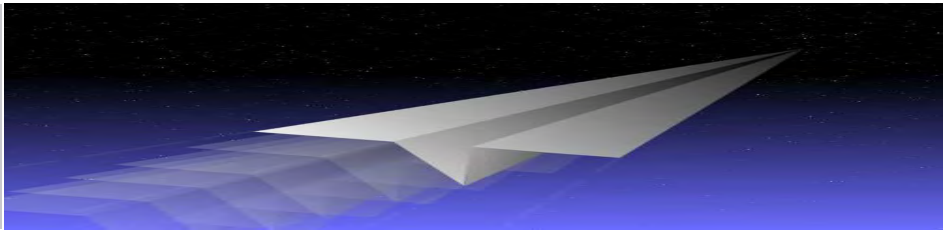
Cyber Security and the importance of your security posture



Bal Matu C.Eng MIET CQP FCQI CISA CEH ECSA

12 May 2022

bal@DevelopCapability.co.uk
www.DevelopCapability.co.uk

Bal Matu

- 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 Lead Auditor
- World Lottery Association Security Control Standard (WLA – SCS) Lead Auditor
- Cyber Essentials Plus Certification Body and Auditor
- EC-Council Certified Ethical Hacker (CEH)
- EC-Council Certified Security Analyst (Practical)
- CREST Registered Penetration Tester
- TickITplus Accredited Training Provider

- www.DevelopCapability.co.uk – Cyber Essentials Certification Body/ISO 27001 Consultancy

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

WEF - Top Short-Term Global Risks

- World Economic Forum Global Risks Report 2022

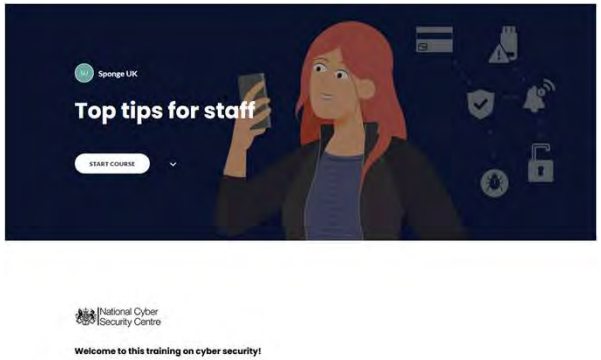
ENISA Threat Landscape 2021 - Prime threats

- **ENISA is the European Union Agency for Cyber Security**
- Compromise through phishing e-mails, and brute-forcing on Remote Desktop Services (RDP) remain the two most common ransomware infection vectors.
- Users are used to the idea of not clicking on suspicious e-mails, but still are not aware that they can also be phished via text messages or phone calls.
- The Phishing-as-a-Service (PhaaS) business model is gaining prevalence.
- https://www.enisa.europa.eu

Figure 1: ENISA Threat Landscape 2021 - Prime threats

What is Security Posture?

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



Part 2

SECURITY FRAMEWORKS

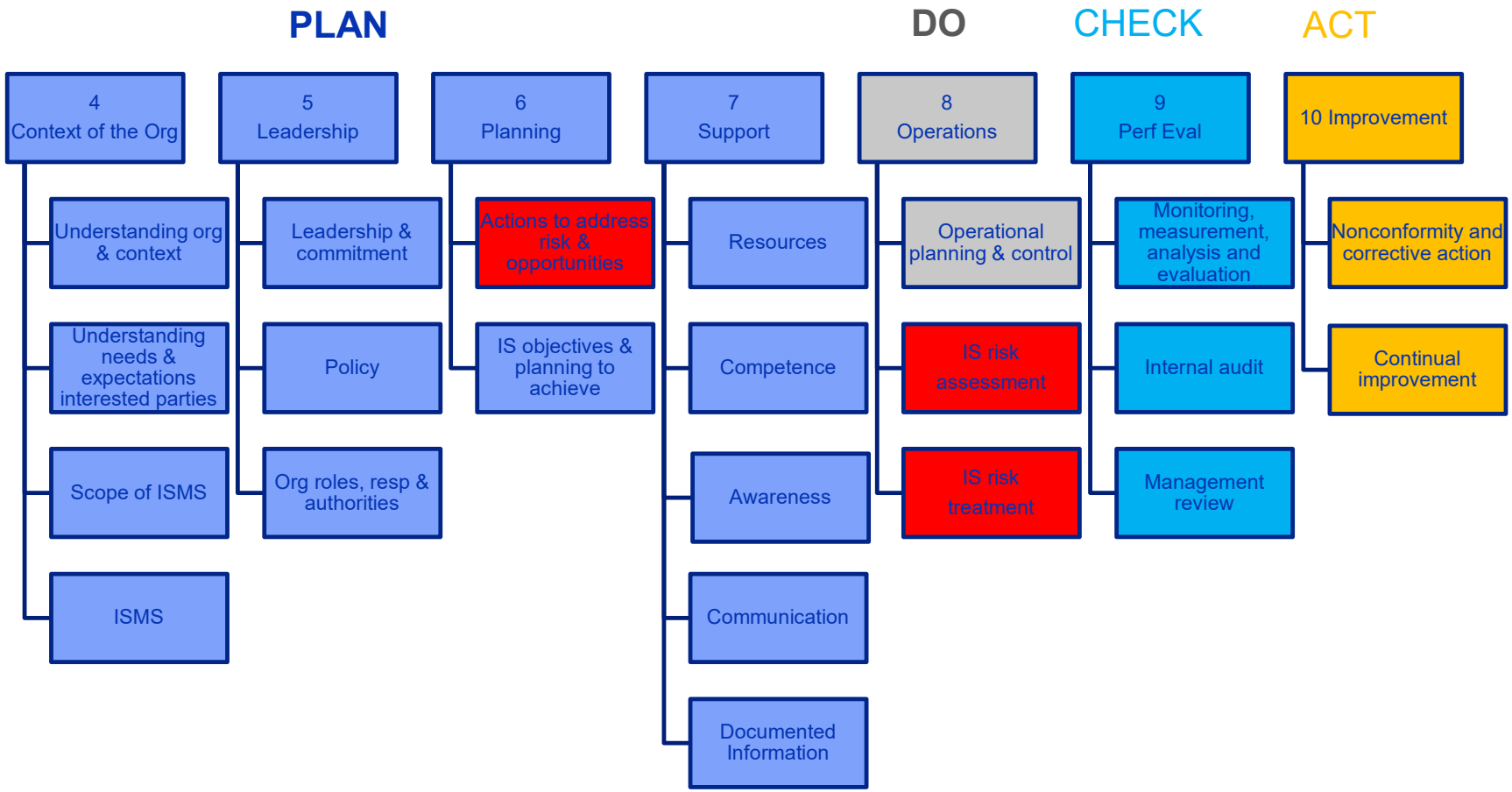
Many Frameworks

- 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

- Focus is on risk from internet, controls are mandated
  - Firewalls
  - Secure configuration
  - User access control
  - Malware protection
  - Security update management/patching

ISO 27001:2013



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 Self Assessment) and an independently tested level (CE Plus)

ISO 27001:2013

- Risk Assessment – By Organisation being assessed
- Controls – 114 technical controls divided into 14 categories (plus section 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 – Admin use of 2FA
- User/Admin account separation

ISO 27001:2013

- 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 114 controls listed in Annex A
- Demonstrate the effectiveness of the management system and justified controls using objective evidence

NIST - Cybersecurity Framework

1 IDENTIFY

Identify and control who has access to your business information

Conduct background checks

Require individual user accounts for each employee

Create policies and procedures for cybersecurity

2 PROTECT

Limit employee access to data and information

Install Surge Protectors and Uninterruptible Power Supplies (UPS)

Patch your operating systems and applications routinely

Install and activate software and hardware firewalls on all your business networks

Secure your wireless access point and networks

Set up web and email filters

Use encryption for sensitive business information

Dispose of old computers and media safely

Train your employees

3 DETECT

Install and update anti-virus, anti-spyware, and other anti-malware programs

Maintain and monitor logs

4 RESPOND

Develop a plan for disasters and information security incidents

5 RECOVER

Make full backups of important business data and information

Continue to schedule incremental backups

Consider cyber insurance

Make improvements to processes/ procedures/ technologies

https://www.nist.gov

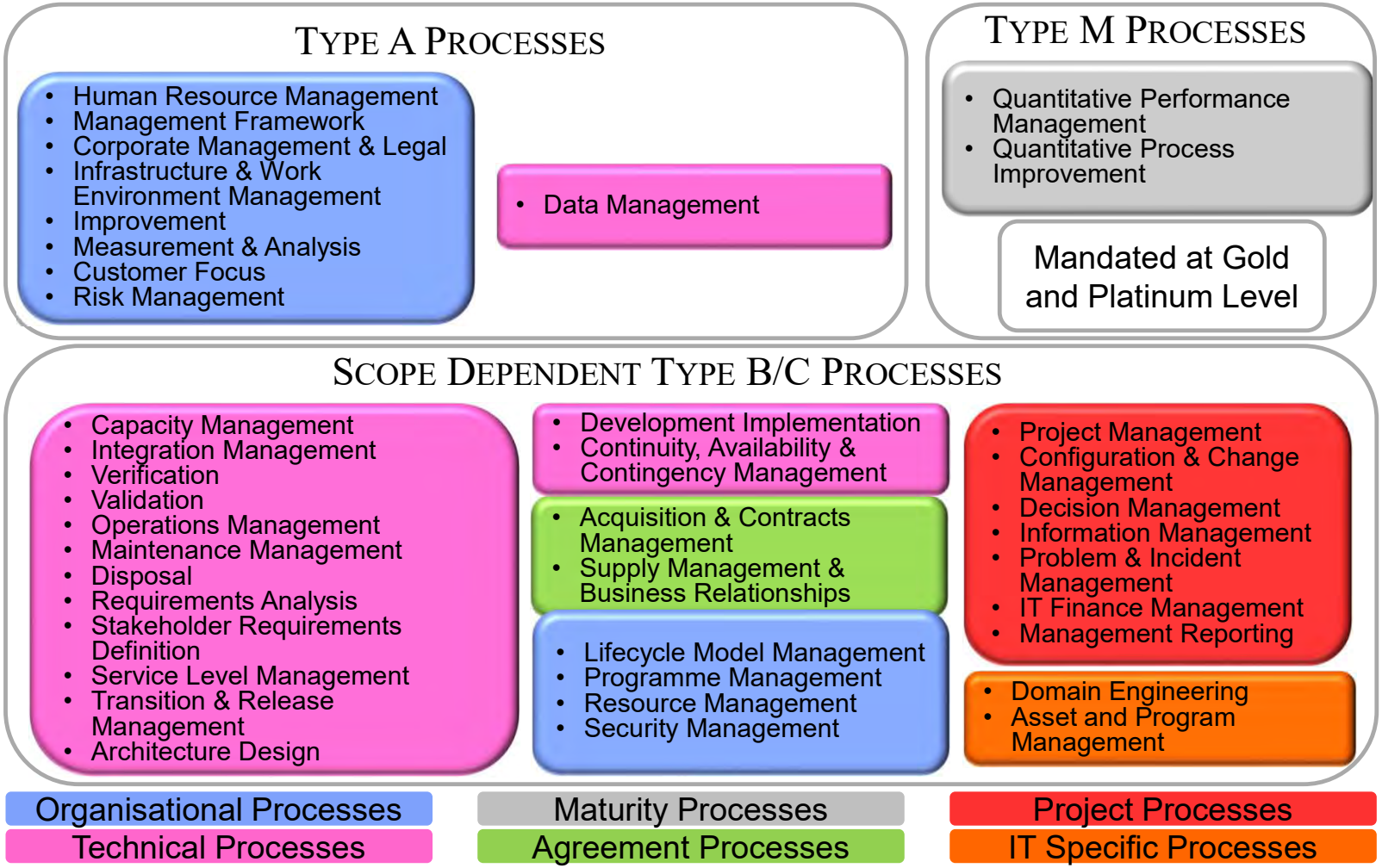
NIST - CSF

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

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

TickITplus BPL Processes



TickITplus Processes

DEVELOP CAPABILITY

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

TickIT*plus* – Base Process Library

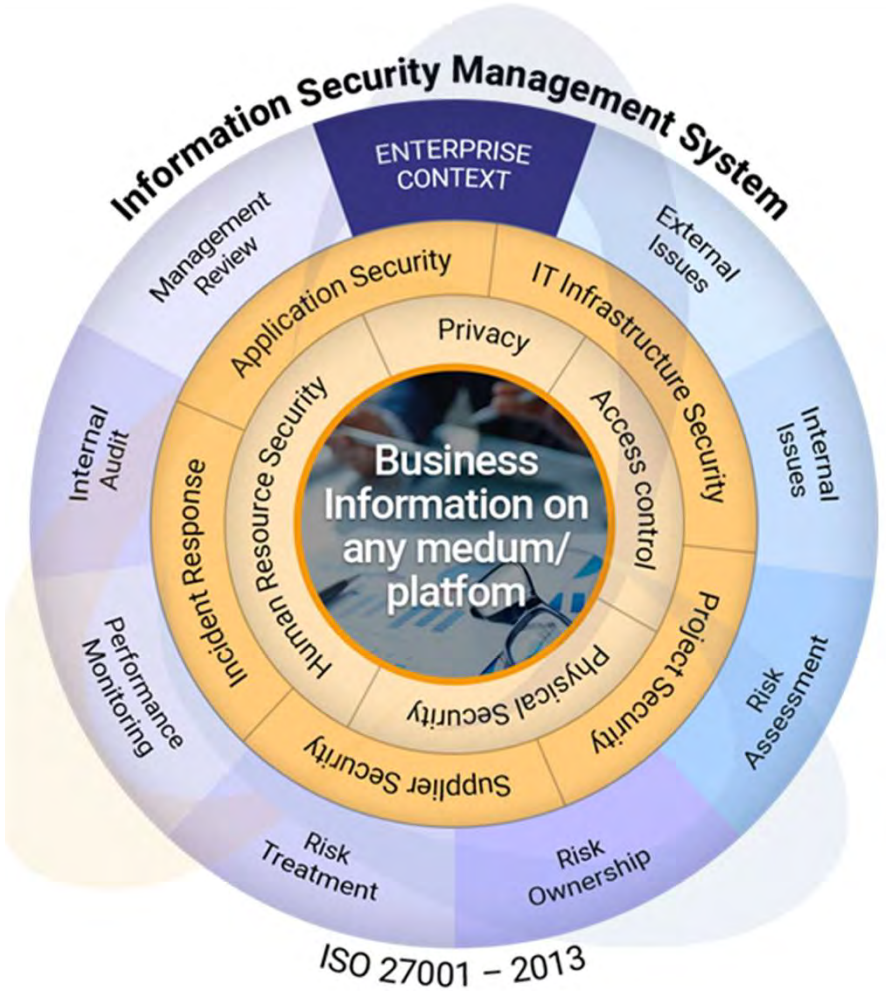
PRJ.5 Problem and Incident Management

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	v4r1

Process Outcome	Process Base Practices	Input Work Products	Output Work Products	ISO 9001:15	ISO 20000:11	ISO 20000:18	PAS 754:14	ISO 27001:13	ISO 26262:11
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, 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	4.3.1 8.1 8.2	4.4 8.6.3		4.4 7.5 A5.1 A16.1	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, 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	4.3.3 6.2 8.1	8.6.1 8.6.2 8.7.3.3	PR.07	10.1 A16.1	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	4.3.3 6.2 7.1 8.2	8.6.3	PR.07	10 A16.1	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	4.3.3 7.1 8.2		PR.07	5.1e 9.3c 10.1 A16.1	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

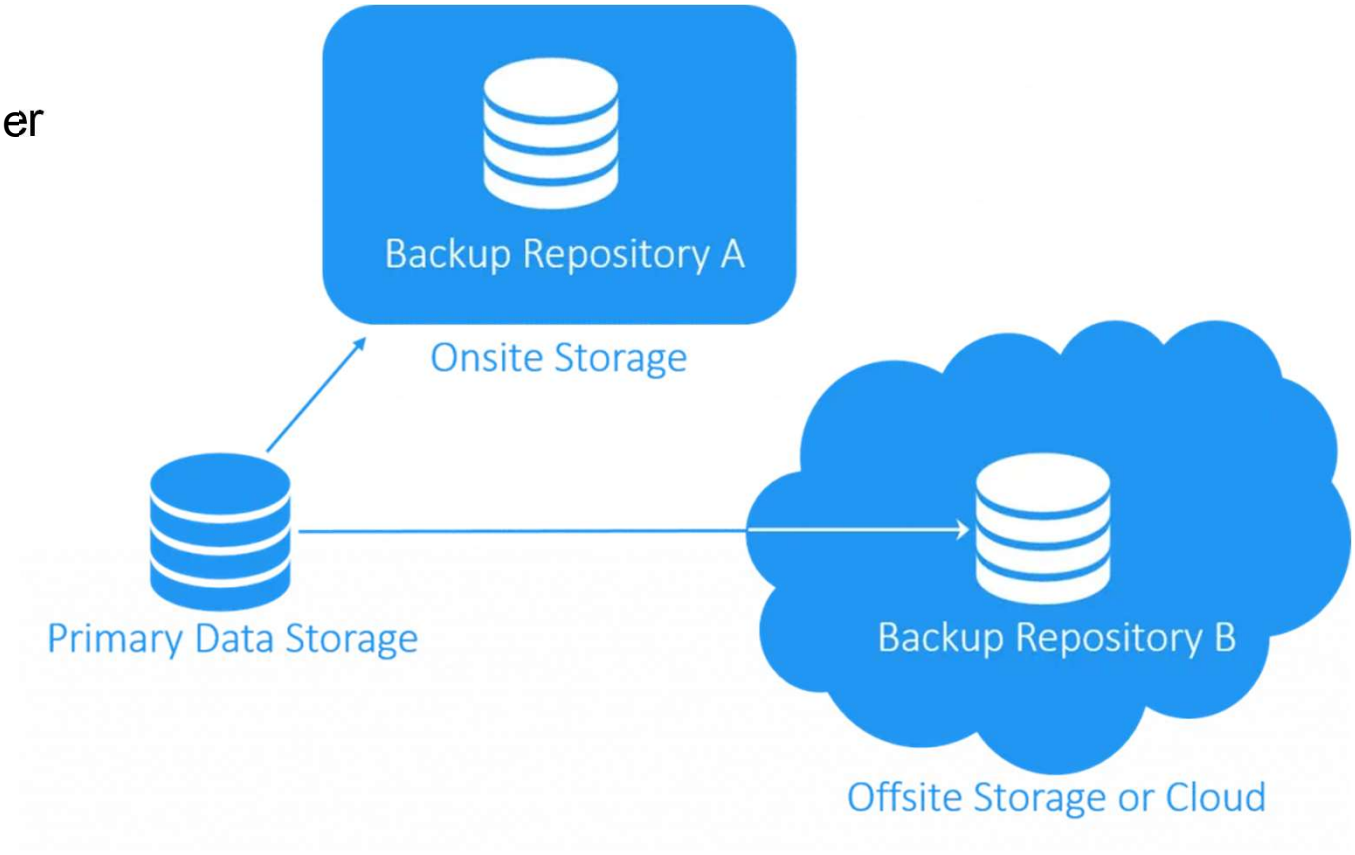
- Prioritise Security Risks
- Track and monitor progress
- Track and monitor effectiveness of controls

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

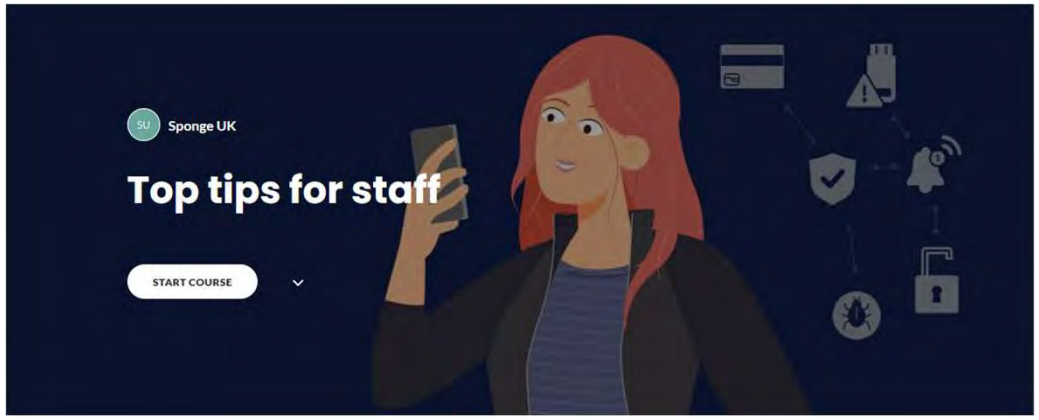
Risk ID #5 - Malware/ransomware risks - Treatment

- 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

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



National Cyber Security Centre

Welcome to this training on cyber security!

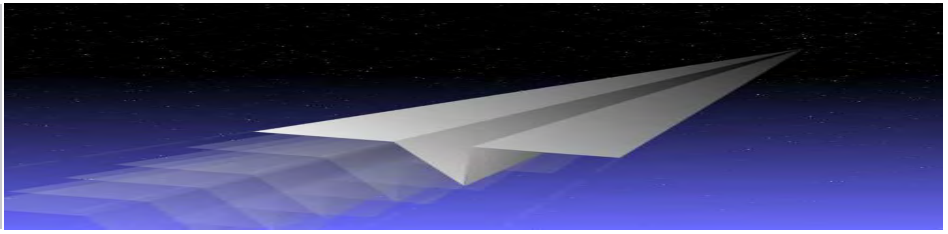
Part 4

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

Thank you



Bal Matu C.Eng MIET CQP FCQI CISA CEH ECSA
Develop Capability Ltd
www.DevelopCapability.co.uk
bal@DevelopCapability.co.uk

`