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: UK - Cyber Assessment Framework for Aviation Guidance (CAP1850) (2020)

Focal Document URL: https://www.caa.co.uk/data-and-publications/publications/documents/content/cap1850/

Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-gbr-cap-1850-2020.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
A1	Governance	The organisation has appropriate management policies and processes in place to govern its approach to the security of critical systems.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
A1	Governance	The organisation has appropriate management policies and processes in place to govern its approach to the security of critical systems.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
A2	Risk management	The organisation takes appropriate steps to identify, assess and understand security risks to the critical systems supporting the operation of essential functions. This includes an overall organisational approach to risk management.	Functional	Intersects With	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	8	
A2	Risk management	The organisation takes appropriate steps to identify, assess and understand security risks to the critical systems supporting the operation of essential functions. This includes an overall organisational approach to risk management.	Functional	Intersects With	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.	3	
A2	Risk management	The organisation takes appropriate steps to identify, assess and understand security risks to the critical systems supporting the operation of essential functions. This includes an overall organisational approach to risk management.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	3	
A2	Risk management	The organisation takes appropriate steps to identify, assess and understand security risks to the critical systems supporting the operation of essential functions. This includes an overall organisational approach to risk management.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	3	
A2	Risk management	The organisation takes appropriate steps to identify, assess and understand security risks to the critical systems supporting the operation of essential functions. This includes an overall organisational approach to risk management.	Functional	Intersects With	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive and/or regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	3	
A2	Risk management	The organisation takes appropriate steps to identify, assess and understand security risks to the critical systems supporting the operation of essential functions. This includes an overall organisational approach to risk management.	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	3	
A2	Risk management	The organisation takes appropriate steps to identify, assess and understand security risks to the critical systems supporting the operation of essential functions. This includes an overall organisational approach to risk management.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	3	
A2	Risk management	The organisation takes appropriate steps to identify, assess and understand security risks to the critical systems supporting the operation of essential functions. This includes an overall organisational approach to risk management.	Functional	Intersects With	Risk Management Program	RSK-01	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	
A2	Risk management	The organisation takes appropriate steps to identify, assess and understand security risks to the critical systems supporting the operation of essential functions. This includes an overall organisational approach to risk management.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	3	
A2	Risk management	The organisation takes appropriate steps to identify, assess and understand security risks to the critical systems supporting the operation of essential functions. This includes an overall organisational approach to risk management.	Functional	Intersects With	Risk Assessment	RSK-04	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).	3	
A3	Asset management	Everything required to deliver, maintain or support critical systems is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5	
A4	Supply chain	The organisation understands and manages security risks to critical systems supporting the operation of essential functions that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	5	
A4	Supply chain	The organisation understands and manages security risks to critical systems supporting the operation of essential functions that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5	
A4	Supply chain	The organisation understands and manages security risks to critical systems supporting the operation of essential functions that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
A4	Supply chain	The organisation understands and manages security risks to critical systems supporting the operation of essential functions that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
A4	Supply chain	The organisation understands and manages security risks to critical systems supporting the operation of essential functions that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
B1	Function protection policies and processes	The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing critical systems and data that support operation of essential functions.	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	5	
B1	Function protection policies and processes	The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing critical systems and data that support operation of essential functions.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5	
B1	Function protection policies and processes	The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing critical systems and data that support operation of essential functions.	Functional	Intersects With	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive and/or regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5	
B2	Identity and access control	The organisation understands, documents, and manages access to critical systems supporting the operation of essential functions. Users (or automated functions) that can access critical data or critical systems are appropriately verified, authenticated and authorised.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
B2	Identity and access control	The organisation understands, documents, and manages access to critical systems supporting the operation of essential functions. Users (or automated functions) that can access critical data or critical systems are appropriately verified, authenticated and authorised.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	8	

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: UK - Cyber Assessment Framework for Aviation Guidance (CAP1850) (2020)
Focal Document URL: https://www.caa.co.uk/data-and-publications/publications/documents/content/cap1850/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-gbr-cap-1850-2020.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
B2	Identity and access control	The organisation understands, documents, and manages access to critical systems supporting the operation of essential functions. Users (or automated functions) that can access critical data or critical systems are appropriately verified, authenticated and authorised.	Functional	Intersects With	Automated System Account Management (Directory Services)	IAC-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5	
B3	Data security	Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause an adverse impact on critical systems. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for the operation of critical systems. It also covers information that would assist an attacker, such as design details of critical systems.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
B3	Data security	Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause an adverse impact on critical systems. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for the operation of critical systems. It also covers information that would assist an attacker, such as design details of critical systems.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
B3	Data security	Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause an adverse impact on critical systems. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for the operation of critical systems. It also covers information that would assist an attacker, such as design details of critical systems.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
B4	System security	Critical systems and technology critical for the operation of essential functions are protected from cyber attack. An organisational understanding of risk to the critical system informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5	
B4	System security	Critical systems and technology critical for the operation of essential functions are protected from cyber attack. An organisational understanding of risk to the critical system informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5	
B4	System security	Critical systems and technology critical for the operation of essential functions are protected from cyber attack. An organisational understanding of risk to the critical system informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.	Functional	Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5	
B4	System security	Critical systems and technology critical for the operation of essential functions are protected from cyber attack. An organisational understanding of risk to the critical system informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5	
B5	Resilient Networks and Systems	The organisation builds resilience against cyber-attack and system failure into the design, implementation, operation and management of critical systems.	Functional	Intersects With	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	5	
B5	Resilient Networks and Systems	The organisation builds resilience against cyber-attack and system failure into the design, implementation, operation and management of critical systems.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to: (1) Unintentional errors (by users or software); and (2) Intentional attack or circumvention.	5	
B6	Staff Awareness and Training	Staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to the security of critical systems supporting the operation of essential functions.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	
B6	Staff Awareness and Training	Staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to the security of critical systems supporting the operation of essential functions.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
C1	Security monitoring	The organisation monitors the security status of the network and systems supporting the operation of critical systems in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
C2	Proactive security event discovery	The organisation detects, within critical systems, malicious activity affecting, or with the potential to affect, the operation of essential functions even when the activity evades standard signature-based security prevent/detect solutions (or when standard solutions are not deployable).	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
D1	Response and recovery planning	There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential functions in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
D1	Response and recovery planning	There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential functions in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
D2	Lessons learned	When an incident occurs, steps are taken to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents.	Functional	Intersects With	Continuous Incident Response Improvements	IRO-04.3	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	
D2	Lessons learned	When an incident occurs, steps are taken to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5	