Strengthening Security in the Public Sector

Webinar / Short Demo

Presented By:

Gerard Joyce, CTO, CalQRisk

Jessicia Clarke, Solutions Specialist, CalQRisk

Thursday 3rd October 2024

Outline

- What’s in the Public Sector Cyber Security Baseline Standard
- What elements are covered by NIST 2 already
- Getting it done

> Most people want security in this world, not liberty
>
> ***H.L. Mencken***

Who we are and what we do

- Experienced Risk & Compliance Professionals
- Members of IRM, IOB, CI (ACOI), IoD, ACCA, ISACA, ….
- We Make A Governance, Risk & Compliance Solution called CalQRisk
  - A cloud-based software solution
- Risk Advisory Service
  - In-house / Virtual Training, Strategic Risk Alignment, Risk Management Framework
- CalQRisk is used by 3,000+ users in regulated firms and others

  Including: Financial Services organisations. Not-For-Profit sector and Public sector

PSCSBS

Full title:

Public Sector Cyber Security Baseline Standards

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

Public Sector Cyber
Security Baseline Standards

November 2021

Revision 1 November 2022

Prepared by the Department of
the Environment, Climate and Communications
gov.ie

Latest: November 2022

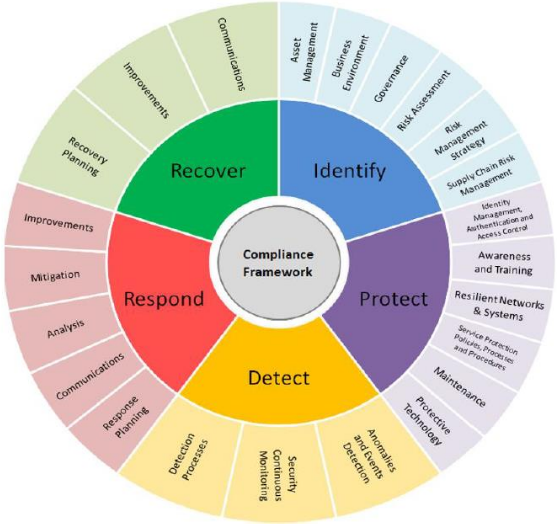
Previous: November 2021

PSCSBS

Who is it for:

- Applies to all Public Service Bodies
- Aimed at the ICT department /governance committee

PSCSBS



Structure:

- Aligned with NIST (Ver 1.1)
- Comprises 5 Themes

Identify	(Cyber Security Governance Processes)	9 sub-sections, 18 Reqs
Protect	(Cyber Security Protection Processes)	14 sub-sections, 58 Reqs
Detect	(Cyber Security Detection Processes)	7 sub-sections, 7 Reqs
Respond	(Cyber Security Respond Processes)	7 sub-sections, 7 Reqs
Recover	(Cyber Security Recover Processes)	6 Sub-sections, 14 Reqs

IDENTIFY / GOVERN

Understand the structures, policies and processes required to manage cybersecurity risk to systems, assets, data and capabilities.

1. Corporate Responsibility
2. Management of ICT Security Policies and Processes
3. Identify and Manage ICT Security Risks
4. Cyber Awareness Training
5. System Information
6. Physical and Environmental Access Control
7. Key Operational and Essential Services
8. Access Control Procedures
9. Joiners, Movers, Leavers Policy

PROTECT / IDENTIFY

Develop and implement the appropriate and proportionate cyber security measures to deliver and protect the organisations essential services and systems

1. Access Control and Responsibility
2. Identification and Authentication
3. ICT Digital Resources
4. Digital Resources - Active Directory
5. Digital Resources - Data
6. Digital Resources - Network
7. Digital Resources – Logging / Auditing
8. Digital Resources – End Point Devices
9. Email Security
10. Secure Web and Infrastructure Config
11. User Account Protection
12. Multi-Factor Authentication
13. Administrator Training
14. Security by Design

DETECT

Develop and implement the appropriate capabilities to identify, detect and defend against a cybersecurity event that may have the potential to affect essential services and systems.

1. Event Capture
2. Cyber Security Incidents
3. Log Retention Period Legal
4. Log Retention Period Malicious Activity Detections
5. CNI Protection
6. Monitoring Controls
7. Anomalous Activity Detection

RESPOND

Develop and implement the appropriate activities, prioritised through the organisations risk management process to take action to contain and minimise the impacts relating to a cybersecurity event.

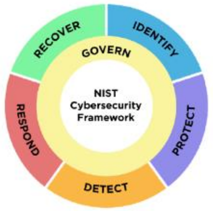
1. Incident Recording (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned)
2. Communications Plans
3. Data Obligations
4. Cyber Incident Response Plan Review
5. Mitigation Measures on Detections
6. Post Incident Sharing
7. Post Incident Lessons Learned

RECOVER

Develop and implement the appropriate capabilities, prioritised through the organisations risk management process, to restore essential services that were affected by a cybersecurity event.

1. Recovery Points
2. Disaster Recovery Plan
3. Disaster Recovery Plan Practice
4. Post Incident
5. Periodic Review
6. Lessons Learned Process

NIST 2.0



Full title:

The NIST cybersecurity Framework (CSF) 2.0

Latest: February 26, 2024

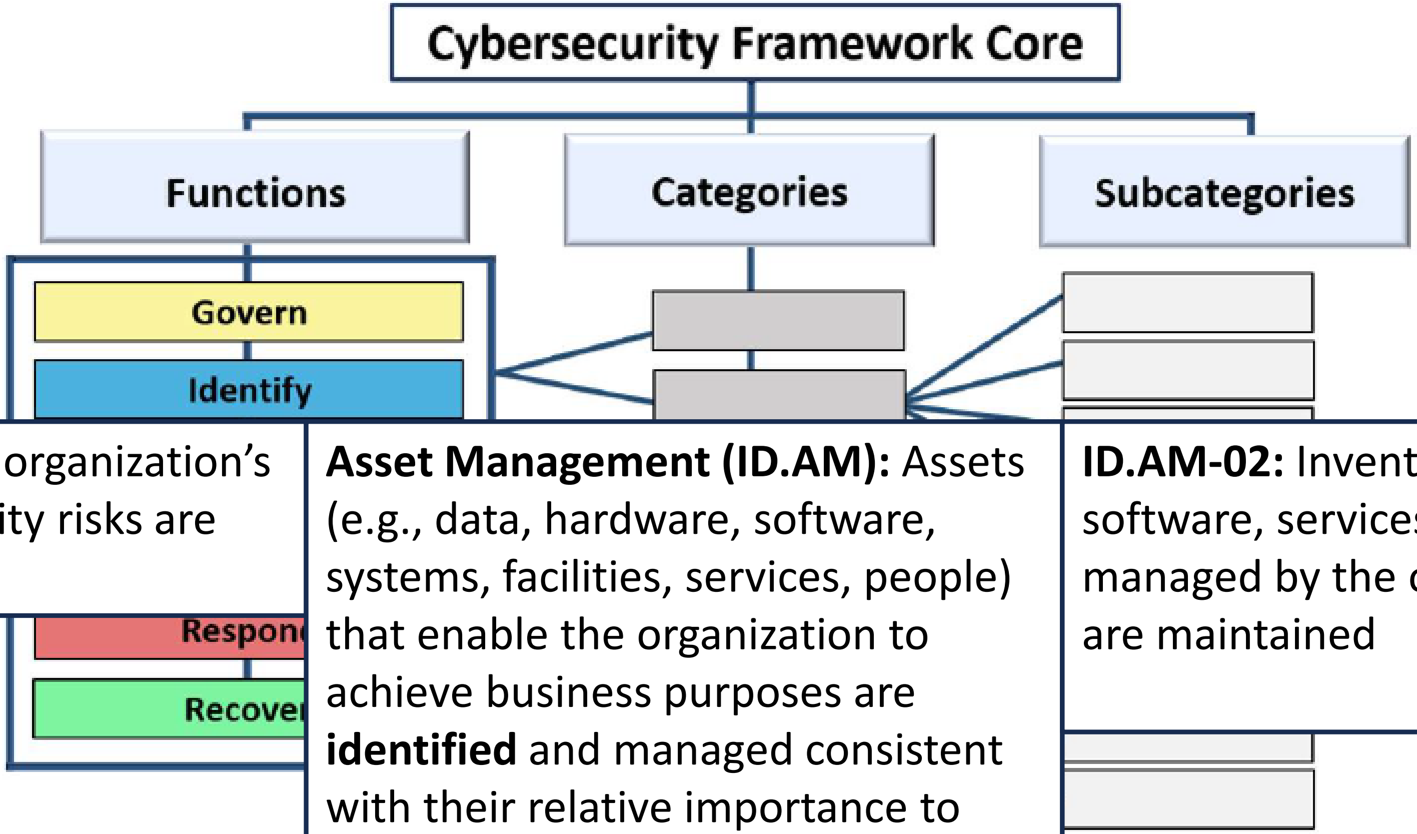
Previous: Ver 1.1 April 16 2018

NIST 2.0

80-85%

50-60%

Structure:



IDENTIFY (ID): The organization's current cybersecurity risks are understood

Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are **identified** and managed consistent with their relative importance to organizational objectives and the organization's risk strategy

ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained

Getting it Done

Over to Jess to demonstrate how using CalQRisk will support you in Getting it Done!

Questions ?

gjoyce@calqrisk.com

Linkedin.com/company/calqrisk

Twitter.com/calqrisk

CalQRisk