MODULE 7 · FREE COURSE

Frameworks Made Simple

NIST CSF, ISO 27001, CIS Controls and more, explained in plain language



Start Your Cybersecurity Career

In this module you will learn



NIST CSF 2.0
Six functions that organise security



ISO/IEC 27001
The certifiable international standard



CIS Controls
A prioritised list of practical actions



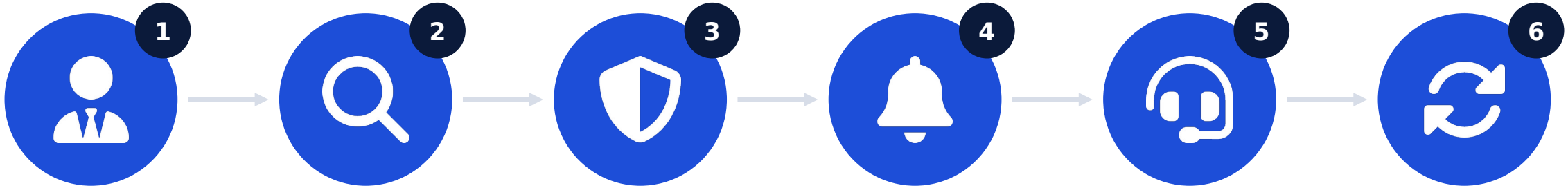
Frameworks at work
Which to use when, and in interviews

07

Module 7 of 8
Frameworks Made Simple

About 20 minutes

NIST Cybersecurity Framework 2.0: six functions



1	2	3	4	5	6
Govern	**Identify**	**Protect**	**Detect**	**Respond**	**Recover**
Strategy, roles, policy	Assets and risks	Safeguards	Find attacks	Act on incidents	Restore operations

Version 2.0 (2024) added Govern, placing security strategy at the centre.

ISO/IEC 27001:2022 at a glance

An international standard for an information security management system (ISMS) that organisations can be certified against.

93

Annex A controls in the 2022 edition

4

themes: organisational, people, physical, technological

ISMS

plan, run, check and improve security continuously

Annex A themes: organisational 37, people 8, physical 14, technological 34 controls

CIS Controls v8.1: start with the essentials



IG1: essential hygiene

56 safeguards every organisation should apply first



IG2: growing teams

Adds safeguards for organisations with IT staff and more risk



IG3: mature security

All 153 safeguards, for highly targeted organisations

Other frameworks you will meet



OWASP Top 10

The most common web application security risks



MITRE ATT&CK

A knowledge base of real attacker tactics and techniques



METI guidelines (Japan)

Cybersecurity Management Guidelines for company leaders



ISO/IEC 27002

Detailed guidance on implementing the ISO 27001 controls

Which framework, when?

Framework	Best for	Typical user
NIST CSF 2.0	Organising and explaining a security programme	Management, consultants
ISO/IEC 27001	Certification that customers trust	Companies serving clients
CIS Controls	A practical, prioritised to-do list	IT and security teams
MITRE ATT&CK	Detection and threat analysis	SOC, threat intelligence
OWASP Top 10	Secure web development and testing	Developers, pentesters

Frameworks in job interviews

Question	What a strong answer shows
“Which framework have you used?”	One framework explained clearly, with a real or lab example
“How would you start securing a small company?”	Begin with CIS IG1 essentials, then grow
“What is the difference between ISO 27001 and NIST CSF?”	Certifiable standard versus flexible framework
“How do you map an attack to ATT&CK?”	Tactics as goals, techniques as methods

Quick check

1. Which function did NIST CSF 2.0 add?

2. How many Annex A controls does ISO/IEC 27001:2022 have?

3. Which CIS Implementation Group should every organisation start with?

Answers are in the lesson article.

Key takeaways

- NIST CSF organises security into six functions, starting with Govern.
- ISO/IEC 27001 is the certifiable standard; CIS Controls give practical priorities.
- Knowing when to use each framework impresses interviewers.

Next: Module 8 · Getting Your First Job