



# CYBERSECURITY TIPS AND TOOLS

## SIMPLIFYING THE TEXAS CYBERSECURITY FRAMEWORK

Frosty Walker

Chief Information Security Officer

Texas Education Agency

[Frosty.Walker@tea.texas.gov](mailto:Frosty.Walker@tea.texas.gov)

(512) 463-5095



# Data Security Advisory Committee

The Data Security Advisory Committee (DSAC) provides guidance to the Texas education communities, maximizing collaboration and communication regarding information security issues and resources which can be utilized within the educational communities served.

The DSAC is currently comprised of representatives from school districts, ESC's, TEA and the private sector.

# Texas Gateway

<https://www.texasgateway.org/>

## Cybersecurity Tips and Tools

Decorative white lines consisting of several parallel diagonal strokes in the bottom right corner of the slide.

## Online resources FOR YOUR CLASSROOM

Find engaging, TEKS-aligned resources that you can use with your students as part of classroom instruction, intervention, acceleration, or additional practice.

show me more

BROWSE TEKS

BROWSE RESOURCES ▶

Search

### Featured Resources

Getting Started Guide

Starting the Conversation

ELA & READING  
Targeting the 2 Percent

T2  
PERCENT

Restorative Discipline Practices in Texas

SOCIAL STUDIES  
Social Studies TEKS: Supporting Information

MATH  
Teacher2Teacher Math Video Series

Teacher2Teacher

cyber security data  
Cyber Security Tips and Tools

Introduction to the Revised Mathematics TEKS  
MATH  
Mathematics TEKS: Supporting Information

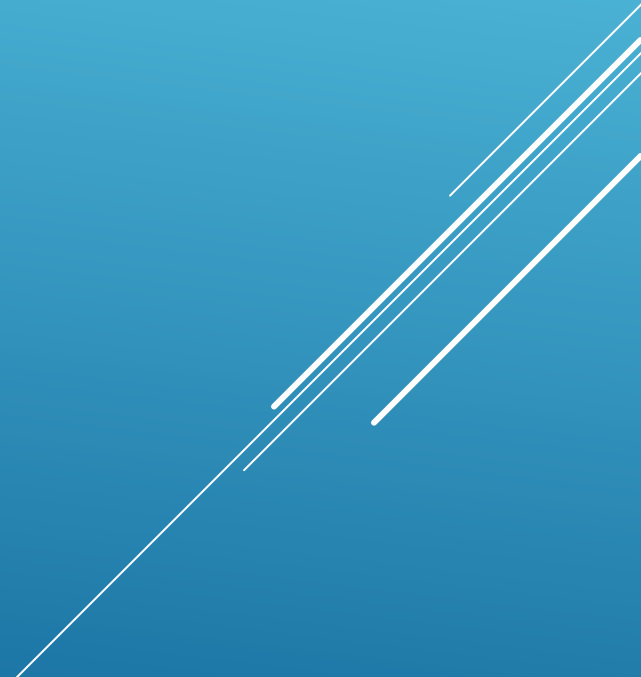
ELA & READING  
OnTRACK English II Reading: Understanding and Analysis of Literary Text

Literary Text



# Texas Cybersecurity Framework

## Five NIST Functions

- Identify
  - Protect
  - Detect
  - Respond
  - Recover
- 
- A decorative graphic consisting of several parallel white lines of varying lengths and thicknesses, slanted diagonally from the bottom right towards the top right, located in the lower right quadrant of the slide.

## New Additions for 2020

Identify	43. *Secure Application Development			100			
Identify	44. *Beta Testing			100			
Identify	45. *Penetration Testing			100			
Identify	46. *Vulnerability Testing			100			
Protect	42. *Systems Currency			25	75		
Detect	41. *Audit Logging			100			

# Texas Cybersecurity Framework Rating Levels

<b>Level 0</b>	<b>Non-Existent</b> -- There is no evidence of the organization meeting the objective.
<b>Level 1</b>	<b>Initial</b> -- The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.
<b>Level 2</b>	<b>Repeatable</b> -- The organization has a consistent overall approach to meeting the objective, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.
<b>Level 3</b>	<b>Defined</b> -- The organization has a documented, detailed approach to meeting the objective, and regularly measures its compliance.
<b>Level 4</b>	<b>Managed</b> -- The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.
<b>Level 5</b>	<b>Optimized</b> -- The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner.

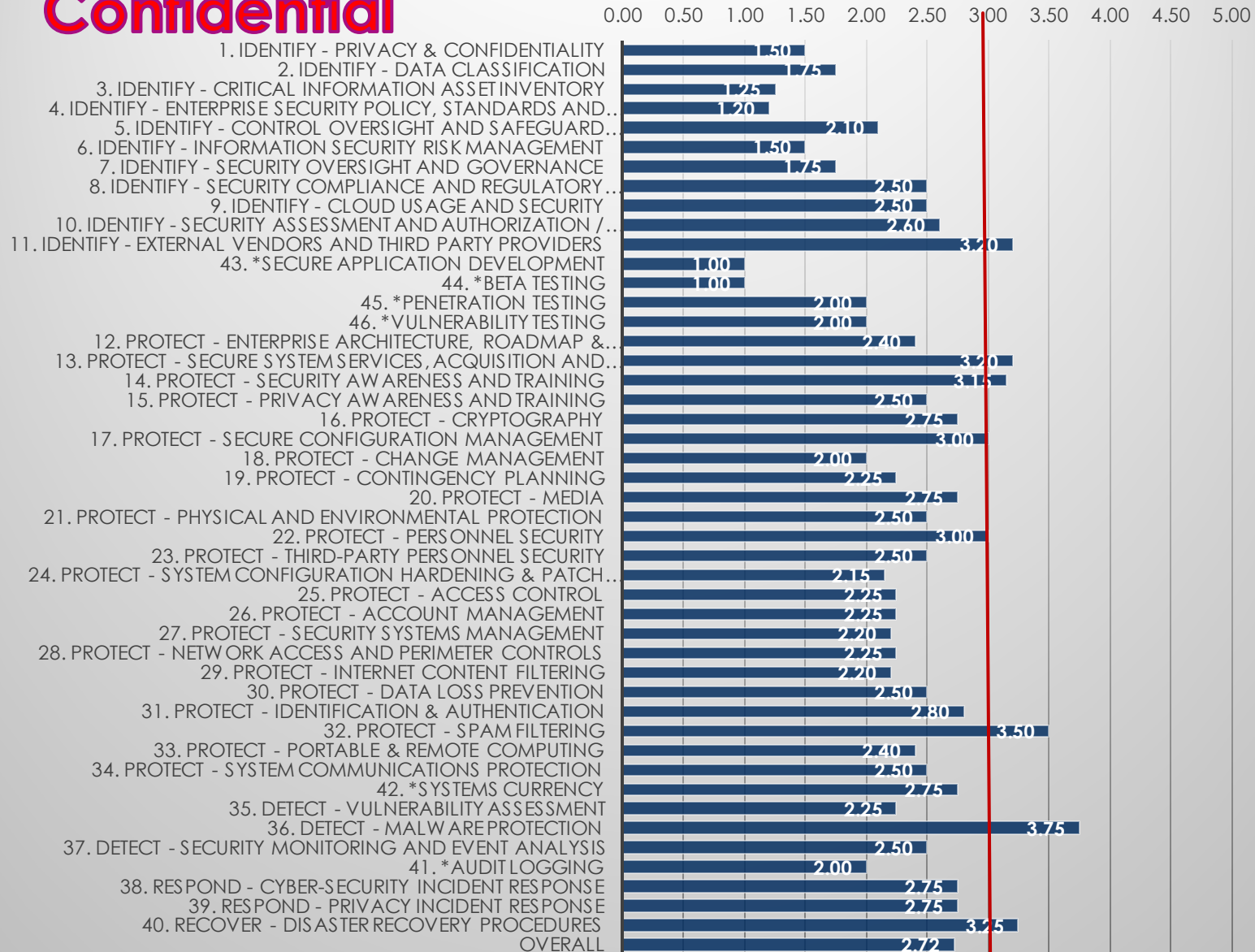
Area	Security Objective	0	1	2	3	4	5
Identify	1. Identify - Privacy & Confidentiality		50	50			
Identify	2. Identify - Data Classification		25	75			
Identify	3. Identify - Critical Information Asset Inventory		75	25			
Identify	4. Identify - Enterprise Security Policy, Standards and Guidelines		80	20			
Identify	5. Identify - Control Oversight and Safeguard Assurance		25	40	35		
Identify	6. Identify - Information Security Risk Management		50	50			
Identify	7. Identify - Security Oversight and Governance		50	25	25		
Identify	8. Identify - Security Compliance and Regulatory Requirements Mgmt			50	50		
Identify	9. Identify - Cloud Usage and Security			50	50		
Identify	10. Identify - Security Assessment and Authorization / Technology Risk Assessments			40	60		
Identify	11. Identify - External Vendors and Third Party Providers			20	40	40	
Identify	43. *Secure Application Development		100				
Identify	44. *Beta Testing		100				
Identify	45. *Penetration Testing			100			
Identify	46. *Vulnerability Testing			100			
Protect	12. Protect - Enterprise Architecture, Roadmap & Emerging Technology			60	40		
Protect	13. Protect - Secure System Services, Acquisition and Development			20	40	40	
Protect	14. Protect - Security Awareness and Training			25	35	40	
Protect	15. Protect - Privacy Awareness and Training			50	50		
Protect	16. Protect - Cryptography			50	25	25	
Protect	17. Protect - Secure Configuration Management			25	50	25	
Protect	18. Protect - Change Management			25	50		
Protect	19. Protect - Contingency Planning			75	25		
Protect	20. Protect - Media			50	25	25	
Protect	21. Protect - Physical and Environmental Protection			50	50		
Protect	22. Protect - Personnel Security				100		
Protect	23. Protect - Third-Party Personnel Security			50	50		
Protect	24. Protect - System Configuration Hardening & Patch Management			85	15		
Protect	25. Protect - Access Control			75	25		
Protect	26. Protect - Account Management			75	25		
Protect	27. Protect - Security Systems Management			80	20		
Protect	28. Protect - Network Access and Perimeter Controls			75	25		
Protect	29. Protect - Internet Content Filtering			80	20		
Protect	30. Protect - Data Loss Prevention			50	50		
Protect	31. Protect - Identification & Authentication			20	80		
Protect	32. Protect - Spam Filtering				50	50	
Protect	33. Protect - Portable & Remote Computing			60	40		
Protect	34. Protect - System Communications Protection			50	50		
Protect	42. *Systems Currency			25	75		
Detect	35. Detect - Vulnerability Assessment			75	25		
Detect	36. Detect - Malware Protection				25	75	
Detect	37. Detect - Security Monitoring and Event Analysis			50	50		
Detect	41. *Audit Logging			100			
Respond	38. Respond - Cyber-Security Incident Response			25	75		
Respond	39. Respond - Privacy Incident Response			25	75		
Recover	40. Recover - Disaster Recovery Procedures				75	25	
	<b>Overall</b>						
	<b>* = New for 2020</b>						



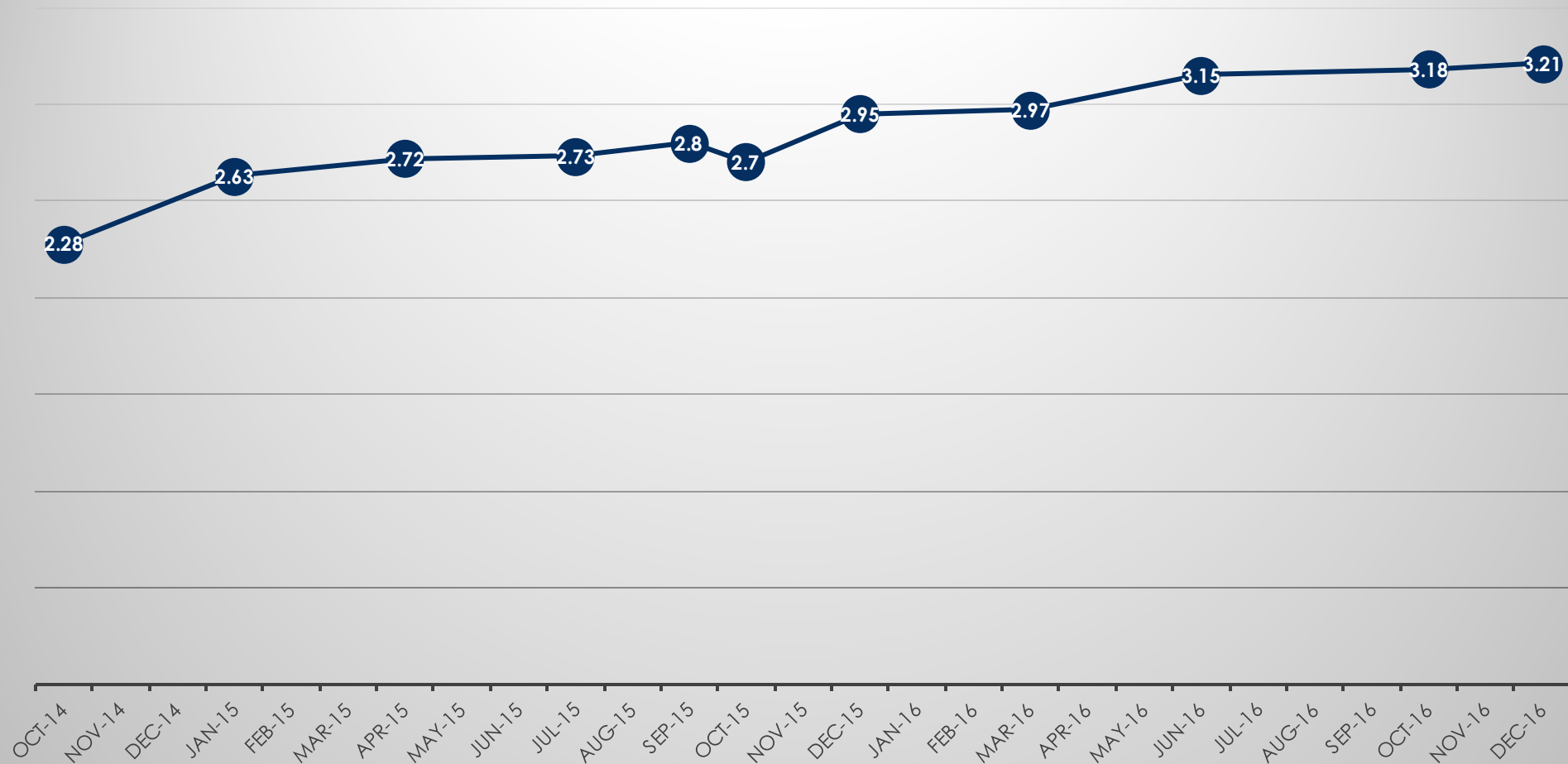
# Texas Cybersecurity Framework 2019

Red Line Indicates Due Diligence 3.00 Monitoring Stage

**Confidential**



## Overall TCF Posture Maturity



# TCF Identify

#	Area	Security Objective	0	1	2	3	4	5	Obj #	Score	TCF Rating
1	Identify	1. Identify - Privacy & Confidentiality		50	50				1	150	1.50
9	Identify	9. Identify - Cloud Usage and Security			50	50			9	250	2.50

Level 0	Non-Existent -- There is no evidence of the organization meeting the objective.
Level 1	Initial -- The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.
Level 2	Repeatable -- The organization has a consistent overall approach to meeting the objective, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.
Level 3	Defined -- The organization has a documented, detailed approach to meeting the objective, and regularly measures its compliance.
Level 4	Managed -- The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.
Level 5	Optimized -- The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner.

# Texas Cybersecurity Framework Roadmap

#	FUNCTIONAL AREA	SECURITY OBJECTIVE	NIST FRAMEWORK MAPPING	DEFINITION/OBJECTIVE	Road Map Information (Recommendations to improve security posture)
2.1	Identify	Privacy & Confidentiality		Ensuring the appropriate security of retained information and approved sharing under defined conditions with required safeguards and assurance. Includes the requirements of HIPAA, Texas Business & Commerce Code, and agency defined privacy policies that include and expand upon regulatory and legal requirements for establishing contractual/legal agreements for appropriate and exchange and protection.	<ol style="list-style-type: none"> <li>1)Ensuring the appropriate security of retained information and approved sharing under defined conditions with required safeguards and assurance.</li> <li>2)Check for appropriate Identity Access Mgmt. (IAM) i.e. Onboarding &amp; Off boarding processes, Principle of Least Privilege Access.</li> <li>3)Establish and adhere to data retention policy.</li> <li>4)Adherence to data protection requirements of FERPA, Texas Business &amp; Commerce Code, Texas Education Code and entity defined privacy policies.</li> <li>5)The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance.</li> <li>6)The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.</li> </ol>
2.9	Identify	Cloud Usage and Security		The assessment and evaluation of risk with the use of "cloud" technologies including Software as a Service (SAAS), Platform as a Service (PAAS), and Information as a Service (IAAS), to ensure that business operations are capable of delivering programs and services efficiently and effectively within acceptable tolerances potential negative outcomes.	<ol style="list-style-type: none"> <li>1)The assessment and evaluation of risk with the use of "cloud" technologies to ensure that business operations can deliver programs and services efficiently and effectively within acceptable tolerances potential negative outcomes.</li> <li>2)Negotiation of acceptable levels of security should be included in the contract negotiation process.</li> <li>3)The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance.</li> <li>4)The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.</li> </ol>

# Questions regarding cloud vendors under Identify

Who owns the data/content uploaded to the application site? ***Vendor/Customer***

What compliance certifications does the vendor's data center have? ***PCIDSS, HIPPA, SP800-53/Fed RAMP***

To what data center standards does the vendor adhere to?

***SOC-1, SOC-2, SOC-3, SAS70/SSAE 16/SSAE 18, ISO27001***

Is the customer data available for download upon cancellation of service? ***YES/NO***

Is all customer data erased upon cancellation of service?  
If so, when? ***Upon Request/Never***

Data segregated by tenant? ***YES/NO***

Has this vendor been recently breached (in the past year)?  
***YES/NO***

#	Area	Security Objective	0	1	2	3	4	5	Obj #	Score	TCF Rating
14	Protect	14. Protect - Security Awareness and Training			25	35	40		14	315	3.15
16	Protect	16. Protect - Cryptography			50	25	25		16	275	2.75

Level 0	Non-Existent -- There is no evidence of the organization meeting the objective.
Level 1	Initial -- The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.
Level 2	Repeatable -- The organization has a consistent overall approach to meeting the objective, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.
Level 3	Defined -- The organization has a documented, detailed approach to meeting the objective, and regularly measures its compliance.
Level 4	Managed -- The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.
Level 5	Optimized -- The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner.

# Texas Cybersecurity Framework Roadmap

2.14	Protect	Security Awareness and Training	PR.AT-1	Define, prepare, deliver, and facilitate an ongoing awareness campaign utilizing a wide variety of mediums and delivery mechanisms to effectively and constantly educate the organization on security related information, threats, and technology risks.	<ol style="list-style-type: none"> <li>1) Establish a Security Awareness Policy.</li> <li>2) Define, prepare, deliver, and facilitate an ongoing Security Awareness campaign utilizing a wide variety of mediums and delivery mechanisms to effectively and constantly educate the organization on security related information, threats, and technology risks based on roles performed in the organization (i.e. privileged users (admins, DBA's), executive users, programmers, contractors and end users).</li> <li>3) Role based training can consist of information as determined appropriate to perform job function from online training, instructor lead training or simple PowerPoint presentation.</li> <li>4) Ensure that every employee, contractor, intern and affiliate is aware of the organization's approach and policies to protecting the assets and information within your organization.</li> <li>5) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance.</li> <li>6) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.</li> </ol>
2.16	Protect	Cryptography		Establish the rules and administrative guidelines governing the use of cryptography and key management in order to ensure that data is not disclosed or made inaccessible due to an inability to decrypt.	<ol style="list-style-type: none"> <li>1) Encryption of mobile laptops, removeable media, data bases and files which may contain sensitive information as defined by the organizational Data Classification Policy commensurate to the protection of information from unauthorized access.</li> <li>2) Implement HTTPS encryption with Strict Transport Security (HSTS) using TLS 1.2 or higher on all public facing websites and applications on locally managed services and with 3rd parties via contract language updates.</li> <li>3) Implement encryption in transit between Internet gateways to application and data base servers.</li> <li>4) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance.</li> <li>5) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.</li> </ol>

# Information on Texas DIR's Certification of Security Awareness Training Programs

<https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=154>

Decorative white lines consisting of several parallel diagonal strokes in the bottom right corner of the slide.



# TEXAS BUSINESS AND COMMERCE CODE

Sec. 521.053. **NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA.** (a) 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.

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).

# Questions regarding cloud vendors under PROTECT

Does the app vendor encrypt data-at-rest?

**YES/NO**

What type of encryption data-at-rest?

***RSA, DES, BitLocker, Blowfish, AES***

Does the app vendor encrypt data-in-transit?

**Yes/No *TLS 1.2?***

#	Area	Security Objective	0	1	2	3	4	5	Obj #	Score	TCF Rating
35	Detect	35. Detect - Vulnerability Assessment			75	25			35	225	2.25
36	Detect	36. Detect - Malware Protection				25	75		36	375	3.75

Level 0	Non-Existent -- There is no evidence of the organization meeting the objective.
Level 1	Initial -- The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.
Level 2	Repeatable -- The organization has a consistent overall approach to meeting the objective, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.
Level 3	Defined -- The organization has a documented, detailed approach to meeting the objective, and regularly measures its compliance.
Level 4	Managed -- The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.
Level 5	Optimized -- The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner.

# Texas Cybersecurity Framework Roadmap

2.35	Detect	Vulnerability Assessment	DE.CM-8	<p>Assessment and monitoring of vulnerability detection and remediation including patch management processes, configuration management, system, database and application security vulnerabilities. Test and evaluate security controls and security defenses to ensure that required security posture levels are met. Perform and/or facilitate ongoing and periodic penetration testing of security defenses. Evaluate results of various penetration tests to provide risk based prioritization of mitigation.</p>	<ol style="list-style-type: none"> <li>1) Establish a documented vulnerability assessment management program.</li> <li>2) The vulnerability assessment management program should include regular assessments and monitoring of vulnerability detection and remediation including patch management processes, configuration management, system, database and application security vulnerabilities.</li> <li>3) Test and evaluate security controls and security defenses to ensure that required security posture levels are met.</li> <li>4) Establish a tracking process to measure the effectiveness of the program.</li> <li>5) Perform and/or facilitate ongoing and periodic penetration testing of security defenses.</li> <li>6) Evaluate results of various penetration tests to provide risk based prioritization of mitigation.</li> <li>7) Re-test to validate the mitigation worked as anticipated.</li> <li>7) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance.</li> <li>8) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.</li> </ol>
2.36	Detect	Malware Protection	DE.CM-4	<p>The prevention, detection and cleanup of Malicious Code (including virus, worm, Trojan, Spyware and other similar variants). Protection is accomplished at varying layers including at the host, at the network, or at the gateway perimeter. Protection mechanisms must be updated periodically and frequently to address evolving threats and monitored to provide manual intervention where required.</p>	<ol style="list-style-type: none"> <li>1) Establish a Malicious Code Policy to reflect the management intent to prevent, detect, protect and cleanup malicious code in your environment.</li> <li>2) Protection is accomplished at varying layers including at the host, at the network, and/or at the gateway perimeter.</li> <li>3) Protection mechanisms must be updated periodically and frequently to address evolving threats and monitored to provide manual intervention where required.</li> <li>4) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance.</li> <li>5) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.</li> </ol>

#	Area	Security Objective	0	1	2	3	4	5	Obj #	Score	TCF Rating
38	Respond	38. Respond - Cyber-Security Incident Response			25	75			38	275	2.75
39	Respond	39. Respond - Privacy Incident Response			25	75			39	275	2.75

Level 0	Non-Existent -- There is no evidence of the organization meeting the objective.
Level 1	Initial -- The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.
Level 2	Repeatable -- The organization has a consistent overall approach to meeting the objective, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.
Level 3	Defined -- The organization has a documented, detailed approach to meeting the objective, and regularly measures its compliance.
Level 4	Managed -- The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.
Level 5	Optimized -- The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner.

# Texas Cybersecurity Framework Roadmap

2.38	Respond	Cyber-Security Incident Response	RS.PL-1	<p>Establishes an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, recovery, and response activities. The Incident Response program is used to track, document, and report incidents to appropriate officials and/or authorities.</p>	<ol style="list-style-type: none"> <li>1) Establish an Incident Response policy and program with the handling capability for information systems that includes adequate preparation, detection, analysis, containment, recovery, and response activities.</li> <li>2) The Incident Response program is used to track, document, and report incidents to appropriate officials and/or authorities.</li> <li>3) Consider including Texas Department of Information Resources' (DIR) Incident Response Team Redbook (<a href="http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Incident%20Response%20Template%202018.pdf">http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Incident%20Response%20Template%202018.pdf</a>) as a guide in your incident response program.</li> <li>4) The Incident Response program should also include the ability to implement changes in protection processes to take advantage of lessons learned from your experiences.</li> <li>5) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance.</li> <li>6) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.</li> </ol>
2.39	Respond	Privacy Incident Response		<p>Management of events, issues, inquiries, and incidents when detected or reported to include all phases from investigation through resolution. Responsible for notifying and escalating incidents to appropriate personnel and coordinating activities to ensure timely isolation and containment, impact analysis, and any resulting remediation / resolution requirements. Incidents include but may not be limited to privacy breach, loss, theft, unauthorized access, malware infections, and occurrences of negligence, human error, or malicious acts.</p>	<ol style="list-style-type: none"> <li>1) Privacy Incident Response includes the management of events, issues, inquiries, and incidents when detected or reported to include all phases from investigation through resolution.</li> <li>2) Incidents include but may not be limited to privacy breach, loss, theft, unauthorized access, malware infections, and occurrences of negligence, human error, or malicious acts.</li> <li>3) Establish and document responsibility for notifying and escalating incidents to appropriate personnel and coordinating activities to ensure timely isolation and containment, impact analysis, and any resulting remediation / resolution requirements.</li> <li>4) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance.</li> <li>5) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.</li> </ol>

## What's the Difference?

### Cybersecurity Incident Response

- Any Cybersecurity Incident
- Comprised PC

### Privacy Incident Response

- An Incident potentially exposing PII

#	Area	Security Objective	0	1	2	3	4	5	Obj #	Score	TCF Rating
40	Recover	40. Recover - Disaster Recovery Procedures				75	25		40	325	3.25

Level 0	Non-Existent -- There is no evidence of the organization meeting the objective.
Level 1	Initial -- The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.
Level 2	Repeatable -- The organization has a consistent overall approach to meeting the objective, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.
Level 3	Defined -- The organization has a documented, detailed approach to meeting the objective, and regularly measures its compliance.
Level 4	Managed -- The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.
Level 5	Optimized -- The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner.



# Texas Cybersecurity Framework Roadmap

2.40	Recover	Disaster Recovery Procedures	RC.RP	<p>Managing the recovery of data and applications in the event of loss or damage (natural disasters, system disk and other systems failures, intentional or unintentional human acts, data entry errors, or systems operator errors).</p>	<ol style="list-style-type: none"> <li>1) Establish a Backup and Disaster Recover policy and program to maximize your efforts to protect your resources during a disaster utilizing the identification and prioritization of all the organization's information assets so that they are prioritized per criticality to the business.</li> <li>2) Managing the recovery of data and applications in the event of loss or damage (natural disasters, system disk and other systems failures, intentional or unintentional human acts, data entry errors, or systems operator errors).</li> <li>3) Regularly perform tabletop and disaster recovery exercises to determine the gaps in your documented process and provide assurances that your resources can be restored in a timely manner as they are prioritized per criticality to the business.</li> <li>4) Perform regular backup restoration testing to validate backups and restoration process.</li> <li>5) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance.</li> <li>6) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.</li> </ol>
------	---------	------------------------------	-------	---	--

## Questions regarding cloud vendors under **RECOVERY**


Does the app vendor back up customer data in a separate location from the main data center? **YES/NO**

Does the application vendor utilize geographically dispersed data centers to serve customers? **YES/NO**

Does the app vendor provide disaster recovery services? **YES/NO**

A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, set against a blue gradient background.

## **Other Frameworks which could be used to:**

- (1) Secure district cyberinfrastructure against cyber-attacks and other cybersecurity incidents
  - (2) Determine cybersecurity risk and implement mitigation planning.
- 

## **NIST Cybersecurity Framework**

<https://www.nist.gov/cybersecurityframework>

## **CIS RAM (Center for Internet Security® Risk Assessment Method)**

<https://learn.cisecurity.org/cis-ram>

## **CIS CAT Lite (Center for Internet Security® Configuration Assessment Tool)**

<https://www.cisecurity.org/blog/introducing-cis-cat-lite/>

A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, set against a blue background.

**Questions?**

