SmartSuite

Framework / Cybersecurity / Other

Texas Cybersecurity Act — Tex. Gov't Code Ch. 2054

Texas Cybersecurity Act establishes governance requirements for state agencies to manage cybersecurity risks, incidents, and reporting.

What it is

The U.S. Texas Cybersecurity Act is a state-level regulatory framework that establishes requirements for cybersecurity governance and risk management across Texas state agencies and institutions. Its primary purpose is to strengthen protection of government information systems, reduce cyber risk, and improve incident response capabilities within the public sector.

The Act is published by the State of Texas, enforced through the Department of Information Resources (DIR), and applies to executive branch agencies, higher education institutions, and related state entities. Its scope covers cybersecurity controls, risk assessments, training, data protection, and mandatory incident reporting, requiring organizations to develop and maintain comprehensive security programs.

At a glance

PUBLISHER Texas Department of Information Resources (DIR)	TYPE Regulation	VERSION 2025
EFFECTIVE September 1, 2025	DOMAIN Cybersecurity	FAMILY Other
REGION Texas	INDUSTRY Government & Public Sector	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY Moderate		

Source: https://capitol.texas.gov/tlodocs/89R/billtext/html/SB02610I.htm

Why it matters

- **Strengthen cybersecurity oversight** Establish clear roles, authority, and responsibilities for cybersecurity governance within state agencies and public sector organizations.
- **Improve risk management practices** Drive consistent risk assessment and mitigation efforts to address threats and vulnerabilities impacting critical state information systems.
- **Enhance statewide regulatory alignment** Support compliance with state laws and directives by ensuring cybersecurity activities adhere to Texas-specific legislative mandates.
- **Increase audit and reporting readiness** Provide frameworks and guidelines that facilitate timely, accurate, and transparent security audit processes and legislative reporting.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports TCSA Ch. 2054

State Security Program Governance

Structure cybersecurity policies, standards, and oversight aligned to Texas state security requirements.

Risk Assessment and Control Implementation

Track risk assessments and implementation of required security controls across systems and agencies.

Asset Inventory and System Classification

Maintain visibility into systems, data, and infrastructure subject to state cybersecurity requirements.

Access Control and Security Operations

Manage user access, authentication, monitoring, and operational security controls across environments.

Cybersecurity Incident Response and Reporting

Track cybersecurity incidents and manage response, escalation, and reporting obligations.

Texas Cybersecurity Compliance Reporting

Provide dashboards showing security posture, risk exposure, and compliance with Texas cybersecurity mandates.

Common framework mappings

CIS Controls v8.1 | CJIS Security Policy | COBIT 2019 | FedRAMP Rev. 5 | FERPA | GLBA Safeguards Rule (16 CFR Part 314) | HIPAA | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5

Official resources

Texas Cybersecurity Act Overview

Provides detailed information on the Texas Cybersecurity Act and its governance requirements.

dir.texas.gov/View-About-DIR/Information-Security/Cybersecurity-Legislation

Texas Department of Information Resources (DIR) Security Standards

Outlines the security standards mandated by Texas DIR for state agencies.

dir.texas.gov/View-Resources/Standards/Information-Security-Standards

Texas Cybersecurity Framework

Defines the Texas Cybersecurity Framework to enhance state-level cybersecurity practices.

dir.texas.gov/View-Resources/Framework/Overview

Texas Administrative Code: Information Security Standards

Official legal text outlining information security standards for Texas state agencies.

texreg.sos.state.tx.us/public/readtac%24ext.ViewTAC?tac_view=5&ti=1&pt=10&ch=202&sch=B&rl=Y

Frequently asked questions

What is the Texas Cybersecurity Act used for?

The Texas Cybersecurity Act establishes statewide requirements for cybersecurity governance within Texas state agencies and public sector entities. Its primary purpose is to improve the protection of sensitive information, establish accountability, and ensure the implementation of consistent cybersecurity practices across state organizations.

Is compliance with the Texas Cybersecurity Act mandatory?

Yes, compliance is mandatory for all Texas state agencies, including public higher education institutions and other designated public sector organizations. The Act stipulates a legal obligation to adhere to its governance, risk management, and incident reporting requirements.

Who does the Texas Cybersecurity Act apply to?

The Texas Cybersecurity Act applies specifically to Texas state agencies, public institutions of higher education, and certain other public organizations. It does not extend to private sector entities, but contractors handling state data may be subject to specific cybersecurity requirements through their engagement.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What are the key governance requirements under the Texas Cybersecurity Act?

Key requirements include the appointment of an information security officer (ISO), regular cybersecurity risk assessments, the establishment of security policies and procedures, mandatory awareness training for employees, and ongoing monitoring and incident reporting. Agencies must also participate in statewide cybersecurity planning and coordination.

How should organizations implement the Texas Cybersecurity Act?

Organizations should begin by designating an ISO, conducting a baseline security assessment, and developing policies that align with the Act's mandates. Implementation involves integrating risk management into organizational processes, adopting required technical and administrative controls, and establishing mechanisms for reporting and responding to cybersecurity incidents.

How does the Texas Cybersecurity Act relate to other cybersecurity frameworks?

The Texas Cybersecurity Act aligns with national standards such as NIST SP 800-53 and NIST Cybersecurity Framework by referencing best practices for governance and controls. Agencies may leverage controls and processes from these frameworks to meet Texas-specific requirements, ensuring broader compliance and interoperability.

What are the ongoing compliance requirements for the Texas Cybersecurity Act?

Ongoing compliance includes conducting regular risk assessments, updating security policies, providing annual cybersecurity training, reporting significant incidents to the Department of Information Resources (DIR), and engaging in periodic compliance reviews or audits as required by state oversight bodies.

How would SmartSuite support the Texas Cybersecurity Act?

SmartSuite can help organizations manage Texas Cybersecurity Act compliance by enabling comprehensive risk tracking, centralizing control management, and streamlining evidence collection for audits. It supports audit readiness and reporting functions, making it easier to document compliance efforts, track remediation activities, and provide transparency for state oversight and review processes.

License included / downloadable: Yes The Texas Cybersecurity Act is published by the State of Texas and is publicly available. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/us-texas-cybersecurity-act-state-cybersecurity-governance-requirements