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 SB820 (2019)**
Focal Document URL: https://capitol.texas.gov/tlodocs/86R/billtext/html/SB00820F.htm
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-tx-sb820-2019.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
11.175	DISTRICT CYBERSECURITY	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11.175(a)	DISTRICT CYBERSECURITY	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11.175(b)	DISTRICT CYBERSECURITY	Each school district shall adopt a cybersecurity policy to:	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
11.175(b)(1)	DISTRICT CYBERSECURITY	secure district cyberinfrastructure against cyberattacks and other cybersecurity incidents; and	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
11.175(b)(2)	DISTRICT CYBERSECURITY	determine cybersecurity risk and implement mitigation planning.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
11.175(c)	DISTRICT CYBERSECURITY	A school district's cybersecurity policy may not conflict with the information security standards for institutions of higher education adopted by the Department of Information Resources under Chapters 2054 and 2059, Government Code.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
11.175(d)	DISTRICT CYBERSECURITY	The superintendent of each school district shall designate a cybersecurity coordinator to serve as a liaison between the district and the agency in cybersecurity matters.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
11.175(e)	DISTRICT CYBERSECURITY	The district's cybersecurity coordinator shall report to the agency any cyber attack or other cybersecurity incident against the district cyberinfrastructure that constitutes a breach of system security as soon as practicable after the discovery of the attack or incident.	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	
11.175(f)	DISTRICT CYBERSECURITY	The district's cybersecurity coordinator shall provide notice to a parent of or person standing in parental relation to a student enrolled in the district of an attack or incident for which a report is required under Subsection (e) involving the student's information.	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	