Killeen ISD Targeted Technology Audit Report Presentation

GIBSON

AN EDUCATION CONSULTING & RESEARCH GROUP

September 7, 2021

Agenda

- Project Background
- Project Objectives and Scope
- Key Takeaways
- Cybersecurity Framework Implementation
- Implementation of Consultant Cybersecurity Recommendations

Project Background

- With the passing of Texas Senate Bill (SB) 820 from the 86th Texas Legislature...
  - Texas school districts are required to implement cybersecurity measures.
  - The requirements include the development of a cybersecurity policy and framework for cybersecurity risk assessment and mitigation planning.
- The Texas Cybersecurity Framework (TCF) 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. KISD chose to adopt this framework.

Project Objectives and Scope

- To evaluate the District's adoption and implementation of the Texas Cybersecurity Framework.
- To evaluate KISD's current Technology Services Department's organizational structure and related areas.
  - This portion of the study could not be completed due to the following:
    - The leadership changes in the Technology Services Department;
    - The vacancy of the Executive Director position at the time of the audit; and
    - The demands of the COVID-19 pandemic on the Technology Services Department.

Key Takeaways

- Killeen ISD is in the early stages of TCF implementation.
- The major obstacles to implementation include:
  - Lack of a formal security governance structure;
  - Lack of an information security implementation plan; and
  - Reliance on vendor data privacy and sharing agreements rather than its own.
- Six recommendations were made to further improve progress in completing the framework and improving information security at KISD.

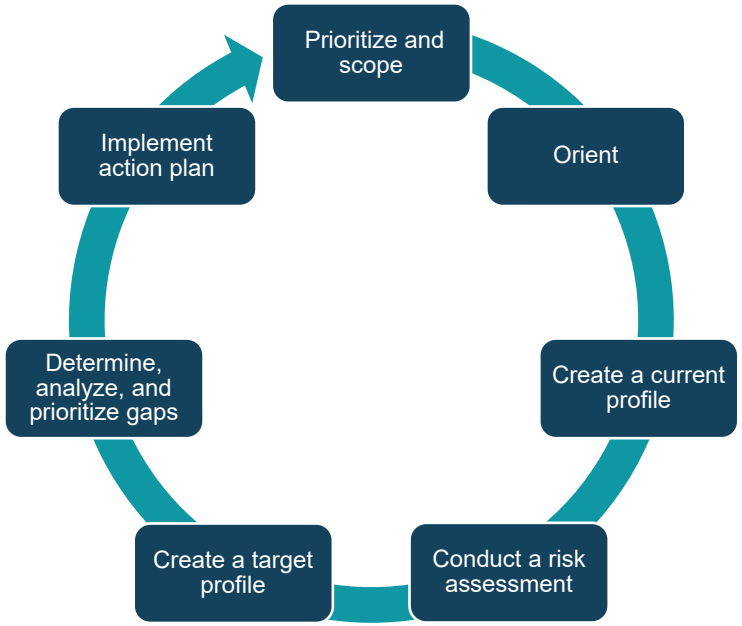
Cybersecurity Framework Implementation

Recommendations

- Develop an information security governance committee.
  - Implementing a cybersecurity framework requires a periodic District-wide risk assessment, staff and monetary resource prioritization, and security goal setting that will impact all stakeholders.
  - Without oversight that includes high levels of District leadership and participation from other key stakeholders, it will be difficult to complete the implementation of the TCF.
  - Developing an information security governance committee would provide strategic direction regarding information security, while ensuring that all cybersecurity framework-related objectives are adequately implemented by appropriately using all available District resources.

Recommendations

- Modify the KISD management approach to the implementation of the TCF.
  - A typical cybersecurity framework implementation consists of seven steps:



Recommendations

- Modify the KISD management approach to the implementation of the TCF (continued).

TCF Implementation Steps	KISD Status
Prioritize and scope	Not Complete
Orient	Not Complete
Create a Current Profile	Completed
Conduct Risk Assessment	Partially Completed
Create Target Profile	Not Complete
Determine, Analyze, and Prioritize Gaps	Not Complete
Implement Action Plan	Not Complete

Recommendations

- Re-perform the current profile step of the TCF implementation process using the following framework.
  - TCF consists of 46 Objectives in five core functions.
    - Core Functions: Identify, Protect, Detect, Respond, Recover.
  - TCF has a maturity matrix scale from Level 0 to Level 5.

Levels	Level Description
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.

Recommendations

- Review and enhance the data confidentiality section of the KISD terms and conditions document.
  - KISD overly relies on vendor provisions regarding data privacy and data sharing agreements to protect the District's sensitive data.
  - KISD should incorporate the applicable data sharing and privacy-related elements from TEA and the Texas Student Data Privacy Alliance.

Recommendations

- Update the Cybersecurity Coordinator job description.
  - Inappropriate segregation of duties exist within the Cybersecurity Coordinator position.
  - The Coordinator's primary responsibility should be to review and assess security functions.

Implementation of Consultant Cybersecurity Recommendations

Recommendations

- Track and monitor the implementation of all information security-related recommendations.
  - KISD does not have documentation in place to inform and update the District with an implementation status of the information security-related reports.
  - With implementation status information, the District and Technology Services leadership can make informed decisions regarding information security in KISD.

Questions?