CIS Controls™

V7

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols, and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

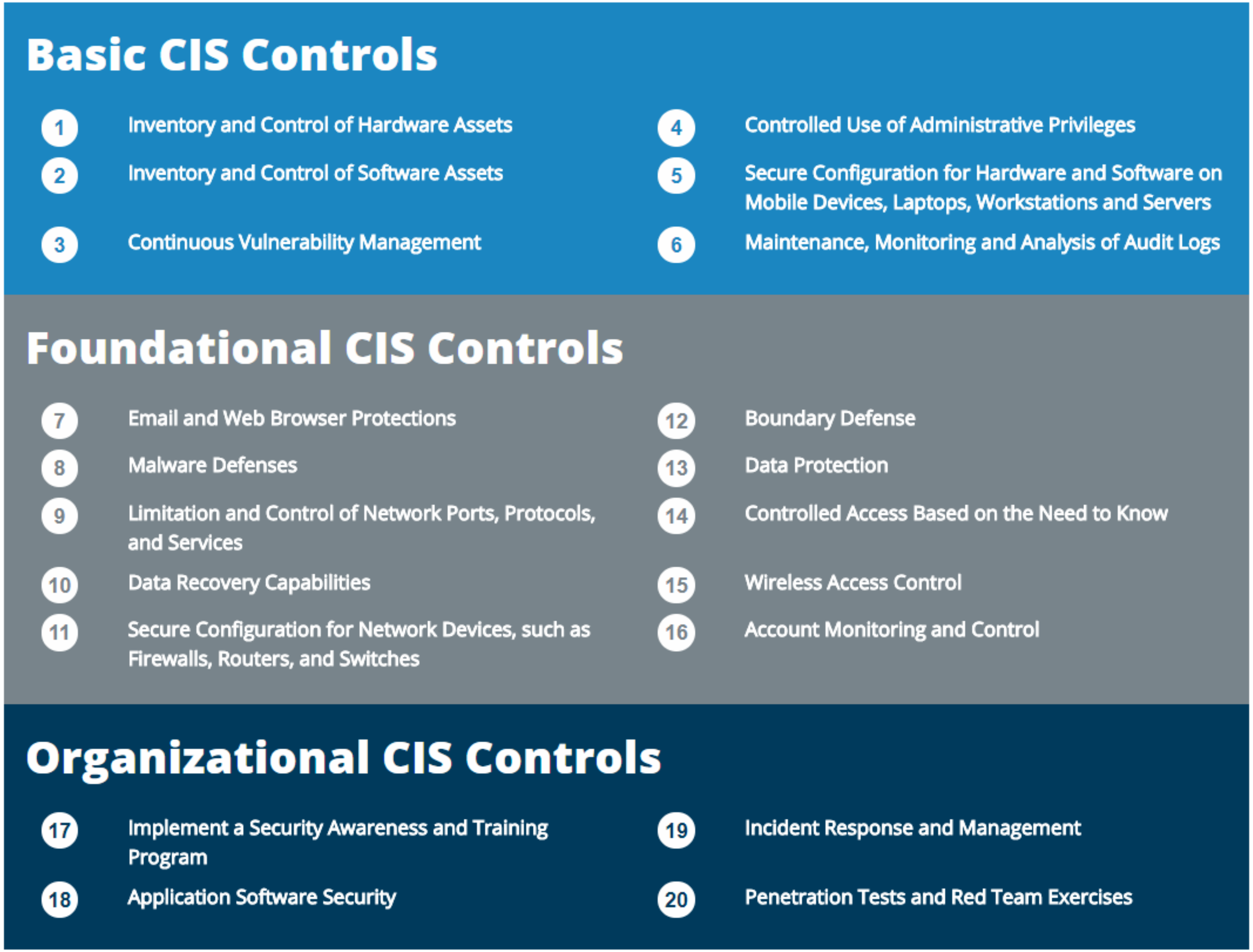
Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises



Basic CIS Controls

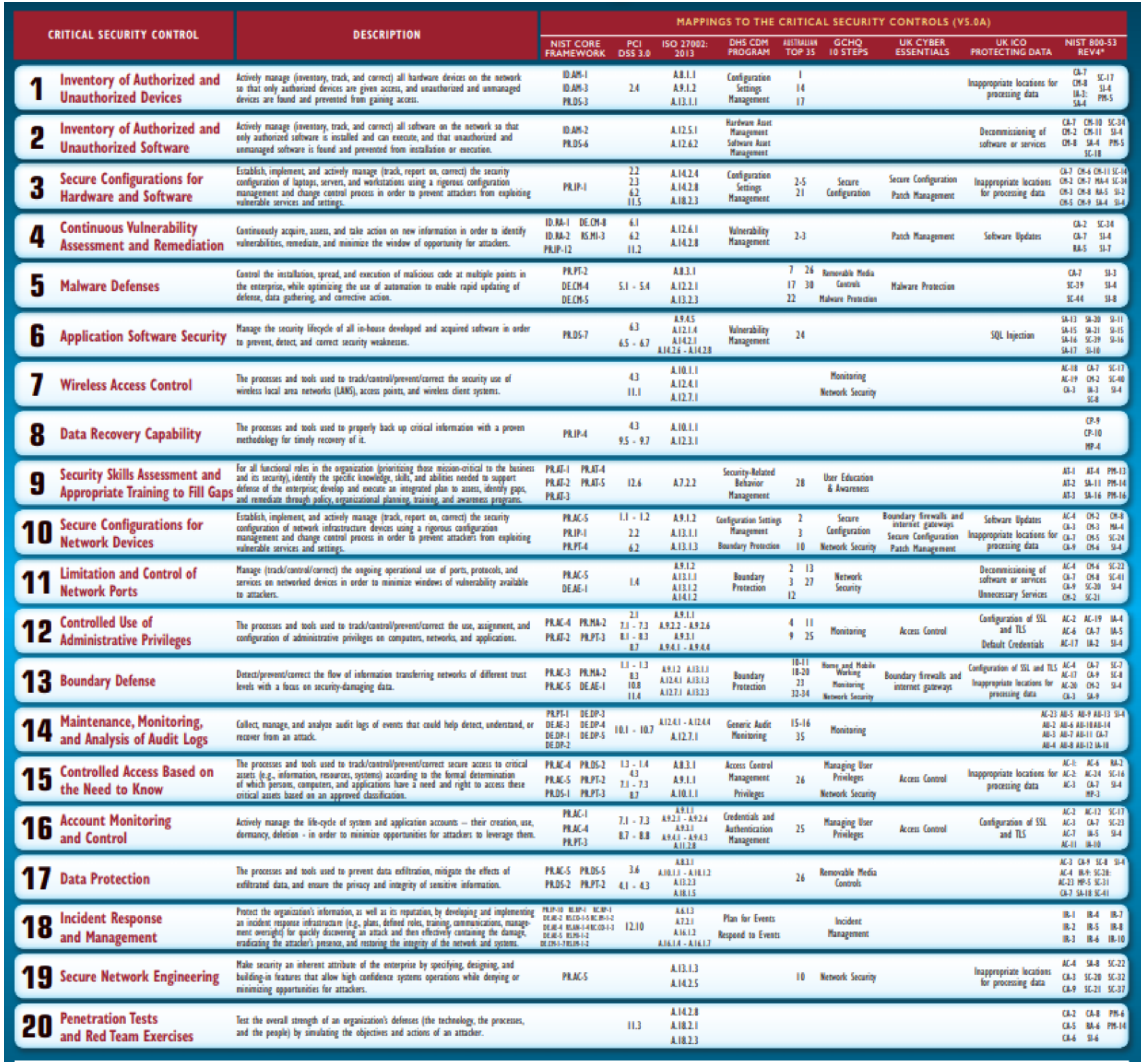
1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational CIS Controls

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational CIS Controls

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises



CRITICAL SECURITY CONTROL	DESCRIPTION	MAPPINGS TO THE CRITICAL SECURITY CONTROLS (V5.0A)								
		NIST CORE FRAMEWORK	PCI DSS 3.0	ISO 27002: 2013	DHS CDM PROGRAM	AUSTRALIAN TOP 35	GCHQ 10 STEPS	UK CYBER ESSENTIALS	UK ICO PROTECTING DATA	NIST 800-53 REV4*
1 Inventory of Authorized and Unauthorized Devices	Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.	ID.AM-1 ID.AM-3 PR.DS-3	2.4	A.8.1.1 A.9.1.2 A.13.1.1	Configuration Settings Management	1 14 17			Inappropriate locations for processing data	CA-7 SC-17 CM-8 SI-4 IA-3: PM-5 SA-4
2 Inventory of Authorized and Unauthorized Software	Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.	ID.AM-2 PR.DS-6		A.12.5.1 A.12.6.2	Hardware Asset Management Software Asset Management				Decommissioning of software or services	CA-7 CM-10 SC-34 CM-2 CM-11 SI-4 CM-8 SA-4 PM-5 SC-18
3 Secure Configurations for Hardware and Software	Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	PR.IP-1	2.2 2.3 6.2 11.5	A.14.2.4 A.14.2.8 A.18.2.3	Configuration Settings Management	2-5 21	Secure Configuration	Secure Configuration Patch Management	Inappropriate locations for processing data	CA-7 CM-6 CM-11 SC-14 CM-2 CM-7 MA-4 SC-34 CM-3 CM-8 RA-5 SI-2 CM-5 CM-9 SA-4 SI-4
4 Continuous Vulnerability Assessment and Remediation	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.	ID.RA-1 DE.CM-8 ID.RA-2 RS.MI-3 PR.IP-12	6.1 6.2 11.2	A.12.6.1 A.14.2.8	Vulnerability Management	2-3		Patch Management	Software Updates	CA-2 SC-34 CA-7 SI-4 RA-5 SI-7
5 Malware Defenses	Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.	PR.PT-2 DE.CM-4 DE.CM-5	5.1 - 5.4	A.8.3.1 A.12.2.1 A.13.2.3		7 26 17 30 22	Removable Media Controls Malware Protection	Malware Protection		CA-7 SI-3 SC-39 SI-4 SC-44 SI-8
6 Application Software Security	Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.	PR.DS-7	6.3 6.5 - 6.7	A.9.4.5 A.12.1.4 A.14.2.1 A.14.2.6 - A.14.2.8	Vulnerability Management	24			SQL Injection	SA-13 SA-20 SI-11 SA-15 SA-21 SI-15 SA-16 SC-39 SI-16 SA-17 SI-10
7 Wireless Access Control	The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.		4.3 11.1	A.10.1.1 A.12.4.1 A.12.7.1			Monitoring Network Security			AC-18 CA-7 SC-17 AC-19 CM-2 SC-40 CA-3 IA-3 SI-4 SC-8
8 Data Recovery Capability	The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.	PR.IP-4	4.3 9.5 - 9.7	A.10.1.1 A.12.3.1						CP-9 CP-10 MP-4
9 Security Skills Assessment and Appropriate Training to Fill Gaps	For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.	PR.AT-1 PR.AT-4 PR.AT-2 PR.AT-5 PR.AT-3	12.6	A.7.2.2	Security-Related Behavior Management	28	User Education & Awareness			AT-1 AT-4 PM-13 AT-2 SA-11 PM-14 AT-3 SA-16 PM-16
10 Secure Configurations for Network Devices	Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	PR.AC-5 PR.IP-1 PR.PT-4	1.1 - 1.2 2.2 6.2	A.9.1.2 A.13.1.1 A.13.1.3	Configuration Settings Management Boundary Protection	2 3 10	Secure Configuration Network Security	Boundary firewalls and internet gateways Secure Configuration Patch Management	Software Updates Inappropriate locations for processing data	AC-4 CM-2 CM-8 CA-3 CM-3 MA-4 CA-7 CM-5 SC-24 CA-9 CM-6 SI-4
11 Limitation and Control of Network Ports	Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.	PR.AC-5 DE.AE-1	1.4	A.9.1.2 A.13.1.1 A.13.1.2 A.14.1.2	Boundary Protection	2 13 3 27 12	Network Security		Decommissioning of software or services Unnecessary Services	AC-4 CM-6 SC-22 CA-7 CM-8 SC-41 CA-9 SC-20 SI-4 CM-2 SC-21
12 Controlled Use of Administrative Privileges	The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.	PR.AC-4 PR.MA-2 PR.AT-2 PR.PT-3	2.1 7.1 - 7.3 8.1 - 8.3 8.7	A.9.1.1 A.9.2.2 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.4		4 11 9 25	Monitoring	Access Control	Configuration of SSL and TLS Default Credentials	AC-2 AC-19 IA-4 AC-6 CA-7 IA-5 AC-17 IA-2 SI-4
13 Boundary Defense	Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.	PR.AC-3 PR.MA-2 PR.AC-5 DE.AE-1	1.1 - 1.3 8.3 10.8 11.4	A.9.1.2 A.13.1.1 A.12.4.1 A.13.1.3 A.12.7.1 A.13.2.3	Boundary Protection	10-11 18-20 23 32-34	Home and Mobile Working Monitoring Network Security	Boundary firewalls and internet gateways	Configuration of SSL and TLS Inappropriate locations for processing data	AC-4 CA-7 SC-7 AC-17 CA-9 SC-8 AC-20 CM-2 SI-4 CA-3 SA-9
14 Maintenance, Monitoring, and Analysis of Audit Logs	Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.	PR.PT-1 DE.DP-3 DE.AE-3 DE.DP-4 DE.DP-1 DE.DP-5 DE.DP-2	10.1 - 10.7	A.12.4.1 - A.12.4.4 A.12.7.1	Generic Audit Monitoring	15-16 35	Monitoring			AC-23 AU-5 AU-9 AU-13 SI-4 AU-2 AU-6 AU-10 AU-14 AU-3 AU-7 AU-11 CA-7 AU-4 AU-8 AU-12 IA-10
15 Controlled Access Based on the Need to Know	The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.	PR.AC-4 PR.DS-2 PR.AC-5 PR.PT-2 PR.DS-1 PR.PT-3	1.3 - 1.4 4.3 7.1 - 7.3 8.7	A.8.3.1 A.9.1.1 A.10.1.1	Access Control Management Privileges	26	Managing User Privileges Network Security	Access Control	Inappropriate locations for processing data	AC-1: AC-6 RA-2 AC-2: AC-24 SC-16 AC-3 CA-7 SI-4 MP-3
16 Account Monitoring and Control	Actively manage the life-cycle of system and application accounts – their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.	PR.AC-1 PR.AC-4 PR.PT-3	7.1 - 7.3 8.7 - 8.8	A.9.1.1 A.9.2.1 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.3 A.11.2.8	Credentials and Authentication Management	25	Managing User Privileges	Access Control	Configuration of SSL and TLS	AC-2 AC-12 SC-17 AC-3 CA-7 SC-23 AC-7 IA-5 SI-4 AC-11 IA-10
17 Data Protection	The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.	PR.AC-5 PR.DS-5 PR.DS-2 PR.PT-2	3.6 4.1 - 4.3	A.8.3.1 A.10.1.1 - A.10.1.2 A.13.2.3 A.18.1.5		26	Removable Media Controls			AC-3 CA-9 SC-8 SI-4 AC-4 IR-9: SC-28: AC-23 MP-5 SC-31 CA-7 SA-18 SC-41
18 Incident Response and Management	Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.	PR.IP-10 RS.RP-1 RC.RP-1 DE.AE-2 RS.CO-1-5 RC.IM-1-2 DE.AE-4 RS.AN-1-4 RC.CO-1-3 DE.AE-5 RS.MI-1-2 DE.CM-1-7 RS.IM-1-2	12.10	A.6.1.3 A.7.2.1 A.16.1.2 A.16.1.4 - A.16.1.7	Plan for Events Respond to Events		Incident Management			IR-1 IR-4 IR-7 IR-2 IR-5 IR-8 IR-3 IR-6 IR-10
19 Secure Network Engineering	Make security an inherent attribute of the enterprise by specifying, designing, and building-in features that allow high confidence systems operations while denying or minimizing opportunities for attackers.	PR.AC-5		A.13.1.3 A.14.2.5		10	Network Security		Inappropriate locations for processing data	AC-4 SA-8 SC-22 CA-3 SC-20 SC-32 CA-9 SC-21 SC-37
20 Penetration Tests and Red Team Exercises	Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.		11.3	A.14.2.8 A.18.2.1 A.18.2.3						CA-2 CA-8 PM-6 CA-5 RA-6 PM-14 CA-6 SI-6