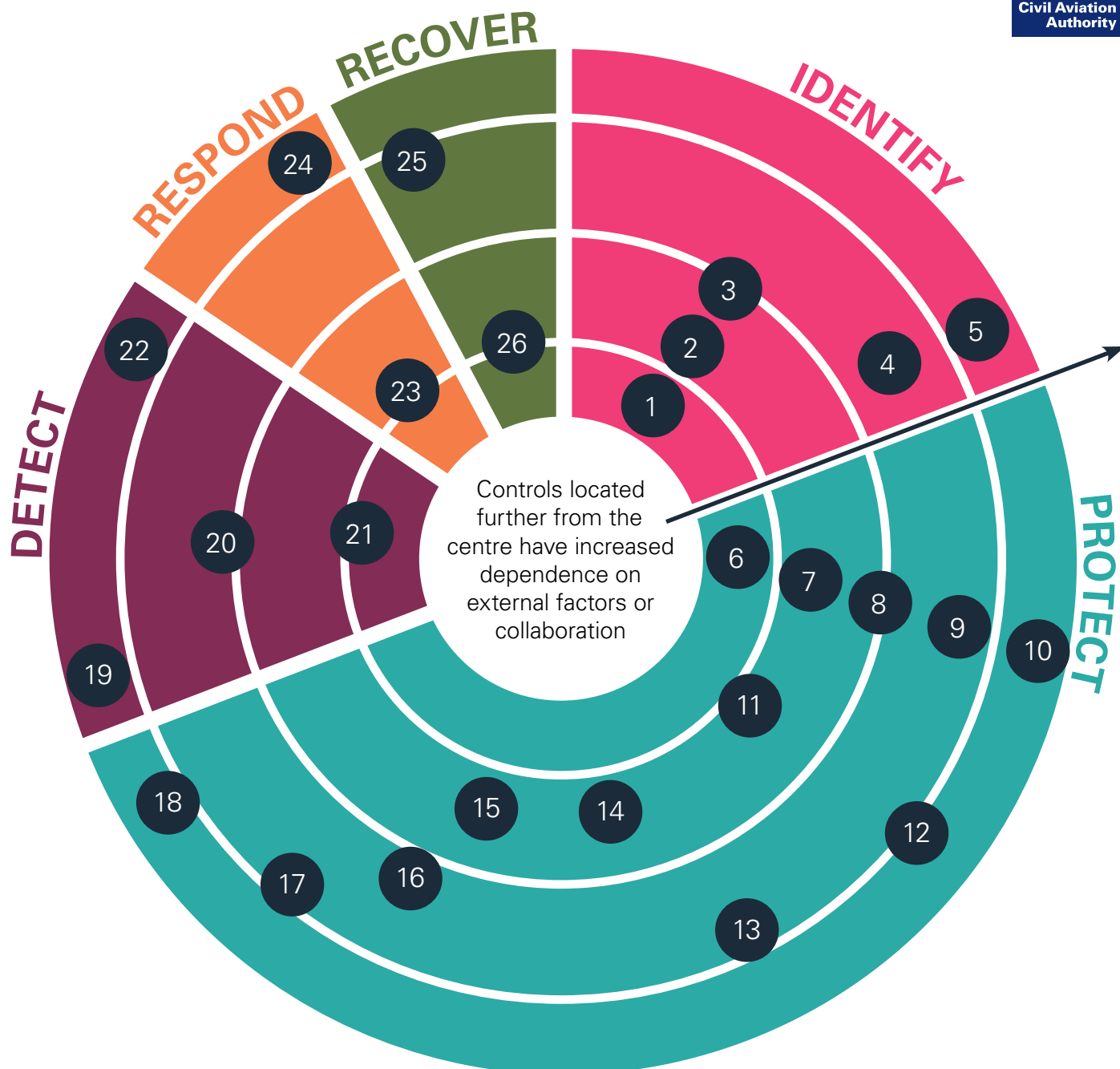


26 security controls for regulation



These control groups provide the focus for regulatory oversight. Reference to some of the international standards in common use are included as examples.

IDENTIFY

1. Responsibility Assigned
2. Asset Management
3. Compliance (Legal/Regs)
4. Risk Management
5. Supply Chain Management

PROTECT

6. Physical Security
7. Administrative Privileges
8. Account Provisioning
9. Controlled Access
10. Personnel Screening
11. Network Perimeter Security
12. Security Awareness
13. Wireless Access Protected
14. Secure Configuration
15. Network Segregation
16. Cryptographic Security
17. Security by Design
18. Software Development

DETECT

19. Vulnerability Assessment
20. Network Monitoring
21. Malware Protection
22. Independent Assurance

RESPOND

23. Incident Management
24. Knowledge Sharing

RECOVER

25. Business Continuity
26. Data Recovery

Documents

Document Sharing Hub

Control group	Description	Example general standards/frameworks
1. Responsibility Assigned	Appropriately trained and experienced resources are assigned responsibility for managing the security of information systems and technology that support critical aviation services.	ISO 27001:2013 A.6.1 NIST 800-53r4 All XX-1 controls, CM-9, CP-2, PS-7, SA-3, SA-9, PM-2, PM-10
2. Asset Management	An inventory of information, systems and technology is maintained for all networked and standalone systems, and includes asset ownership and classification of criticality.	ISO 27002:2013 A.8 NIST 800-53r4 CM-8, RA-2
3. Compliance (Legal/Regs)	The organisation has identified and documented the legal and regulatory requirements for information security controls.	ISO 27002:2013 A.18.1 NIST 800-53r4 XX-1
4. Risk Management	An organisational process is used to provide a reliable and repeatable process for identifying and prioritising the treatment of information security risks.	ISO 27001:2013, ISO 27005 NIST SP800-30, NIST SP800-37r1 NIST 800-53r4 RA-1, RA-3
5. Supply Chain Management	Reasonable and appropriate supply chain measures for data, hardware, software and services are applied; including information flows to and from third parties.	ISO 27002:2013 A.15, ISO 28000:2007 ISO/IEC 27036-1:2014 NIST 800-53r4 SA-4, SA-9, SA-12
6. Physical Security	A suitable level of physical protection of information systems and processing facilities is in place.	ISO 27002:2013 A.11 NIST 800-53r4 PE-2, PE-3, PE-4, PE-5, PE-13
7. Administrative Privileges	Privileged administration accounts are created for essential administrative purposes only, and are not used to access untrusted systems (e.g. the Internet).	ISO 27002:2013 A.9.2.3 NIST 800-53r4 AC-2, AC-3, AC-6, CM-5
8. Account Provisioning	All system accounts are created, maintained and revoked appropriately, to ensure that users and administrators only have the essential access required for their current role.	ISO 27002:2013 A.9.2 NIST 800-53r4 AC-2, IA-2, IA-4, IA-5, IA-8
9. Controlled Access	Access to critical aviation networks and information systems is restricted to only those people and computers that are authorised and have a specific need to access those critical systems and data.	ISO 27002:2013 A.9 NIST 800-53r4 AC-1, AC-3, AC-6
10. Personnel Screening	Employees and contractors who have access to aviation systems, data, or sensitive environments have been subject to appropriate pre-employment screening and background verification checks.	ISO 27002:2013 A.7.1 NIST 800-53r4 PS-3, SA-21
11. Network Perimeter Security	Network boundary protection controls are in place for all systems and services that have connections to untrusted networks, such as the Internet. Such connections are minimised.	ISO 27002:2013 A.13.1 NIST 800-53r4 AC-4, SC-7
12. Security Awareness	Personnel are provided with appropriate security awareness training, including regular updates to policies and procedures, and suitable deterrents are in place to protect against violations.	ISO 27002:2013 A.7.2 NIST SP800-50, NIST SP800-16 NIST 800-53r4 AT-2, AT-3, CP-3, IR-2, PM-13, PS-8
13. Wireless Access Protected	The security risks of wireless working are managed in terms of secured endpoints and encryption of traffic, and the risks of unavailability have been recognised and accepted.	NIST SP800-153, NIST SP800-121, NIST SP800-127 NIST 800-53r4 AC-18
14. Secure Configuration	A robust hardware and software configuration and change control process is in place to ensure systems are configured to a secure baseline build and are patched against known vulnerabilities.	ISO 27002:2013 A.12.6 NIST SP800-40 NIST 800-53r4 RA-3, RA-5, SI-2, SI-5, CM-11, SA-10
15. Network Segregation	Networks used for critical aviation information systems are isolated, protected and monitored to an appropriate standard.	ISO 27002:2013 A.13.1.3 NIST 800-53r4 AC-4, SC-7
16. Cryptographic Security	Cryptography is used where the confidentiality or integrity of the data requires it. Encryption software is up-to-date, correctly implemented and keys are securely managed.	ISO 27002:2013 A.10.1 NIST 800-53r4 SC-12, SC-13, SC-17
17. Security by Design	Security measures are considered in the design, implementation, operation and disposal of new aviation information systems.	ISO 27002:2013 A.14 NIST SP800-160, NIST SP800-82, NIST SP800-64 IEC-62443; ATA Spec 42 (Aircraft); BS EN 16495:2014 (Airspace) NIST 800-53r4 SA-3, SA-8, SA-15, SA-17
18. Software Development	Software developed in-house or procured externally is carefully managed and tested to minimise the potential for security vulnerabilities to be introduced to the production environment.	ISO 27002:2013 A.14.2 NIST 800-53r4 SA-3, SA-4, SA-8
19. Vulnerability Assessment	Regular vulnerability assessments are conducted of the network and information systems, so that the opportunities for attackers can then be identified and reduced.	ISO 27002:2013 A.12.6, A.18.2 NIST 800-53r4 RA-3, RA-5, SI-2, SI-5
20. Network Monitoring	Accurate logs of security events are being generated and all essential network services and information systems are being legally monitored for suspicious activity and specific security-related events.	ISO 27002:2013 A.12.4 NIST SP800-137, NIST SP800-94 NIST 800-53r4 AU-1, AU-2, AU-3, AU-6
21. Malware Protection	Suitable technical controls and user awareness initiatives are in place to protect against the installation and execution of malicious software.	ISO 27002:2013 A.12.2 NIST SP800-83, NIST 800-53r4 AT-2, SI-3
22. Independent Assurance	Security controls for essential services are independently assessed at regular intervals, or whenever major changes have been made, to test their effectiveness.	ISO 27002:2013 A.18.2 ISO 15408 (CC) NIST 800-53r4 CA-2
23. Incident Management	Processes and systems are in place to detect security incidents and provide an effective response that minimises the impact of a security breach and supports timely recovery.	ISO 27002:2013 A.16 NIST SP800-92, NIST SP800-61, NIST SP800-86, NIST SP800-137 NIST 800-53r4 IR-4, IR-5, IR-6, IR-7, IR-8
24. Knowledge Sharing	The organisation actively participates in security information sharing forums to discover new security threats, share successes and learn from the mistakes of others.	ISO 27002:2013 A.6.1.4 NIST 800-53r4 SI-5, PM-15
25. Business Continuity	Appropriate business continuity plans and disaster recovery systems and processes are in place, and these plans preserve the effectiveness of existing essential cyber security controls.	ISO 27002:2013 A.17 NIST 800-53r4 CP-1, CP-2, CP-3, CP-4, CP-7, CP-8, CP-11, CP-12, CP-13
26. Data Recovery	All essential information systems and data is included in a suitable backup regime that will allow full data recovery.	ISO 27002:2013 A.12.3 NIST 800-53r4 CP-9, CP-10