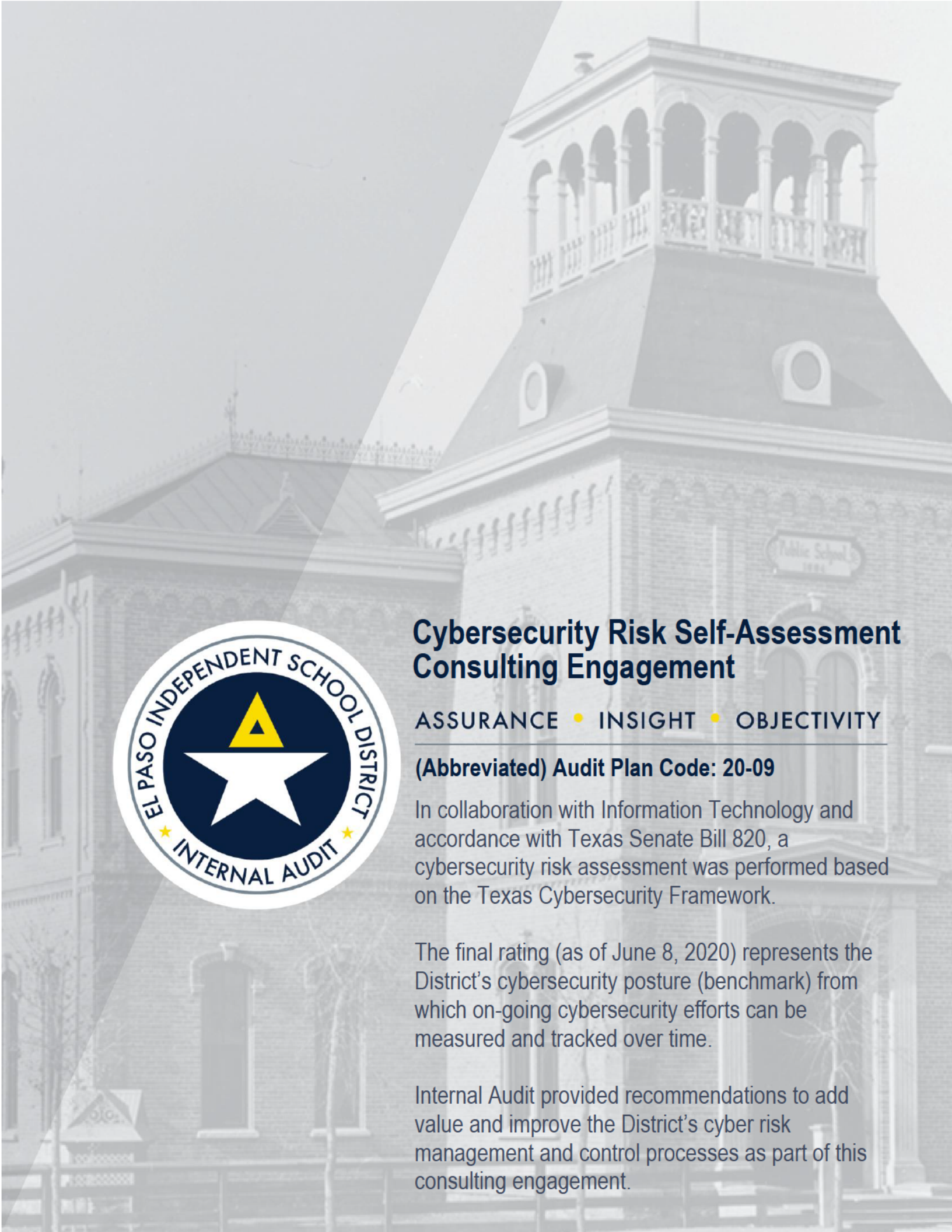


Cybersecurity Risk Self-Assessment Consulting Engagement

ASSURANCE • INSIGHT • OBJECTIVITY

(Abbreviated) Audit Plan Code: 20-09

In collaboration with Information Technology and accordance with Texas Senate Bill 820, a cybersecurity risk assessment was performed based on the Texas Cybersecurity Framework.

The final rating (as of June 8, 2020) represents the District's cybersecurity posture (benchmark) from which on-going cybersecurity efforts can be measured and tracked over time.

Internal Audit provided recommendations to add value and improve the District's cyber risk management and control processes as part of this consulting engagement.

Contents

Consulting Engagement Report

Abbreviations

BOT	Board of Trustees
CMMI	Capability Maturity Model Integration
DIR	Department of Information Resources
EPISD	El Paso Independent School District
IT	Information Technology
NIST	National Institute of Standards and Terminology
SB	Senate Bill
TCF	Texas Cybersecurity Framework
TEA	Texas Education Agency

Introduction

"**Cybersecurity means the measures taken to protect a computer, computer network, or computer system against unauthorized use or access,**" according to Texas Education Code 11.175. Implementation of these measures is crucial to support the District's mission of a "premier educational institution, source of pride and innovation…" and ensure the security of critical student and business systems.

With the passing of Texas Senate Bill (SB) 820 from the 86th Texas Legislature, Texas school districts are required to implement cybersecurity measures. It requires that beginning September 1, 2019, school districts develop a cybersecurity policy and maintain a framework for cybersecurity risk assessment and mitigation planning. To build on the District's cybersecurity policy, the District performed a cybersecurity risk self-assessment tailored to Texas educational institutions. This self-assessment shows the District's current cybersecurity posture (the "as is" state) according to Information Technology (IT) staff who have the best understanding of the District's IT operations.

A framework is a series of documents defining the best practices an organization follows to manage its cybersecurity risk. Educational institutions have the latitude in selecting the cybersecurity framework that best assesses their risks, situations, and needs. The framework, commonly known as the Texas Cybersecurity Framework (TCF), was selected for EPISD's cybersecurity risk self-assessment. This framework is promoted by the Texas Department of Information Resources (DIR) and the Texas Education Agency (TEA) as the standard cybersecurity framework and assessment across Texas school districts. Additionally, the rating "areas" of this assessment are the same core functions used by the National Institute of Standards and Terminology (NIST) to help public and private sectors better manage and reduce cybersecurity risk. Each area is essential to a well-operating security posture and successful management of cybersecurity risk.

These five core areas in the TCF are organized concurrently with one another to represent a continuous security lifecycle. The five core areas are divided among 46 cybersecurity objectives. The objectives are rated in percentages of maturity using the Capability Maturity Model Integration scale (aka CMMI) from Level 0 to Level 5. The percentage ratings under each level represent how mature that cybersecurity objective is understood to be currently documented, operating, and/or managed across the District in the current state (aka the "as is" state).

According to TCF's methodology and CMMI scale, Level 3 is a "Defined" maturity level and represents "due diligence" on the part of the educational institution. All 46 cybersecurity objectives in the assessment are expected to reach Level 3 status. Cybersecurity objectives lower than Level 3 are opportunities for improvement the District can focus on and prioritize as part of a cybersecurity program.

After rating all areas, the assessment will calculate an overall rating known as the Texas Cybersecurity Framework Rating (TCF Rating). This overall rating represents the District's Cybersecurity posture (the "as is" state) and provides a benchmark for cybersecurity strategies and mitigation planning moving forward.

As part of mitigation planning, the District may use the "roadmap" (guidance) provided in the TCF to identify processes and documentation needed to reach Level 3 in each cybersecurity objective. The District should evaluate on an on-

going basis which cybersecurity objectives require/need higher levels (the desired "to be" state) under each area based on evaluation of District priorities, regulatory requirements, conditions (i.e., cyber threats) and resources available.

Background

After SB 820 went in effect on September 1, 2019, Internal Audit revisited the approved 2019-2020 Audit Plan to determine if adjustments needed to be made based on risk and regulatory requirements introduced with this bill. After evaluation of these factors and increasing cyber-attacks affecting educational communities, the Chief Internal Auditor proposed and the Board of Trustees (BOT) approved to include a cybersecurity project in the 2019-2020 Audit Plan on October 15, 2019. The project became a consulting engagement to collaborate with the District's Information Technology (IT) Department to complete a cybersecurity risk self-assessment.

According to the Institute of Internal Auditors' Standards, "…When performing consulting services, the internal auditor should maintain objectivity and not assume management responsibility." The nature and scope of consulting engagements, which are agreed upon with the client, are intended to add value and improve the District's governance, risk management, and control processes. As such, we contacted IT leadership to communicate the availability of our consulting services as approved by the BOT and start planning a cybersecurity risk self-assessment.

IT leadership welcomed combining efforts to complete a cybersecurity risk self-assessment with participation from their staff. A kick-off meeting was held on February 12, 2020. Internal Audit proposed, and IT agreed in selecting the 2020 Texas Cybersecurity Framework and its 46 cybersecurity objectives self-assessment to be rolled out to all IT staff in all functioning areas for the best results possible. All IT functioning areas are represented in this assessment, which are: (i) Applications (ii) Security (iii) Operations and (iv) Support.

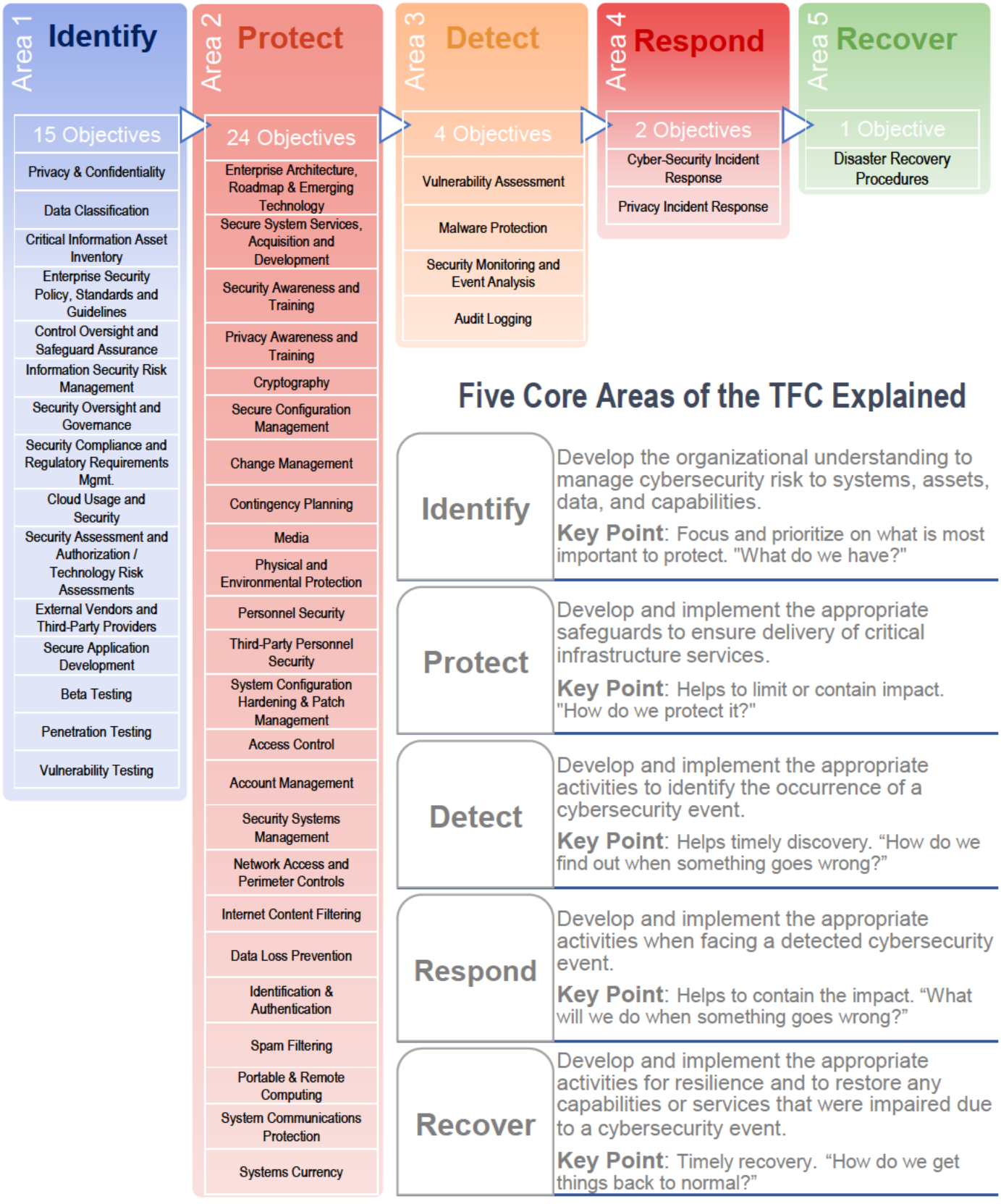
This report is an abbreviated version of the full report. The full report contains sensitive and confidential information that relates to current cybersecurity levels of protection, which, if made publicly available, may expose the District to unnecessary/new cyber risks on its computers, networks, or computer systems. As such, this information is not subject to disclosure requirements of the Texas Public Information Act based on the exception found in Government Code 552.139. The full report was released to the appropriate levels of leadership and management

Objective and Scope

The objective in performing a cybersecurity self-assessment is to (i) determine the District's current cybersecurity posture (the "as is" state) by identifying areas of risks using the 2020 Texas Cybersecurity Framework (TCF) and (ii) establish the basis for continuous mitigation planning (to minimize cyber risks) as required by SB 820.

The scope is the 46 cybersecurity objectives within five core areas (Identify, Protect, Detect, Respond, Recover) contained in the self-assessment. The five core areas are described in **Exhibit 1,** along with the corresponding 46 cybersecurity objectives.

Exhibit 1 – Five Core Areas with the 46 Cybersecurity Objectives



Five Core Areas of the TFC Explained

Identify

Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Key Point: Focus and prioritize on what is most important to protect. "What do we have?"

Protect

Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

Key Point: Helps to limit or contain impact. "How do we protect it?"

Detect

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Key Point: Helps timely discovery. "How do we find out when something goes wrong?"

Respond

Develop and implement the appropriate activities when facing a detected cybersecurity event.

Key Point: Helps to contain the impact. "What will we do when something goes wrong?"

Recover

Develop and implement the appropriate activities for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Key Point: Timely recovery. "How do we get things back to normal?"

Methodology

In collaboration with IT leadership and their staff, a cybersecurity risk self-assessment was completed based on the 2020 Texas Cybersecurity Framework. The assessments were completed by IT staff from March 2020 to June 2020. *Note: After receiving most of the assessments before the COVID-19 disruption, we re-opened the assessments to all IT staff in case they wanted to update their previous ratings after dealing with the pressures and real-life scenarios brought by COVID-19 on District operations.* We received the last assessment on June 8, 2020.

Based on their current duties, knowledge, and experience of the area, every IT staff member rated each cybersecurity objective using a maturity scale of Level 0 to Level 5. The Capability Maturity Model Integration scale (aka CMMI) used is described in **Exhibit 2**.

Exhibit 2 – Maturity Scale (CMMI)

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

All cybersecurity objectives are expected to meet Level 3 or otherwise known as the "due diligence" level.

Each cybersecurity objective could receive a percentage rating (1 to 100%) unless the IT staff member felt they could not provide a rating based on the above reasons. The percentage ratings under each level represent how mature that cybersecurity objective is understood to be currently documented, operating, and/or managed across the District in the current state (the "as is" state).

As an **example**, the cybersecurity objective titled "Privacy & Confidentiality" could have received a rating of 70% under Level 3 (Defined) and 30% under Level 2 (Repeatable). *Why*? It may be that most (70%) of the computers/networks/systems are documented, operating, and managed with privacy and confidentiality. However, in 30% of them, the District has a consistent overall approach to meeting the objective, but it is still mostly reactive and undocumented. The District also does not routinely measure or enforce policy compliance with said objective. In this

example, the Texas Cybersecurity Framework (TCF) Rating for this objective is precisely calculated at 2.7 and 3.0 when rounding is applied. This individual cybersecurity objective would meet the "due diligence" level expected, as explained above. This example is illustrated below.

Example:	Non-Existent	Initial	Repeatable	Defined	Managed	Optimized		
Cybersecurity Objective	0	1	2	3	4	5	**Score**	**TCF Rating**
Identify - Privacy & Confidentiality			30	70			270	**2.70**
							TCF Rating with Rounding Applied	**3**

The final ratings from this self-assessment are provided under the Summary of Results section of this report. The final calculation started by adding the ratings from every cybersecurity objective and obtaining an average. These averages were entered into the TFC's self-assessment for computation (based on TCF's methodology) to produce the final rating. The final calculation represents the District's Cybersecurity maturity rating "posture" as of June 8, 2020.

In accomplishing our objective, we also performed the following main tasks:

- Contacted the Texas Education Agency's Chief Information Security Officer to seek guidance on best practices in performing the TCF self-assessment.
- Attended TEA webinars explaining the TCF.
- Held meetings with IT leadership to identify and agree upon the methodology for IT staff to complete the self-assessments.
- Agreed on a list of IT staff who would participate in the assessment. The list is shown in **Exhibit 3**.
- Prepared and disseminated assessment information to IT leadership based on TEA information.
- Attended an IT-led hands-on presentation on how to understand and adequately complete the assessment.
- Developed 37 on-line versions of the TCF for confidential deployment and collection.
- Reviewed security and operational documentation provided by the Information Security Officer.
- Combined ratings and calculated averages for the final calculation of the TFC rating.

Inherent Limitations

The TCF does not provide either detailed guidance regarding how to measure (rate) each of the cybersecurity objectives, or a quantitative method to determine the percentage under any of the maturity levels. Due to these reasons, the ratings provided may be subjective in nature. To mitigate the risk of subjectivity, each participant was asked to consider their (i) experience with the objective (ii) current duties in relation to the objective and if they have (iii) enough knowledge to formulate a professional and unbiased rating.

Acknowledgement

We would like to acknowledge all of the Information Technology staff for their input and expertise they provided. Specifically, we would like to thank the Chief Information Officer, Director Information Technology Operations, and the Information Security Office for their leadership and collaboration to complete this engagement.

Summary of Results

This section of the report contains confidential information that relates to current cybersecurity levels of protection, which, if made public, may expose the District to unnecessary/new cyber risks on its computers, networks, or computer systems. As such, this information is not subject to disclosure requirements of the Texas Public Information Act based on the exception found in Government Code 552.139. The full report, which contains the overall rating of the District's cybersecurity rating posture as of June 8, 2020, was released to the appropriate levels of leadership and management.

Recommendations

1. We recommend the results of this Texas Cybersecurity Framework cybersecurity self-assessment serve as part of the District's cybersecurity program to:
   1.1. Establish the benchmark (starting posture) to begin measuring and track cybersecurity efforts over time.

   1.2. Identify opportunities for improving cybersecurity objectives to achieve a Level 3 rating in all 46 objectives.

   1.3. Facilitate cybersecurity mitigation planning required by Senate Bill 820.

   1.4. Prioritize Information Technology (IT) department cybersecurity efforts and resources based on cyber risks identified.

   1.5. Evaluate the return on cybersecurity efforts being made and their cost-effectiveness and align the District's cybersecurity program with the desired "to be" state.

2. We recommend the Texas Cybersecurity Framework risk self-assessment is completed on an on-going basis. IT leadership should:
   2.1. Complete full-assessments (where all cybersecurity objectives are rated), at least on a bi-annual basis.

   2.2. Present results to the Board of Trustees, District leadership, and others deemed as relevant stakeholders. IT leadership may include specific District committees if considered appropriate. The goal of presenting results to this audience is to:
      (i) inform and support proper risk responses,
      (ii) increase awareness of the District's cybersecurity efforts and
      (iii) obtain their feedback to gauge alignment with IT resources, goals, and objectives.

   2.3. Report progress made between full-assessments at a minimum once a year to the same audiences stated above.

   2.4 Conduct partial self-assessments (when not all cybersecurity objectives are rated) on a more frequent basis, as determined and stated in IT standard operating procedures (see recommendation 4).

   2.5. Ensure the self-assessments are completed by the most experienced, knowledgeable, and appropriate staff.

3. We recommend the roadmap included in the Texas Cybersecurity Framework roadmap be used as a guide (in combination with other best practices) to help achieve a Level 3 rating for all cybersecurity objectives.

4. We recommend IT leadership develop an IT standard operating procedure that requires a cybersecurity assessment to be completed as part of a cybersecurity program. This procedure should, at a minimum include the following key elements related to the cybersecurity assessment process:

   4.1. Who is responsible for coordinating/conducting, accountable for completing, consulted, and/or informed,

4.2. Clear objectives and detailed instructions,

4.3. Frequency and due dates for all self-assessments and progress reports,

4.4. References to relevant forms and documents, and

4.5. Applicable records retention requirements.

Exhibit 3 – List of Information Technology staff who participated

No.	Title (A to Z)	Division
1	Application Specialist	Applications
2	Business Systems Programmer / Analyst	Applications
3	Business Systems Programmer / Analyst	Applications
4	Business Systems Sr. Programmer / Analyst	Applications
5	Business Systems Sr. Programmer / Analyst	Applications
6	Business Systems Sr. Programmer / Analyst	Applications
7	Chief Technology Officer	Ch ef
8	Communications Systems Coordinator	Operations
9	Computer Technician	Operations
10	Director Technology Services Applications	Applications
11	Director Technology Services Operations	Operations
12	Help Desk Applications Support Specialist	Support
13	Help Desk Technician	Support
14	Help Desk Technology Support Specialist	Support
15	Information Assurance Administrator	Operations
16	Information Security Manager	Security
17	Information Security Network Administrator	Security
18	Information Security Officer	Security
19	Information Security Systems Administrator	Security
20	Network Administrator	Operations
21	Network Engineer	Operations
22	Network Infrastructure Manager	Operations
23	Operations Deployment Manager	Operations
24	Programmer / Analyst	Applications
25	Sr Programmer / Analyst	Operations
26	Sr. Programmer / Analyst	Applications
27	Student Systems Application Support Specialist	Applications
28	Student Systems Application Support Specialist	Applications
29	Student Systems Manager	Applications
30	Systems Administrator	Operations
31	Systems Administrator	Operations
32	Systems Analyst	Operations
33	Systems Analyst	Operations
34	Technology Specialist	Operations
35	Technology Specialist	Operations
36	Technology Support Manager	Support
37	Web Solutions Manager	Applications

EL PASO INDEPENDENT
SCHOOL DISTRICT

BOARD OF TRUSTEES

Bob Geske, Board President
Al Velarde, Vice President
Diane Dye, Secretary
Josh Acevedo
Daniel Call
Freddy Khlayel
Chuck Taylor