Texas Education Agency

CYBERSECURITY TIPS AND TOOLS -
SB820 AND HB3834 (86TH) IMPACT AND REQUIREMENTS TO TEXAS SCHOOL DISTRICTS

Frosty Walker

Chief Information Security Officer

Texas Education Agency

Frosty.Walker@tea.texas.gov

(512) 463-5095

Data Security Advisory Committee

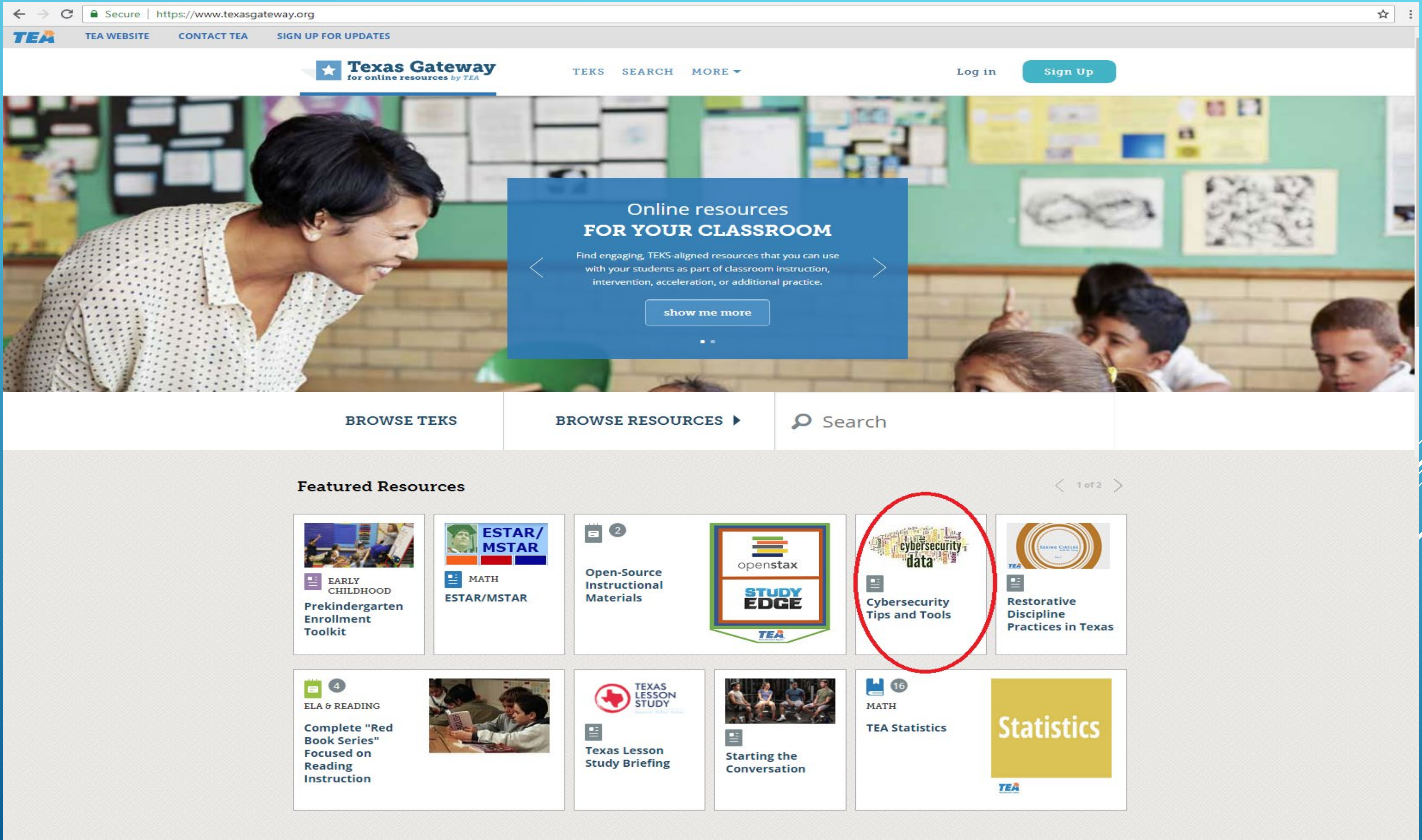
The Data Security Advisory Committee (DSAC) provides guidance to the Texas education communities, maximizing collaboration and communication regarding information security issues and resources which can be utilized within the educational communities served.

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

Texas Gateway

https://www.texasgateway.org/

Cybersecurity Tips and Tools



Secure | https://www.texasgateway.org

TEA WEBSITE CONTACT TEA SIGN UP FOR UPDATES

Texas Gateway for online resources by TEA

TEKS SEARCH MORE ▾ Log in Sign Up

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

1 of 2

EARLY CHILDHOOD
Prekindergarten Enrollment Toolkit

MATH
ESTAR/MSTAR

2
Open-Source Instructional Materials

Cybersecurity Tips and Tools

Restorative Discipline Practices in Texas

4
ELA & READING
Complete "Red Book Series" Focused on Reading Instruction

Texas Lesson Study Briefing

Starting the Conversation

16
MATH
TEA Statistics

SB 820

(1) “ Breach of system security" means an incident in which student information that is sensitive, protected, or confidential, as provided by state or federal law, is stolen or copied, transmitted, viewed, or used by a person unauthorized to engage in that action.

(2) "Cyber attack" means an attempt to damage, disrupt, or gain unauthorized access to a computer, computer network, or computer system.

(3) "Cybersecurity" means the measures taken to protect a computer, computer network, or computer system against unauthorized use or access.

SB 820

(b) Each school district shall adopt a cybersecurity policy to:

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

(c) 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. (**Texas Cybersecurity Framework**)

SB 820

Texas Cybersecurity Framework

Five NIST Functions

- Identify
- Protect
- Detect
- Respond
- Recover

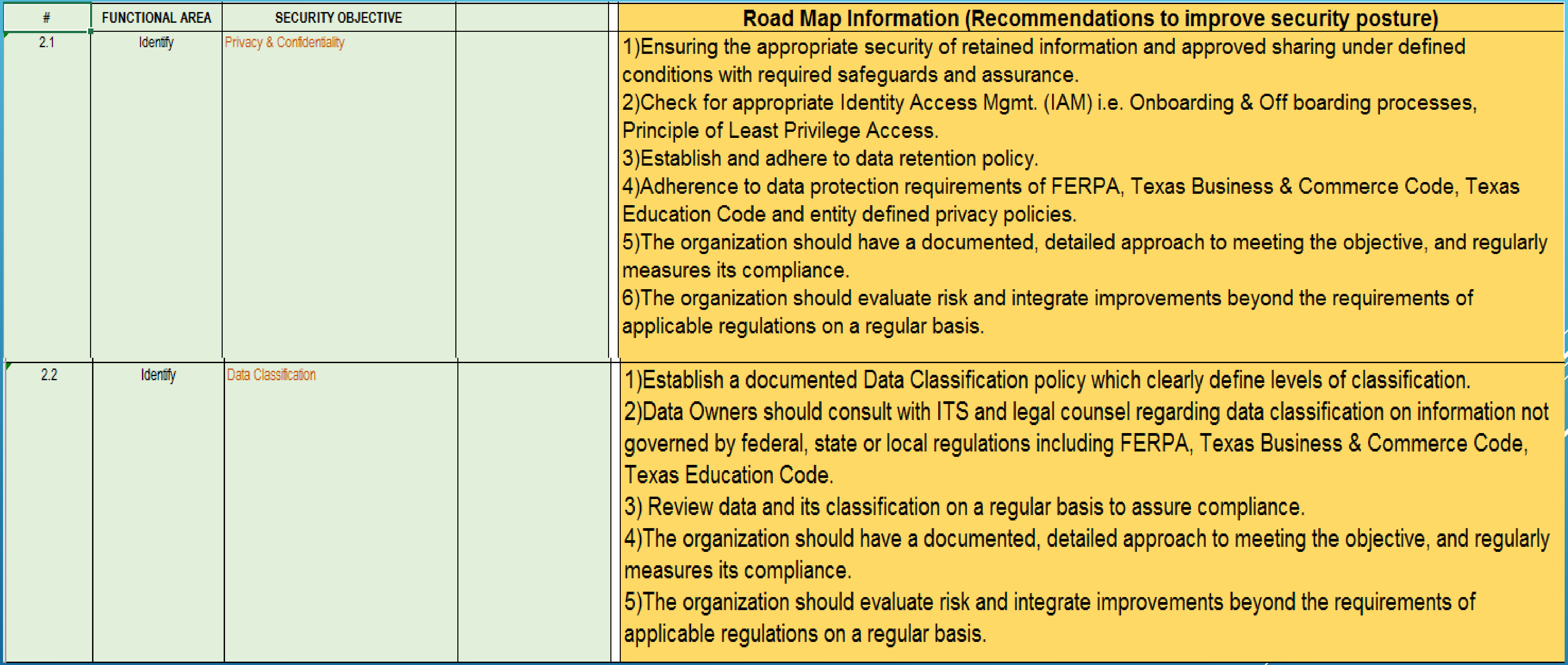
SB 820

- **Identify**

Security Objective	0	1	2	3	4	5
1. Identify - Privacy & Confidentiality		100				
2. Identify - Data Classification		25	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.

Roadmap



#	FUNCTIONAL AREA	SECURITY OBJECTIVE		Road Map Information (Recommendations to improve security posture)
2.1	Identify	Privacy & Confidentiality		1)Ensuring the appropriate security of retained information and approved sharing under defined conditions with required safeguards and assurance. 2)Check for appropriate Identity Access Mgmt. (IAM) i.e. Onboarding & Off boarding processes, Principle of Least Privilege Access. 3)Establish and adhere to data retention policy. 4)Adherence to data protection requirements of FERPA, Texas Business & Commerce Code, Texas Education Code and entity defined privacy policies. 5)The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 6)The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.
2.2	Identify	Data Classification		1)Establish a documented Data Classification policy which clearly define levels of classification. 2)Data Owners should consult with ITS and legal counsel regarding data classification on information not governed by federal, state or local regulations including FERPA, Texas Business & Commerce Code, Texas Education Code. 3) Review data and its classification on a regular basis to assure compliance. 4)The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5)The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.

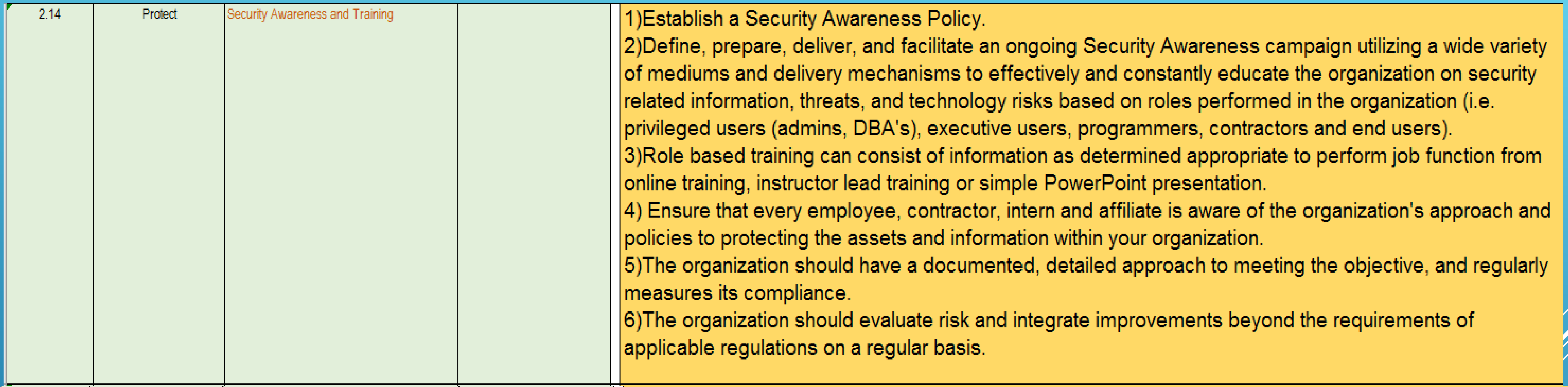
SB 820

- Protect

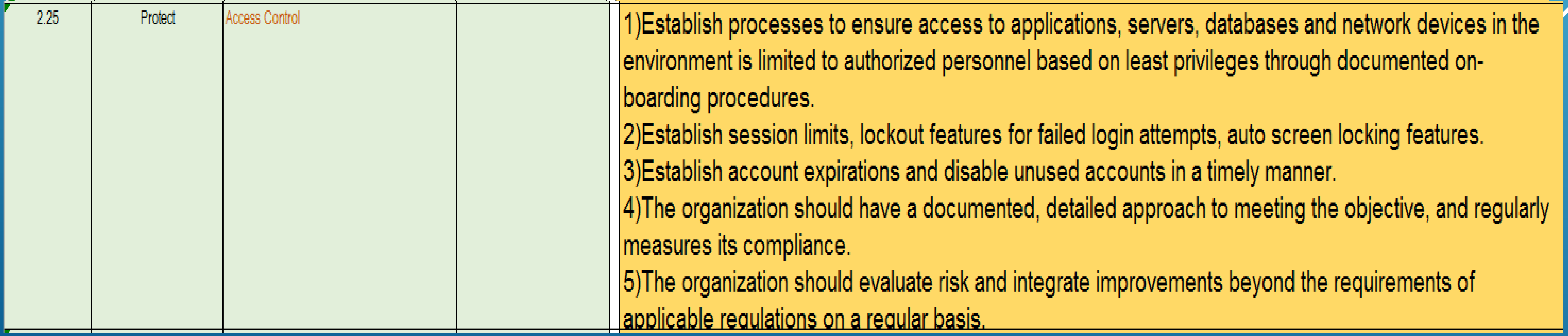
Security Objective	0	1	2	3	4	5
14. Protect - Security Awareness Training					100	
25. Protect – Access Control			25	75		

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.

Roadmap



2.14	Protect	Security Awareness and Training			1)Establish a Security Awareness Policy. 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). 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. 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. 5)The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 6)The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.



2.25	Protect	Access Control			1)Establish processes to ensure access to applications, servers, databases and network devices in the environment is limited to authorized personnel based on least privileges through documented on-boarding procedures. 2)Establish session limits, lockout features for failed login attempts, auto screen locking features. 3)Establish account expirations and disable unused accounts in a timely manner. 4)The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5)The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.

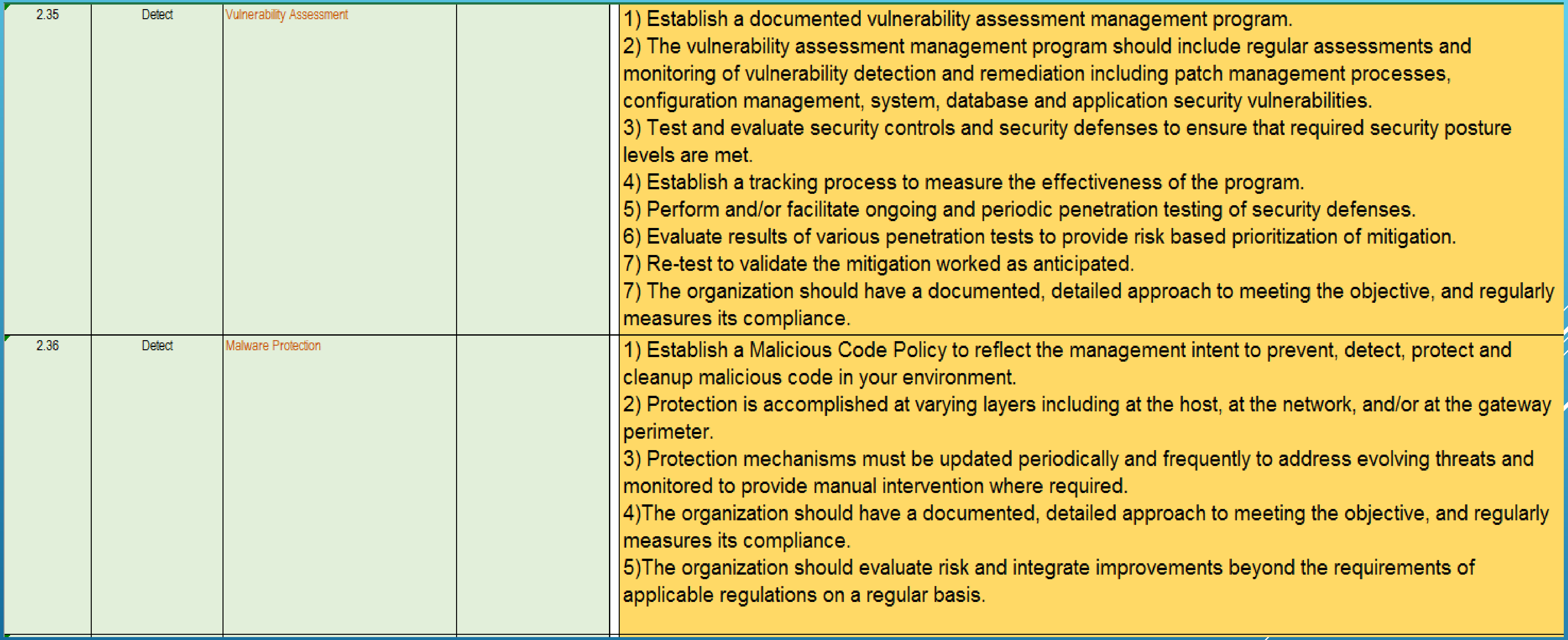
SB 820

- Detect

Security Objective	0	1	2	3	4	5
35. Detect– Vulnerability Assessment		100				
36. Detect– Malware Protection					100	

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.

Roadmap



2.35	Detect	Vulnerability Assessment			1) Establish a documented vulnerability assessment management program. 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. 3) Test and evaluate security controls and security defenses to ensure that required security posture levels are met. 4) Establish a tracking process to measure the effectiveness of the program. 5) Perform and/or facilitate ongoing and periodic penetration testing of security defenses. 6) Evaluate results of various penetration tests to provide risk based prioritization of mitigation. 7) Re-test to validate the mitigation worked as anticipated. 7) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance.
2.36	Detect	Malware Protection			1) Establish a Malicious Code Policy to reflect the management intent to prevent, detect, protect and cleanup malicious code in your environment. 2) Protection is accomplished at varying layers including at the host, at the network, and/or at the gateway perimeter. 3) Protection mechanisms must be updated periodically and frequently to address evolving threats and monitored to provide manual intervention where required. 4)The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5)The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.

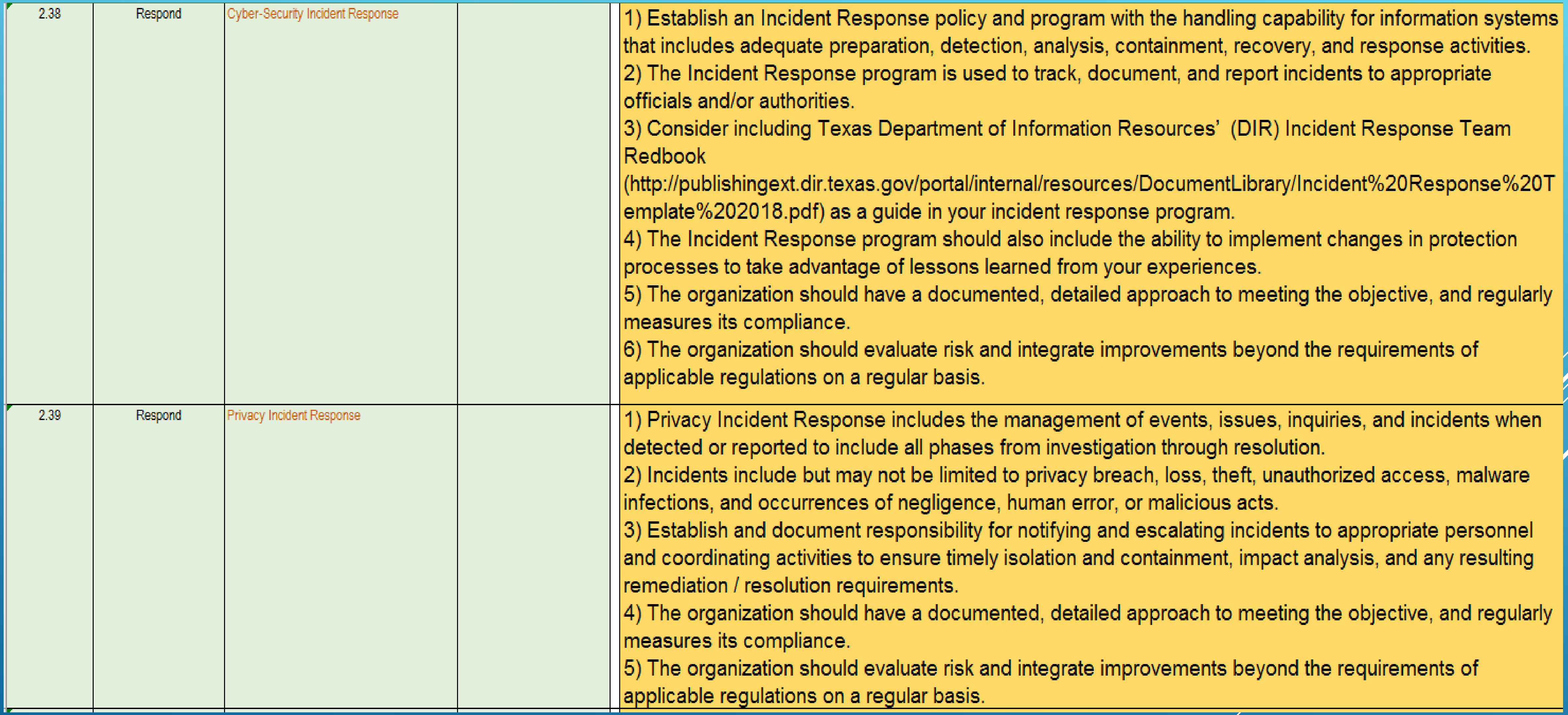
SB 820

- Respond

Security Objective	0	1	2	3	4	5
38. Respond – Cyber-Security Incident Response			100			
39. Respond – Privacy Incident Response			100			

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.

Roadmap



2.38	Respond	Cyber-Security Incident Response			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. 2) The Incident Response program is used to track, document, and report incidents to appropriate officials and/or authorities. 3) Consider including Texas Department of Information Resources' (DIR) Incident Response Team Redbook (http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Incident%20Response%20Template%202018.pdf) as a guide in your incident response program. 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. 5) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 6) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.
2.39	Respond	Privacy Incident Response			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. 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. 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. 4) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.

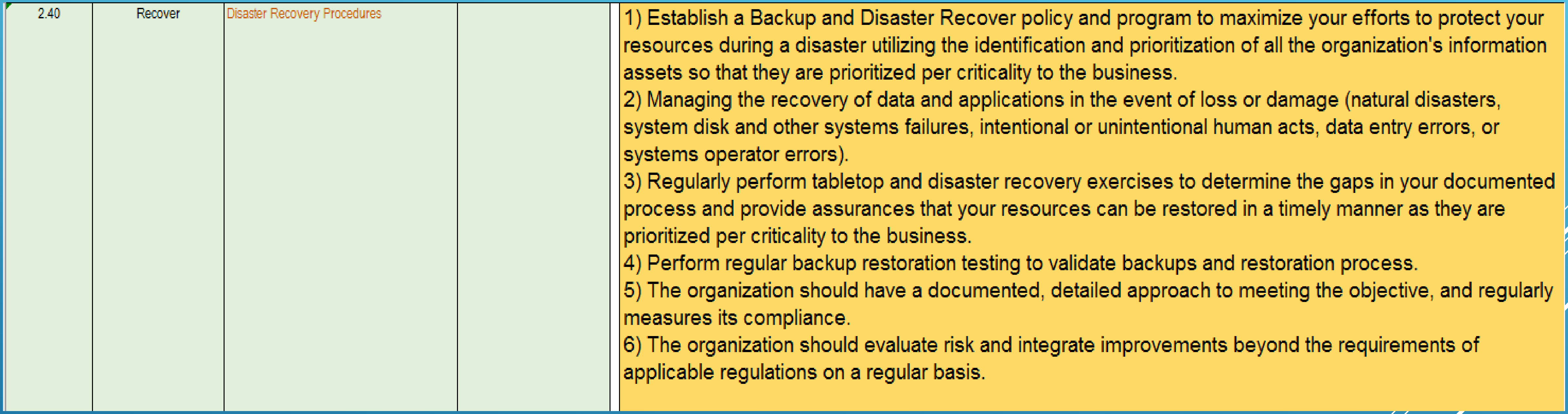
SB 820

- Recover

Security Objective	0	1	2	3	4	5
40. Recover- Disaster Recovery Plan				100		

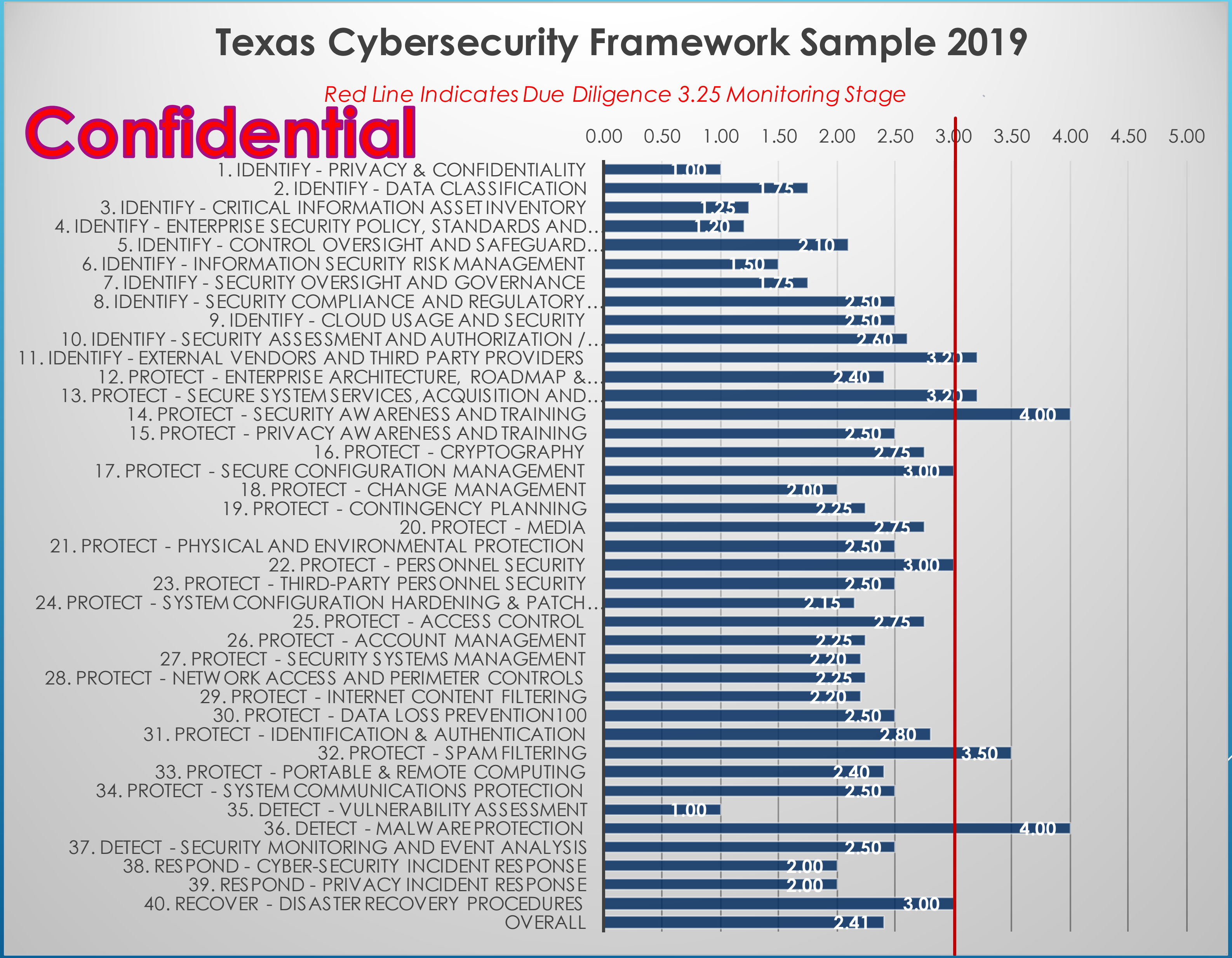
Level 0	Non-Existent -- There is no evidence of the organization meeting the objective.
Level 1	Initial -- The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.
Level 2	Repeatable -- The organization has a consistent overall approach to meeting the objective, but 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.

Roadmap



2.40	Recover	Disaster Recovery Procedures			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. 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). 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. 4) Perform regular backup restoration testing to validate backups and restoration process. 5) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 6) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.

SB 820



Texas Cybersecurity Framework Sample 2019

Red Line Indicates Due Diligence 3.25 Monitoring Stage

SB 820

(d) 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.

(e) 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.

> (1) “ **Breach of system security"** means an incident in which student information that is sensitive, protected, or confidential, as provided by state or federal law, is stolen or copied, transmitted, viewed, or used by a person unauthorized to engage in that action.

SB 820

(f) 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.

This Act takes effect September 1, 2019.

SB 820

- Relating to a requirement that a school district adopt a cybersecurity policy.

How will school districts report their liaison to TEA?

** Via AskTed: The role of Cybersecurity Coordinator will be added to the application where superintendents or their designee will be able to assign the designated individual to this role.*

How will school district's Cybersecurity Coordinator report incidents to TEA?

** TEA has setup a special email to receive incident reports*

cybersecurity@tea.texas.gov

HB 3834

SECTION 1. The heading to Subchapter N-1, Chapter 2054, Government Code, is amended to read as follows:

Sec. 2054.519. STATE CERTIFIED CYBERSECURITY TRAINING PROGRAMS

DIR, in consultation with the cybersecurity council established under Section 2054.512 and industry stakeholders, shall annually certify at least five cybersecurity training programs for state and local government employees.

HB 3834

Government Code Title 10 Chapter Section 2054.003. DEFINITIONS.

(9) "Local government" means a county, municipality, special district, school district, junior college district, or other political subdivision of the state.

HB 3834

Sec. 2054.5191. CYBERSECURITY TRAINING REQUIRED: CERTAIN EMPLOYEES.

(a-1) At least once each year, a local government shall identify local government employees who have access to a local government computer system or database and require those employees and elected officials of the local government to complete a cybersecurity training program certified under Section 2054.519 or offered under Section 2054.519(f).

HB 3834

(b) The governing body of a local government may select the most appropriate cybersecurity training program certified under Section 2054.519 or offered under **Section 2054.519(f) for employees of the local government to complete.** The governing body shall:

(1) verify and report on the completion of a cybersecurity training program by employees of the local government to the department (DIR); and

(2) require periodic audits to ensure compliance with this section.

- If this Act does not receive the vote necessary for immediate effect, this Act takes effect September 1, 2019.

Questions?