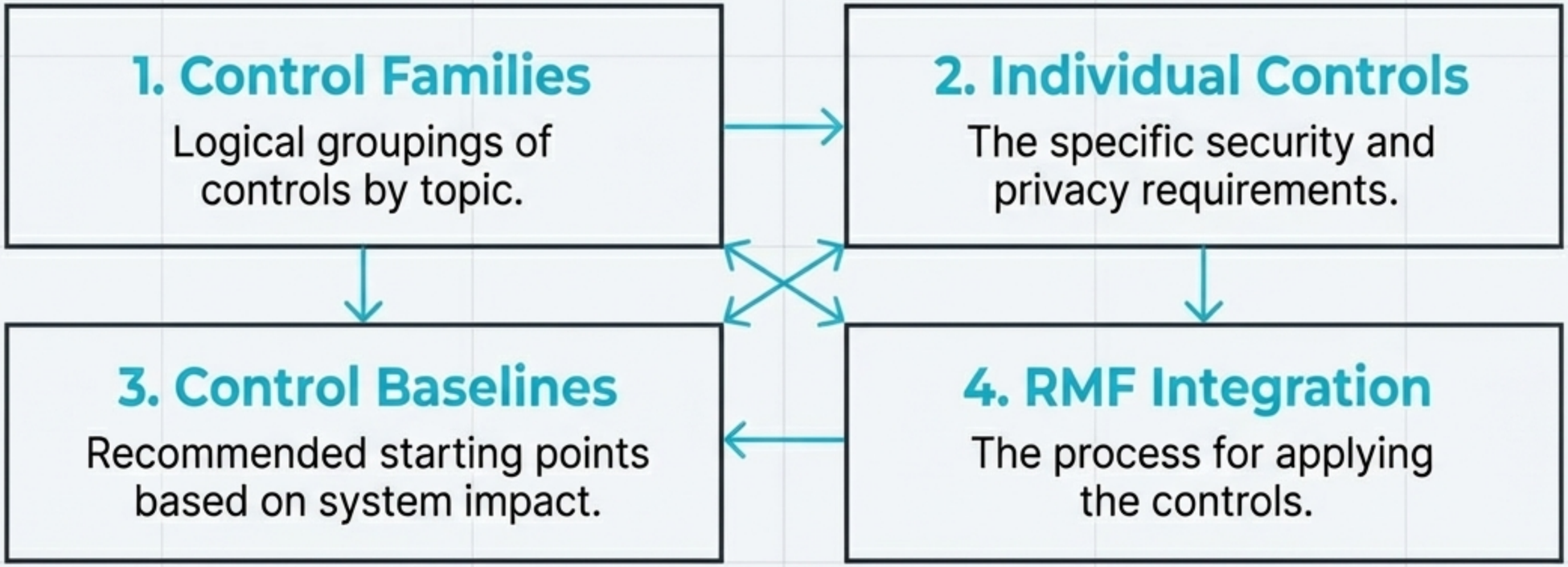
The Blueprint for Organisational Security

A Strategic Deconstruction of NIST Special Publication 800-53

NIST SP 800-53 Provides a Comprehensive Catalogue of Security and Privacy Controls

- Its primary purpose is to protect organisational operations, assets, individuals, and information systems.
- It provides a structured catalogue of controls that enables organisations to manage risk in a consistent, repeatable manner.
- While originating for U.S. federal environments, it is the de facto standard for organisations aligned with the NIST Risk Management Framework (RMF).

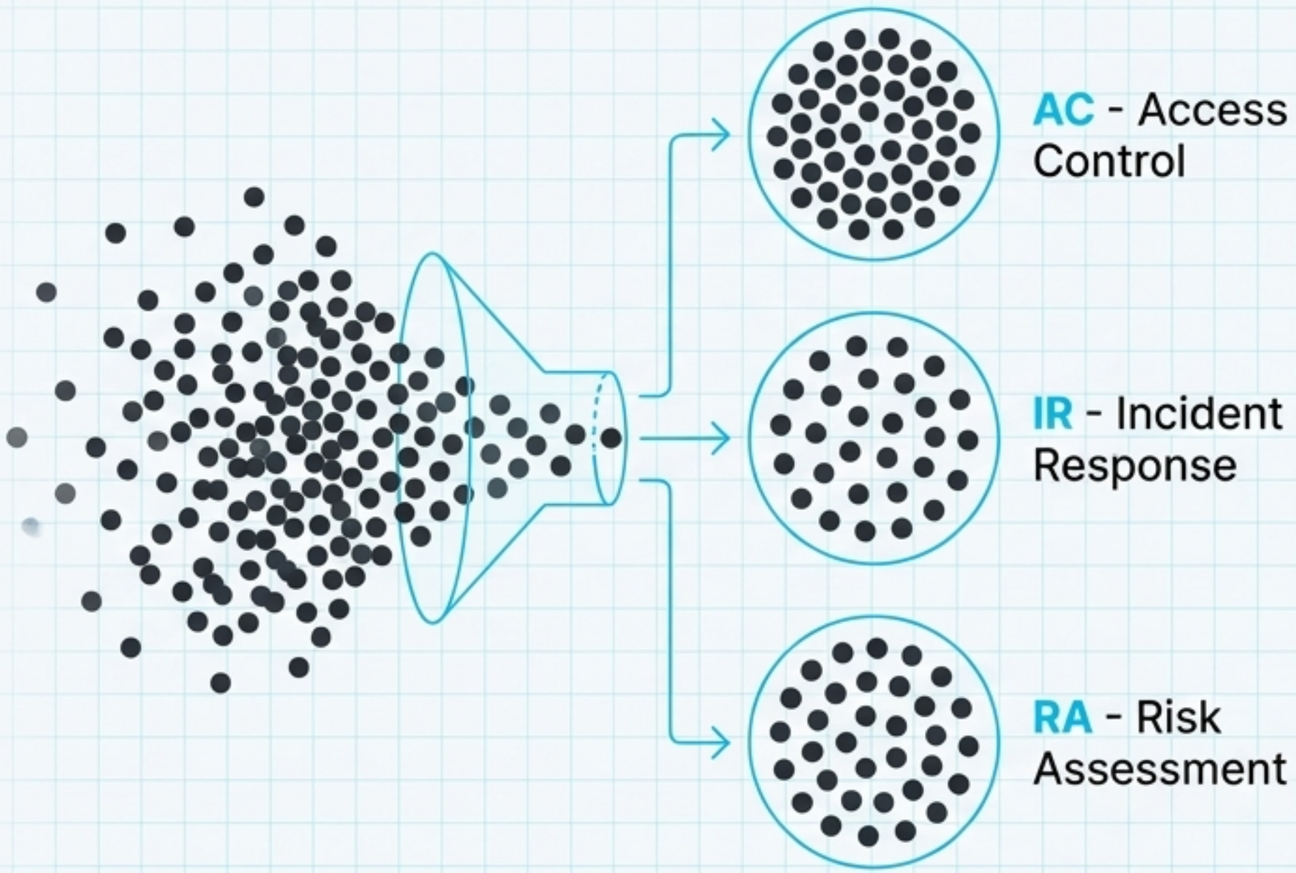
The Standard Standard is Built from Four Controlaent Interlocking Components



This structure is designed for a systematic, risk-based approach to selecting, implementing, and monitoring controls.

Controls Are Grouped into Logical Families for Cohesion and Clarity

- The framework organises its catalogue of over a thousand controls and enhancements into approximately 20 families.
- Each family covers a specific security or privacy domain, allowing specialists to focus on relevant areas.

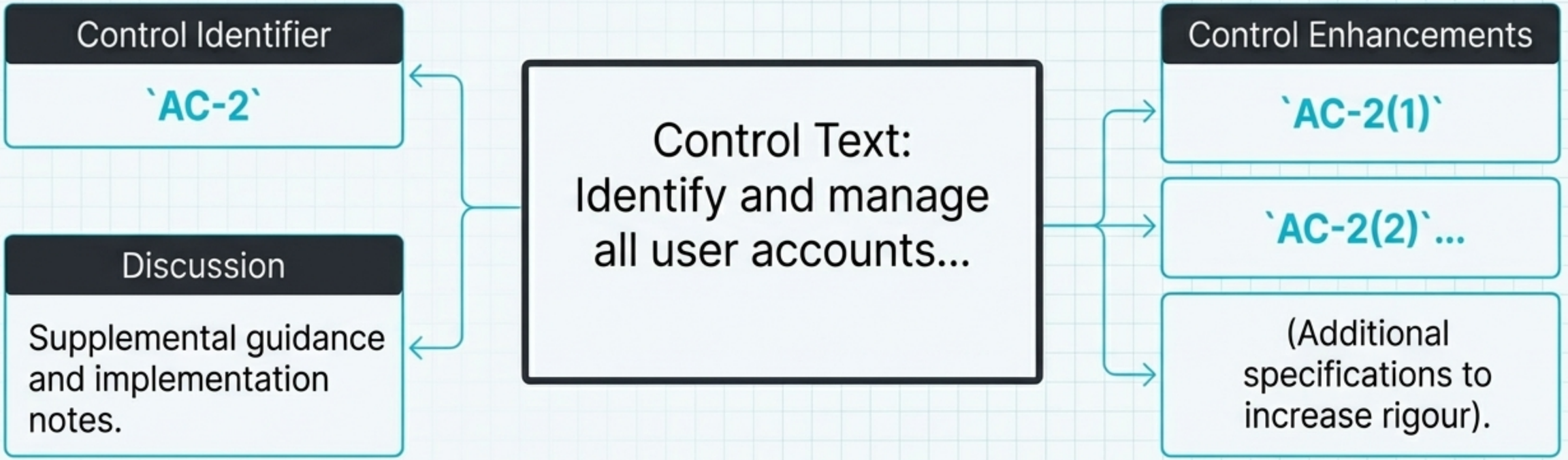


The 20+ Families Cover the Full Spectrum of Cybersecurity Operations

Key examples of control families include:

AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CM	Configuration Management
CP	Contingency Planning
IR	Incident Response
RA	Risk Assessment
SC	System and Communications Protection
SI	System and Information Integrity
...	...and others covering personnel security, physical protection, etc.

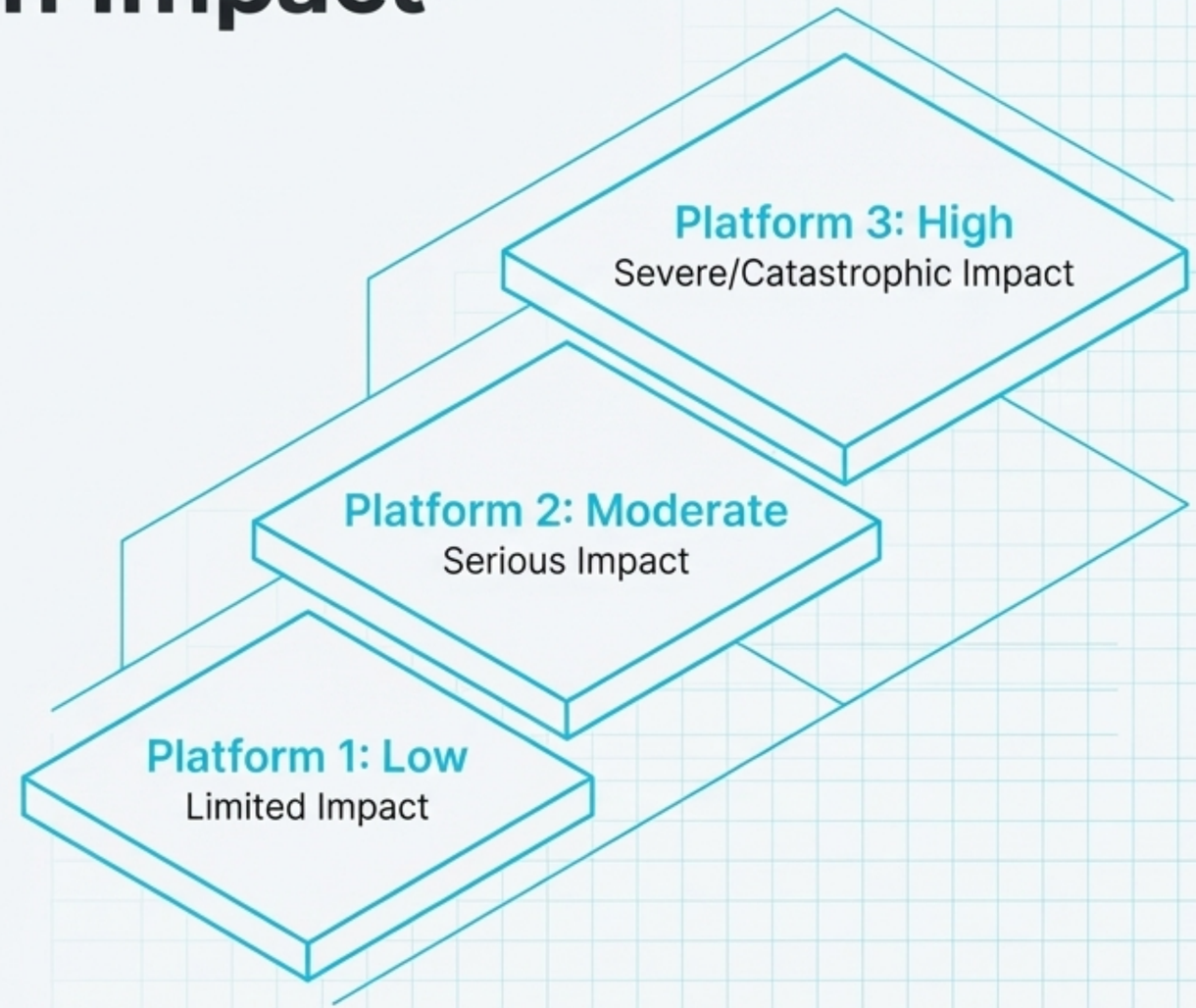
Each Individual Control Follows a Detailed and Prescriptive Structure



This structure ensures requirements are **clear** and **provides context** for effective implementation.

Control Baselines Provide a Standardised Starting Point Based on Impact

- NIST defines three control baselines in a companion document (SP 800-53B): Low, Moderate, and High.
- These baselines directly correspond to the system impact levels defined in FIPS 199 (Federal Information Processing Standards).
- An organisation selects a baseline as the initial set of controls for a given system.



Baselines are Tailored to Align with Specific Organisational Risk and Mission Needs

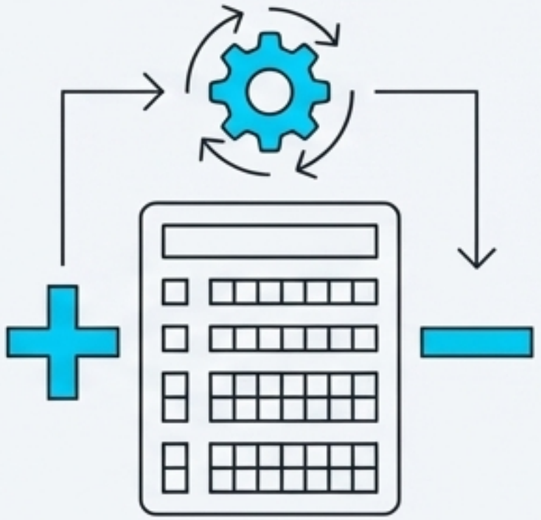
Step 1: Categorise

A system is assessed and labelled ‘Low’, ‘Moderate’, or ‘High’.

Step 2: Select

The corresponding baseline of controls is chosen from a library.

Step 3: Tailor



The control set is modified by adding, removing, or adjusting controls.

This ensures the final control set is both comprehensive and precisely suited to the system’s unique environment.

SP 800-53 is the ‘What’; The RMF is the ‘How’

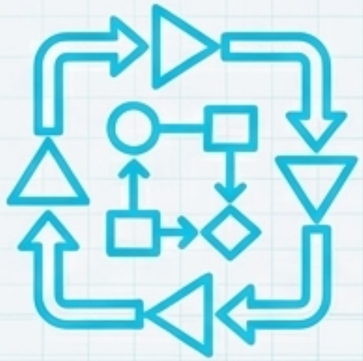
The ‘WHAT’

NIST SP 800-53

A comprehensive catalogue of security and privacy controls.

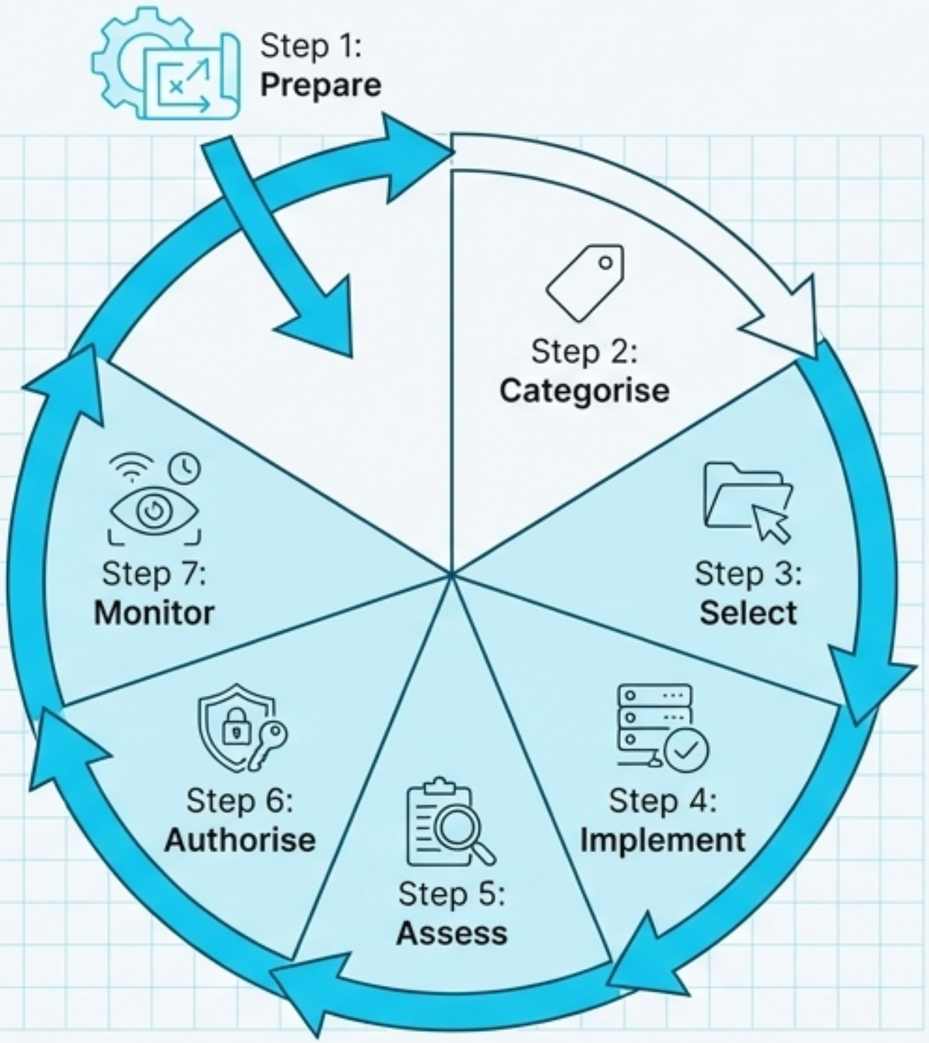
The ‘HOW’

NIST SP 800-37 (The RMF)



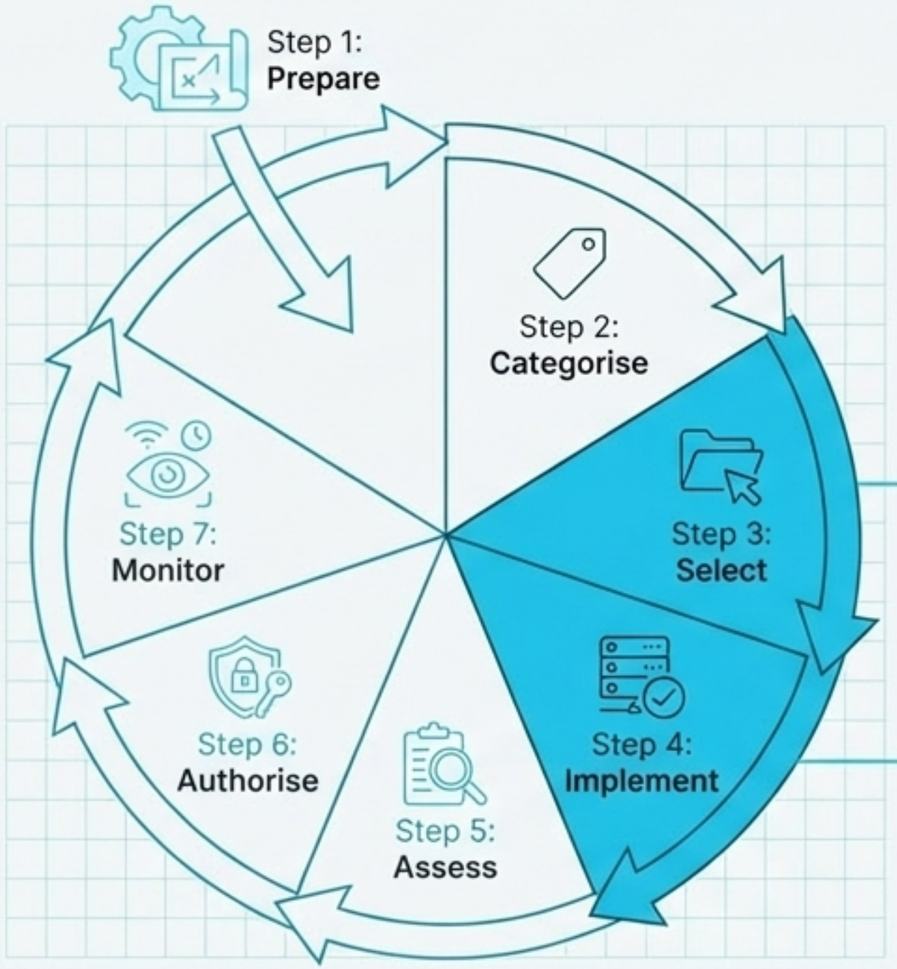
The risk management process for selecting, implementing, and monitoring those controls.

The Risk Management Framework is a Disciplined, Six-Step Process



NIST SP 800-53 is central to the successful execution of the Select, Implement, Assess, Authorise, and Monitor steps.

The ‘Select’ and ‘Implement’ Steps Bring the Control Blueprint to Life



Select

- This is where the appropriate control baseline (Low, Moderate, High) is chosen.
- The baseline is then tailored based on specific organisational risk assessments.
- The output is a finalised set of required controls.

Implement

- The selected controls are put into place within the information system.
- Implementation details are documented to provide evidence for the next step.

Control Evidence is Used to ‘Assess’, ‘Authorise’, and ‘Monitor’ the System

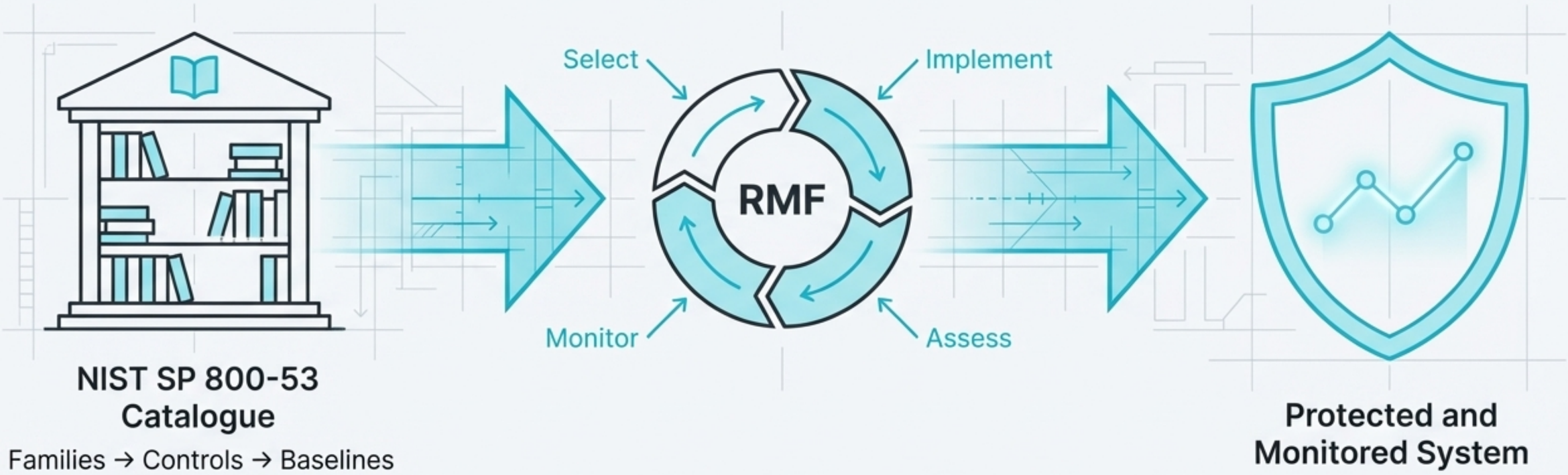
Assess

- The effectiveness of the implemented controls is tested and verified.
- This determines if the controls are operating as intended.

Authorise & Monitor

- Senior leadership makes a formal risk-based decision based on the assessment evidence.
- The status of the controls is continuously monitored to maintain the system's security posture over time.

The Complete Blueprint: From Catalogue to Continuous Monitoring



By integrating the comprehensive control catalogue of NIST SP 800-53 with the procedural rigour of the RMF, organisations can build and maintain a systematic, defensible, and risk-based security environment.