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

Reference Document : Secure Controls Framework (SCF) version 2025.4
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: **ISO/IEC 29100:2024 Information technology — Security techniques — Privacy framework**
Focal Document URL: https://www.iso.org/standard/85938.html
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-general-iso-29100-2024.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
6.1	Overview of privacy principles	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	Functional	no relationship	N/A	N/A	N/A		
6.2	Consent and choice	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
6.3	Purpose legitimacy and specification	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	8	
6.3	Purpose legitimacy and specification	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	Functional	Intersects With	Purpose Specification	PRI-02.1	Mechanisms exist to ensure data privacy notices identify the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared.	8	
6.3	Purpose legitimacy and specification	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	Functional	Intersects With	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD), either generally or in support of a specific business process.	5	
6.4	Collection limitation	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	Functional	Intersects With	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.	8	
6.5	Data minimization	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	Functional	Subset Of	Minimize Sensitive / Regulated Data	DCH-18.1	Mechanisms exist to minimize sensitive/regulated data that is collected, received, processed, stored and/or transmitted throughout the information lifecycle to only those elements necessary to support necessary business processes.	10	
6.5	Data minimization	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	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	
6.5	Data minimization	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	Functional	Intersects With	Active Participation By Data Subjects	PRI-03.7	Mechanisms exist to compel data subjects to select the level of consent deemed appropriate by the data subject for the relevant business purpose (e.g., opt-in, opt-out, accept all cookies, etc.).	8	
6.5	Data minimization	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	Functional	Intersects With	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.	8	
6.5	Data minimization	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	
6.6	Use, retention and disclosure limitation	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	Functional	Intersects With	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	5	
6.6	Use, retention and disclosure limitation	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	Functional	Intersects With	Continued Use of Personal Data (PD)	PRI-03.9	Mechanisms exist to govern the continued use of Personal Data (PD) as it is collected, received, processed, stored, transmitted, shared and/or updated until: (1) Disposal of PD occurs when there is no longer a legitimate business purpose; (2) Disposal of PD occurs when the data retention timeline for the use case is met; and/or (3) Continued use of PD is prohibited upon withdrawal of data subject consent.	5	
6.6	Use, retention and disclosure limitation	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	
6.6	Use, retention and disclosure limitation	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	5	
6.7	Accuracy and quality	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	Functional	Intersects With	Primary Source Personal Data (PD) Collection	DCH-22.3	Mechanisms exist to collect Personal Data (PD) directly from the individual.	8	
6.7	Accuracy and quality	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	Functional	Intersects With	Personal Data (PD) Collection Methods	PRI-04.7	Mechanisms exist to ensure that Personal Data (PD) collection methods are: (1) In accordance with applicable statutory and/or regulatory requirements; (2) Appropriate for the circumstances of the data subject; (3) Unambiguous; and (4) Secure.	5	
6.7	Accuracy and quality	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	Functional	Intersects With	Personal Data (PD) Accuracy & Integrity	PRI-05.2	Mechanisms exist to ensure the accuracy and relevance of Personal Data (PD) throughout the information lifecycle by: (1) Keeping PD up-to-date; and (2) Remediating identified inaccuracies, as necessary.	5	
6.8	Openness, transparency and notice	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	Functional	Subset Of	Dissemination of Data Privacy Program Information	PRI-01.3	Mechanisms exist to: (1) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role; (2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories; (3) Utilize publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy office(s) regarding data privacy practices; and (4) Inform data subjects when changes are made to the privacy notice and the nature of such changes.	10	

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
6.8	Openness, transparency and notice	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	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.	8	
6.9	Individual participation and access	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	10	
6.9	Individual participation and access	Buy a copy of ISO 29100 for control content: https://www.iso.org/standard/85938.html	Functional	Intersects With	Correcting Inaccurate Personal Data (PD)	PRI-06.1	Mechanisms exist to maintain a process for: (1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and (2) Disseminating corrections or amendments of PD to other authorized users of the PD.	5	