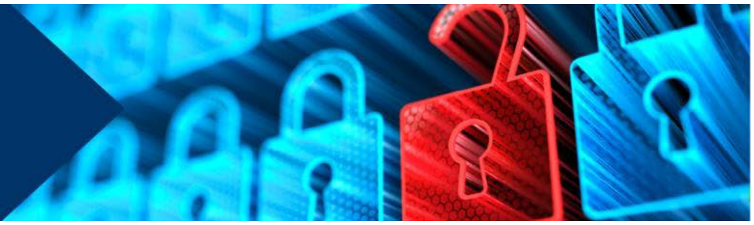


Cybersecurity Policy Compliance:

A Roadmap for Districts

Identify

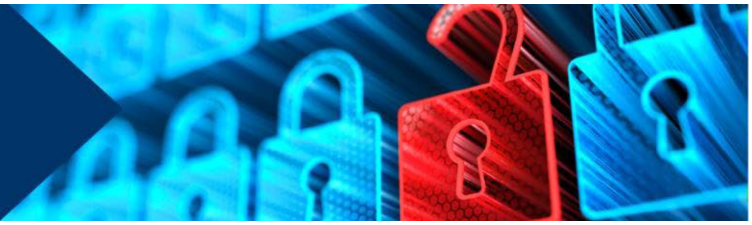
Detect

Respond

Protect

Recover

TASB Risk Management Fund

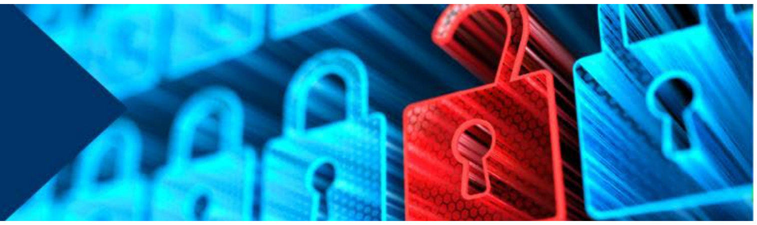


Texas law requires school districts to implement a cybersecurity plan designed to protect against and recover from breaches. The TASB Risk Management Fund developed this resource with four goals in mind:

1. Explain the rationale behind the law
2. Uncover its requirements and implications for districts
3. Detail the process of creating a cybersecurity plan
4. Share an example of what your cybersecurity plan might look

For more information about cybersecurity regulations that apply to schools, visit our InsideRM blog.

Contents



The case for cybersecurity

The significant increase in worldwide cybercriminal activity is cause for concern among people, private enterprise, and federal and local governments alike. In recent years, hackers have increasingly directed their attacks against school districts:

- Publicly disclosed cyberattacks against schools exploded by 235 percent between 2018 and 2020: K-12 Cybersecurity Resource Center
- Educational institutions lose an average of $2.73 million in a typical ransomware incident: Sophos cybersecurity firm
- In 2020, cyberattacks cost schools an estimated $6.62 billion in down time: Comparitech
- Parents' greatest worry is the compromise of their children's sensitive data (43 percent). Just 11 percent worry about the impact that beefing up security will have on taxpayers: Kaspersky

Considering the wealth of sensitive, highly valuable information school districts manage, as well as the increased number of attacks directed against schools, it becomes clear why the Texas Legislature has prioritized district cybersecurity in recent years.

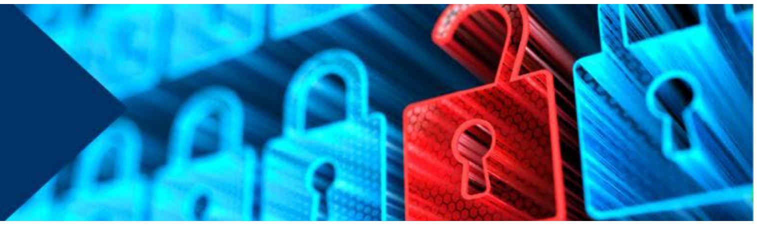
What does the law require?

Each district must develop a cybersecurity plan via a two-step process. First, the board will adopt a cybersecurity policy. The board policy, in turn, will require the development of a district cybersecurity plan. You can find additional information regarding the district policy, as well as recommended language, in U114 to the CQB policy manual and U60 to the RRM on the TASB Policy Service Resources site. You need a myTASB User ID and Password to access the documents, or you can reach out to your TASB policy service consultant for additional information.

Under the law, your district's cybersecurity policy must:

1. "Secure district cyberinfrastructure against cyberattacks and other cybersecurity incidents"
2. "Determine cybersecurity risk and implement mitigation planning"
3. Not "conflict with the information security standards for institutions of higher education adopted by the Department of Information Resources under Chapters 2054 (Information Resources) and 2059 (Texas Computer Network Security System), Government Code."

These three requirements are relatively flexible. The fundamental objective is to encourage districts to engage with cybersecurity issues the education sector faces, not to overwhelm them and their IT departments with onerous regulations and requirements.



Texas Cybersecurity Framework basics

The third district cybersecurity policy requirement explained above directs us to the Texas Cybersecurity Framework (TCF). The TCF was created by DIR to guide districts and state agencies in developing cybersecurity plans. As such, your district cybersecurity policy cannot conflict with the TCF.

If the TCF states, for example, that multi-factor authentication should be used for remote access to district networks, you cannot create a cybersecurity plan that states, “We will not use multi-factor authentication for remote access.”

DIR based the TCF on the federal National Institute of Standards and Technology (NIST) cybersecurity framework. The NIST framework was then augmented through a public/private collaboration to create a “common language to address and manage cybersecurity risk in a cost-effective way, based on business needs, without placing additional regulatory requirements on agencies.”

The TCF consists of five key cybersecurity functions – Identify, Protect, Detect, Respond, and Recover. Spread across these five functions are 46 distinct security objectives. You can find a spreadsheet that lists and defines each objective on the DIR website under the section “2020 Security Plan Documents and Links” (Works best in Chrome, but click Cancel if the system asks for administrator credentials).

IDENTIFY – What processes and assets need protection?

PROTECT – What safeguards are available?

DETECT – What techniques can identify incidents?

RESPOND – What techniques can contain impacts of incidents?

RECOVER – What techniques can restore capabilities?

You don’t necessarily have to audit your network against the 46 TCF security objectives to meet your regulatory obligation. Your plan simply must “not conflict” with these standards. However, DIR recommends using the TCF, as this process will undoubtedly enhance understanding of your network infrastructure and improve your overall cybersecurity posture.

With that in mind, let’s examine how you can create a district cybersecurity plan using the TCF.

Putting the TCF to work

Your first step will be to audit your information technology infrastructure, network, and policies against the TCF security objectives. It is important to consider your district’s size. The system equipment and configuration of a small, rural school district will be markedly different than those of a large, urban district. This difference in scale will impact the scope of your audit. Some security objectives that an urban district needs to evaluate might not apply to a rural district.

Identify applicable objectives

To illustrate this point, we’re going to look at two sets of objectives. The first set will be examples of universally applicable security objectives every district will likely need to use in their audits. We will also examine examples of TCF objectives that may or may not apply to your district. When you are running your audit, if an objective doesn’t apply to you, skip it or mark it “N/A” (not applicable). Gauging the applicability of the objectives before you begin your audit can save you significant time as you work through the process.

Universally applicable objectives

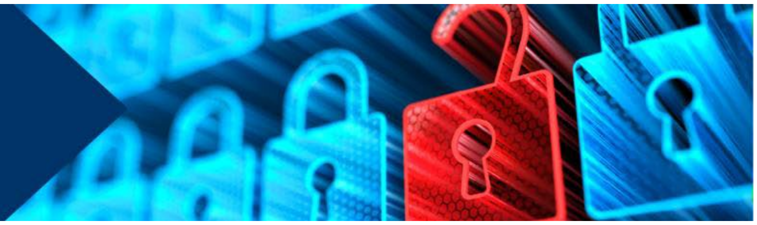
Below are examples of objectives that will likely apply to every district. They are shown here by naming their functions first (Identify, Security), and then stating their specific security objectives, as well as official definitions, within those functions.

Identify – Privacy and Confidentiality

- Ensure the appropriate security of retained information and approved sharing under defined conditions with required safeguards and assurance.
- Includes the requirements of the Health Insurance Portability and Accountability Act (HIPAA) and the Texas Business & Commerce Code

Security - Access Control

- Ensure access to applications, servers, databases, and network devices is limited to authorized personnel
- Access is to be limited to authorized users, processes acting on behalf of authorized users, or authorized devices (principle of least privilege)
- Activate session limits, lockout features for failed login attempts, and account expirations, as well as disable unused accounts.



Regarding the first objective above, every district should be aware of which sensitive information it retains, as well as which category the information falls under. Additionally, familiarity with HIPAA and Family Educational Rights and Privacy Act (FERPA) regulations should already be part of your approach to information security and data privacy management.

The second objective should also already be in practice to some degree within your district. The principle of least privilege is fundamental in network security. Many of the safeguards described above come as part of out-of-the-box infrastructure solutions. Others were likely configured during setup or scheduled maintenance by your IT department.

You would need to address these objectives when performing your infrastructure audit using the TCF as your guide. The silver lining is that you're probably already doing it right! Objectives like these will be an easy 3 or 4 rating (we'll address ratings shortly) for many districts.

Potentially applicable objectives:

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)

Identify – Secure Application Development

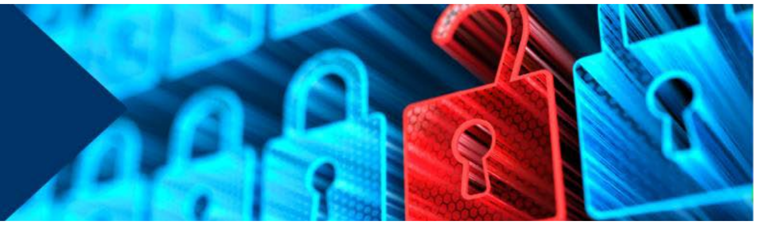
- Ensuring the code and processes that go into developing applications are as secure as possible
- Includes application's processes and the processes used in application development

Here we see examples of security objectives that may or may not apply to your district. In the first example, if you are not using cloud-based infrastructure, you can skip this objective or mark it N/A. The second example applies to districts that develop unique applications to deploy within their information infrastructure. Though application development can be a great exercise in technological vocational training, few districts create and implement native applications within their networks.

It is important to identify security objectives that probably won't apply to your district. Why? Because when you hear there are 46 objectives to reckon with, you might feel overwhelmed. Rightsizing the process for YOUR infrastructure is crucial to ensuring an efficient TCF audit.

Conduct your audit

Once you determine which objectives you need to assess, you can move on to the next step. At this point, you will work with your network and system administrator(s), your IT director/department representative, or an outside auditor/vendor to perform your audit.



Each objective has a robust definition that will provide a frame of reference for performing your audit. After assessing each applicable objective, you will award yourself a score from levels 0 - 5.

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.

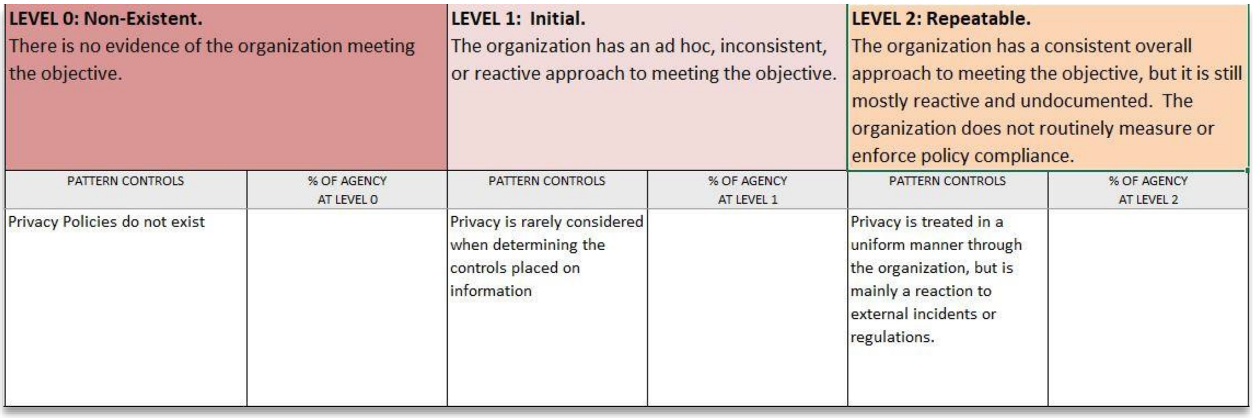
Level 2: Repeatable. The organization has a consistent overall approach to meeting the objective, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.

Level 3: Defined. The organization has a documented, detailed approach to meeting the objective, and regularly measures its compliance.

Level 4: Risk-based. 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.

It is important to be honest and critical when you perform your audit. The goal of the process is to improve your cybersecurity posture. If you overstate your preparedness and then experience a cybercriminal event, you will have done your staff and students a disservice.



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.	
PATTERN CONTROLS	% OF AGENCY AT LEVEL 0	PATTERN CONTROLS	% OF AGENCY AT LEVEL 1	PATTERN CONTROLS	% OF AGENCY AT LEVEL 2
Privacy Policies do not exist		Privacy is rarely considered when determining the controls placed on information		Privacy is treated in a uniform manner through the organization, but is mainly a reaction to external incidents or regulations.	

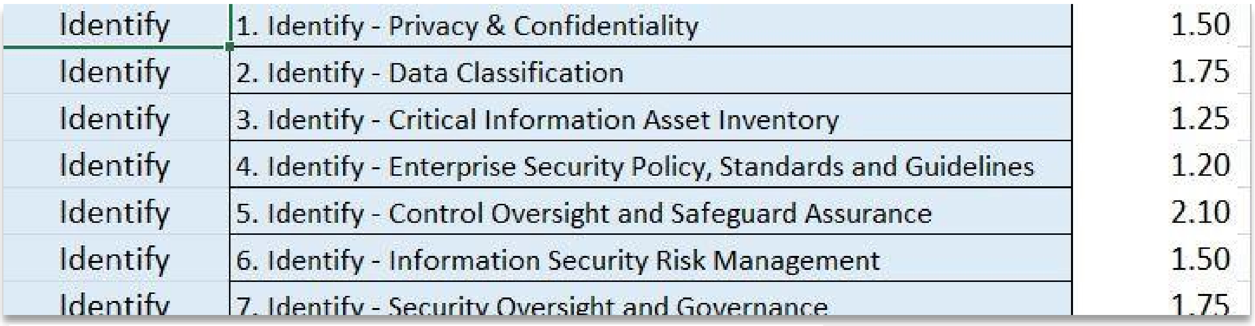
Image courtesy Texas Department of Information Resources

Above is an example of how you can utilize the indicated levels to score your district against the security objectives. You can even rate some parts of your organization at one level and other parts at a different level.

For example, your HR department might score a 3 with regard to the privacy and confidentiality objective, while the admin department might score a 2. Incorporating this level of granularity could result in an overall objective score expressed in the tenths and hundredths (2.5, for example).

Sample ratings for functions and objectives

TEA expects districts to achieve at least a 3.0 rating against applicable security objectives. If you find yourself below that threshold, don't worry. This is a great opportunity to improve your network security, and the TCF is an extremely efficient mechanism for identifying deficiencies in your network configuration. This is the point of the exercise. No district is going to come out of this process with 5.0 scores for every objective.



Identify	1. Identify - Privacy & Confidentiality	1.50
Identify	2. Identify - Data Classification	1.75
Identify	3. Identify - Critical Information Asset Inventory	1.25
Identify	4. Identify - Enterprise Security Policy, Standards and Guidelines	1.20
Identify	5. Identify - Control Oversight and Safeguard Assurance	2.10
Identify	6. Identify - Information Security Risk Management	1.50
Identify	7. Identify - Security Oversight and Governance	1.75

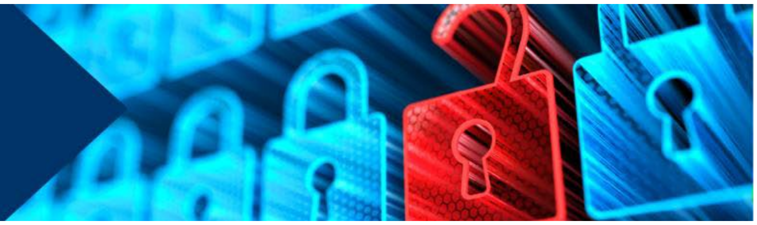
Image courtesy Texas Department of Information Resources

Set goals

If you achieve scores under 3.0 on some objectives, develop plans and budget proposals to move those numbers higher in the future. Productive conversations are often a result of the auditing process, so ask probing questions:

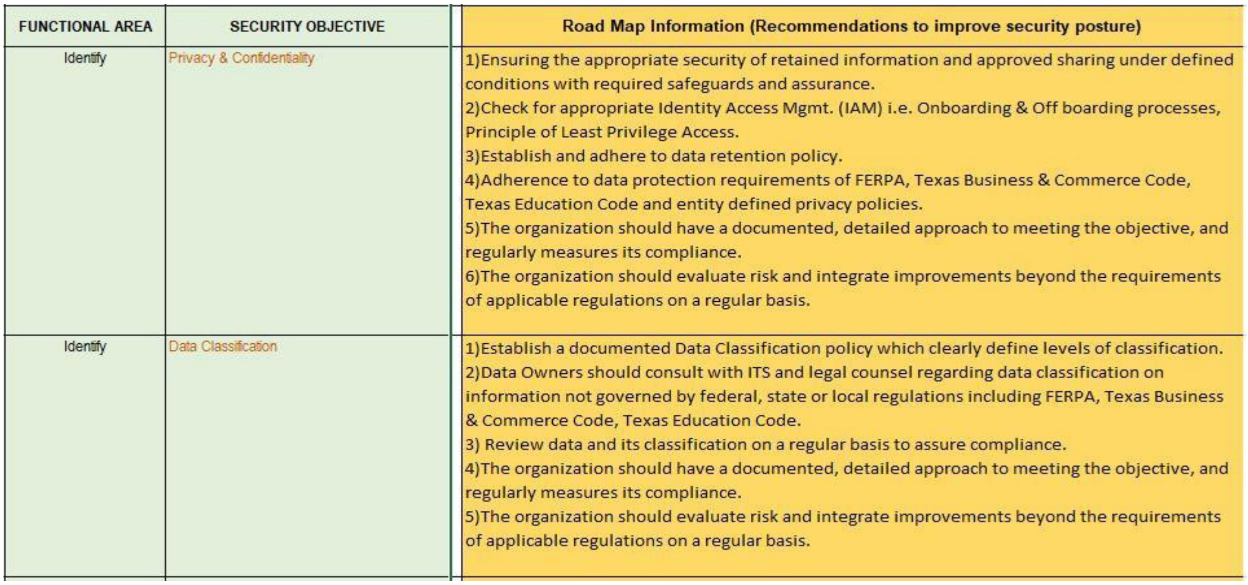
- Why was your rating below a 3?
- Are there obvious improvement opportunities?
- Are new policies needed?
- Are new IT positions called for?
- Does your environment require organizational restructuring or new equipment?

If you scored 3.0 or higher on some objectives, take time to congratulate your team. But remember that complacency can negatively impact the impressive results everyone worked hard to achieve. Use this opportunity to come up with long-term strategies to maintain or improve your great ratings.



Cybersecurity plan example

“What does this plan look like on paper?” is one of the most frequently asked questions we hear at the Fund. The legislation is general enough that it leads to confusion about deliverables. To simply the process, we developed this example.



FUNCTIONAL AREA	SECURITY OBJECTIVE	Road Map Information (Recommendations to improve security posture)
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.
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.

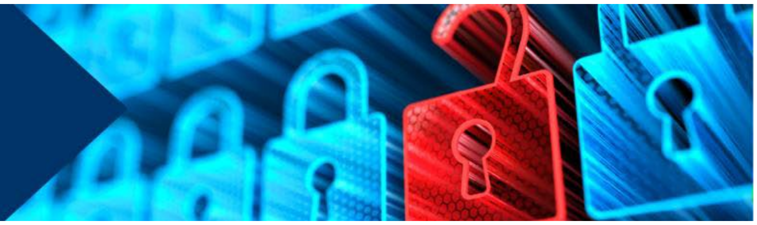
Image courtesy Texas Education Agency – Cybersecurity Tips and Tools

A detailed description of planned improvements (or steady-state maintenance) associated with each objective is clearly expressed in actionable terms. A simple Excel spreadsheet with all the data points we discussed previously (Function, Objective, Rating, Future Plans/Road Map) meets the legislative requirement. Beyond that, it can provide your district with a path toward greater overall network and data security.

Technological developments are ceaseless, so your cybersecurity plan cannot be static. It must evolve with technology.

Currently, there is no government repository for district security plans. They are meant to be maintained by the district and routinely updated.

Technological developments are ceaseless, so your plan cannot be static. It must evolve with technology. Routine updates (backed by implementation) to your plan will ensure you maintain high ratings for the TCF security objectives applicable to your district.



Compliance enforcement

There is currently no penalty for non-compliance with the cybersecurity policy requirement. That does not mean there will not be a penalty in the future. When you consider the number and scope of cybersecurity bills recently passed, it is clear the Legislature considers protecting sensitive data a priority.

This is new terrain for many districts, and lawmakers know that an onerous, punitive action on their part could be viewed as unreasonable. This is no reason to ignore the requirements, however. In fact, this is an opportunity to engage with procedures, models, and processes that will increase information security in your district—at your pace.

The Fund is here for you

The Fund is always here to help our members. However, each district is different. The work of auditing your system with the TCF must be done in-house, but we can advise you on how to approach the process. If you have questions, feel free to contact TASB Privacy and Cyber Risk Consultant Lucas Anderson at lucas.anderson@tasb.org .

Additionally, the Fund routinely provides helpful posts on our InsideRM blog related to developments in cybersecurity. We also deliver training through webinars, online courses, conferences, and district-specific events such as board meetings. If you have a particular training need, contact us and we can work together to provide you with an effective solution.