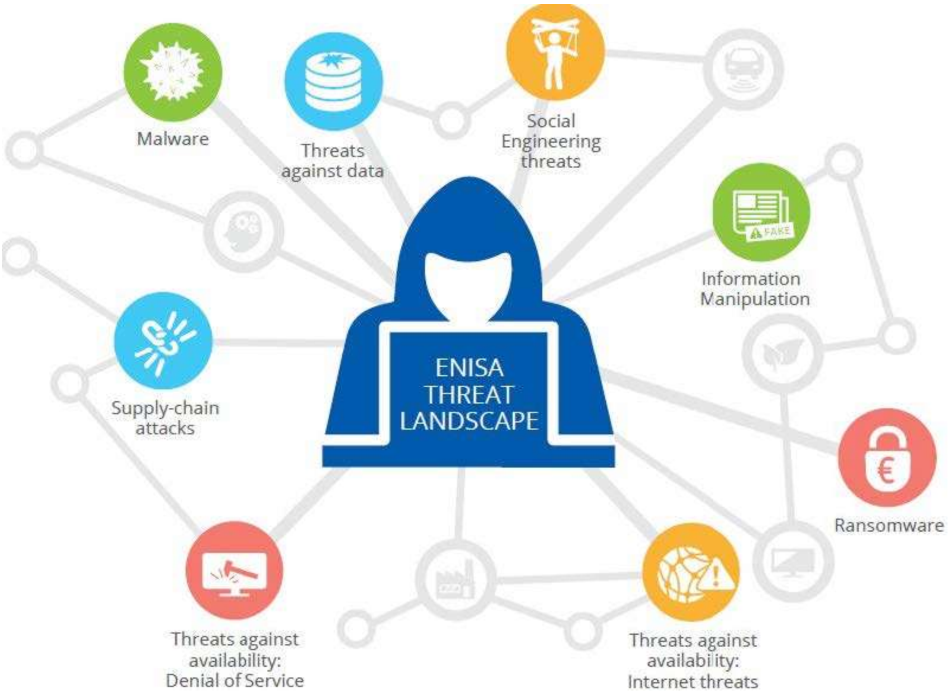
Current risk landscape

"Please select up to five risks that you believe are most likely to present a material crisis on a global scale in 2024."



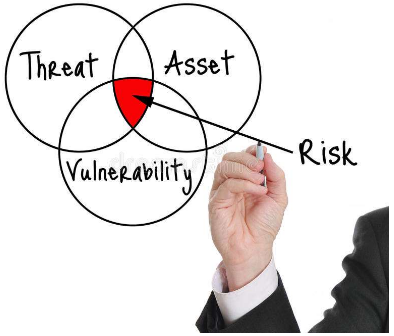
ENISA Threat Landscape 2023 - Prime threats

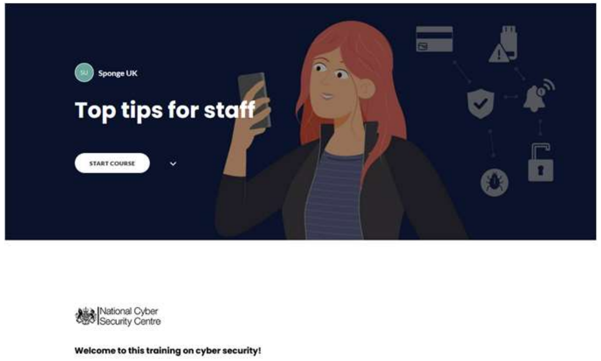
- **ENISA is the European Union Agency for Cyber Security**
- **Ransomware** and threats against availability ranked at the top during the reporting period
- **Phishing** is once again the most common vector for initial access.
- **Further professionalised** As-a-Service programmes (eg Phishing-as-a-Service (PhaaS).
- **Business and Vendor e-mail compromise (BEC, VEC)** remains one of the attacker's favourite means for obtaining financial gain.
- **Increase in supply chain attacks and use of employees as entry points.** Continue to target employees with elevated privileges, such as developers or system administrators
- https://www.enisa.europa.eu


Malware
Threats against data
Social Engineering threats
Information Manipulation
FAKE
Supply-chain attacks
ENISA THREAT LANDSCAPE
Ransomware
Threats against availability: Denial of Service
Threats against availability: Internet threats

What is Security Posture?

- It’s a measure of how well an organisation can predict, prevent, and respond to threats.





Top tips for staff

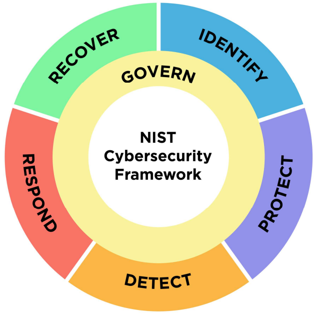
Welcome to this training on cyber security!

Part 2

SECURITY FRAMEWORKS

Many Frameworks

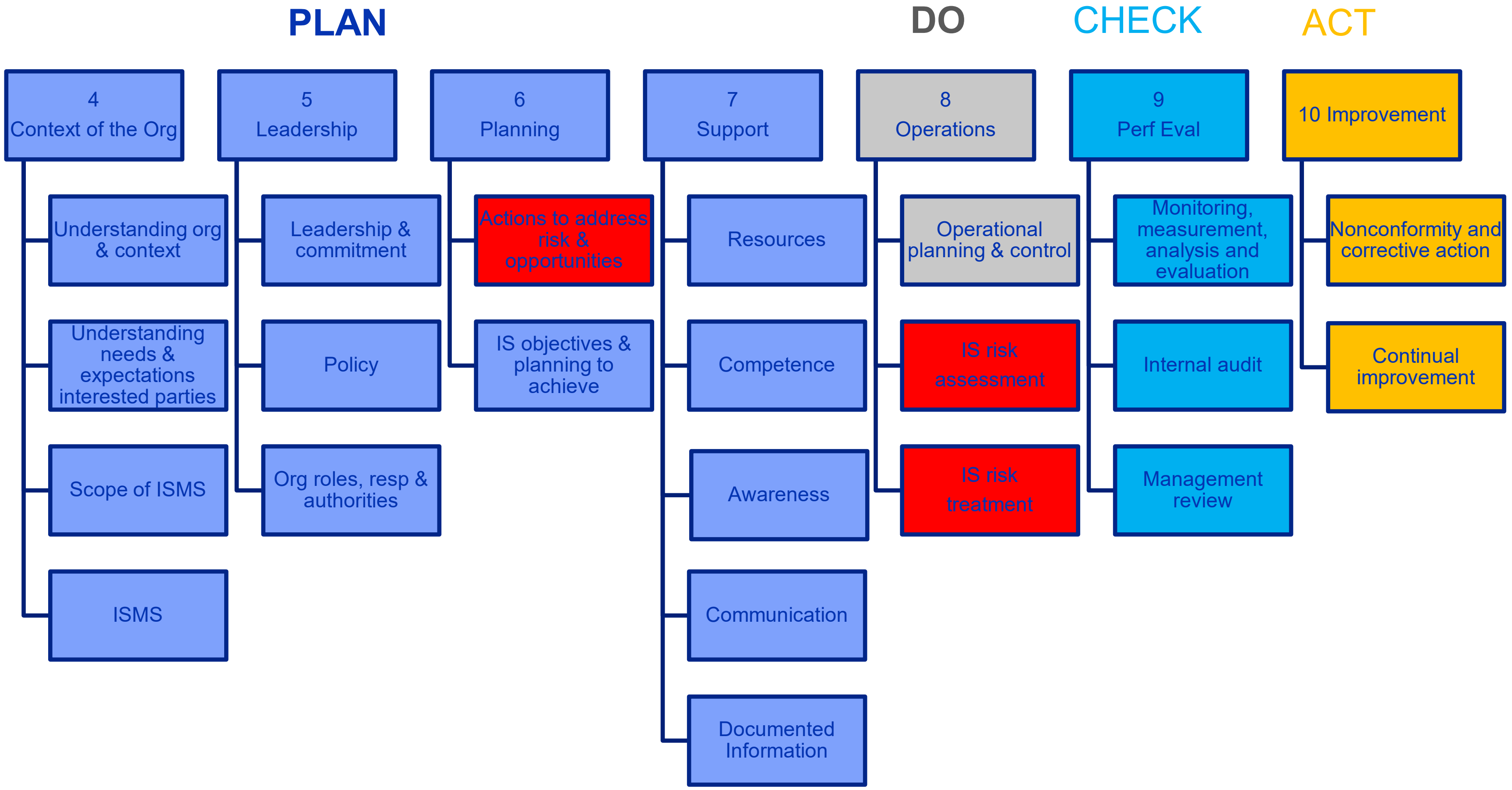
- Cyber Essentials and Cyber Essentials Plus – focus is on risk from internet controls are mandated
- ISO 27001 – broader (includes risk from internet) but organisation sets own acceptable level of risk
- NIST CSF – risk based – catalogue of outcomes – Function-Category-Subcategory-Info Refs
- TickITplus – ISO 9001; ISO 20000-1 and ISO 27001 as one Integrated Management System



Cyber Essentials Scheme Requirements

- UK Government backed scheme that will help any size of organisation, protect against the most common cyber attacks
- Scheme owner is NCSC
- Focus is on risk from internet, controls are mandated
  - Firewalls
  - Secure configuration
  - User access control
  - Malware protection
  - Security update management/patching

ISO 27001:2022



PLAN

- 4 Context of the Org
  - Understanding org & context
  - Understanding needs & expectations interested parties
  - Scope of ISMS
  - ISMS
- 5 Leadership
  - Leadership & commitment
  - Policy
  - Org roles, resp & authorities
- 6 Planning
  - Actions to address risk & opportunities
  - IS objectives & planning to achieve
- 7 Support
  - Resources
  - Competence
  - Awareness
  - Communication
  - Documented Information

DO

- 8 Operations
  - Operational planning & control
  - IS risk assessment
  - IS risk treatment

CHECK

- 9 Perf Eval
  - Monitoring, measurement, analysis and evaluation
  - Internal audit
  - Management review

ACT

- 10 Improvement
  - Nonconformity and corrective action
  - Continual improvement

CE v ISO 27001 Comparison - Requirements

Cyber Essentials Scheme

- Risk Assessment – By Scheme owner - NCSC
- Controls – 5 technical control themes - firewalls, secure configuration, user access control, malware protection and security update management
- Two levels
  - Self-declared level (CE Verified Self-Assessment)
  - An independently tested level (CE Plus)

ISO 27001:2022

- Risk Assessment – By Organisation being assessed
- Controls – 93 technical controls divided into 4 categories Organizational, People, Physical, Technological. Sections 4-10 covering Management System Requirements covering Plan-Do-Check-Act)
- Accredited Certification based on process effectiveness checks (no actual testing by the Auditors)

Comparison - Controls

Cyber Essentials Scheme

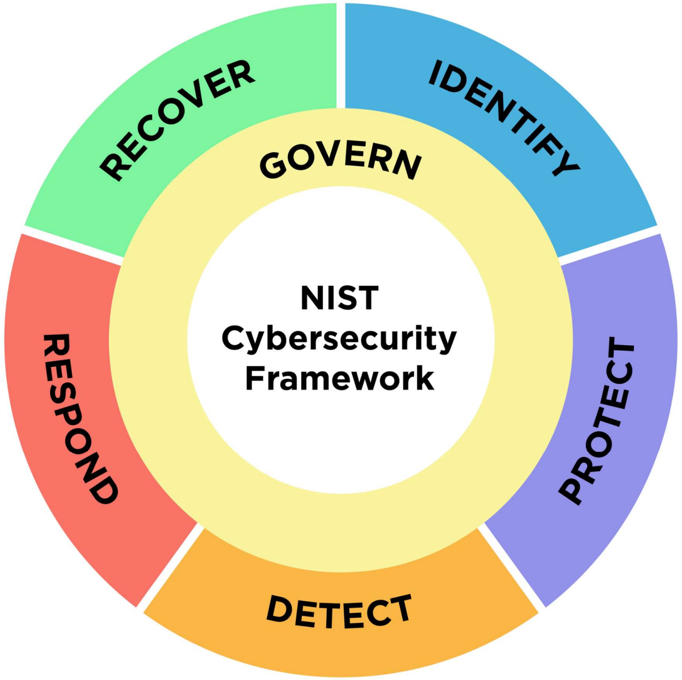
- Focus is on exploitable vulnerabilities and weaknesses within an organisation's infrastructure through the internet
- External vulnerabilities (all TCP/UDP ports for all external IP addresses)
- End User Devices for vulnerabilities
- Effectiveness of malware protection
- Effectiveness of security while browsing
- Cloud services – use of MFA/2FA
- User/Admin account separation

ISO 27001:2022

- Risk Methodology is selected/defined by the organisation
- Risk Assessment determines level of risk based on information assets, threats and vulnerabilities
- Create a risk treatment plan and define risk treatment/acceptance criteria
- Statement of Applicability justifies inclusion and exclusion of the 93 controls listed in Annex A
- Demonstrate the effectiveness of the management system and justified controls using objective evidence

NIST - CSF

- The CSF 2.0 is organized by six Functions — Govern, Identify, Protect, Detect, Respond, and Recover.



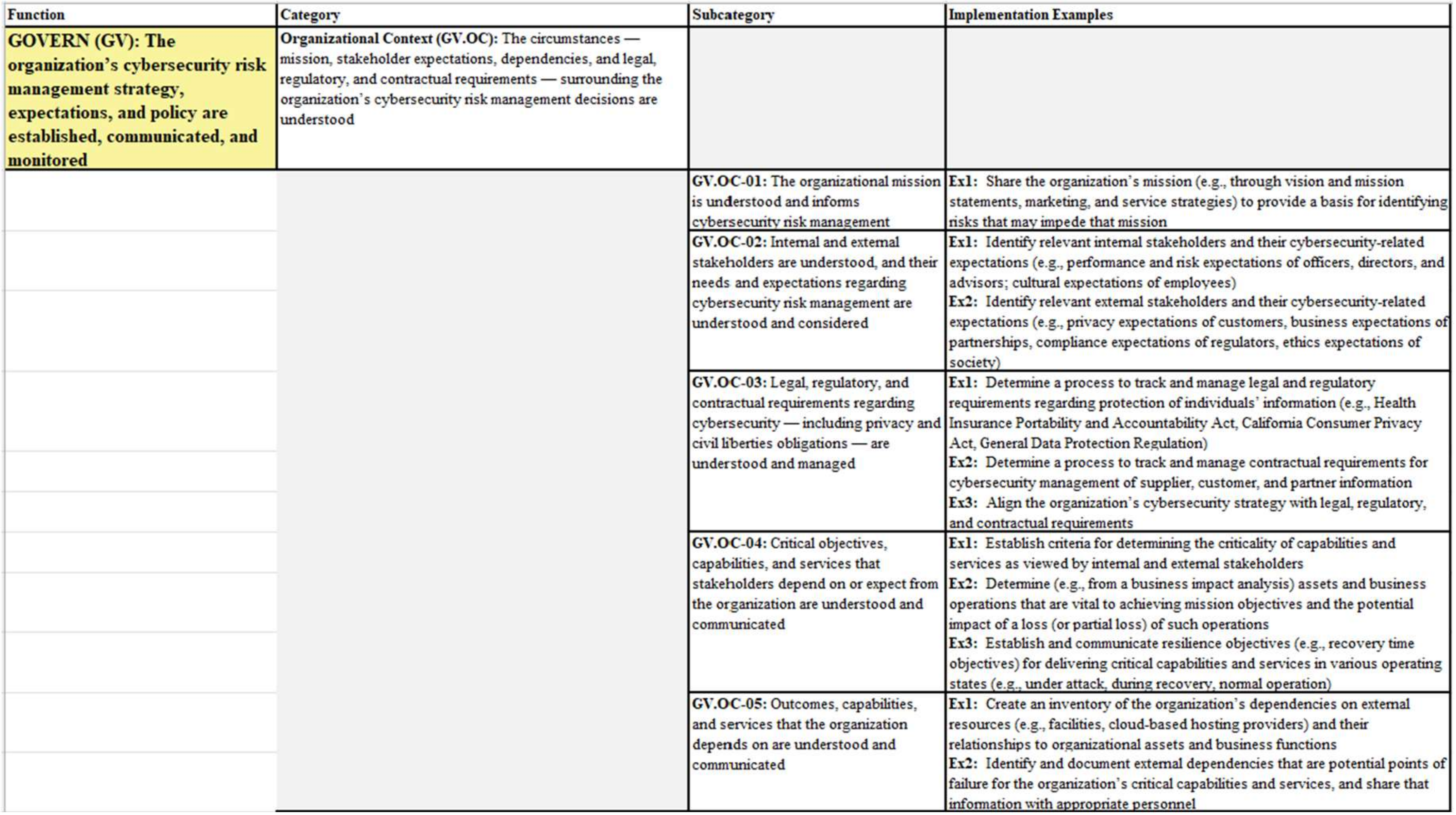
https://www.nist.gov/cyberframework

NIST - Cybersecurity Framework 2.0

- The CSF 2.0 is organized by six Functions — Govern, Identify, Protect, Detect, Respond, and Recover.
- **CSF Core** - A catalogue of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks.
- **CSF Organizational Profiles** - A mechanism for describing an organization’s current and/or target cybersecurity posture in terms of the CSF Core’s outcomes.
- **CSF Tiers** - Can be applied to CSF Organizational Profiles to characterize the rigor of an organization’s cybersecurity risk governance and management practices.

https://www.nist.gov

NIST - Cybersecurity Framework

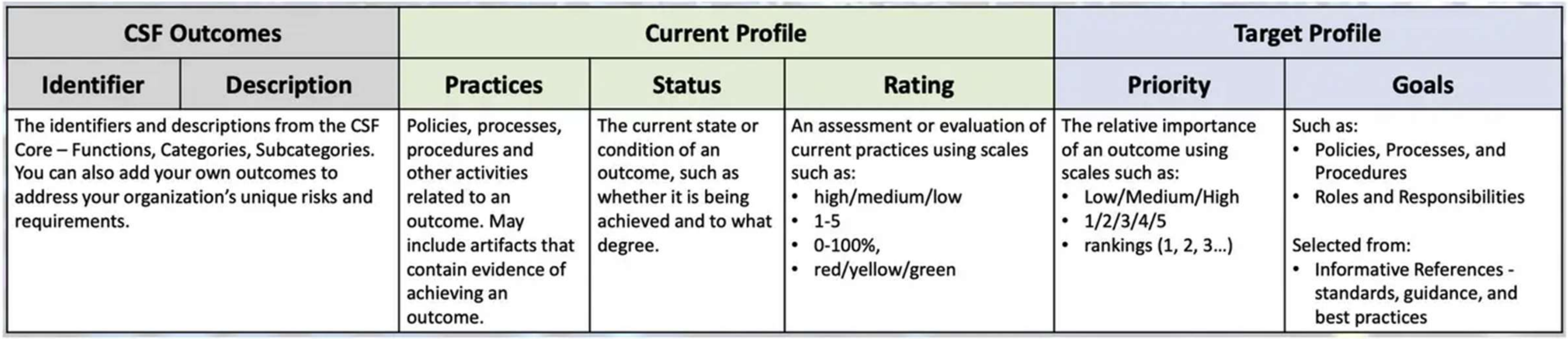


Function	Category	Subcategory	Implementation Examples
GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored	**Organizational Context (GV.OC):** The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood		
		GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	**Ex1:** Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission
		GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	**Ex1:** Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., performance and risk expectations of officers, directors, and advisors; cultural expectations of employees) **Ex2:** Identify relevant external stakeholders and their cybersecurity-related expectations (e.g., privacy expectations of customers, business expectations of partnerships, compliance expectations of regulators, ethics expectations of society)
		GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed	**Ex1:** Determine a process to track and manage legal and regulatory requirements regarding protection of individuals' information (e.g., Health Insurance Portability and Accountability Act, California Consumer Privacy Act, General Data Protection Regulation) **Ex2:** Determine a process to track and manage contractual requirements for cybersecurity management of supplier, customer, and partner information **Ex3:** Align the organization's cybersecurity strategy with legal, regulatory, and contractual requirements
		GV.OC-04: Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are understood and communicated	**Ex1:** Establish criteria for determining the criticality of capabilities and services as viewed by internal and external stakeholders **Ex2:** Determine (e.g., from a business impact analysis) assets and business operations that are vital to achieving mission objectives and the potential impact of a loss (or partial loss) of such operations **Ex3:** Establish and communicate resilience objectives (e.g., recovery time objectives) for delivering critical capabilities and services in various operating states (e.g., under attack, during recovery, normal operation)
		GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated	**Ex1:** Create an inventory of the organization's dependencies on external resources (e.g., facilities, cloud-based hosting providers) and their relationships to organizational assets and business functions **Ex2:** Identify and document external dependencies that are potential points of failure for the organization's critical capabilities and services, and share that information with appropriate personnel

https://www.nist.gov

NIST - Cybersecurity Framework

- Improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state)



CSF Outcomes		Current Profile			Target Profile	
Identifier	**Description**	**Practices**	**Status**	**Rating**	**Priority**	**Goals**
The identifiers and descriptions from the CSF Core – Functions, Categories, Subcategories. You can also add your own outcomes to address your organization's unique risks and requirements.		Policies, processes, procedures and other activities related to an outcome. May include artifacts that contain evidence of achieving an outcome.	The current state or condition of an outcome, such as whether it is being achieved and to what degree.	An assessment or evaluation of current practices using scales such as: • high/medium/low • 1-5 • 0-100%, • red/yellow/green	The relative importance of an outcome using scales such as: • Low/Medium/High • 1/2/3/4/5 • rankings (1, 2, 3...)	Such as: • Policies, Processes, and Procedures • Roles and Responsibilities Selected from: • Informative References - standards, guidance, and best practices

TickITplus

- https://www.tickitplus.org

Excellent resource if you need

to implement ISO Standards

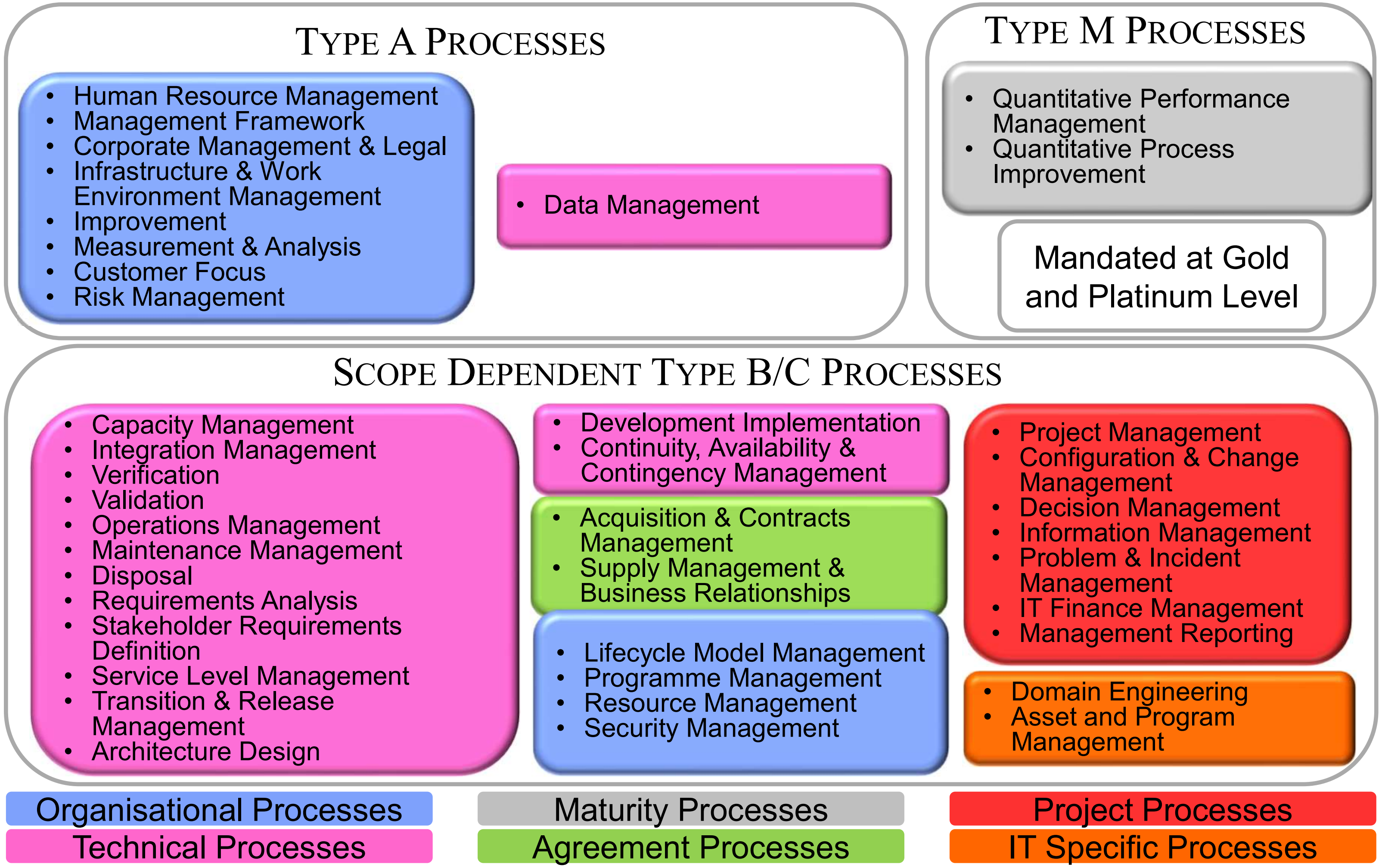
such as:-

ISO 9001

ISO 27001

ISO 20000-1

TickITplus BPL Processes



Type A Processes

- Human Resource Management
- Management Framework
- Corporate Management & Legal
- Infrastructure & Work Environment Management
- Improvement
- Measurement & Analysis
- Customer Focus
- Risk Management

- Data Management

Type M Processes

- Quantitative Performance Management
- Quantitative Process Improvement

Mandated at Gold and Platinum Level

Scope Dependent Type B/C Processes

- Capacity Management
- Integration Management
- Verification
- Validation
- Operations Management
- Maintenance Management
- Disposal
- Requirements Analysis
- Stakeholder Requirements Definition
- Service Level Management
- Transition & Release Management
- Architecture Design

- Development Implementation
- Continuity, Availability & Contingency Management

- Acquisition & Contracts Management
- Supply Management & Business Relationships

- Lifecycle Model Management
- Programme Management
- Resource Management
- Security Management

- Project Management
- Configuration & Change Management
- Decision Management
- Information Management
- Problem & Incident Management
- IT Finance Management
- Management Reporting

- Domain Engineering
- Asset and Program Management

Organisational Processes

Technical Processes

Maturity Processes

Agreement Processes

Project Processes

IT Specific Processes

TickITplus Processes

- The 40 BPL processes are presented in eight process profiles

- ISO 12207 Software Lifecycle processes
- ISO 15288 Systems and software engineering - System life cycle processes

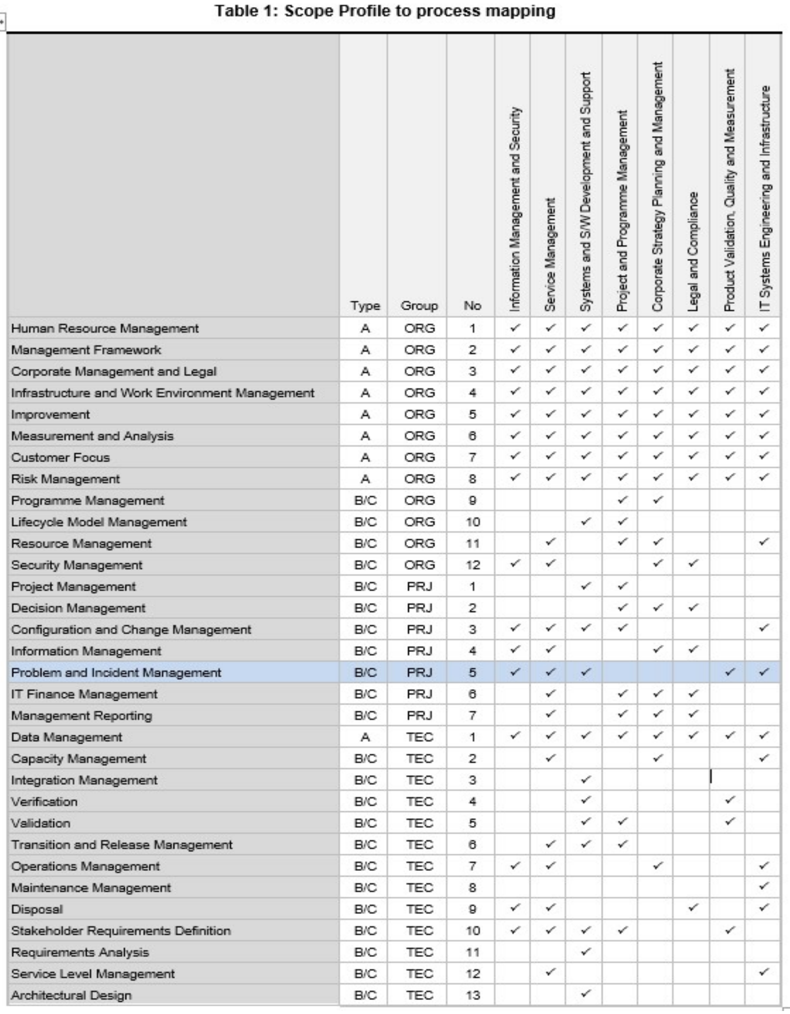
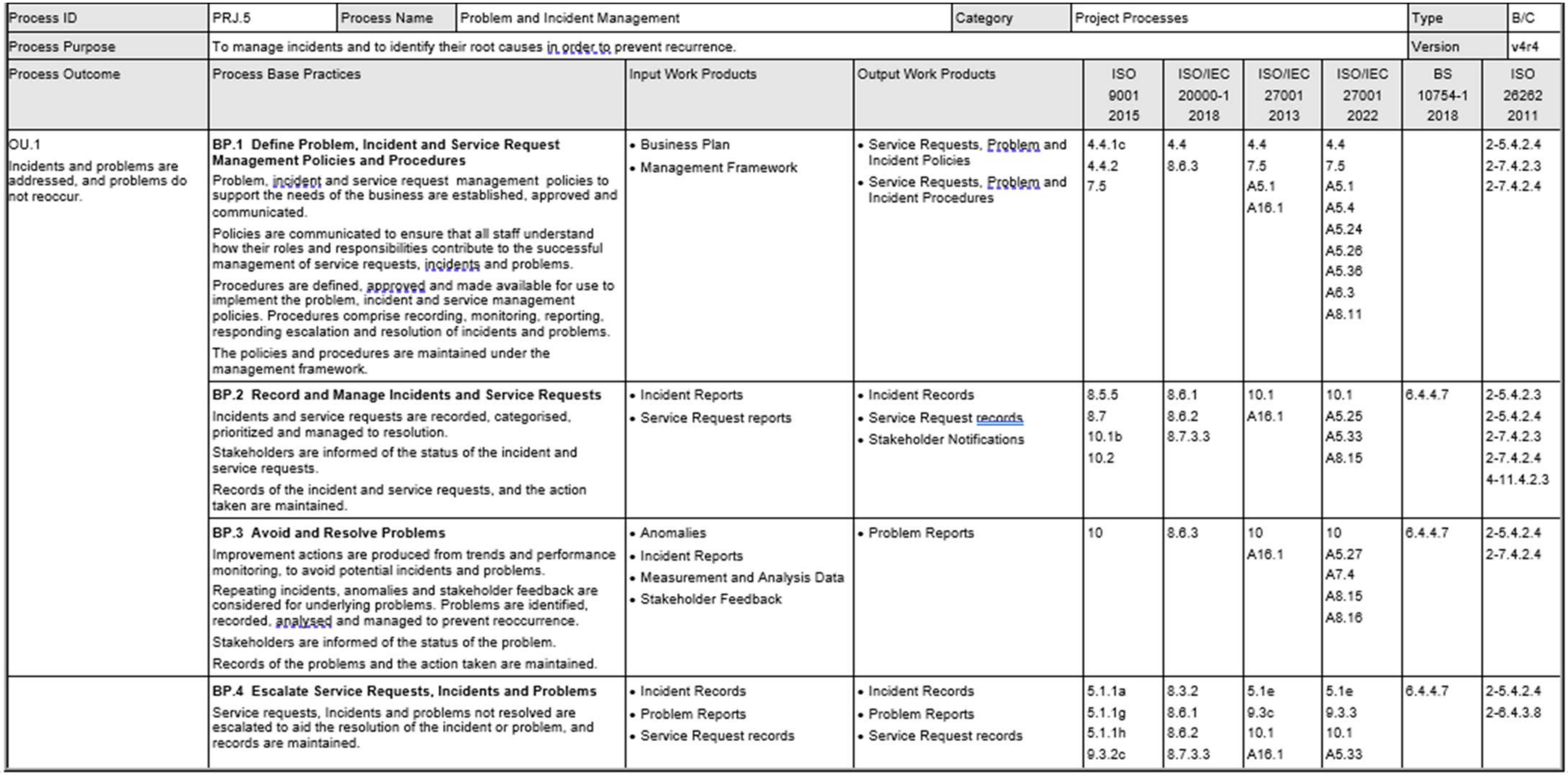


Table 1: Scope Profile to process mapping

	Type	Group	No	Information Management and Security	Service Management	Systems and S/W Development and Support	Project and Programme Management	Corporate Strategy Planning and Management	Legal and Compliance	Product Validation, Quality and Measurement	IT Systems Engineering and Infrastructure
Human Resource Management	A	ORG	1	✓	✓	✓	✓	✓	✓	✓	✓
Management Framework	A	ORG	2	✓	✓	✓	✓	✓	✓	✓	✓
Corporate Management and Legal	A	ORG	3	✓	✓	✓	✓	✓	✓	✓	✓
Infrastructure and Work Environment Management	A	ORG	4	✓	✓	✓	✓	✓	✓	✓	✓
Improvement	A	ORG	5	✓	✓	✓	✓	✓	✓	✓	✓
Measurement and Analysis	A	ORG	6	✓	✓	✓	✓	✓	✓	✓	✓
Customer Focus	A	ORG	7	✓	✓	✓	✓	✓	✓	✓	✓
Risk Management	A	ORG	8	✓	✓	✓	✓	✓	✓	✓	✓
Programme Management	B/C	ORG	9				✓	✓			
Lifecycle Model Management	B/C	ORG	10			✓	✓				
Resource Management	B/C	ORG	11		✓		✓	✓			✓
Security Management	B/C	ORG	12	✓	✓			✓	✓		
Project Management	B/C	PRJ	1			✓	✓				
Decision Management	B/C	PRJ	2				✓	✓	✓		
Configuration and Change Management	B/C	PRJ	3	✓	✓	✓	✓				✓
Information Management	B/C	PRJ	4	✓	✓			✓	✓		
Problem and Incident Management	B/C	PRJ	5	✓	✓	✓				✓	✓
IT Finance Management	B/C	PRJ	6		✓		✓	✓	✓		
Management Reporting	B/C	PRJ	7		✓		✓	✓	✓		
Data Management	A	TEC	1	✓	✓	✓	✓	✓	✓	✓	✓
Capacity Management	B/C	TEC	2		✓			✓			✓
Integration Management	B/C	TEC	3			✓					
Verification	B/C	TEC	4			✓				✓	
Validation	B/C	TEC	5			✓	✓			✓	
Transition and Release Management	B/C	TEC	6		✓	✓	✓				
Operations Management	B/C	TEC	7	✓	✓			✓			✓
Maintenance Management	B/C	TEC	8								✓
Disposal	B/C	TEC	9	✓	✓				✓		✓
Stakeholder Requirements Definition	B/C	TEC	10	✓	✓	✓	✓			✓	
Requirements Analysis	B/C	TEC	11			✓					
Service Level Management	B/C	TEC	12		✓						✓
Architectural Design	B/C	TEC	13			✓					

TickITplus Mapping

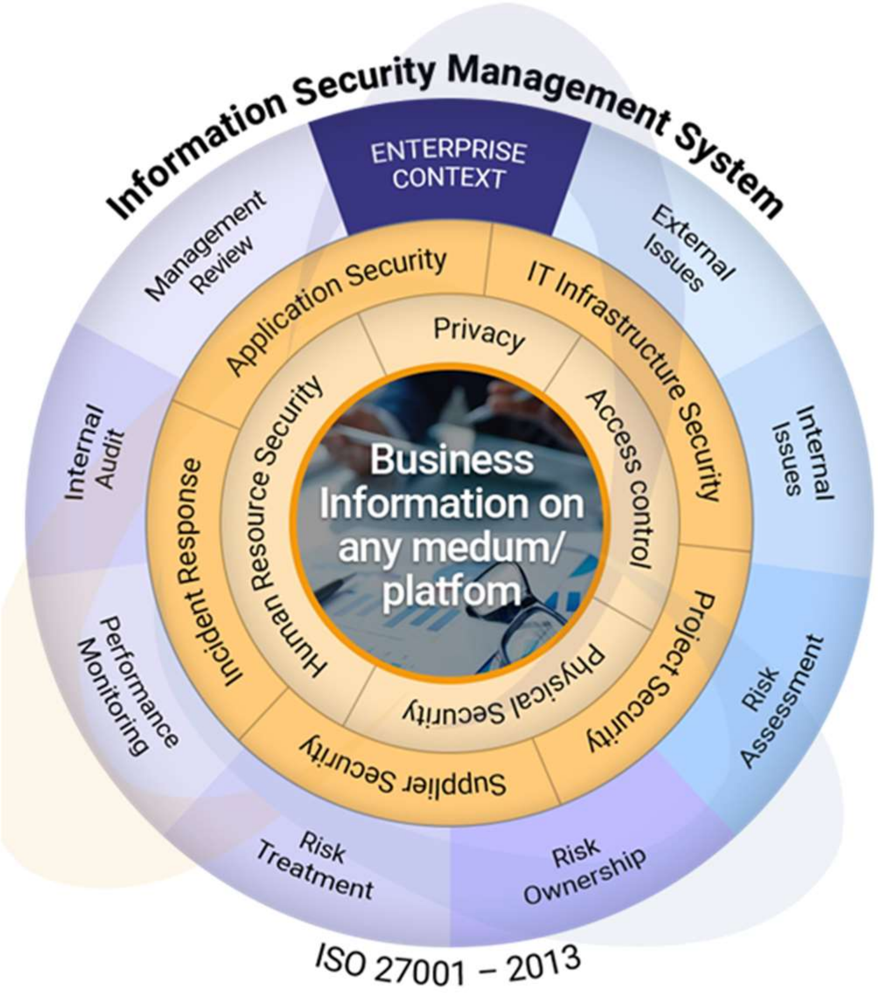
PRJ.5 Problem and Incident Management



Process ID	PRJ.5	Process Name	Problem and Incident Management	Category	Project Processes			Type	B/C
Process Purpose	To manage incidents and to identify their root causes in order to prevent recurrence.							Version	v4r4
Process Outcome	Process Base Practices	Input Work Products	Output Work Products	ISO 9001 2015	ISO/IEC 20000-1 2018	ISO/IEC 27001 2013	ISO/IEC 27001 2022	BS 10754-1 2018	ISO 26262 2011
OU.1 Incidents and problems are addressed, and problems do not reoccur.	**BP.1 Define Problem, Incident and Service Request Management Policies and Procedures** Problem, incident and service request management policies to support the needs of the business are established, approved and communicated. Policies are communicated to ensure that all staff understand how their roles and responsibilities contribute to the successful management of service requests, incidents and problems. Procedures are defined, approved and made available for use to implement the problem, incident and service management policies. Procedures comprise recording, monitoring, reporting, responding escalation and resolution of incidents and problems. The policies and procedures are maintained under the management framework.	• Business Plan • Management Framework	• Service Requests, Problem and Incident Policies • Service Requests, Problem and Incident Procedures	4.4.1c 4.4.2 7.5	4.4 8.6.3	4.4 7.5 A5.1 A16.1	4.4 7.5 A5.1 A5.4 A5.24 A5.26 A5.36 A6.3 A8.11		2-5.4.2.4 2-7.4.2.3 2-7.4.2.4
	BP.2 Record and Manage Incidents and Service Requests Incidents and service requests are recorded, categorised, prioritized and managed to resolution. Stakeholders are informed of the status of the incident and service requests. Records of the incident and service requests, and the action taken are maintained.	• Incident Reports • Service Request reports	• Incident Records • Service Request records • Stakeholder Notifications	8.5.5 8.7 10.1b 10.2	8.6.1 8.6.2 8.7.3.3	10.1 A16.1	10.1 A5.25 A5.33 A8.15	6.4.4.7	2-5.4.2.3 2-5.4.2.4 2-7.4.2.3 2-7.4.2.4 4-11.4.2.3
	BP.3 Avoid and Resolve Problems Improvement actions are produced from trends and performance monitoring, to avoid potential incidents and problems. Repeating incidents, anomalies and stakeholder feedback are considered for underlying problems. Problems are identified, recorded, analysed and managed to prevent reoccurrence. Stakeholders are informed of the status of the problem. Records of the problems and the action taken are maintained.	• Anomalies • Incident Reports • Measurement and Analysis Data • Stakeholder Feedback	• Problem Reports	10	8.6.3	10 A16.1	10 A5.27 A7.4 A8.15 A8.16	6.4.4.7	2-5.4.2.4 2-7.4.2.4
	BP.4 Escalate Service Requests, Incidents and Problems Service requests, Incidents and problems not resolved are escalated to aid the resolution of the incident or problem, and records are maintained.	• Incident Records • Problem Reports • Service Request records	• Incident Records • Problem Reports • Service Request records	5.1.1a 5.1.1g 5.1.1h 9.3.2c	8.3.2 8.6.1 8.6.2 8.7.3.3	5.1e 9.3c 10.1 A16.1	5.1e 9.3.3 10.1 A5.33	6.4.4.7	2-5.4.2.4 2-6.4.3.8

What is common to these Frameworks?

- They all promote a good Security Posture
- Identify Business Critical Assets and their owners
- Risk Assessment/Gap Assessment – using a Framework
- Implement controls to treat risks/gaps
- Identify accountable Leadership Roles
- Use scorecards – monitor and track progress against desirable outcomes
- Learn from incidents
- Training program for all levels of the organisation



Part 3

SCENARIO

Scenario

- Context - Consider typical Software development company
- Use cloud tools (Atlassian/JIRA/GitLab)
- Develop products
- Have staff working at more than one-site
- Outsource some activities

Information Assets – Software Development Company

- Identify the business-critical information assets and nominate an owner for each

- E.g.
- JIRA – Owner is Development Director
- Developer Laptops – Owner is Development Director
- Source Code - Owner is Development Director

- Owner – Identifies business criticality value of the data (H/M/L)
- Owner - Authorises and reviews access to users
- Owner - Agrees backup frequency with IT

Risk Assessment

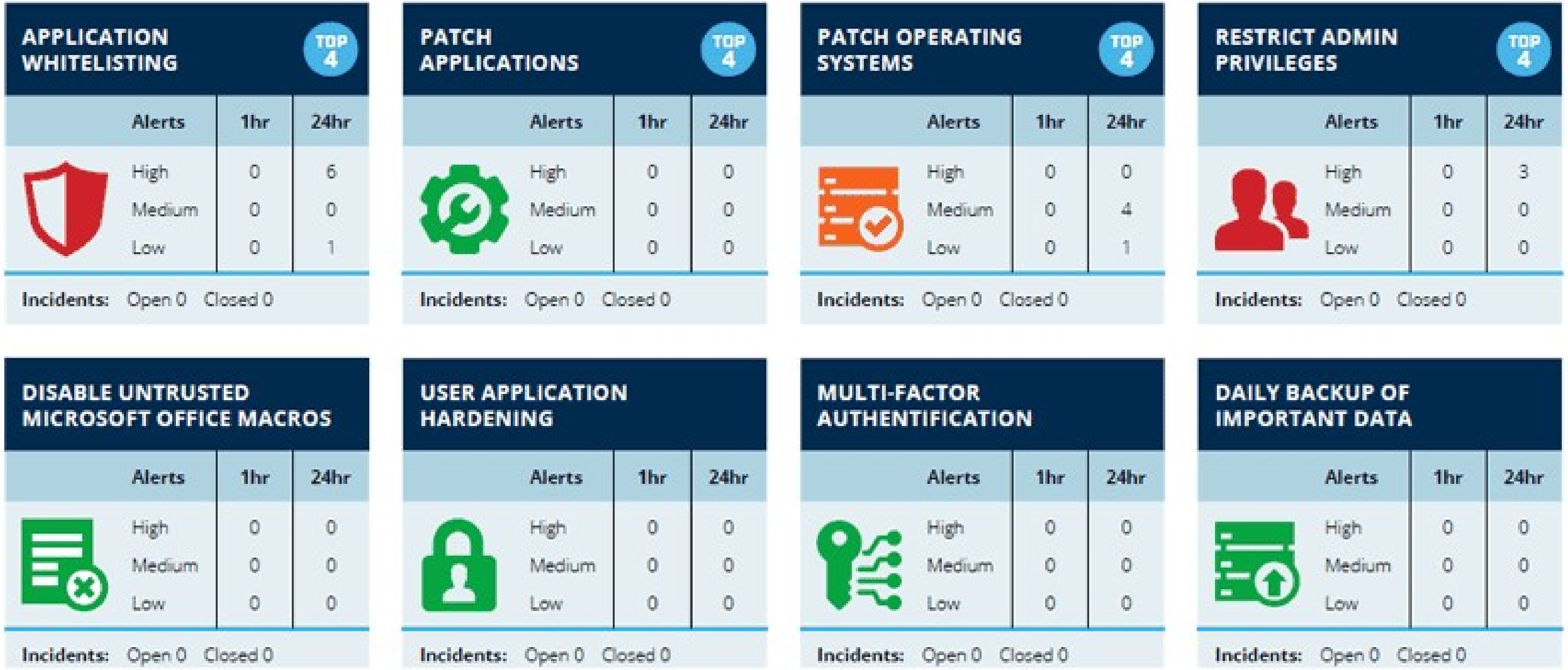
Risk ID	Risk	Control Requirement
1	Unauthorised Access	Acceptable Use Policy, Password Policy, Least privilege, 2FA
2	Corruption/Hardware Failure	Backups
3	Environmental	UPS, Business Continuity Plan, Physical access control
4	Theft/Loss	Staff vetting, encryption, security incident process
5	Malware/ransomware	Firewall, malware protection, secure configuration, vulnerability management
6	User error	Staff security awareness training, security incident process

Leadership, Accountability and Responsibility

Risk ID	Control Requirement	Board	IT	Users	Asset Owner
1	■ Acceptable Use Policy, Password Policy, Least privilege, 2FA	A	C	I	R
2	■ Backups	A	R		C
3	■ UPS, Business Continuity Plan, Physical access control	A	R		C
4	■ Staff vetting, encryption, security incident process	A	R	I	C
5	■ Firewall, malware protection, secure configuration, vulnerability management	A	R		C
6	■ Staff security awareness training, security incident process	A	R	I	C

Scorecards/Dashboards

- Prioritise Security Risks
- Track and monitor progress
- Track and monitor effectiveness of controls



APPLICATION WHITELISTING TOP 4

Alerts	1hr	24hr
High	0	6
Medium	0	0
Low	0	1

Incidents: Open 0 Closed 0

PATCH APPLICATIONS TOP 4

Alerts	1hr	24hr
High	0	0
Medium	0	0
Low	0	0

Incidents: Open 0 Closed 0

PATCH OPERATING SYSTEMS TOP 4

Alerts	1hr	24hr
High	0	0
Medium	0	4
Low	0	1

Incidents: Open 0 Closed 0

RESTRICT ADMIN PRIVILEGES TOP 4

Alerts	1hr	24hr
High	0	3
Medium	0	0
Low	0	0

Incidents: Open 0 Closed 0

DISABLE UNTRUSTED MICROSOFT OFFICE MACROS

Alerts	1hr	24hr
High	0	0
Medium	0	0
Low	0	0

Incidents: Open 0 Closed 0

USER APPLICATION HARDENING

Alerts	1hr	24hr
High	0	0
Medium	0	0
Low	0	0

Incidents: Open 0 Closed 0

MULTI-FACTOR AUTHENTIFICATION

Alerts	1hr	24hr
High	0	0
Medium	0	0
Low	0	0

Incidents: Open 0 Closed 0

DAILY BACKUP OF IMPORTANT DATA

Alerts	1hr	24hr
High	0	0
Medium	0	0
Low	0	0

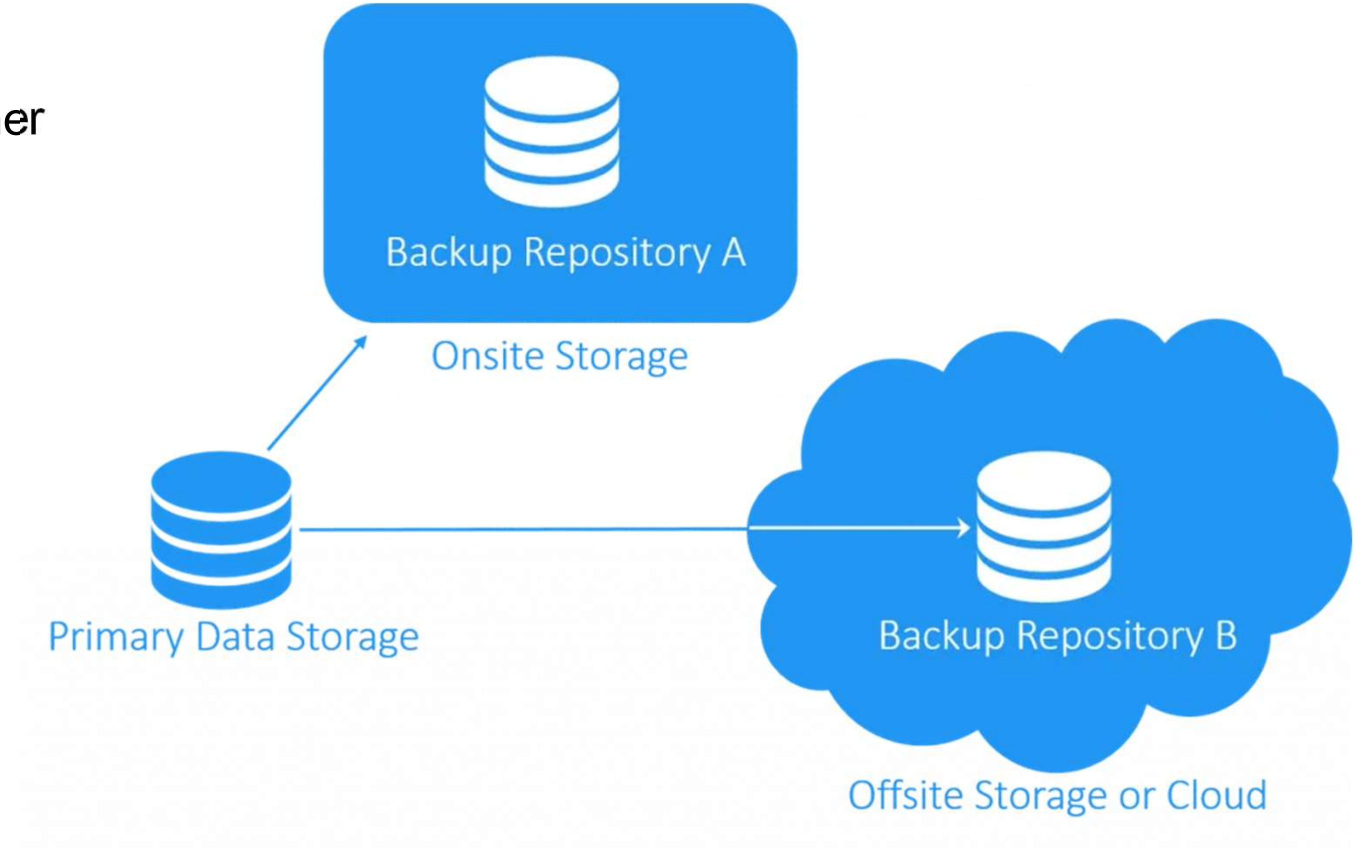
Incidents: Open 0 Closed 0

Risk ID #1 - Unauthorised Access Risks - Treatment

- Password Management - Complex – Three Random Words
- Clear requirements in Acceptable Use Policy
- Use Two-Factor Access wherever possible for Cloud Services
- Least privilege - only provide access needed for role
- Separate Standard User and Administrator accounts

Risk ID #2 - Corruption/Hardware Failure Risk - Treatment

- Backup and Restores
- Frequency agreed with Asset Owner
- Regular restore tests



Risk ID #3 - Environmental Risks - Treatment

- Business Continuity Plan
  - Based on Business Impact Assessment (BIA)
- Business Continuity Plan Test Scenarios.
  - Data Loss/Breach.
  - Power Outage.
  - Network Outage.
  - Physical disruption.

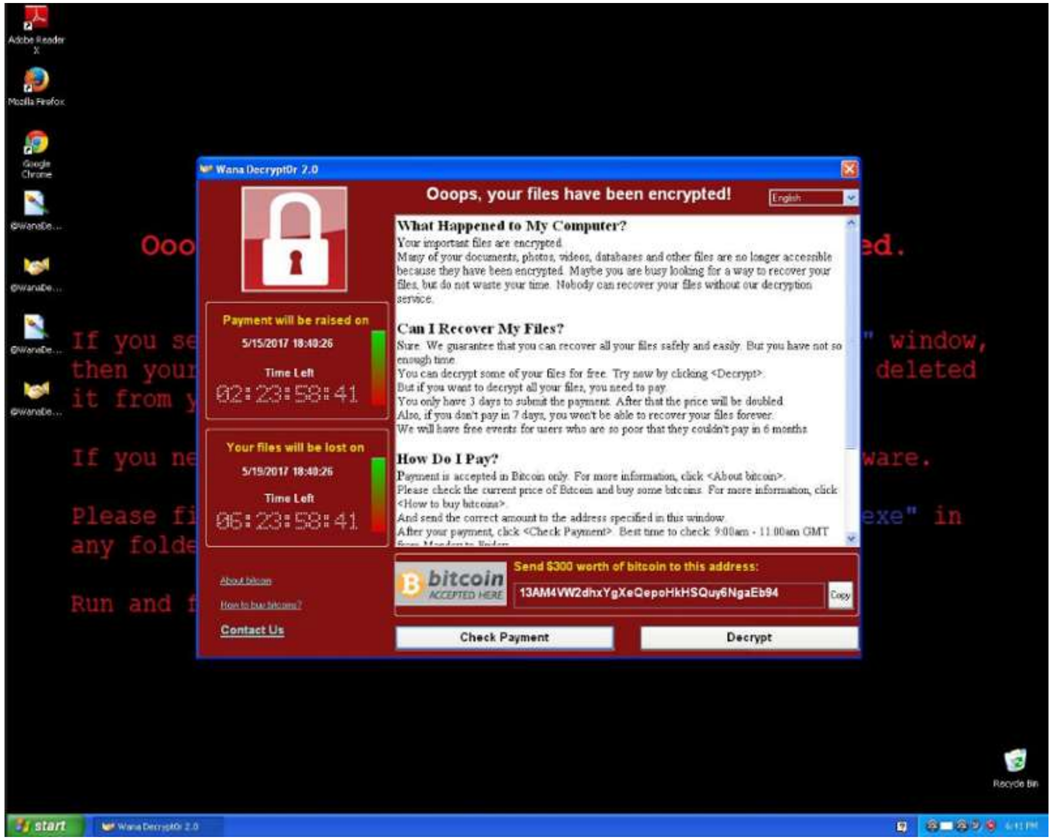
Risk ID #4 - Theft/Loss Risk - Treatment

- Physical controls – Access Control, secure zones, entry controls, encryption, secure disposal, acceptable use policy etc.
- Security incident process
- Learn from incidents
  - Root Cause Analysis

Risk ID #5 - Malware/ransomware risks - Treatment

- Technical Controls
  - Asset discovery
  - Malware protection, patching,
  - Separate User and Admin accounts
  - Vulnerability assessment
  - Intrusion detection

- Monitor/Dashboards
  - Security Information and Event Management (SIEM)
  - Unauthorised access attempts
  - Virus/malware dashboard
  - Firewall open ports
  - Patching status
  - IDS system



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT

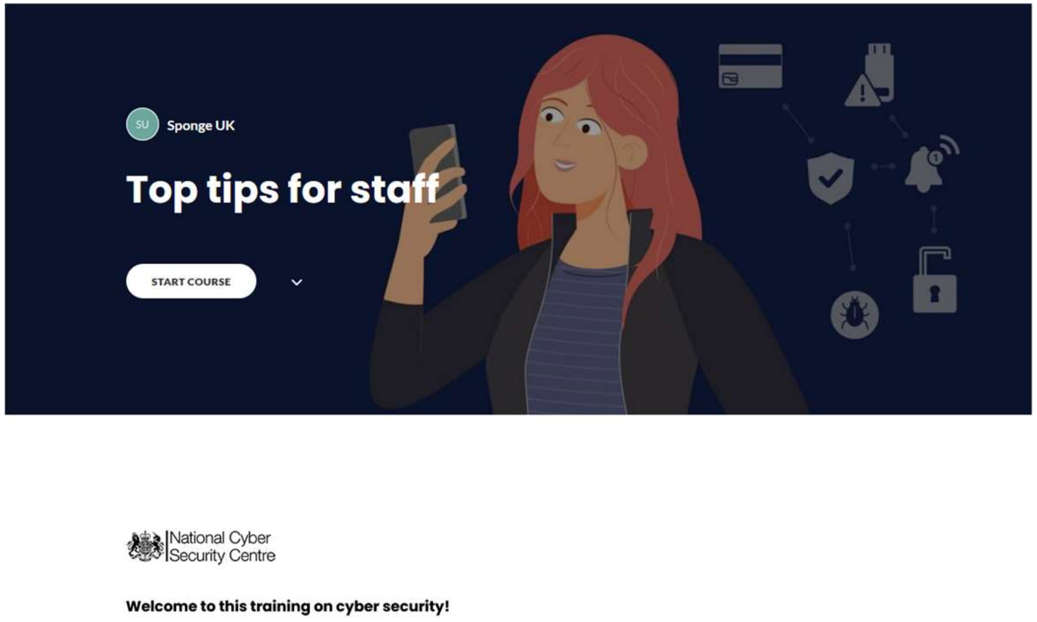
Send $300 worth of bitcoin to this address:

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Risk ID #6 - User error risks - Treatment

- Breaches often occur because of human error and the majority of breaches are the result of unsuspecting, untrained or complacent staff being socially engineered
- Top tips for staff training video is available on NCSC website

- Defending yourself against phishing
- Creating strong passwords
- Securing your devices
- Reporting incidents
- Quiz



Top tips for staff

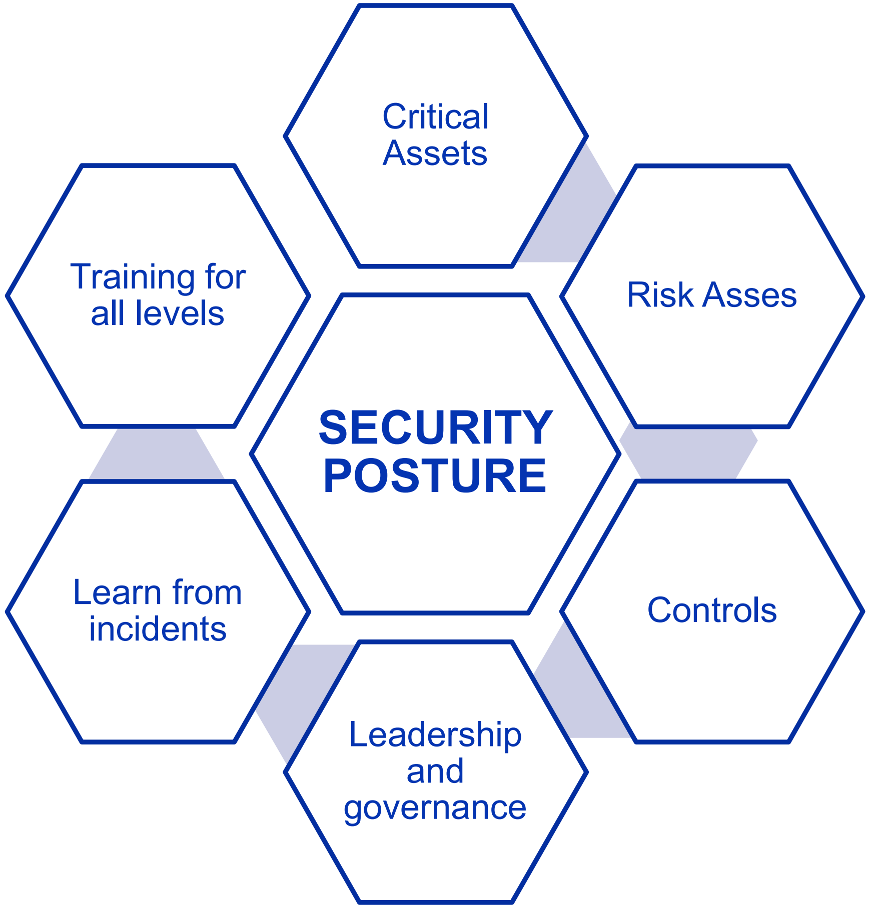
Welcome to this training on cyber security!

Part 4

SUMMARY

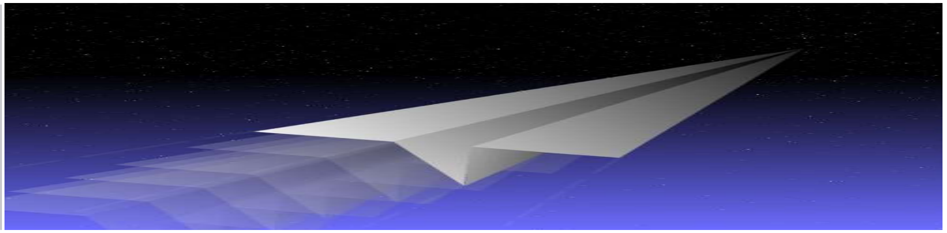
Summary - How can we optimise our Security Posture?

- Identify Business Critical Assets and their **owners**
- Risk Assessment/Gap Assessment – **using a Framework**
- Implement controls to treat risks/gaps – **Involve Asset/Risk Owners**
- Leadership roles, **scorecards to monitor and track progress against desirable outcomes**
- **Learn** from incidents
- Training program **for all levels** of the organisation



DEVELOP CAPABILITY

Thank you



Bal Matu C.Eng MIET CQP FCQI CISA CEH ECSA CPSA

Develop Capability Ltd
www.DevelopCapability.co.uk
bal@DevelopCapability.co.uk

`