Set Theory Relationship Mapping (STRM)

Reference Document : Secure Controls Framework (SCF) version 2024.2
Focal Document: Tennessee Information Protection Act
Focal Document URL: https://www.capitol.tn.gov/Bills/113/Amend/HA0348.pdf
STRM URL: https://content.securecontrolsframework.com/strm/scf-2024-2-tn-information-protection-act.pdf

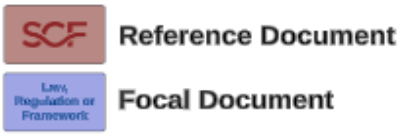
Set Theory Relationship Mapping (STRM) is well-suited for mapping between sets of elements that exist in two distinct concepts that are mostly the same as each other (e.g., cybersecurity & data privacy requirements). STRM also allows the strength of the mapping to be captured.

STRM relies on a justification for the relationship claim. There are three (3) options for the rationale, which is a high-level context within which the two concepts are related:

1. **Syntactic**: How similar is the wording that expresses the two concepts? This is a word-for-word analysis of the relationship, not an interpretation of the language.
2. **Semantic**: How similar are the meanings of the two concepts? This involves some interpretation of each concept's language.
3. **Functional**: How similar are the results of executing the two concepts? This involves understanding what will happen if the two concepts are implemented, performed, or otherwise executed.

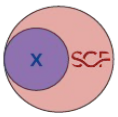
Based on NIST IR 8477, STRM supports five (5) five relationship types to describe the logical similarity between two distinct concepts:

1. **Subset Of**
2. **Intersects With**
3. **Equal**
4. **Superset Of**
5. **No Relationship**

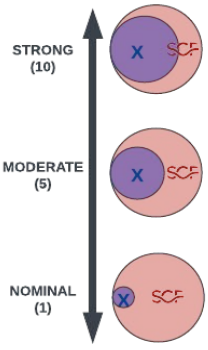


Relationship Type #1: SUBSET OF

Focal Document Element is a subset of SCF control. In other words, SCF control contains everything that Focal Document Element does and more.

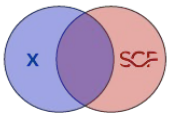


SUBSET OF
Relative Relationship Strength (control versus control)

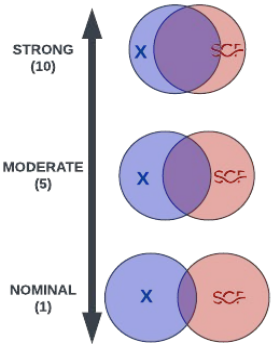


Relationship Type #2: INTERSECTS WITH

SCF control has some overlap with Focal Document Element, but each includes content that the other does not.

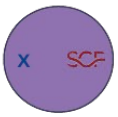


INTERSECTS WITH
Relative Relationship Strength (control versus control)

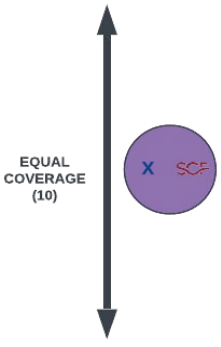


Relationship Type #3: EQUAL

SCF control and Focal Document Element are the same, although not necessarily identical.

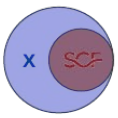


EQUAL
Relative Relationship Strength (control versus control)

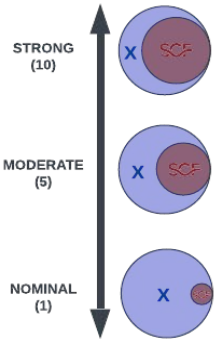


Relationship Type #4: SUPERSET OF

Focal Document Element is a superset of SCF control. In other words, Focal Document Element contains everything that SCF control does and more.

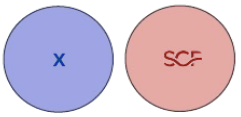


SUPERSET OF
Relative Relationship Strength (control versus control)

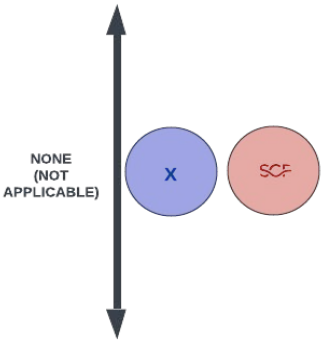


Relationship Type #5: NO RELATIONSHIP

SCF control and Focal Document Element are unrelated; their content does not overlap.



NO RELATIONSHIP
Relative Relationship Strength (control versus control)



FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
47-18-3201	Definitions	(see definitions section)	Functional	intersects with	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	5	
47-18-3202	Scope	This part applies to persons that conduct business in this state producing products or services that target residents of this state and that: (1) Exceed twenty-five million dollars ($25,000,000) in revenue; and (2) (A) Control or process personal information of at least twenty-five thousand (25,000) consumers and derive more than fifty percent (50%) of gross revenue from the sale of personal information; or (B) During a calendar year, control or process personal information of at least one hundred seventy-five thousand (175,000) consumers	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
47-18-3203	Personal information rights – Consumers	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
47-18-3203(a)	N/A	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
47-18-3203(a)(1)	N/A	A consumer may invoke the consumer rights authorized pursuant to subdivision (a)(2) at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to invoke. A known child's parent or legal guardian may invoke the consumer rights authorized pursuant to subdivision (a)(2) on behalf of the child regarding processing personal information belonging to the known child.	Functional	intersects with	Data Subject Access	PRI-06	Mechanisms exist to provide data subjects the ability to access their Personal Data (PD) maintained in organizational systems of records.	5	
			Functional	intersects with	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	5	
47-18-3203(a)(2)	N/A	A controller shall comply with an authenticated consumer request to exercise the right to:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
47-18-3203(a)(2)(A)	N/A	Confirm whether a controller is processing the consumer's personal information and to access the personal information;	Functional	intersects with	Data Subject Access	PRI-06	Mechanisms exist to provide data subjects the ability to access their Personal Data (PD) maintained in organizational systems of records.	5	
47-18-3203(a)(2)(B)	N/A	Correct inaccuracies in the consumer's personal information, taking into account the nature of the personal information and the purposes of the processing of the consumer's personal information;	Functional	intersects with	Correcting Inaccurate Personal Data	PRI-06.1	Mechanisms exist to establish and implement a process for: • Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and • Disseminating corrections or amendments of PD to other authorized users of the PD.	5	
47-18-3203(a)(2)(C)	N/A	Delete personal information provided by or obtained about the consumer. A controller is not required to delete information that it maintains or uses as aggregate or de-identified data; provided, that such data in the possession of the controller is not linked to a specific consumer. A controller that obtained personal information about a consumer from a	Functional	intersects with	De-Identification (Anonymization)	DCH-23	Mechanisms exist to anonymize data by removing Personal Data (PD) from datasets.	5	
			Functional	intersects with	Right to Erasure	PRI-06.5	Mechanisms exist to erase Personal Data (PD) of a data subject, without delay.	5	
47-18-3203(a)(2)(C)(i)	N/A	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
47-18-3203(a)(2)(C)(i)(a)	N/A	Retaining a record of the deletion request and the minimum information necessary for the purpose of ensuring that the consumer's personal information remains deleted from the controller's records; and	Functional	intersects with	Personal Data Retention & Disposal	PRI-05	Mechanisms exist to: • 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; • Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and • Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	
			Functional	intersects with	Right to Erasure	PRI-06.5	Mechanisms exist to erase Personal Data (PD) of a data subject, without delay.	5	
47-18-3203(a)(2)(C)(i)(b)	N/A	Not using such retained personal information for any purpose prohibited under this part; or	Functional	intersects with	Usage Restrictions of Sensitive Personal Data	PRI-05.4	Mechanisms exist to restrict the use of Personal Data (PD) to only the authorized purpose(s) consistent with applicable laws, regulations and in data privacy notices.	5	
			Functional	intersects with	Right to Erasure	PRI-06.5	Mechanisms exist to erase Personal Data (PD) of a data subject, without delay.	5	
47-18-3203(a)(2)(C)(ii)	N/A	Opting the consumer out of the processing of such personal data for any purpose except for those exempted under this part;	Functional	intersects with	Usage Restrictions of Sensitive Personal Data	PRI-05.4	Mechanisms exist to restrict the use of Personal Data (PD) to only the authorized purpose(s) consistent with applicable laws, regulations and in data privacy notices.	5	
			Functional	intersects with	Right to Erasure	PRI-06.5	Mechanisms exist to erase Personal Data (PD) of a data subject, without delay.	5	
47-18-3203(a)(2)(D)	N/A	Obtain a copy of the consumer's personal information that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means; or	Functional	intersects with	Data Portability	PRI-06.6	Mechanisms exist to export Personal Data (PD) in a structured, commonly used and machine-readable format that allows the data subject to transmit the data to another controller without hindrance.	5	
			Functional	intersects with	Personal Data Exportability	PRI-06.7	Mechanisms exist to digitally export Personal Data (PD) in a secure manner upon request by the data subject.	5	
47-18-3203(a)(2)(E)	N/A	Opt out of a controller's processing of personal information for purposes of:	Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to authorize the processing of their Personal Data (PD) prior to its collection that: • Uses plain language and provide examples to illustrate the potential data privacy risks of the authorization; and • Provides a means for users to decline the authorization.	5	
47-18-3203(a)(2)(E)(i)	N/A	Selling personal information about the consumer;	Functional	intersects with	Prohibition Of Selling or Sharing Personal Data	PRI-03.3	Mechanisms exist to prevent the sale or sharing of Personal Data (PD) when instructed by the data subject.	5	
			Functional	intersects with	Tailored Consent	PRI-03.1	Mechanisms exist to allow data subjects to modify the use permissions to selected attributes of their Personal Data (PD).	5	
47-18-3203(a)(2)(E)(ii)	N/A	Targeted advertising; or	Functional	intersects with	Tailored Consent	PRI-03.1	Mechanisms exist to allow data subjects to modify the use permissions to selected attributes of their Personal Data (PD).	5	
			Functional	intersects with	Prohibition Of Selling or Sharing Personal Data	PRI-03.3	Mechanisms exist to prevent the sale or sharing of Personal Data (PD) when instructed by the data subject.	5	
47-18-3203(a)(2)(E)(iii)	N/A	Profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.	Functional	intersects with	Prohibition Of Selling or Sharing Personal Data	PRI-03.3	Mechanisms exist to prevent the sale or sharing of Personal Data (PD) when instructed by the data subject.	5	
			Functional	intersects with	Tailored Consent	PRI-03.1	Mechanisms exist to allow data subjects to modify the use permissions to selected attributes of their Personal Data (PD).	5	
47-18-3203(b)	N/A	Except as otherwise provided in this part, a controller shall comply with an authenticated request by a consumer to exercise the consumer rights authorized pursuant to subdivision (a)(2) as follows:	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.).	5	
			Functional	intersects with	Tailored Consent	PRI-03.1	Mechanisms exist to allow data subjects to modify the use permissions to selected attributes of their Personal Data (PD).	5	
			Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to authorize the processing of their Personal Data (PD) prior to its collection that: • Uses plain language and provide examples to illustrate the potential data privacy risks of the authorization; and • Provides a means for users to decline the authorization.	5	
47-18-3203(b)(1)	N/A	A controller shall respond to the consumer without undue delay, but in all cases within forty-five (45) days of receipt of a request submitted pursuant to subsection (a). The response period may be extended once by forty-five (45) additional days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of the extension within the initial forty-five-day response period, together with the reason for the extension;	Functional	intersects with	Notice of Correction or Processing Change	PRI-06.2	Mechanisms exist to notify affected data subjects if their Personal Data (PD) has been corrected or amended.	5	
			Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to implement a process for receiving and responding to complaints, concerns or questions from data subjects about the organizational data privacy practices.	5	
47-18-3203(b)(2)	N/A	If a controller declines to take action regarding the consumer's request, then the controller shall inform the consumer without undue delay, but in all cases and at the latest within forty-five (45) days of receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision pursuant to subsection (c);	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to implement a process for receiving and responding to complaints, concerns or questions from data subjects about the organizational data privacy practices.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
47-18-3203(b)(3)	N/A	Information provided in response to a consumer request must be provided by a controller free of charge, up to twice annually per consumer. If requests from a consumer are manifestly unfounded, technically infeasible, excessive, or repetitive, then the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, technically infeasible, excessive, or repetitive nature of the request; and	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to implement a process for receiving and responding to complaints, concerns or questions from data subjects about the organizational data privacy practices.	5	
47-18-3203(b)(4)	N/A	If a controller is unable to authenticate the request using commercially reasonable efforts, then the controller is not required to comply with a request to initiate an action under subsection (a) and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to implement a process for receiving and responding to complaints, concerns or questions from data subjects about the organizational data privacy practices.	5	
			Functional	intersects with	Reject Unauthorized Disclosure Requests	PRI-07.4	Mechanisms exist to reject unauthorized disclosure requests.	5	
47-18-3203(c)	N/A	A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision pursuant to subdivision (b)(2). The appeal process must be made available to the consumer in a conspicuous manner, must be available at no cost to the consumer, and must be similar to the process for submitting requests to initiate action pursuant to subsection (a). Within sixty (60) days of receipt of an appeal, a controller shall inform the consumer in writing of action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, then the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general and reporter to submit a complaint	Functional	intersects with	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to provide an organization-defined process for data subjects to appeal an adverse decision and have incorrect information amended.	5	
47-18-3204	Data controller responsibilities – Transparency	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
47-18-3204(a)	N/A	A controller shall:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
47-18-3204(a)(1)	N/A	Limit the collection of personal information to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer;	Functional	intersects with	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to collect Personal Data (PD) only for the purposes identified in the data privacy notice and includes protections against collecting PD from minors without appropriate parental, or legal guardian, consent.	5	
			Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: • Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; • Ensures that data privacy notices are clear and easy-to-understand, expressing information about Personal Data (PD) processing in plain language that meets all legal obligations; • Defines 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; • Content of the privacy notice is periodically reviewed and updates made as necessary; and • Prior versions of the privacy notice are retained in accordance with data retention requirements.	5	
47-18-3204(a)(2)	N/A	Except as otherwise provided in this part, not process personal information for purposes that are beyond what is reasonably necessary to and compatible with the disclosed purposes for which the personal information is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;	Functional	intersects with	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to collect Personal Data (PD) only for the purposes identified in the data privacy notice and includes protections against collecting PD from minors without appropriate parental, or legal guardian, consent.	5	
			Functional	intersects with	Internal Use of Personal Data For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: • Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and • Authorizes the use of PD when such information is required for internal testing, training and research.	5	
47-18-3204(a)(3)	N/A	Establish, implement, and maintain reasonable administrative, technical, and physical data security practices, as described in § 47-18-3213, to protect the confidentiality, integrity, and accessibility of personal information. The data security practices must be appropriate to the volume and nature of the personal information at issue;	Functional	intersects with	Security of Personal Data	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	5	
47-18-3204(a)(4)	N/A	Not be required to delete information that it maintains or uses as aggregate or de-identified data, provided that such data in the possession of the business is not linked to a specific consumer;	Functional	intersects with	Personal Data Retention & Disposal	PRI-05	Mechanisms exist to: • 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; • Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and • Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	
47-18-3204(a)(5)	N/A	Not process personal information in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising the consumer rights contained in this part, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. However, this subdivision (a)(5) does not require a controller to provide a product or service that requires the personal information of a consumer that the controller does not collect or maintain, or prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised the right to opt out pursuant to § 47-18-3203(a)(2)(F) or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program; and	Functional	intersects with	Authority To Collect, Use, Maintain & Share Personal Data	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the collection, use, maintenance and sharing of Personal Data (PD), either generally or in support of a specific program or system need.	5	
47-18-3204(a)(6)	N/A	Not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing the data in accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.) and its implementing regulations	Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to authorize the processing of their Personal Data (PD) prior to its collection that: • Uses plain language and provide examples to illustrate the potential data privacy risks of the authorization; and • Provides a means for users to decline the authorization.	5	
			Functional	intersects with	Usage Restrictions of Sensitive Personal Data	PRI-05.4	Mechanisms exist to restrict the use of Personal Data (PD) to only the authorized purpose(s) consistent with applicable laws, regulations and in data privacy notices.	5	
47-18-3204(b)	N/A	A provision of a contract or agreement that purports to waive or limit the consumer rights described in § 47-18-3203 is contrary to public policy and is void and unenforceable	Functional	intersects with	Authority To Collect, Use, Maintain & Share Personal Data	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the collection, use, maintenance and sharing of Personal Data (PD), either generally or in support of a specific program or system need.	5	
47-18-3204(c)	N/A	A controller shall provide a reasonably accessible, clear, and meaningful privacy notice that includes:	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: • Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; • Ensures that data privacy notices are clear and easy-to-understand, expressing information about Personal Data (PD) processing in plain language that meets all legal obligations; • Defines 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; • Content of the privacy notice is periodically reviewed and updates made as necessary; and • Prior versions of the privacy notice are retained in accordance with data retention requirements.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
47-18-3204(c)(1)	N/A	The categories of personal information processed by the controller;	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: • Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; • Ensures that data privacy notices are clear and easy-to-understand, expressing information about Personal Data (PD) processing in plain language that meets all legal obligations; • Defines 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; • Content of the privacy notice is periodically reviewed and updates made as necessary; and • Prior versions of the privacy notice are retained in accordance with data retention requirements.	5	
47-18-3204(c)(2)	N/A	The purpose for processing personal information;	Functional	intersects with	Purpose Specification	PRI-02.1	Mechanisms exist to identify and document the purpose(s) for which Personal Data (PD) is collected, used, maintained and shared in its data privacy notices.	5	
			Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: • Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; • Ensures that data privacy notices are clear and easy-to-understand, expressing information about Personal Data (PD) processing in plain language that meets all legal obligations; • Defines 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; • Content of the privacy notice is periodically reviewed and updates made as necessary; and • Prior versions of the privacy notice are retained in accordance with data retention requirements.	5	
47-18-3204(c)(3)	N/A	How consumers may exercise their consumer rights pursuant to § 47-18-3203, including how a consumer may appeal a controller's decision with regard to the consumer's request;	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: • Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; • Ensures that data privacy notices are clear and easy-to-understand, expressing information about Personal Data (PD) processing in plain language that meets all legal obligations; • Defines 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; • Content of the privacy notice is periodically reviewed and updates made as necessary; and • Prior versions of the privacy notice are retained in accordance with data retention requirements.	5	
47-18-3204(c)(4)	N/A	The categories of personal information that the controller sells to third parties, if any; and	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: • Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; • Ensures that data privacy notices are clear and easy-to-understand, expressing information about Personal Data (PD) processing in plain language that meets all legal obligations; • Defines 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; • Content of the privacy notice is periodically reviewed and updates made as necessary; and • Prior versions of the privacy notice are retained in accordance with data retention requirements.	5	
47-18-3204(c)(5)	N/A	The categories of third parties, if any, to whom the controller sells personal information	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: • Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; • Ensures that data privacy notices are clear and easy-to-understand, expressing information about Personal Data (PD) processing in plain language that meets all legal obligations; • Defines 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; • Content of the privacy notice is periodically reviewed and updates made as necessary; and • Prior versions of the privacy notice are retained in accordance with data retention requirements.	5	
47-18-3204(d)	N/A	If a controller sells personal information to third parties or processes personal information for targeted advertising, then the controller shall clearly and conspicuously disclose the processing, as well as the manner in which a consumer may exercise the right to opt out of the processing	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: • Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; • Ensures that data privacy notices are clear and easy-to-understand, expressing information about Personal Data (PD) processing in plain language that meets all legal obligations; • Defines 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; • Content of the privacy notice is periodically reviewed and updates made as necessary; and • Prior versions of the privacy notice are retained in accordance with data retention requirements.	5	
			Functional	intersects with	Prohibition Of Selling or Sharing Personal Data	PRI-03.3	Mechanisms exist to prevent the sale or sharing of Personal Data (PD) when instructed by the data subject.	5	
47-18-3204(e)	N/A	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
47-18-3204(e)(1)	N/A	A controller shall provide, and shall describe in a privacy notice, one (1) or more secure and reliable means for a consumer to submit a request to exercise the consumer rights in § 47-18-3203. Such means must take into account the:	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: • Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; • Ensures that data privacy notices are clear and easy-to-understand, expressing information about Personal Data (PD) processing in plain language that meets all legal obligations; • Defines 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; • Content of the privacy notice is periodically reviewed and updates made as necessary; and • Prior versions of the privacy notice are retained in accordance with data retention requirements.	5	
47-18-3204(e)(1)(A)	N/A	Ways in which a consumer normally interacts with the controller;	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to implement a process for receiving and responding to complaints, concerns or questions from data subjects about the organizational data privacy practices.	5	
47-18-3204(e)(1)(B)	N/A	Need for secure and reliable communication of such requests; and	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to implement a process for receiving and responding to complaints, concerns or questions from data subjects about the organizational data privacy practices.	5	
47-18-3204(e)(1)(C)	N/A	Ability of a controller to authenticate the identity of the consumer making the request.	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to implement a process for receiving and responding to complaints, concerns or questions from data subjects about the organizational data privacy practices.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
47-18-3204(e)(2)	N/A	A controller shall not require a consumer to create a new account in order to exercise consumer rights in § 47-18-3203, but may require a consumer to use an existing account	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to implement a process for receiving and responding to complaints, concerns or questions from data subjects about the organizational data privacy practices.	5	
47-18-3205	Responsibility according to role – Controller and processor.	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
47-18-3205(a)	N/A	A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under this part. The assistance must include:	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	
47-18-3205(a)(1)	N/A	Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as this is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests pursuant to § 47-18-3203; and	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	
47-18-3205(a)(2)	N/A	Providing necessary information to enable the controller to conduct and document data protection assessments pursuant to § 47-18-3206.	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	
47-18-3205(b)	N/A	A contract between a controller and a processor governs the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract is binding and must clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract must also include requirements that the processor shall:	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	
47-18-3205(b)(1)	N/A	Ensure that each person processing personal information is subject to a duty of confidentiality with respect to the data;	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	
47-18-3205(b)(2)	N/A	At the controller's direction, delete or return all personal information to the controller as requested at the end of the provision of services, unless retention of the personal information is required by law;	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	
47-18-3205(b)(3)	N/A	Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this part;	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	
47-18-3205(b)(4)	N/A	Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this part using an appropriate and accepted control standard or framework and assessment procedure for the assessments. The processor shall provide a report of each assessment to the controller upon request; and	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	
47-18-3205(b)(5)	N/A	Engage a subcontractor pursuant to a written contract in that requires the subcontractor to meet the obligations of the processor with respect to the personal information	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	
47-18-3205(c)	N/A	This section does not relieve a controller or a processor from the liabilities imposed on it by virtue of its role in the processing relationship as described in subsection (b)	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	
47-18-3205(d)	N/A	Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal information is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal information remains a processor.	Functional	intersects with	Joint Processing of Personal Data	PRI-07.2	Mechanisms exist to clearly define and communicate the organization's role in processing Personal Data (PD) in the data processing ecosystem.	5	
			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	
47-18-3206	Data protection assessments.	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
47-18-3206(a)	N/A	A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal information:	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
47-18-3206(a)(1)	N/A	The processing of personal information for purposes of targeted advertising;	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
47-18-3206(a)(2)	N/A	The sale of personal information;	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
47-18-3206(a)(3)	N/A	The processing of personal information for purposes of profiling, where the profiling presents a reasonably foreseeable risk of:	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
47-18-3206(a)(3)(A)	N/A	Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
47-18-3206(a)(3)(B)	N/A	Financial, physical, or reputational injury to consumers;	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
47-18-3206(a)(3)(C)	N/A	A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where the intrusion would be offensive to a reasonable person; or	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
47-18-3206(a)(3)(D)	N/A	Other substantial injury to consumers;	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
47-18-3206(a)(4)	N/A	The processing of sensitive data; and	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
47-18-3206(a)(5)	N/A	Processing activities involving personal information that present a heightened risk of harm to consumers	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
47-18-3206(b)	N/A	Data protection assessments conducted pursuant to subsection (a) must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards that can be employed by the controller to reduce the risks. The use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal information will be processed, must be factored into this assessment by the controller	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
47-18-3206(c)	N/A	The attorney general and reporter may request pursuant to a civil investigative demand that a controller disclose a data protection assessment that is relevant to an investigation conducted by the attorney general and reporter, and the controller shall make the data protection assessment available to the attorney general and reporter. The attorney general and reporter may evaluate the data protection assessment for compliance with the responsibilities set forth in § 47-18-3204. Data protection assessments are confidential and not open to public inspection and copying. The disclosure of a data protection assessment pursuant to a request from the attorney general and reporter does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and information contained in the assessment	Functional	intersects with	Investigation Access Restrictions	CPL-05.2	Mechanisms exist to support official investigations by provisioning government investigators with "least privileges" and "least functionality" to ensure that government investigators only have access to the data and systems needed to perform the investieation.	5	
			Functional	intersects with	Legal Assessment of Investigative Inquires	CPL-05	Mechanisms exist to determine whether a government agency has an applicable and valid legal basis to request data from the organization and what further steps need to be taken, if necessary.	5	
			Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
47-18-3206(d)	N/A	A single data protection assessment may address a comparable set of processing operations that include similar activities.	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
47-18-3206(e)	N/A	Data protection assessments conducted by a controller for the purpose of compliance with other laws, rules, or regulations may comply with this section if the assessments have a reasonably comparable scope and effect.	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
47-18-3206(f)	N/A	Data protection assessment requirements apply to processing activities created or generated on or after July 1, 2024, and are not retroactive.	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
47-18-3207	Processing de-identified data – Exemptions	N/A	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
47-18-3207(a)	N/A	The controller in possession of de-identified data shall:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
47-18-3207(a)(1)	N/A	Take reasonable measures to ensure that the data cannot be associated with a natural person;	Functional	intersects with	Internal Use of Personal Data For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: • Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and • Authorizes the use of PD when such information is required for internal testing, training and research.	5	
47-18-3207(a)(2)	N/A	Publicly commit to maintaining and using de-identified data without attempting to reidentify the data; and	Functional	intersects with	Internal Use of Personal Data For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: • Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and • Authorizes the use of PD when such information is required for internal testing, training and research.	5	
47-18-3207(a)(3)	N/A	Contractually obligate recipients of the de-identified data to comply with this part.	Functional	intersects with	Internal Use of Personal Data For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: • Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and • Authorizes the use of PD when such information is required for internal testing, training and research.	5	
47-18-3207(b)	N/A	This section does not require a controller or processor to:	Functional	intersects with	Usage Restrictions of Sensitive Personal Data	PRI-05.4	Mechanisms exist to restrict the use of Personal Data (PD) to only the authorized purpose(s) consistent with applicable laws, regulations and in data privacy notices.	5	
47-18-3207(b)(1)	N/A	Reidentify de-identified data or pseudonymous data;	Functional	intersects with	Internal Use of Personal Data For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: • Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and • Authorizes the use of PD when such information is required for internal testing, training and research.	5	
47-18-3207(b)(2)	N/A	Maintain data in identifiable form, or collect, obtain, retain, or access data or technology, in order to be capable of associating an authenticated consumer request with personal information; or	Functional	intersects with	Internal Use of Personal Data For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: • Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and • Authorizes the use of PD when such information is required for internal testing, training and research.	5	
47-18-3207(b)(3)	N/A	Comply with an authenticated consumer rights request, pursuant to § 47-18-3203, if:	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to implement a process for receiving and responding to complaints, concerns or questions from data subjects about the organizational data privacy practices.	5	
			Functional	intersects with	Internal Use of Personal Data For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: • Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and • Authorizes the use of PD when such information is required for internal testing, training and research.	5	
47-18-3207(b)(3)(A)	N/A	The controller is not reasonably capable of associating the request with the personal information or it would be unreasonably burdensome for the controller to associate the request with the personal information;	Functional	intersects with	Internal Use of Personal Data For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: • Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and • Authorizes the use of PD when such information is required for internal testing, training and research.	5	
			Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to implement a process for receiving and responding to complaints, concerns or questions from data subjects about the organizational data privacy practices.	5	
47-18-3207(b)(3)(B)	N/A	The controller does not use the personal information to recognize or respond to the specific consumer who is the subject of the personal information, or associate the personal information with other personal information about the same specific consumer; and	Functional	intersects with	Internal Use of Personal Data For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: • Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and • Authorizes the use of PD when such information is required for internal testing, training and research.	5	
			Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to implement a process for receiving and responding to complaints, concerns or questions from data subjects about the organizational data privacy practices.	5	
47-18-3207(b)(3)(C)	N/A	The controller does not sell the personal information to a third party or otherwise voluntarily disclose the personal information to a third party other than a processor, except as otherwise permitted in this section.	Functional	intersects with	Internal Use of Personal Data For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: • Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and • Authorizes the use of PD when such information is required for internal testing, training and research.	5	
			Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to implement a process for receiving and responding to complaints, concerns or questions from data subjects about the organizational data privacy practices.	5	
47-18-3207(c)	N/A	The consumer rights contained in §§ 47-18-3203 and 47-18-3204 do not apply to pseudonymous data in cases where the controller is able to demonstrate information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing that information.	Functional	intersects with	Usage Restrictions of Sensitive Personal Data	PRI-05.4	Mechanisms exist to restrict the use of Personal Data (PD) to only the authorized purpose(s) consistent with applicable laws, regulations and in data privacy notices.	5	
47-18-3207(d)	N/A	A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address breaches of those contractual commitments.	Functional	intersects with	Usage Restrictions of Sensitive Personal Data	PRI-05.4	Mechanisms exist to restrict the use of Personal Data (PD) to only the authorized purpose(s) consistent with applicable laws, regulations and in data privacy notices.	5	