



Cybersecurity standards - which one?

Presented By:

Gerard Joyce, CTO, CalQRisk

Tuesday 11th June 2024

Outline



- Some Statistics
- What's new in 27001:2022
- What's new in NIST 2.0
- What's in Cyber Essentials 3.1
- How do they compare?

66

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

Buster Posey

99

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, Housing Associations, Charities and Public sector

Some Statistics

Top threat vectors



- 45% of experts identify cyber incidents as the top cause of business disruption (Cobalt)
- Misconfiguration ranks as 2024 top threat vector (Splunk Report)
- Ransomware affected 66% of organisations in 2023
 - Only 8% of business that paid got all their data back (Cobalt)
 - 39% said their data was irretrievable (Barracuda Networks)
- There has been a notable increase in attacks via third-parties

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

NIST 2.0

Full title:

The NIST cybersecurity Framework (CSF) 2.0

Latest: February 26, 2024

Previous: Ver 1.1 April 16 2018



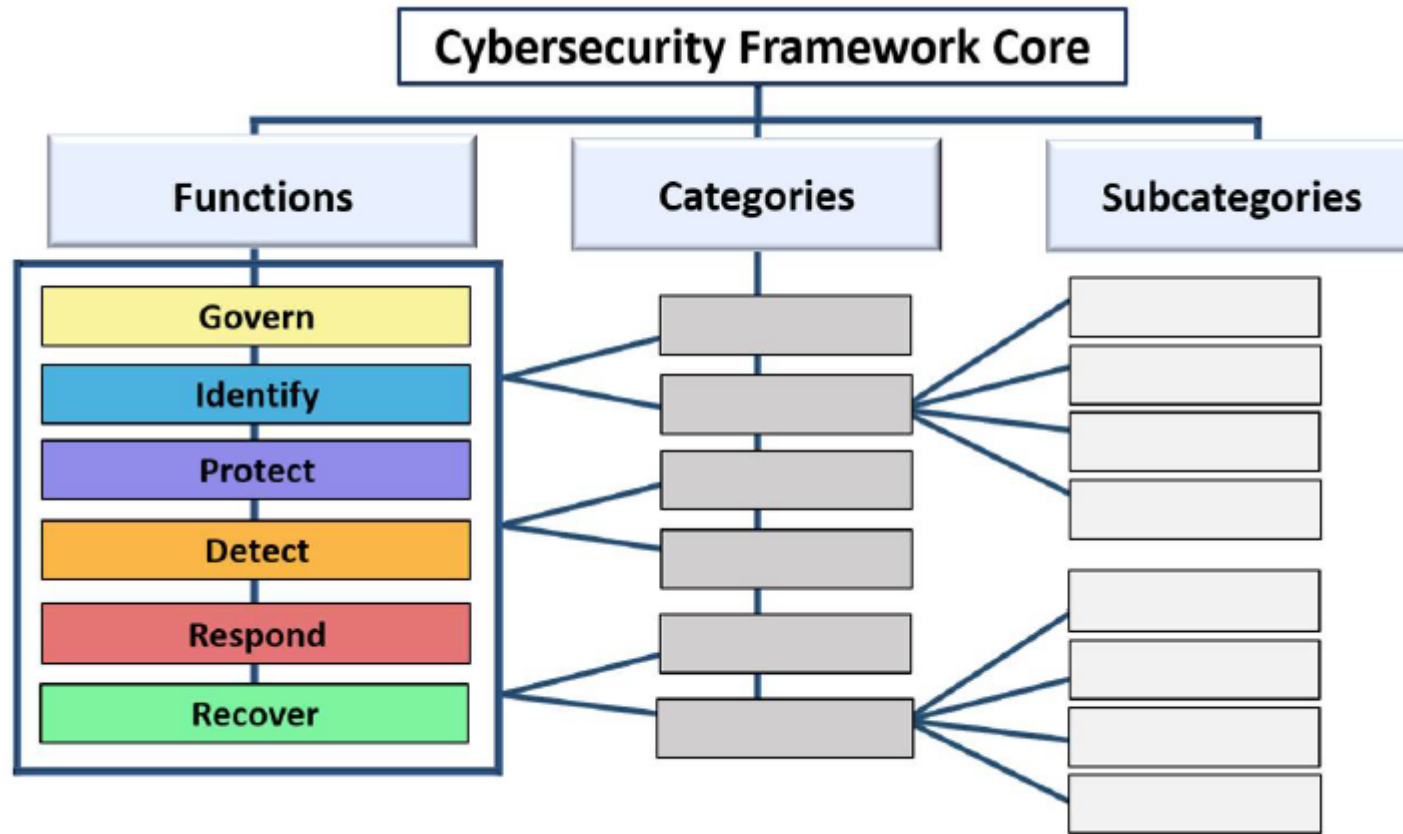
NIST 2.0

Who is it for:

- Industry
- Government Agencies
- Other Organisations

NIST 2.0

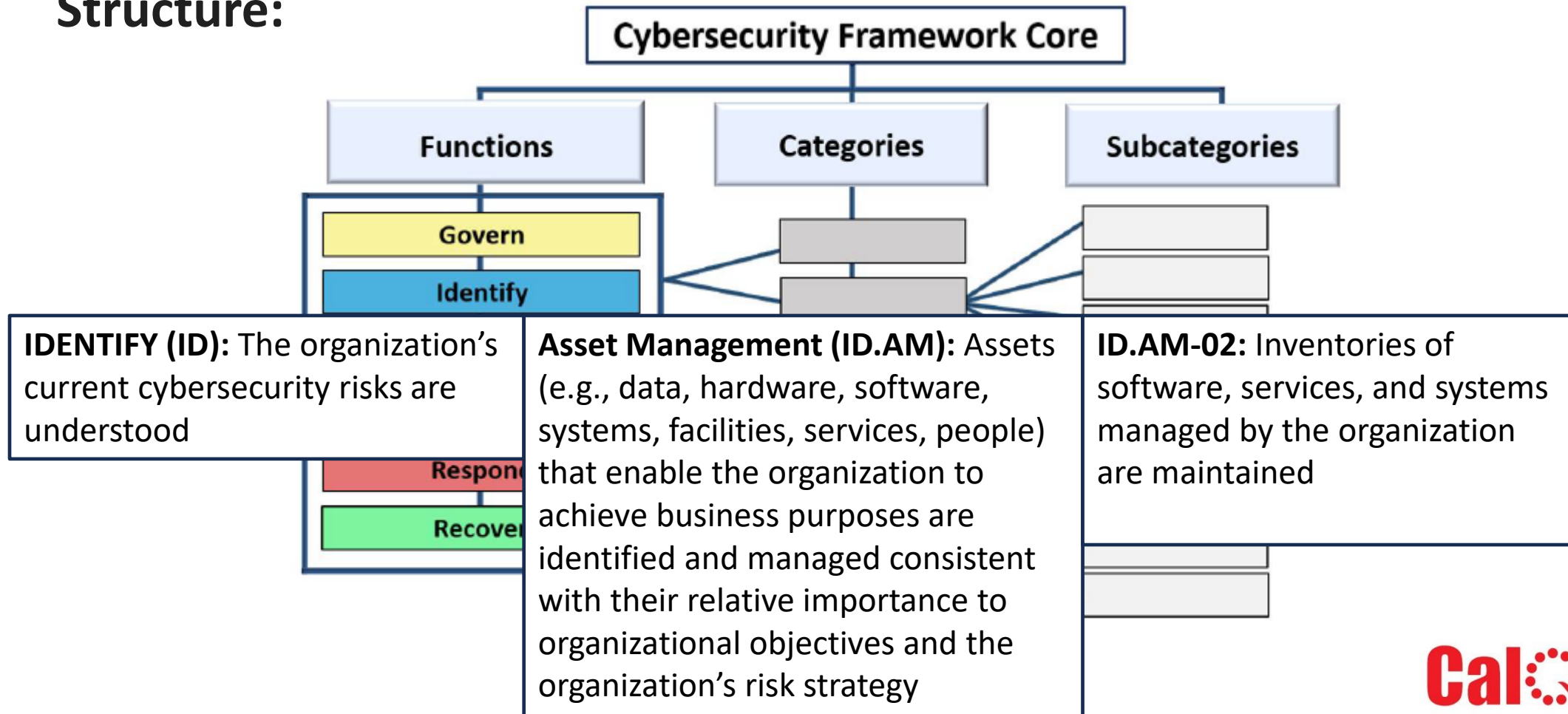
Structure:



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

NIST 2.0

Structure:



NIST 2.0

Changes / What's New

- 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.

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

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

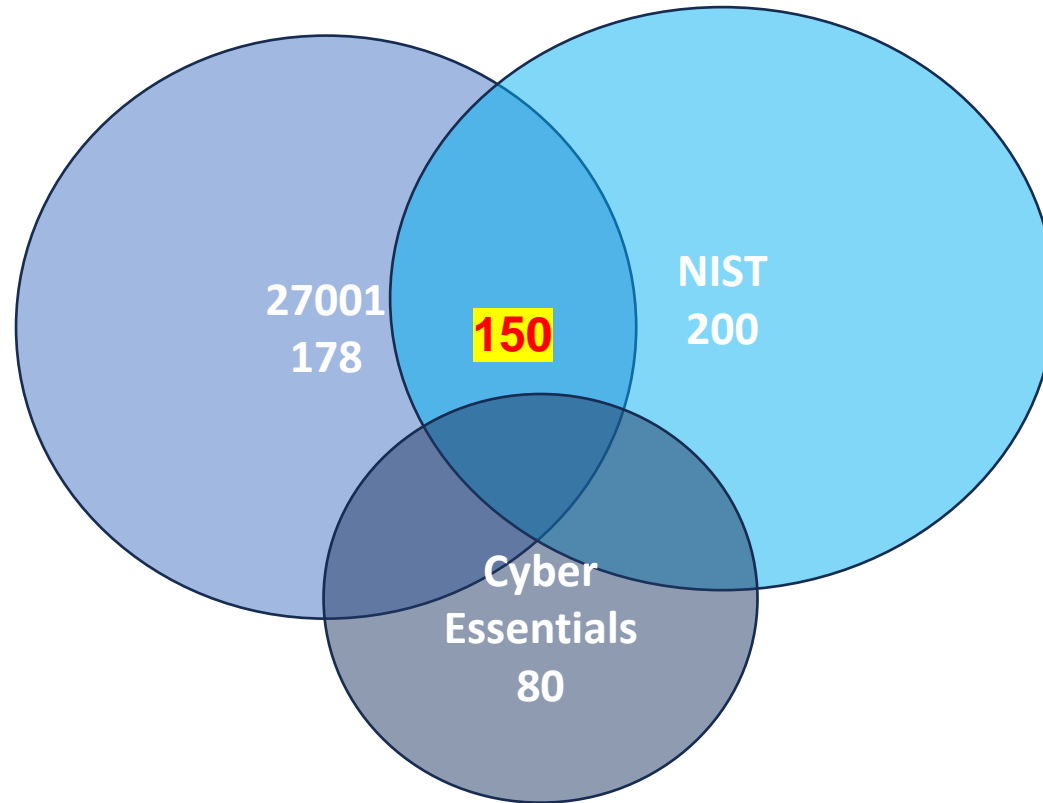


Cyber Essentials

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

So, Which One?

- Cyber Essentials: If your focus is on securing your systems
- NIST 2.0: If you want guidance across the spectrum, that you can tailor to your organisation / your desired outcomes.
- ISO27001: If you want / need to be certified to an international recognised Management System standard.
- All three: ?



Questions ?

gjoyce@calqrisk.com

[Linkedin.com/company/calqrisk](https://www.linkedin.com/company/calqrisk)

[Twitter.com/calqrisk](https://twitter.com/calqrisk)

CalQRisk