NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference document: Secure Controls Framework (SCF) version 2026.1
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Texas Identity Theft Enforcement and Protection Act (BC521) (2009)**
Focal Document URL: https://statutes.capitol.texas.gov/?tab=1&code=BC&chapter=BC.521&artSec=
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-tx-bc521-2009.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
521.001	SHORT TITLE	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
521.002	DEFINITIONS	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
521.051	UNAUTHORIZED USE OR POSSESSION OF PERSONAL IDENTIFYING INFORMATION	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
521.051(a)	UNAUTHORIZED USE OR POSSESSION OF PERSONAL IDENTIFYING INFORMATION	A person may not obtain, possess, transfer, or use personal identifying information of another person without the other person's consent or effective consent and with intent to obtain a good, a service, insurance, an extension of credit, or any other thing of value in the other person's name.	Functional	Subset Of	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.	10	
521.051(a)	UNAUTHORIZED USE OR POSSESSION OF PERSONAL IDENTIFYING INFORMATION	A person may not obtain, possess, transfer, or use personal identifying information of another person without the other person's consent or effective consent and with intent to obtain a good, a service, insurance, an extension of credit, or any other thing of value in the other person's name.	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.	8	
521.051(a-1)	UNAUTHORIZED USE OR POSSESSION OF PERSONAL IDENTIFYING INFORMATION	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
521.051(b)	UNAUTHORIZED USE OR POSSESSION OF PERSONAL IDENTIFYING INFORMATION	It is a defense to an action brought under this section that an act by a person:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
521.051(b)(1)	UNAUTHORIZED USE OR POSSESSION OF PERSONAL IDENTIFYING INFORMATION	is covered by the Fair Credit Reporting Act (15 U.S.C. Section 1681 et seq.); and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
521.051(b)(2)	UNAUTHORIZED USE OR POSSESSION OF PERSONAL IDENTIFYING INFORMATION	is in compliance with that Act and regulations adopted under that Act.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
521.051(c)	UNAUTHORIZED USE OR POSSESSION OF PERSONAL IDENTIFYING INFORMATION	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
521.052	BUSINESS DUTY TO PROTECT SENSITIVE PERSONAL INFORMATION	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
521.052(a)	BUSINESS DUTY TO PROTECT SENSITIVE PERSONAL INFORMATION	A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.	Functional	Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	8	
521.052(a)	BUSINESS DUTY TO PROTECT SENSITIVE PERSONAL INFORMATION	A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.	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	
521.052(b)	BUSINESS DUTY TO PROTECT SENSITIVE PERSONAL INFORMATION	A business shall destroy or arrange for the destruction of customer records containing sensitive personal information within the business's custody or control that are not to be retained by the business by:	Functional	Subset Of	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).	10	
521.052(b)(1)	BUSINESS DUTY TO PROTECT SENSITIVE PERSONAL INFORMATION	shredding;	Functional	Subset Of	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).	10	
521.052(b)(2)	BUSINESS DUTY TO PROTECT SENSITIVE PERSONAL INFORMATION	erasing; or	Functional	Subset Of	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).	10	
521.052(b)(3)	BUSINESS DUTY TO PROTECT SENSITIVE PERSONAL INFORMATION	otherwise modifying the sensitive personal information in the records to make the information unreadable or indecipherable through any means.	Functional	Subset Of	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).	10	
521.052(c)	BUSINESS DUTY TO PROTECT SENSITIVE PERSONAL INFORMATION	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
521.052(d)	BUSINESS DUTY TO PROTECT SENSITIVE PERSONAL INFORMATION	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
521.053	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
521.053(a)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	In this section, "breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
521.053(b)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred, except as provided by Subsection (d) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
521.053(b-1)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	If the individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person is a resident of a state that requires a person described by Subsection (b) to provide notice of a breach of system security, the notice of the breach of system security required under Subsection (b) may be provided under that state's law or under Subsection (b).	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
521.053(c)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	Any person who maintains computerized data that includes sensitive personal information not owned by the person shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
521.053(d)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	A person may delay providing notice as required by Subsection (b) or (c) at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that the notification will not compromise the investigation.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
521.053(e)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	A person may give notice as required by Subsection (b) or (c) by providing:	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
521.053(e)(1)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	written notice at the last known address of the individual;	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	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
521.053(e)(2)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	electronic notice, if the notice is provided in accordance with 15 U.S.C. Section 7001; or	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
521.053(e)(3)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	notice as provided by Subsection (f).	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
521.053(f)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	If the person required to give notice under Subsection (b) or (c) demonstrates that the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the person does not have sufficient contact information, the notice may be given by:	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
521.053(f)(1)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	electronic mail, if the person has electronic mail addresses for the affected persons;	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
521.053(f)(2)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	conspicuous posting of the notice on the person's website; or	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
521.053(f)(3)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	notice published in or broadcast on major statewide media.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
521.053(g)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	Notwithstanding Subsection (e), a person who maintains the person's own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under this section complies with this section if the person notifies affected persons in accordance with that policy.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
521.053(h)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	If a person is required by this section to notify at one time more than 10,000 persons of a breach of system security, the person shall also notify each consumer reporting agency, as defined by 15 U.S.C. Section 1681a, that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices. The person shall provide the notice required by this subsection without unreasonable delay.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
521.053(i)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	A person who is required to disclose or provide notification of a breach of system security under this section shall notify the attorney general of that breach as soon as practicable and not later than the 30th day after the date on which the person determines that the breach occurred if the breach involves at least 250 residents of this state. The notification under this subsection must be submitted electronically using a form accessed through the attorney general's Internet website and must include:	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
521.053(i)(1)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	a detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach;	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
521.053(i)(2)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	the number of residents of this state affected by the breach at the time of notification;	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
521.053(i)(3)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	the number of affected residents that have been sent a disclosure of the breach by mail or other direct method of communication at the time of notification;	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
521.053(i)(4)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	the measures taken by the person regarding the breach;	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
521.053(i)(5)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	any measures the person intends to take regarding the breach after the notification under this subsection; and	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
521.053(i)(6)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	information regarding whether law enforcement is engaged in investigating the breach.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
521.053(j)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	The attorney general shall post on the attorney general's publicly accessible Internet website:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
521.053(j)(1)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	an electronic form for submitting a notification under Subsection (i); and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
521.053(j)(2)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	a listing of the notifications received by the attorney general under Subsection (i), excluding any sensitive personal information that may have been reported to the attorney general under that subsection, any information that may compromise a data system's security, and any other information reported to the attorney general that is made confidential by law. The attorney general shall:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
521.053(j)(2)(A)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	update the listing not later than the 30th day after the date the attorney general receives notification of a new breach of system security;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
521.053(j)(2)(B)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	remove a notification from the listing not later than the first anniversary of the date the attorney general added the notification to the listing if the person who provided the notification has not notified the attorney general of any additional breaches under Subsection (i) during that period; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
521.053(j)(2)(C)	NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA	maintain only the most recently updated listing on the attorney general's website.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control