Data Center Consulting Engagement

ASSURANCE • INSIGHT • OBJECTIVITY

Audit Plan Code: 18-03

Recommendations were provided to strengthen physical, logical, and environmental controls over the data center.

Contents

Consulting Engagement Report

Abbreviations

CAP   Corrective Action Plan
EPISD   El Paso Independent School District
ISO   Information Security Officer
TS   Technology Services

Introduction

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. According to the Institute of Internal Auditors' Standards, "…When performing consulting services the internal auditor should maintain objectivity and not assume management responsibility." As such, throughout a consulting engagement we make recommendations to the process owner(s) to minimize risks or increase efficiencies, but the process owner is ultimately responsible for making decisions on implementing recommendations made. If the process owner accepts a level of risk that may be unacceptable to the District, the Chief Internal Auditor must discuss the matter with cabinet level administration and the Board of Trustees if the matter has not been resolved.

The consulting engagement did not include an audit of the District's data center (the data center is officially referred to as the Network Operations Center, but for reporting purposes hereafter it will be referred to as the "data center"). As such, we are not providing assurances that procedures and internal controls were followed and adhered to in accordance with the federal, state, local policies and guidelines.

The Data Center Consulting Engagement was approved by the Board of Trustees as part of the 2017-2018 Internal Audit Plan. This is a summarized version of the Data Center Consulting Engagement Report (the report). The full version of the report contains confidential information associated with network and system security that has a risk of being misused if made publicly available. As such, we are issuing this summarized version of the report. The full version of the report was made available to appropriate members of management/administration responsible for overseeing and implementing our recommendations and the Board of Trustees.

Background

The El Paso Independent School District (EPISD) currently maintains two data center locations. One of them is being phased out and replaced by the newest data center at a different location. The new data center resides within the boundaries of El Paso County. Technology Services (TS) operates and is responsible for the operations of both data centers. The day-to-day operations of the new data center are maintained in-house by two TS employees, systems administrators (hereinafter referred to as the "data center staff"). The new data center hosts servers supporting the District's business-critical day-to-day technology operations and is essential for the District's system of networks. As such, the focus of this consulting engagement was the new data center.

The data in the data center is highly sensitive and of great value to the District. The data center requires the highest level of security available, both physically and virtually, for the securing of data in motion, in use, and at rest. In addition, the data center hosts key TS systems and provides technology services to students, parents, and staff.

Objective and Scope

The objective of the consulting engagement is to add value to the District by providing both verbal and written recommendations throughout the consulting engagement based on discussions with management, best practices, and our knowledge and understanding of internal controls. The scope included: (i) reviewing draft policies and procedures, (ii) walkthrough(s) of the data center's physical, logical, and environmental controls, and (iii) interviewing data center process owners and the Information Security Officer (ISO).

Methodology

To achieve our objectives, we:
- Reviewed the District's information security policy.
- Researched best practices published by information security organizations.
- Reviewed data center documentation provided by process owners.
- Performed walkthroughs of the data center to observe physical, logical, and environmental controls.
- Met with process owners (i.e., Director Technology Services Operations and the two Systems Administrators) to discuss those topics included under the scope of the consulting engagement, including future planned controls and enhancements to the data center.
- Met with the District's ISO to discuss security controls related to the data center.
- Met with the District's Security Surveillance Manager to discuss video surveillance for the cameras deployed at the data center.

Acknowledgement

We would like to acknowledge and thank the Chief Information Officer, Director Technology Services Operations, and the two Systems Administators from Technology Services for their cooperation and assistance during the consulting engagement.

Recommendations and Management's Response

We made 26 recommendations to minimize risks and strengthen physical, logical, and environmental controls over the data center. Management and administration accepted our recommendations and developed a Corrective Action Plan (CAP) with 25 corrective action activities to address them. The CAP appears to be sufficient to address the recommendations outlined in this report.