Cybersecurity standards for the public sector - which one?

Presented By:

Gerard Joyce, CTO, CalQRisk

Tuesday 21st May 2024

Outline

- What’s new in 27001:2022
- What’s new in NIST 2.0
- What’s in the Public Sector Cyber Security Baseline Standard
- What’s in Cyber Essentials 3.1
- How do they compare?

“

You should shoot for high standards, and believe they’re obtainable

Buster Posey

”

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

ISO 27001

Full title:

Information security, cybersecurity and privacy protection — Information security management systems — **Requirements**

Latest: 27001:2022

Previous 27001:2013

ISO 27001

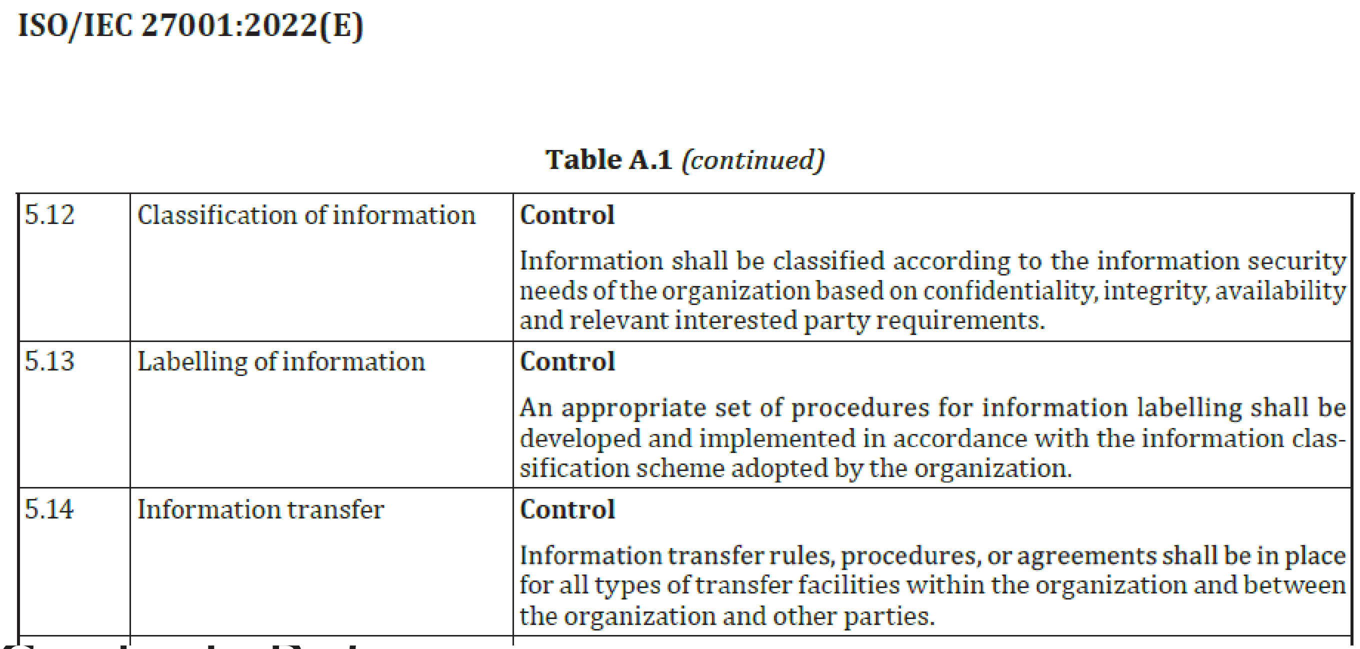
Who is it for:

- ➢ Chief Information Security Officers (CISOs)
- ➢ Cyber security risk analysts/advisors
- ➢ Information security consultants
- ➢ Risk managers in compliance and information security

ISO 27001

Structure:

- Aligned with ISO format for Management System standards
  - 4. Context of the Organisation
  - 5. Leadership
  - 6. Planning
  - 7. Support
  - 8. Operation
  - 9. Performance Evaluation
  - 10.Improvement



ISO/IEC 27001:2022(E)

Table A.1 *(continued)*

5.12	Classification of information	**Control** Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.
5.13	Labelling of information	**Control** An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
5.14	Information transfer	**Control** Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.

- Annex A Information Security Controls Reference

ISO 27001

Changes / What’s New

- Number of controls in Annex reduced from 114 to 93
- Merged 57 into 24
- 11 new controls added, 3 removed, 23 renamed
- Controls grouped differently (were in 14 domains, now in 4 themes)
  - People (8 controls)
  - Organizational (37 controls)
  - Technological (34 controls
  - Physical (14 controls)

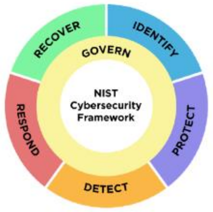
ISO 27001

The 11 New Controls:

➢ A.5.7	Threat Intelligence
➢ A.5.23	Information security for use of cloud services
➢ A.5.30	ICT readiness for business continuity
➢ A.7.4	Physical security monitoring
➢ A.8.9	Configuration Management
➢ A8.10	Information Deletion
➢ A.8.11	Data Masking
➢ A.8.12	Data Leakage Prevention
➢ A.8.16	Monitoring Activities
➢ A.8.23	Web Filtering
➢ A.8.28	Secure Coding

CalRisk

NIST 2.0



Full title:

The NIST cybersecurity Framework (CSF) 2.0

Latest: February 26, 2024

Previous: Ver 1.1 April 16 2018

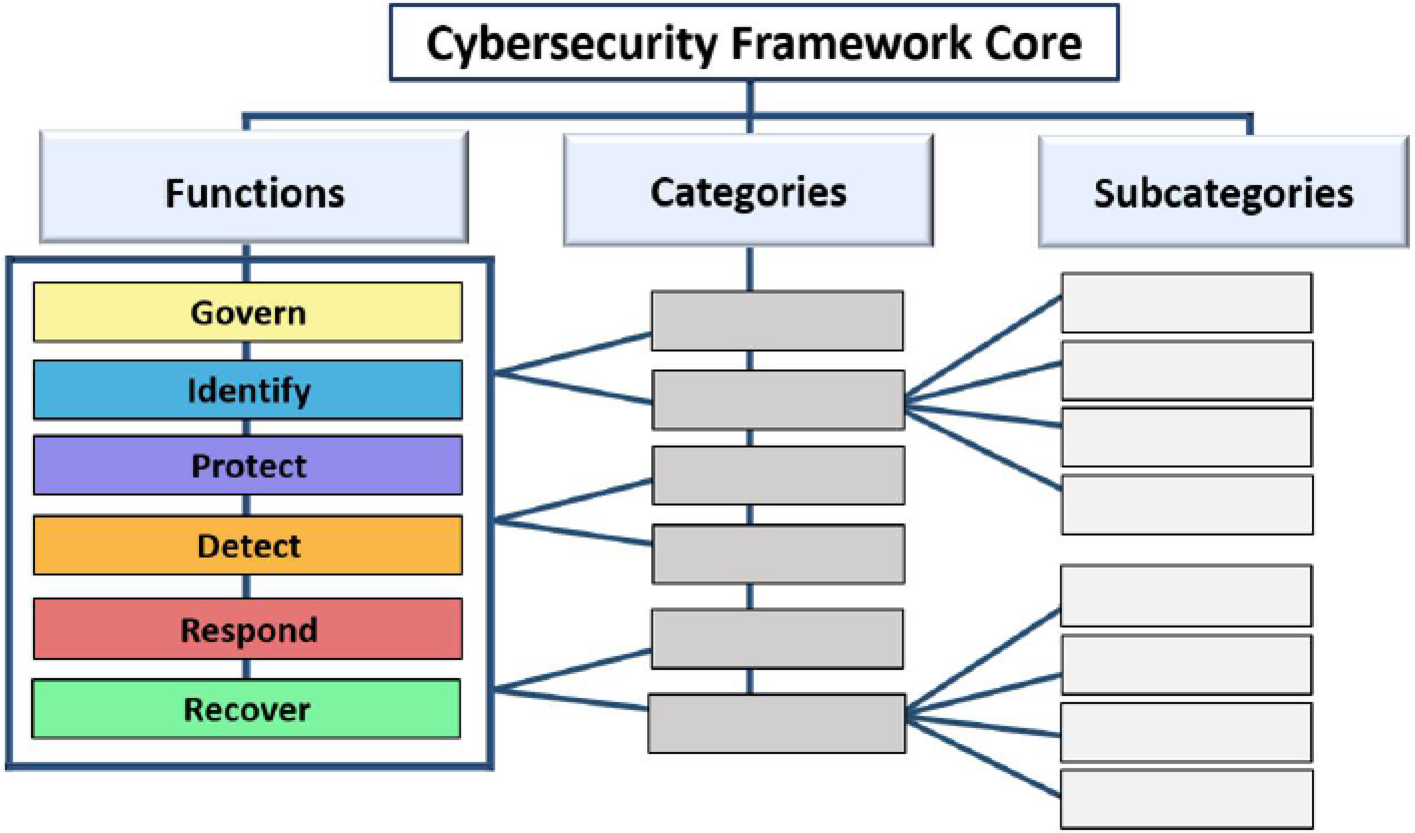
NIST 2.0

Who is it for:

- Industry
- Government Agencies
- Other Organisations

NIST 2.0

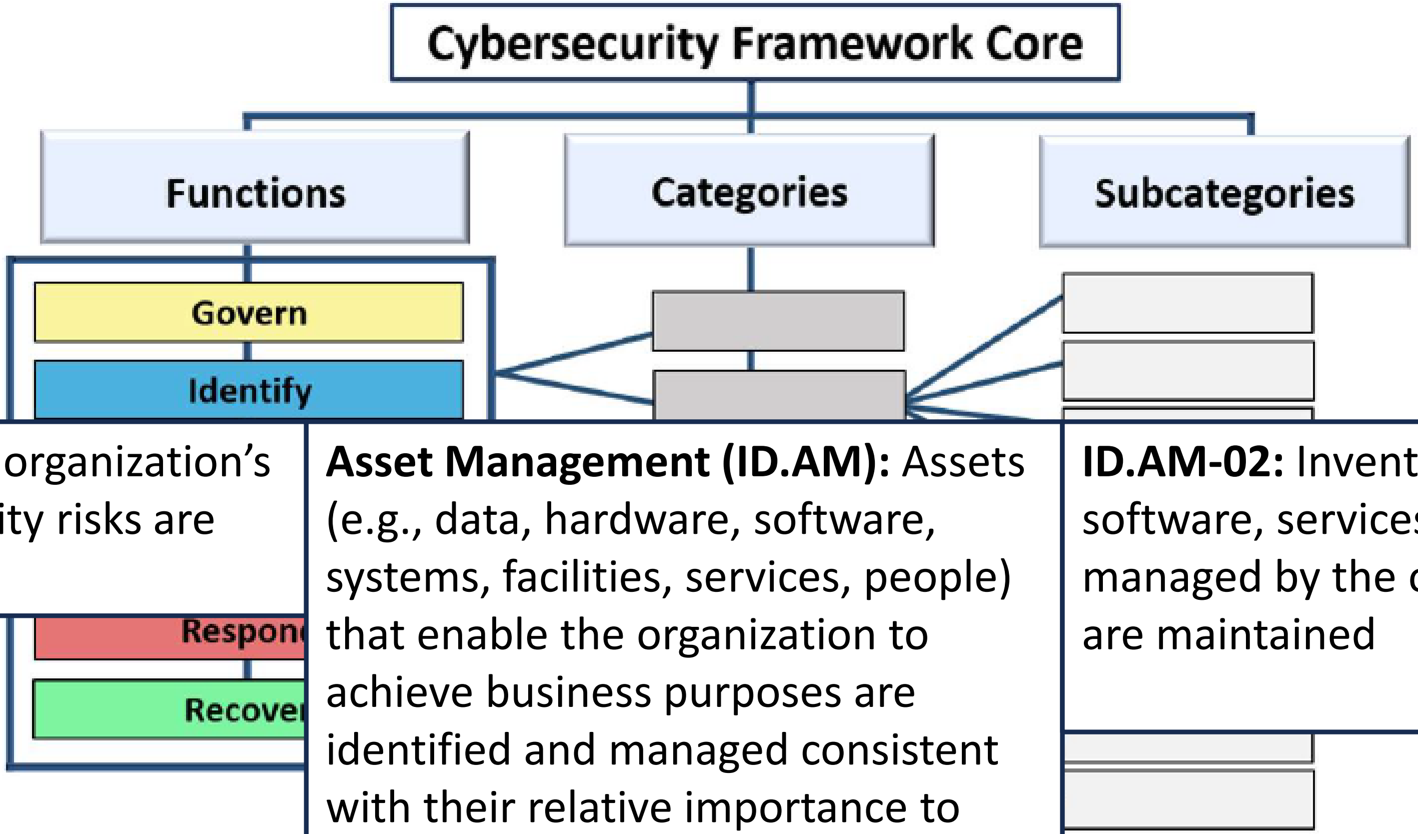
Structure:



The CSF *describes* desired outcomes that are intended to be understood by a broad audience,

NIST 2.0

Structure:



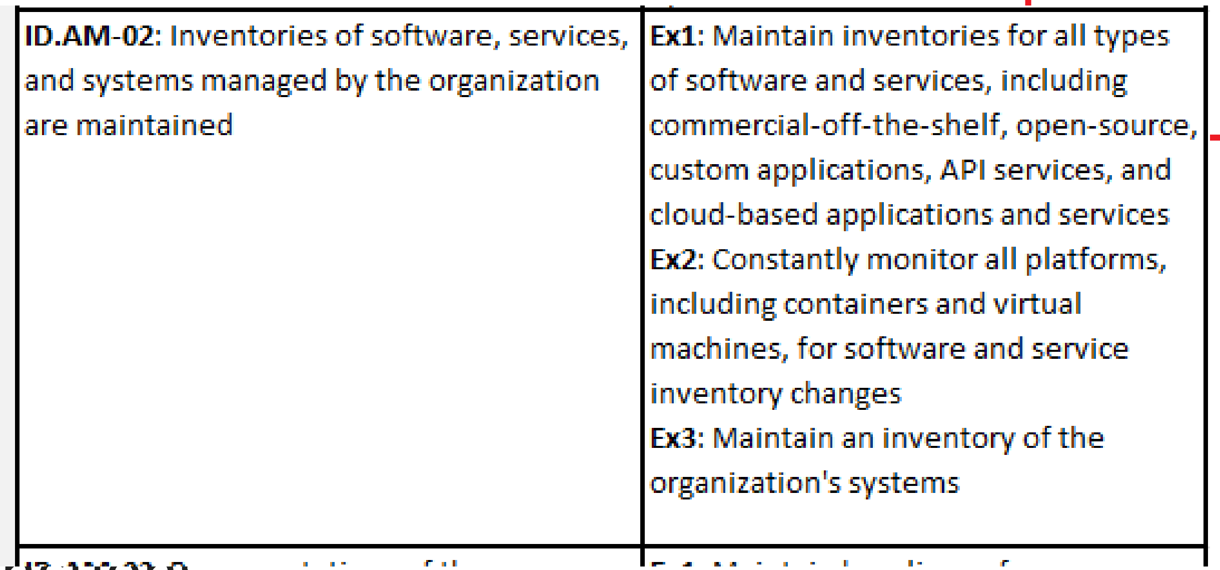
IDENTIFY (ID): The organization’s current cybersecurity risks are understood

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

NIST 2.0

Changes / What's New



ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained	**Ex1:** Maintain inventories for all types of software and services, including commercial-off-the-shelf, open-source, custom applications, API services, and cloud-based applications and services **Ex2:** Constantly monitor all platforms, including containers and virtual machines, for software and service inventory changes **Ex3:** Maintain an inventory of the organization's systems

- ➢ Added 1 function, "Govern", now 6 Functions
- ➢ 22 Categories, down from 23, 106 sub-categories, down from 108
- ➢ Greater emphasis on integrating cybersecurity into business strategy
- ➢ Managing Third Parties / Supply Chain risk now a key consideration
- ➢ Includes many references to other frameworks (e.g. Secure Software Development Framework)
- ➢ Added "Implementation Examples"
- ➢ Added "Improvement" category to the Identify function … applies to all areas.

CalRisk

PSCSBS

Full title:

Public Sector Cyber Security Baseline Standards

Latest: November 2022

Previous: November 2021

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

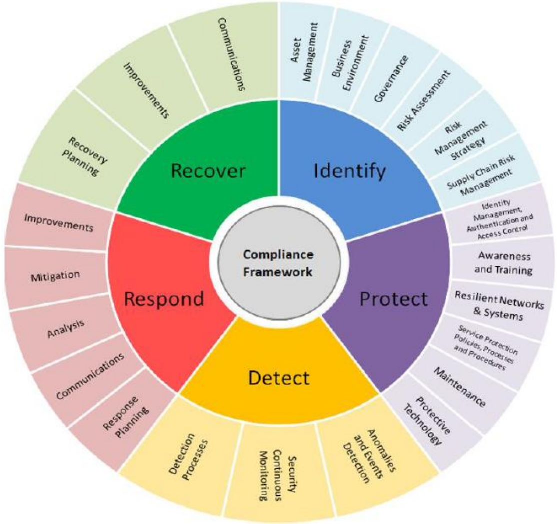
Prepared by the Department of
the Environment, Climate and Communications
gov.ie

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

PSCSBS

What's in it?

CIRP will use commonly known processes…: Preparation, Identification, Containment, Eradication, Recover and Lessons Learned

- 5 Themes, 42 Subsections, 104 high-level requirements / measures
- The 104 high level requirements translate into ~ 222 detail Reqs
  - Shown as "Guidance Notes", but language mostly indicates "expected"
- 40 of these are specific to the PSCSBS and do not appear elsewhere
- Some are at a detail level. E.g. detail section in your CIRP
- Cyber Incident Response Plan Checklist
- Links to Useful Resources

Cyber Essentials

Full title:

Cyber Essentials: Requirements for IT infrastructure v3.1

Latest: April 2023

Previous: January 2023 (3.0)

First Version: June 2014

Cyber Essentials

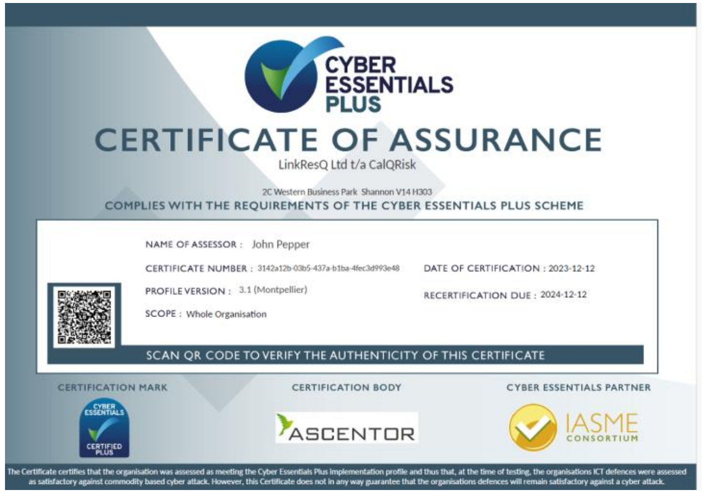
Who is it for:

- Applies to all organisations, any size, any sector
- Required if bidding for UK government contracts
- To protect against common online security threats

Cyber Essentials

Structure:

- Comprises 5 Technical Control Themes
  - Firewalls
  - Secure Configuration
  - Security update Management
  - User Access Control
  - Malware Protection
- Covers the IT infrastructure
- Evidence of actual working controls



CYBER ESSENTIALS PLUS

CERTIFICATE OF ASSURANCE

LinkResQ Ltd t/a CalQRisk

2C Western Business Park Shannon V14 H303

COMPLIES WITH THE REQUIREMENTS OF THE CYBER ESSENTIALS PLUS SCHEME

NAME OF ASSESSOR : John Pepper

CERTIFICATE NUMBER : 3142a12b-03b5-437a-b1ba-4fec3d993e48

DATE OF CERTIFICATION : 2023-12-12

PROFILE VERSION : 3.1 (Montpellier)

RECERTIFICATION DUE : 2024-12-12

SCOPE : Whole Organisation

SCAN QR CODE TO VERIFY THE AUTHENTICITY OF THIS CERTIFICATE

CERTIFICATION MARK: CYBER ESSENTIALS CERTIFIED PLUS

CERTIFICATION BODY: ASCENTOR

CYBER ESSENTIALS PARTNER: IASME CONSORTIUM

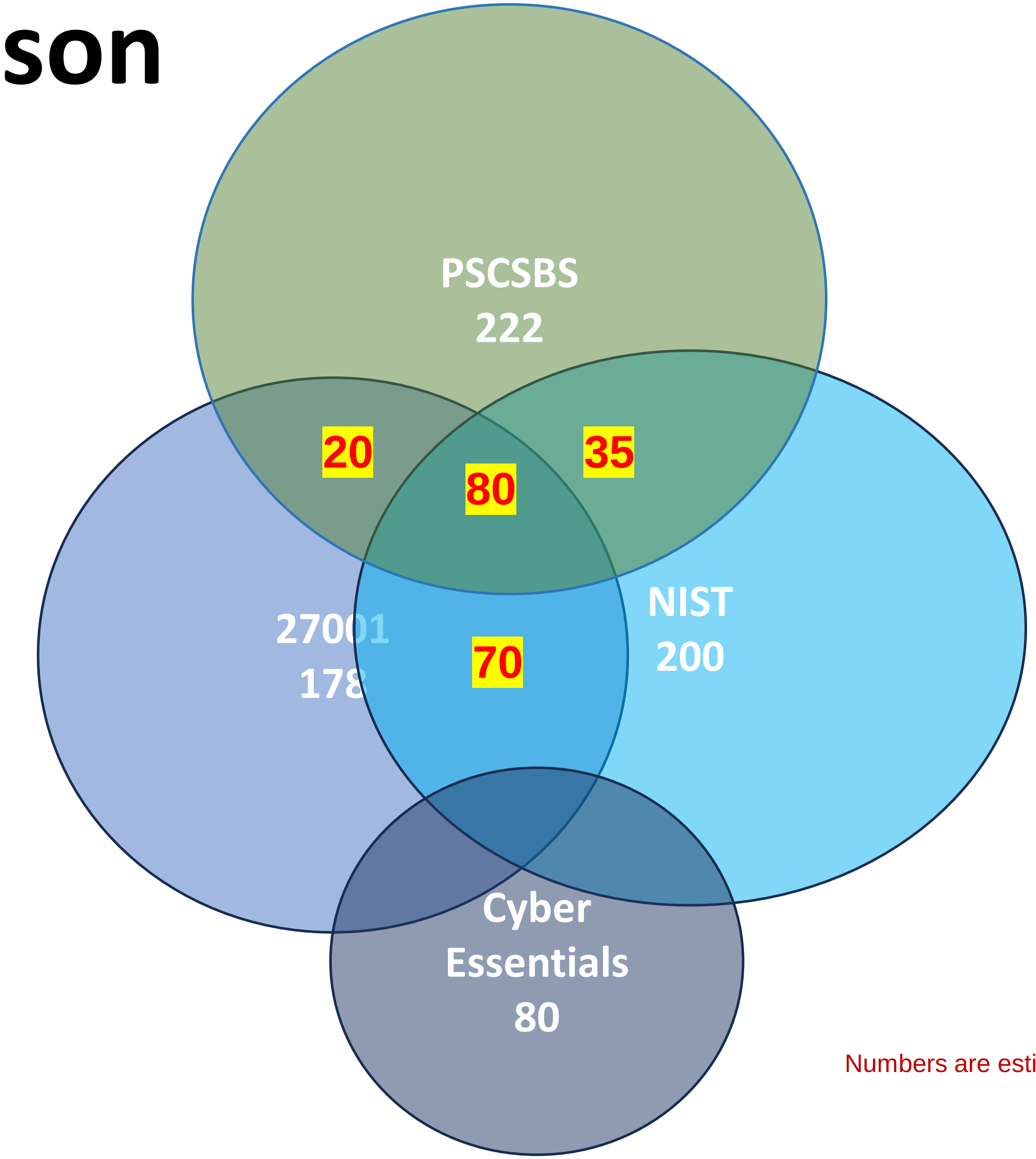
The Certificate certifies that the organisation was assessed as meeting the Cyber Essentials Plus implementation profile and thus that, at the time of testing, the organisations ICT defences were assessed as satisfactory against commodity based cyber attack. However, this Certificate does not in any way guarantee that the organisations defences will remain satisfactory against a cyber attack.

Cyber Essentials

What's in it

- Comprises 5 Technical Control Themes
  - 35 High Level Requirements
  - 80 Detail requirements
- Cyber Essentials Certification based on Questionnaire
- Cyber Essentials Plus Certification
- Cyber Essentials Readiness Toolkit with links to guidance

Comparison



Numbers are estimates

Questions ?

gjoyce@calqrisk.com

Linkedin.com/company/calqrisk

Twitter.com/calqrisk

CalQRisk