NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Australia - Code of Practice - Securing the Internet of Things for Consumers (2020)
Focal Document URL: https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-cop-sitc-2020.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1	No duplicated default or weak passwords	IoT device (and associated backend/cloud account) passwords should be unique, unpredictable, complex and unfeasible to guess, and not resettable to any factory default value that is common to multiple devices. Associated web services should use Multi-Factor Authentication, not provide any unnecessary user information prior to authentication, and any password reset process should appropriately authenticate the user. Primarily applies to Device Manufacturers.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5	
1	No duplicated default or weak passwords	IoT device (and associated backend/cloud account) passwords should be unique, unpredictable, complex and unfeasible to guess, and not resettable to any factory default value that is common to multiple devices. Associated web services should use Multi-Factor Authentication, not provide any unnecessary user information prior to authentication, and any password reset process should appropriately authenticate the user. Primarily applies to Device Manufacturers.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
1	No duplicated default or weak passwords	IoT device (and associated backend/cloud account) passwords should be unique, unpredictable, complex and unfeasible to guess, and not resettable to any factory default value that is common to multiple devices. Associated web services should use Multi-Factor Authentication, not provide any unnecessary user information prior to authentication, and any password reset process should appropriately authenticate the user. Primarily applies to Device Manufacturers.	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	5	
2	Implement a vulnerability disclosure policy	IoT device manufacturers, IoT service providers and mobile application developers should provide a public point of contact as part of a vulnerability disclosure policy in order for security researchers and others to report issues. Disclosed vulnerabilities should be acted on in a timely manner. Implementing a bug bounty program encourages and rewards the cyber security community for identifying and reporting vulnerabilities, thereby facilitating the responsible and coordinated disclosure and remediation of vulnerabilities. Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	5	
2	Implement a vulnerability disclosure policy	IoT device manufacturers, IoT service providers and mobile application developers should provide a public point of contact as part of a vulnerability disclosure policy in order for security researchers and others to report issues. Disclosed vulnerabilities should be acted on in a timely manner. Implementing a bug bounty program encourages and rewards the cyber security community for identifying and reporting vulnerabilities, thereby facilitating the responsible and coordinated disclosure and remediation of vulnerabilities. Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.	Functional	Intersects With	Security Disclosure Contact Information	THR-06.1	Mechanisms exist to enable public submissions of discovered or potential security vulnerabilities.	5	
3	Keep software securely updated	Software (including firmware) on IoT devices, including third party and open source software, as well as associated web services, should be securely updateable. Updates should be timely and not impact the device's functionality. Updates should also not change user-configured preferences, security or privacy settings without prior approval from the user. The need for each update should be made clear to consumers, and updates should be easy to implement and applied automatically by default. The device should verify that updates are from a trusted source e.g. via use of a trusted digital signature. Updates should be distributed via secure IT infrastructure to mitigate the trusted source being compromised. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable. Where possible, vendors should inform the user when their constrained device is no longer fit for purpose. An end-of-life policy should be clear to the consumer including when they acquire the device, which explicitly states the minimum length of time for which a device will receive software updates, the reasons for this timeframe and a commitment and method to warn consumers when the product will no longer receive updates. If a user interface is available it should clearly display when a device has reached its end-of-life, inform the user of the risk of security updates no longer being available and provide suggestions for mitigating this risk. Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.	Functional	Intersects With	Embedded Technology Maintenance	EMB-07	Mechanisms exist to securely update software and upgrade functionality on embedded devices.	5	
3	Keep software securely updated	Software (including firmware) on IoT devices, including third party and open source software, as well as associated web services, should be securely updateable. Updates should be timely and not impact the device's functionality. Updates should also not change user-configured preferences, security or privacy settings without prior approval from the user. The need for each update should be made clear to consumers, and updates should be easy to implement and applied automatically by default. The device should verify that updates are from a trusted source e.g. via use of a trusted digital signature. Updates should be distributed via secure IT infrastructure to mitigate the trusted source being compromised. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable. Where possible, vendors should inform the user when their constrained device is no longer fit for purpose. An end-of-life policy should be clear to the consumer including when they acquire the device, which explicitly states the minimum length of time for which a device will receive software updates, the reasons for this timeframe and a commitment and method to warn consumers when the product will no longer receive updates. If a user interface is available it should clearly display when a device has reached its end-of-life, inform the user of the risk of security updates no longer being available and provide suggestions for mitigating this risk. Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	TDA-17	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	5	
3	Keep software securely updated	Software (including firmware) on IoT devices, including third party and open source software, as well as associated web services, should be securely updateable. Updates should be timely and not impact the device's functionality. Updates should also not change user-configured preferences, security or privacy settings without prior approval from the user. The need for each update should be made clear to consumers, and updates should be easy to implement and applied automatically by default. The device should verify that updates are from a trusted source e.g. via use of a trusted digital signature. Updates should be distributed via secure IT infrastructure to mitigate the trusted source being compromised. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable. Where possible, vendors should inform the user when their constrained device is no longer fit for purpose. An end-of-life policy should be clear to the consumer including when they acquire the device, which explicitly states the minimum length of time for which a device will receive software updates, the reasons for this timeframe and a commitment and method to warn consumers when the product will no longer receive updates. If a user interface is available it should clearly display when a device has reached its end-of-life, inform the user of the risk of security updates no longer being available and provide suggestions for mitigating this risk. Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Australia - Code of Practice - Securing the Internet of Things for Consumers (2020)
Focal Document URL: https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-cop-sitc-2020.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
3	Keep software securely updated	Software (including firmware) on IoT devices, including third party and open source software, as well as associated web services, should be securely updateable. Updates should be timely and not impact the device's functionality. Updates should also not change user-configured preferences, security or privacy settings without prior approval from the user. The need for each update should be made clear to consumers, and updates should be easy to implement and applied automatically by default. The device should verify that updates are from a trusted source e.g. via use of a trusted digital signature. Updates should be distributed via secure IT infrastructure to mitigate the trusted source being compromised. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable. Where possible, vendors should inform the user when their constrained device is no longer fit for purpose. An end-of-life policy should be clear to the consumer including when they acquire the device, which explicitly states the minimum length of time for which a device will receive software updates, the reasons for this timeframe and a commitment and method to warn consumers when the product will no longer receive updates. If a user interface is available it should clearly display when a device has reached its end-of-life, inform the user of the risk of security updates no longer being available and provide suggestions for mitigating this risk. Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.	Functional	Intersects With	Software Patch Integrity	VPM-05.8	Mechanisms exist to ensure software and/or firmware patches are: (1) Obtained from trusted sources; and (2) Checked for integrity.	5	
4	Securely store credentials	Any credentials should be stored securely within devices and on services. Hard-coded credentials (e.g. usernames and passwords) should not be embedded in device software or hardware since they can be discovered via reverse engineering. Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.	Functional	Intersects With	No Embedded Unencrypted Static Authenticators	IAC-10.6	Mechanisms exist to ensure that unencrypted, static authenticators are not embedded in applications, scripts or stored on function keys.	8	
4	Securely store credentials	Any credentials should be stored securely within devices and on services. Hard-coded credentials (e.g. usernames and passwords) should not be embedded in device software or hardware since they can be discovered via reverse engineering. Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5	
4	Securely store credentials	Any credentials should be stored securely within devices and on services. Hard-coded credentials (e.g. usernames and passwords) should not be embedded in device software or hardware since they can be discovered via reverse engineering. Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
4	Securely store credentials	Any credentials should be stored securely within devices and on services. Hard-coded credentials (e.g. usernames and passwords) should not be embedded in device software or hardware since they can be discovered via reverse engineering. Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.	Functional	Intersects With	Secure Settings By Default	TDA-09.6	Mechanisms exist to implement secure configuration settings by default to reduce the likelihood of Technology Assets, Applications and/or Services (TAAS) being deployed with weak security settings that would put the TAAS at a greater risk of compromise.	5	
5	Ensure that personal data is protected	Where devices and/or services process personal data, they must do so in accordance with data protection law e.g. the Privacy Act 1988 and Australian Privacy Principles. Personal data should only be collected if necessary for the operation of the device, and privacy settings on a device should be set to privacy protective by default. Adequate industry-standard encryption, as articulated in the Australian Government Information Security Manual, should be applied to personal data in transit and data at rest. Consumers should be provided with clear and transparent information about what data is being used and how, by whom, and for what purposes, for each device and service. This also applies to any third parties that may be involved (including advertisers). Where personal data is processed on the basis of consumers' consent, this should be validly and lawfully obtained from an adult, with those consumers being given the opportunity to withdraw it at any time. Several other principles in this document are related to protecting personal data, such as installing and securely configuring devices, as well as deleting personal data. Primarily applies to Device Manufacturers, IoT Service Providers, Mobile Application Developers and Retailers.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
5	Ensure that personal data is protected	Where devices and/or services process personal data, they must do so in accordance with data protection law e.g. the Privacy Act 1988 and Australian Privacy Principles. Personal data should only be collected if necessary for the operation of the device, and privacy settings on a device should be set to privacy protective by default. Adequate industry-standard encryption, as articulated in the Australian Government Information Security Manual, should be applied to personal data in transit and data at rest. Consumers should be provided with clear and transparent information about what data is being used and how, by whom, and for what purposes, for each device and service. This also applies to any third parties that may be involved (including advertisers). Where personal data is processed on the basis of consumers' consent, this should be validly and lawfully obtained from an adult, with those consumers being given the opportunity to withdraw it at any time. Several other principles in this document are related to protecting personal data, such as installing and securely configuring devices, as well as deleting personal data. Primarily applies to Device Manufacturers, IoT Service Providers, Mobile Application Developers and Retailers.	Functional	Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	5	
5	Ensure that personal data is protected	Where devices and/or services process personal data, they must do so in accordance with data protection law e.g. the Privacy Act 1988 and Australian Privacy Principles. Personal data should only be collected if necessary for the operation of the device, and privacy settings on a device should be set to privacy protective by default. Adequate industry-standard encryption, as articulated in the Australian Government Information Security Manual, should be applied to personal data in transit and data at rest. Consumers should be provided with clear and transparent information about what data is being used and how, by whom, and for what purposes, for each device and service. This also applies to any third parties that may be involved (including advertisers). Where personal data is processed on the basis of consumers' consent, this should be validly and lawfully obtained from an adult, with those consumers being given the opportunity to withdraw it at any time. Several other principles in this document are related to protecting personal data, such as installing and securely configuring devices, as well as deleting personal data. Primarily applies to Device Manufacturers, IoT Service Providers, Mobile Application Developers and Retailers.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Australia - Code of Practice - Securing the Internet of Things for Consumers (2020)
Focal Document URL: https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-cop-sitc-2020.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
5	Ensure that personal data is protected	Where devices and/or services process personal data, they must do so in accordance with data protection law e.g. the Privacy Act 1988 and Australian Privacy Principles. Personal data should only be collected if necessary for the operation of the device, and privacy settings on a device should be set to privacy protective by default. Adequate industry-standard encryption, as articulated in the Australian Government Information Security Manual, should be applied to personal data in transit and data at rest. Consumers should be provided with clear and transparent information about what data is being used and how, by whom, and for what purposes, for each device and service. This also applies to any third parties that may be involved (including advertisers). Where personal data is processed on the basis of consumers' consent, this should be validly and lawfully obtained from an adult, with those consumers being given the opportunity to withdraw it at any time. Several other principles in this document are related to protecting personal data, such as installing and securely configuring devices, as well as deleting personal data. Primarily applies to Device Manufacturers, IoT Service Providers, Mobile Application Developers and Retailers.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
6	Minimise exposed attack surfaces	Devices and services should operate on the 'principle of least privilege'. Unused functionality should be disabled; hardware should not unnecessarily expose access (e.g. unrequired ports should be closed, the web management interface should only be accessible to the local network unless the device needs to be managed remotely via the Internet); functionality should not be available if they are not used; and code should be minimised to the functionality necessary for devices and services to operate. Software should run with appropriate privileges, taking account of both security and functionality. To further reduce the number of vulnerabilities, use a secure software development process and perform penetration testing. Primarily applies to Device Manufacturers and IoT Service Providers	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
6	Minimise exposed attack surfaces	Devices and services should operate on the 'principle of least privilege'. Unused functionality should be disabled; hardware should not unnecessarily expose access (e.g. unrequired ports should be closed, the web management interface should only be accessible to the local network unless the device needs to be managed remotely via the Internet); functionality should not be available if they are not used; and code should be minimised to the functionality necessary for devices and services to operate. Software should run with appropriate privileges, taking account of both security and functionality. To further reduce the number of vulnerabilities, use a secure software development process and perform penetration testing. Primarily applies to Device Manufacturers and IoT Service Providers	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	
6	Minimise exposed attack surfaces	Devices and services should operate on the 'principle of least privilege'. Unused functionality should be disabled; hardware should not unnecessarily expose access (e.g. unrequired ports should be closed, the web management interface should only be accessible to the local network unless the device needs to be managed remotely via the Internet); functionality should not be available if they are not used; and code should be minimised to the functionality necessary for devices and services to operate. Software should run with appropriate privileges, taking account of both security and functionality. To further reduce the number of vulnerabilities, use a secure software development process and perform penetration testing. Primarily applies to Device Manufacturers and IoT Service Providers	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
6	Minimise exposed attack surfaces	Devices and services should operate on the 'principle of least privilege'. Unused functionality should be disabled; hardware should not unnecessarily expose access (e.g. unrequired ports should be closed, the web management interface should only be accessible to the local network unless the device needs to be managed remotely via the Internet); functionality should not be available if they are not used; and code should be minimised to the functionality necessary for devices and services to operate. Software should run with appropriate privileges, taking account of both security and functionality. To further reduce the number of vulnerabilities, use a secure software development process and perform penetration testing. Primarily applies to Device Manufacturers and IoT Service Providers	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
7	Ensure communication security	Data requiring confidentiality or integrity protection, or associated with remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage. All credentials and certificates should be managed securely. All remote access should be logged, with logs including the date, time and source of access at a minimum. Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
7	Ensure communication security	Data requiring confidentiality or integrity protection, or associated with remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage. All credentials and certificates should be managed securely. All remote access should be logged, with logs including the date, time and source of access at a minimum. Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5	
7	Ensure communication security	Data requiring confidentiality or integrity protection, or associated with remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage. All credentials and certificates should be managed securely. All remote access should be logged, with logs including the date, time and source of access at a minimum. Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
7	Ensure communication security	Data requiring confidentiality or integrity protection, or associated with remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage. All credentials and certificates should be managed securely. All remote access should be logged, with logs including the date, time and source of access at a minimum. Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.	Functional	Intersects With	Protection of Confidentiality / Integrity Using Encryption	NET-14.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).	5	
8	Ensure software integrity	Software (including firmware) on IoT devices should be verified using secure boot mechanisms. If an unauthorised change is detected, the device should alert the consumer/administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function. Primarily applies to Device Manufacturers.	Functional	Intersects With	Embedded Technology Configuration Monitoring	EMB-05	Mechanisms exist to generate log entries on embedded devices when configuration changes or attempts to access interfaces are detected.	5	
8	Ensure software integrity	Software (including firmware) on IoT devices should be verified using secure boot mechanisms. If an unauthorised change is detected, the device should alert the consumer/administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function. Primarily applies to Device Manufacturers.	Functional	Intersects With	Protection of Boot Firmware	END-06.6	Automated mechanisms exist to protect the integrity of boot firmware in systems.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Australia - Code of Practice - Securing the Internet of Things for Consumers (2020)
Focal Document URL: https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-cop-sitc-2020.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
9	Make systems resilient to outages	Resilience should be built into IoT devices and services where required by their usage or by other relying systems, taking into account the possibility of outages of data networks and power. As far as reasonably possible, IoT devices should remain operating and locally functional in the case of a loss of network, without compromising security or safety. They should recover cleanly in the case of restoration of a loss of power. Devices should be able to return to a network in a sensible state and in an orderly fashion, rather than all attempt to reconnect at the same time. Implementing redundancy and DDoS mitigation helps ensure that IoT services remain online. Architect IoT devices to continue functioning as much as possible if an associated IoT service becomes unavailable, and disclose upfront to the consumer which features will cease working in this case. IoT service providers should also update data when network connection is restored. Primarily applies to Device Manufacturers and IoT Service Providers.	Functional	Intersects With	Resilience To Outages	EMB-08	Mechanisms exist to configure embedded technology to be resilient to data network and power outages.	8	
10	Monitor system telemetry data	If telemetry data is collected from IoT devices and services, such as usage and measurement data, it should be monitored for security anomalies. Primarily applies to Device Manufacturers and IoT Service Providers	Functional	Intersects With	Power Level Monitoring	EMB-09	Automated mechanisms exist to monitor the power levels of embedded technologies for decreased or excessive power usage, including battery drainage, to investigate for device tampering.	5	
10	Monitor system telemetry data	If telemetry data is collected from IoT devices and services, such as usage and measurement data, it should be monitored for security anomalies. Primarily applies to Device Manufacturers and IoT Service Providers	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
11	Make it easy for consumers to delete personal data	Devices and services should be configured such that personal data can easily be removed when there is a transfer of ownership, when the consumer wishes to delete it and/or when the consumer wishes to dispose of the device. Consumers should be given clear instructions on how to delete their personal data, including how to reset the device to “factory default” and delete data stored on the device and in associated backend/cloud accounts and mobile applications. Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
11	Make it easy for consumers to delete personal data	Devices and services should be configured such that personal data can easily be removed when there is a transfer of ownership, when the consumer wishes to delete it and/or when the consumer wishes to dispose of the device. Consumers should be given clear instructions on how to delete their personal data, including how to reset the device to “factory default” and delete data stored on the device and in associated backend/cloud accounts and mobile applications. Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.	Functional	Intersects With	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5	
12	Make installation and maintenance of devices easy	Installation and maintenance of IoT devices should employ minimal steps and follow Australian Government best practice on security1 and usability.2 Consumers should also be provided with clear and straightforward guidance on how to securely set up their device and maintain it through its lifecycle. Accessibility options on a device should be enabled by default. Primarily applies to Device Manufacturers, IoT Services Providers and Mobile Application Developers.	Functional	Intersects With	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5	
13	Validate input data	Data received via user interfaces, application programming interfaces (APIs) and network interfaces should be validated. Ensure data input is authorised and conforms to expectations. Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.	Functional	Intersects With	Interface Security	EMB-04	Mechanisms exist to protect embedded devices against unauthorized use of the physical factory diagnostic and test interface(s).	5	
13	Validate input data	Data received via user interfaces, application programming interfaces (APIs) and network interfaces should be validated. Ensure data input is authorised and conforms to expectations. Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.	Functional	Intersects With	Prevent Alterations	EMB-06	Mechanisms exist to protect embedded devices by preventing the unauthorized installation and execution of software.	5	
13	Validate input data	Data received via user interfaces, application programming interfaces (APIs) and network interfaces should be validated. Ensure data input is authorised and conforms to expectations. Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.	Functional	Intersects With	Restrict Communications	EMB-12	Mechanisms exist to require embedded technologies to initiate all communications and drop new, incoming communications.	5	
13	Validate input data	Data received via user interfaces, application programming interfaces (APIs) and network interfaces should be validated. Ensure data input is authorised and conforms to expectations. Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.	Functional	Intersects With	Authorized Communications	EMB-13	Mechanisms exist to restrict embedded technologies to communicate only with authorized peers and service endpoints.	5	