NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Australia - Security of Critical Infrastructure Act 2018 (Compilation No. 9, 4 June 2026)
Focal Document URL: https://www.legislation.gov.au/C2018A00029/latest/text
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-soci-2018.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	Legacy SCF #
1	Short title	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
2	Commencement	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
3	Object	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
4	Simplified outline of this Act	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
5	Definitions	See FDE for details	Functional	Intersects With	Standardized Terminology	GOV-03.2	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	5		SEA-02.1
5A	Meaning of protected information and relevant information	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
6	Meaning of interest and control information	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
7	Meaning of operational information	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
8	Meaning of direct interest holder	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
8A	Meaning of influence or control	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
8B	Meaning of associate	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
8C	Meanings of subsidiary and holding entity	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
8D	Meaning of critical infrastructure sector	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
8E	Meaning of critical infrastructure sector asset	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
8F	Critical infrastructure sector for a critical infrastructure asset	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
8G	Meaning of relevant impact	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
9	Meaning of critical infrastructure asset	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
10	Meaning of critical electricity asset	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
11	Meaning of critical port	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
12	Meaning of critical gas asset	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
12A	Meaning of critical liquid fuel asset	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
12B	Meaning of critical freight infrastructure asset	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
12C	Meaning of critical freight services asset	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
12D	Meaning of critical financial market infrastructure asset	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
12E	Meaning of critical broadcasting asset	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
12F	Meaning of critical data storage or processing asset	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
12G	Meaning of critical banking asset	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
12H	Meaning of critical insurance asset	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
12J	Meaning of critical superannuation asset	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
12K	Meaning of critical food and grocery asset	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
12KA	Meaning of critical domain name system	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
12L	Meaning of responsible entity	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
12M	Meaning of cyber security incident	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
13	Application of this Act	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
14	Extraterritoriality	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
15	This Act binds the Crown	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
16	Concurrent operation of State and Territory laws	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
17	State constitutional powers	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
18	Simplified outline of this Part	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
18A	Application of this Part	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
18AA	Consultation-rules	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
19	Secretary must keep Register	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
20	Secretary may add information to Register	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
21	Secretary may correct or update information in the Register	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
22	Register not to be made public	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
23	Initial obligation to give information	A reporting entity for a critical infrastructure asset must give the Secretary the required operational information and interest and control information in relation to the asset within the applicable grace period, for inclusion in the Register of Critical Infrastructure Assets.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	3		GOV-17
24	Ongoing obligation to give information and notify of events	A reporting entity must notify the Secretary of notifiable events affecting the operational, interest or control information reported for a critical infrastructure asset, and give updated information, within the timeframes specified in this section.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	3		GOV-17
25	Information that is not able to be obtained	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
26	Meaning of notifiable event	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30	Agents may give notice or information	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30AA	Simplified outline of this Part	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30AB	Application of this Part	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30ABA	Consultation-rules	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30AE	Review of critical infrastructure risk management program	The responsible entity must review its critical infrastructure risk management program on a regular basis.	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	5		RSK-01
30AF	Update of critical infrastructure risk management program	The responsible entity must take all reasonable steps to ensure its critical infrastructure risk management program is up to date, including updating the program after each review.	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	5		RSK-01
30AG	Responsible entity must submit annual report	The responsible entity must submit an annual report relating to its critical infrastructure risk management program, approved by the entity's board, council or other governing body, to the relevant Commonwealth regulator within 90 days after the end of each financial year.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Australia - Security of Critical Infrastructure Act 2018 (Compilation No. 9, 4 June 2026)
Focal Document URL: https://www.legislation.gov.au/C2018A00029/latest/text
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-soci-2018.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	Legacy SCF #
30AH	Critical infrastructure risk management program	A critical infrastructure risk management program is a written program that applies to the responsible entity, the purpose of which is, for each critical infrastructure asset, to: (i) identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset; (ii) so far as it is reasonably practicable to do so, minimise or eliminate any material risk of such a hazard occurring; and (iii) so far as it is reasonably practicable to do so, mitigate the relevant impact of such a hazard on the asset; and that complies with requirements specified in the rules (including requirements relating to cyber and information security hazards, personnel hazards, supply chain hazards, and physical and natural hazards).	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	8		RSK-01
30AH	Critical infrastructure risk management program	A critical infrastructure risk management program is a written program that applies to the responsible entity, the purpose of which is, for each critical infrastructure asset, to: (i) identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset; (ii) so far as it is reasonably practicable to do so, minimise or eliminate any material risk of such a hazard occurring; and (iii) so far as it is reasonably practicable to do so, mitigate the relevant impact of such a hazard on the asset; and that complies with requirements specified in the rules (including requirements relating to cyber and information security hazards, personnel hazards, supply chain hazards, and physical and natural hazards).	Functional	Intersects With	Material Risks	RSK-06	Mechanisms exist to define criteria necessary to designate a risk as a material risk.	5		GOV-16.1
30AH	Critical infrastructure risk management program	A critical infrastructure risk management program is a written program that applies to the responsible entity, the purpose of which is, for each critical infrastructure asset, to: (i) identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset; (ii) so far as it is reasonably practicable to do so, minimise or eliminate any material risk of such a hazard occurring; and (iii) so far as it is reasonably practicable to do so, mitigate the relevant impact of such a hazard on the asset; and that complies with requirements specified in the rules (including requirements relating to cyber and information security hazards, personnel hazards, supply chain hazards, and physical and natural hazards).	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		RSK-04
30AH	Critical infrastructure risk management program	A critical infrastructure risk management program is a written program that applies to the responsible entity, the purpose of which is, for each critical infrastructure asset, to: (i) identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset; (ii) so far as it is reasonably practicable to do so, minimise or eliminate any material risk of such a hazard occurring; and (iii) so far as it is reasonably practicable to do so, mitigate the relevant impact of such a hazard on the asset; and that complies with requirements specified in the rules (including requirements relating to cyber and information security hazards, personnel hazards, supply chain hazards, and physical and natural hazards).	Functional	Intersects With	Risk Remediation	RSK-17	Mechanisms exist to remediate risks to an acceptable level.	5		RSK-06
30AJ	Variation of critical infrastructure risk management program	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30AM	Review of rules	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30ANA	Application, adoption or incorporation of certain documents	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30ANC	Disallowance of rules	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30AP	Simplified outline of this Part	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30BA	Simplified outline of this Part	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30BB	Application of this Part	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30BBA	Consultation-rules	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30BC	Notification of critical cyber security incidents	If a responsible entity becomes aware that a cyber security incident has occurred or is occurring and the incident has had or is having a significant impact on the availability of a critical infrastructure asset, the entity must notify the relevant Commonwealth body as soon as practicable, and in any event within 12 hours after becoming aware of the incident. Oral notifications must be followed by a written record within the period specified in this section.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	8		IRO-10
30BC	Notification of critical cyber security incidents	If a responsible entity becomes aware that a cyber security incident has occurred or is occurring and the incident has had or is having a significant impact on the availability of a critical infrastructure asset, the entity must notify the relevant Commonwealth body as soon as practicable, and in any event within 12 hours after becoming aware of the incident. Oral notifications must be followed by a written record within the period specified in this section.	Functional	Intersects With	Serious Incident Reporting	IRO-16.3	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	8		IRO-10.5
30BD	Notification of other cyber security incidents	If a responsible entity becomes aware that a cyber security incident has occurred, is occurring or is imminent, and the incident has had, is having or is likely to have a relevant impact on a critical infrastructure asset, the entity must notify the relevant Commonwealth body within 72 hours after becoming aware of the incident. Oral notifications must be followed by a written record within the period specified in this section.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	8		IRO-10
30BD	Notification of other cyber security incidents	If a responsible entity becomes aware that a cyber security incident has occurred, is occurring or is imminent, and the incident has had, is having or is likely to have a relevant impact on a critical infrastructure asset, the entity must notify the relevant Commonwealth body within 72 hours after becoming aware of the incident. Oral notifications must be followed by a written record within the period specified in this section.	Functional	Intersects With	Serious Incident Reporting	IRO-16.3	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	8		IRO-10.5
30BE	Liability	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30BEA	Significant impact	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30BEB	Consultation-rules	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30BF	Relevant Commonwealth body	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30CA	Simplified outline of this Part	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30CC	Revocation of determination	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30CD	Responsible entity must have an incident response plan	If an entity is the responsible entity for a system of national significance and the statutory incident response planning obligations apply to the entity, the entity must adopt and maintain an incident response plan that applies to the entity, relates to the system, and relates to cyber security incidents. Civil penalty applies.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8		IRO-04
30CE	Compliance with incident response plan	The responsible entity must comply with its incident response plan.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5		IRO-04
30CF	Review of incident response plan	The responsible entity must review its incident response plan on a regular basis.	Functional	Intersects With	Continuous Incident Response Improvements	IRO-03	Mechanisms exist to use qualitative and quantitative data from incident response testing to: (1) Determine the effectiveness of incident response processes; (2) Continuously improve incident response processes; and (3) Provide incident response measures and metrics that are accurate, consistent and in a reproducible format.	5		IRO-04.3
30CF	Review of incident response plan	The responsible entity must review its incident response plan on a regular basis.	Functional	Subset Of	Incident Response Plan (IRP) Update	IRO-08.1	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	10		IRO-04.2
30CG	Update of incident response plan	The responsible entity must take all reasonable steps to ensure its incident response plan is up to date.	Functional	Intersects With	Incident Response Plan (IRP) Update	IRO-08.1	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	5		IRO-04.2
30CJ	Incident response plan	An incident response plan is a written plan that applies to the responsible entity for a system of national significance, relates to the system and to cyber security incidents, has the purpose of planning for responding to cyber security incidents that could have a relevant impact on the system, and complies with such requirements (if any) as are specified in the rules.	Functional	Equal	Incident Response Plan (IRP)	IRO-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	10		IRO-04
30CK	Variation of incident response plan	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Australia - Security of Critical Infrastructure Act 2018 (Compilation No. 9, 4 June 2026)
Focal Document URL: https://www.legislation.gov.au/C2018A00029/latest/text
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-soci-2018.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	Legacy SCF #
30CL	Revocation of adoption of incident response plan	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30CM	Requirement to undertake cyber security exercise	The Secretary may, by written notice, require the responsible entity for a system of national significance to undertake a cyber security exercise in relation to the system and all types (or one or more specified types) of cyber security incidents, within the period specified in the notice.	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5		IRO-06
30CN	Cyber security exercise	A cyber security exercise is an exercise undertaken for the purposes of testing the entity's ability to respond appropriately to cyber security incidents that could have a relevant impact on the system, the entity's preparedness for such incidents, and the entity's ability to mitigate the relevant impacts of such incidents.	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5		IRO-06
30CQ	Internal evaluation report	If an entity undertakes a cyber security exercise under section 30CM, the entity must prepare an evaluation report relating to the exercise and give a copy of the report to the Secretary within 30 days after the completion of the exercise (or a longer period allowed by the Secretary). Civil penalty: 200 penalty units.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	8		GOV-17
30CQ	Internal evaluation report	If an entity undertakes a cyber security exercise under section 30CM, the entity must prepare an evaluation report relating to the exercise and give a copy of the report to the Secretary within 30 days after the completion of the exercise (or a longer period allowed by the Secretary). Civil penalty: 200 penalty units.	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5		IRO-06
30CQ	Internal evaluation report	If an entity undertakes a cyber security exercise under section 30CM, the entity must prepare an evaluation report relating to the exercise and give a copy of the report to the Secretary within 30 days after the completion of the exercise (or a longer period allowed by the Secretary). Civil penalty: 200 penalty units.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	3		IRO-13
30CR	External evaluation report	The Secretary may require the entity to appoint an external auditor to prepare an external evaluation report relating to the cyber security exercise and to give a copy of the report to the Secretary.	Functional	Intersects With	Independent Assessors	CPL-08	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	5		CPL-03.1
30CS	Meaning of evaluation report	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30CT	External auditors	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30CU	Requirement to undertake vulnerability assessment	The Secretary may require the responsible entity for a system of national significance to undertake a vulnerability assessment in relation to the system, and the entity must comply with such a requirement. (See section text for details.)	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06
30CY	Vulnerability assessment	A vulnerability assessment is an assessment that relates to a system of national significance and to all types (or specified types) of cyber security incidents, the purpose of which is to test the vulnerability of the system to those cyber security incidents.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06
30CZ	Vulnerability assessment report	If a vulnerability assessment is undertaken, a vulnerability assessment report must be prepared and a copy given to the Secretary.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17
30CZ	Vulnerability assessment report	If a vulnerability assessment is undertaken, a vulnerability assessment report must be prepared and a copy given to the Secretary.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06
30DA	Meaning of vulnerability assessment report	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30DD	Consultation	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30DG	Self-incrimination etc.	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30DH	Admissibility of report etc.	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30DK	Consultation	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30DL	Duration of system information software notice	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30DM	Compliance with system information software notice	An entity given a system information software notice must comply with the notice.	Functional	Intersects With	Non-Conformity Oversight	CPL-06	Mechanisms exist to identify and document instances of non-conformity with statutory, regulatory and/or contractual obligations, in order to develop appropriate risk mitigation actions.	5		CPL-01.1
30DM	Compliance with system information software notice	An entity given a system information software notice must comply with the notice.	Functional	Intersects With	Non-Conformity Corrective Action	CPL-06.1	Mechanisms exist to implement corrective action to remediate instances of non-conformity with applicable statutory, regulatory, and/or contractual compliance obligations.	5		CPL-02.3
30DN	Self-incrimination etc.	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30DP	Admissibility of information etc.	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30DQ	Designated officer	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30EA	Simplified outline of this Part	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
30ED	Secretary to assess notified changes and proposed changes	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
31	Simplified outline of this Part	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
33	Consultation before giving direction	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
34	Requirement to comply with direction	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35	Exception-acquisition of property	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AAB	Liability	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AA	Simplified outline of this Part	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AB	Ministerial authorisation	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AD	Consultation	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AE	Form and notification of Ministerial authorisation	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AF	Form of application for Ministerial authorisation	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AG	Duration of Ministerial authorisation	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AH	Revocation of Ministerial authorisation	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AJ	Minister to exercise powers personally	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AK	Information gathering direction	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AL	Form of direction	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AM	Compliance with an information gathering direction	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AN	Self-incrimination etc.	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AP	Admissibility of information etc.	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AQ	Action direction	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AR	Form of direction	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AS	Revocation of direction	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AT	Compliance with direction	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AV	Directions prevail over inconsistent obligations	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AW	Liability	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AX	Intervention request	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AY	Form and notification of request	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35AZ	Compliance with request	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35BA	Revocation of request	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Australia - Security of Critical Infrastructure Act 2018 (Compilation No. 9, 4 June 2026)
Focal Document URL: https://www.legislation.gov.au/C2018A00029/latest/text
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-aus-soci-2018.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	Legacy SCF #
35BB	Relevant entity to assist the authorised agency	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35BC	Constable may assist the authorised agency	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35BD	Removal and return of computers etc.	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35BE	Use of force against an individual not authorised	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35BF	Liability	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35BG	Evidentiary certificates	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
35BJ	Approved staff members of the authorised agency	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
36	Simplified outline of this Part	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
37	Secretary may obtain information or documents from entities	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
38	Copies of documents	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
39	Retention of documents	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
40	Self-incrimination	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
41	Authorised use and disclosure-performing functions etc.	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
42	Authorised use and disclosure-other person's functions etc.	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
43	Authorised disclosure relating to law enforcement	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
43AA	Authorised disclosure to Ombudsman official	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
43A	Authorised disclosure to IGIS official	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
43B	Authorised use and disclosure-Ombudsman official	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
43C	Authorised use and disclosure-IGIS official	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
43D	Authorised use and disclosure-ASD	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
44	Secondary use and disclosure of protected information	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
44A	Authorised APS employees	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
46	Exceptions to offence for unauthorised use or disclosure	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
47	No requirement to provide information	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
48	Simplified outline of this Part	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
49	Civil penalties, enforceable undertakings and injunctions	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
49A	Monitoring powers	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
49B	Investigation powers	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
49C	Infringement notices	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
50	Simplified outline of this Part	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
51	Declaration of assets by the Minister	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
51A	Consultation-declaration	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
52	Notification of change to reporting entities for asset	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
52A	Simplified outline of this Part	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
52C	Consultation-declaration	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
52E	Review of declaration	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
52F	Revocation of determination	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
53	Simplified outline of this Part	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
53A	How certain entities hold interests	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
54	Treatment of partnerships	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
55	Treatment of trusts and superannuation funds that are trusts	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
56	Treatment of unincorporated foreign companies	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
57	Additional power of Secretary	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
58	Assets ceasing to be critical infrastructure assets	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
59	Delegation of Secretary's powers	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
60	Periodic report	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
60AA	Compensation for acquisition of property	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
60A	Independent review	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
60B	Review of this Act	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		
61	Rules	See FDE for details	Functional	No Relationship	N/A	N/A	N/A	0		