SAMPLE
IT Audit & Needs Assessment

School Name & Logo Here

Month | Year

Introduction

The purpose of this report is to provide School Name with a review of the school's current IT environment. Based upon our findings, we have provided a series of recommendations aimed at improving the school's technology infrastructure and capabilities to enhance security, operations and instruction.

IT Audit Findings & Recommendations

Focus Area #1

Team Structure and Communication

Observations & Concerns

On Date, I [EdTechTeacher IT Consultant Andrew Marcinek] met with the Information Technology Team. The team consisted of the Director of IT, Desktop Specialist 1, and Desktop Specialist 2. The conversation started with each team member sharing their information about their respective roles and duties within the school and the IT team. During these initial conversations I began to notice a theme of vision, mission, and direction of the IT team being cloudy and not very clear. It was also evident that there seemed to be some tensions with the team about who owned what within the team and who took new projects or changes up to the Administration.

Other observations and concerns that were clearly evident were tier 1 support and a position that used to exist within the team. This position managed a lot of the tickets coming in and would either handle or delegate to the team.

Desktop Specialist 1 and Desktop Specialist 2 each spend half of their time stationed in School Building 1. While this structure provides great facetime and training opportunities for students and faculty/staff, it doesn't provide an efficient, sustainable paradigm without having someone to support or manage projects. Additionally, if either Desktop Specialist 1 or Desktop Specialist 2 are out for any period of time, there is insufficient support for the school. As I continued my conversation with the IT team, it was very clear what Desktop Specialist 1's day-to-day was like, but I had trouble finding clarity around what Desktop Specialist 2 and the Director of IT did on a day-to-day basis.

Communication was another area of concern. In speaking with members of the Administration, I got the sense that there was limited communication coming from the technology department and that there was limited transparency around budget purchases and new initiatives or projects.

Recommendations

- Develop a 3 year IT strategic plan that aligns with the school's goals and objectives.
- Adopt a centralized communication platform for better coordination within the IT team and with other departments.
- Look at the structure of the IT department and design a new structure that has a clear leadership structure, defined roles and responsibilities, and accountability structures that can help support workload management.

Focus Area #2

Support Systems and Operational Efficiency

Observations & Concerns

Because the team is small and not fully organized, it presents inefficiencies across the board for the Director of IT, Desktop Specialist 1, and Desktop Specialist 2. I got the impression, when talking with members of the Administration, that Desktop Specialist 1 covered many of the tickets and responded promptly and followed through with communication after the incident was submitted. Desktop Specialist 2 was also supportive with many of the support tickets, but got the impression that he mostly covered the printer/copier solution and some of the device management.

As mentioned above, I got the sense from the IT team that they communicated effectively outward and that support tickets and projects were thoroughly communicated and followed through on; however, when talking outside of the team I only received positive feedback about Desktop Specialist 1 and his strong communication and follow up.

Below are some direct notes from my visit that serves as evidence of the operational efficiencies both within the team structure as it is now and the communication and training the community needs to ensure optimal efficiency of the help ticketing system:

- Desktop Specialist 1: problem with emails coming in instead of tickets.
- Desktop Specialist 2: comes in on Saturdays to update servers and maintenance.

Recommendations

- Train faculty, staff, and administration on effective use of ticketing systems and enforce its use for all IT-related issues. Provide a one-pager for “What to expect when putting in a help ticket”.
- Consider rehiring or reallocating resources for front desk support to improve operational efficiency.
- Outline and define operational duties for each member of the IT department. It remains unclear both within the team and outside of the team that there is no consistency to the operational structure.
- Create SOP (Standard Operating Procedure) Documents that can be shared with administration, faculty, and staff. This will help educate the community on various IT topics as well as serve as a succession plan for the team

Focus Area #3

IT Governance and Risk Management

Observations & Concerns

- Unclear IT organizational structure and decision-making processes.
- Potential risks due to on-premises servers and lack of a comprehensive disaster recovery plan.

While it was clear what each member of the IT team’s title was and their day to day schedule, what was not clear was the overall IT decision making process and how issues got communicated up to the administration. Evidence of this came through from both the Director of IT and Desktop Specialist 1 in statements below:

Desktop Specialist 1: How do we elevate this type of project (changing directory from opentext to Azure) to Senior Admin?

Director of IT: How does this get agenda time?

This conversation gave me pause when I was listening to both the Director of IT and Desktop Specialist 1 speak. Desktop Specialist 1 seemed frustrated that he wanted to get this project moving, but it was never communicated up to the administration. Additionally, the Director of IT mentioned that it was “hard for him to get on the agenda in the administration meetings.” My assessment of this conversation reinforced an earlier assertion that there is no leadership within the IT team and that projects and changes are not fully communicated up to the administration for conversation and dialogue.

In the area of risk management, I was able to identify several areas that posed a potential risk, but not imminent.

1. Disaster Recovery Plan and Cyber Attack Plan

In my conversations with the IT team, I asked for both a disaster recovery plan and a cyber attack plan. These documents did not exist, but should be available and understood by all members of the IT team and the Administration.

2. Non-Technical Explanation and Support Documentation

As mentioned above, there is limited documentation for support documents and how to support technical aspects of the network, security measures, etc. when things go down, or a member of the team transitions. This presents security and sustainability issues with the technical aspects of the network infrastructure and its continued security. For example: If all three members of the IT department left, how would the network and security measures be supported and maintained?

3. Budget Detail and Communication

While this is not a security risk, there is limited detail and communication about what is purchased annually within the scope of the technology budget. There should be detailed communication and conversation throughout the year and especially during the budget process. The CFO should understand purchases and also fully understand any potential risks related to data breaches or cyber attacks

4. Physical, On-Premise Servers

When I asked about file storage and server maintenance, Desktop Specialist 1 informed me of the process for maintaining and backing up server tapes on a week to week basis.This process, while secure based on Desktop Specialist 1’s process, is cumbersome and somewhat costly. The team mentioned that only a handful of users use the shared network drives. These types of drives require weekly maintenance and backups, and present a possible security vulnerability if breached.

5. Asset Management

During my meeting with the IT team, I tried to get an understanding of the hardware inventory process and systems used to track and manage hardware inventory. There are two systems used for laptop and iPad

management and inventory. The team uses Zenworks for laptops and JAMF Pro for iPads. These are two separate systems that do not communicate with each other so there is no centralized method for tracking inventory. There is also no clear evidence of any inventory of projectors and tv screens, peripheral technology, and network access points and hardware.

Recommendations

- Define clear roles and responsibilities within the IT team and establish a formal decision-making framework.
- Develop and implement a robust disaster recovery and cybersecurity response plan.
- Create a cache of support and training documents for sustainability and transparency within the organization and the IT department.
- Create and design budget narratives that detail the purchases made in each fiscal year along with a forecast and projection of future projects and maintenance. In addition to this, redesign your device refresh cycle to ensure all devices are not coming to end of life in the same fiscal year.
- Consider using Filewave for laptop and iPad management. It will create a single asset management tool for PC laptops, Mac computers, and iPads.
- Decommission physical, on premise servers and transition and train users still using shared network drive to Google Drive.

Focus Area #4

Technology Integration and Training

Observations & Concerns

- Technology not fully integrated into the school's strategic plan and learning enhancement.
- Lack of comprehensive training for staff, faculty, and students on IT systems

Throughout my visit I got a sense that technology was present and available for faculty, staff, and students; however, I did not get a thorough understanding of how it is seamlessly integrated into teaching and learning. While this was not the primary focus of my visit, I did not sense that the IT team had the instructional technology capacity within its department. The training and support provided by the IT team was primarily focused on the systems and technology itself, and not focusing on how to purposefully and intentionally integrate technology into the classroom.

One aspect of this that stood out during my visit was the amount of applications that were purchased and paid for by the school. A document of approved school applications is 36 pages long and has multiple apps per page. There was no information about how the applications can be used in the

classroom, nor was there any indication of application use redundancy. Meaning, how many apps are on this list that do the same thing.

Recommendations

- Align IT initiatives with educational goals and include technology integration in the school's strategic planning.
- Inventory school-wide applications and provide information on how each application is used in the classroom and what the application's primary function is.
- The IT team needs to have someone to collaborate with who understands instructional technology and how the technology is leveraged in the classroom for teaching and learning

Focus Area #5

Infrastructure and Security

Observations & Concerns

- Outdated physical security measures for IT assets.
- No disaster recovery plan and no cyber attack plan in place .
- Lack of communication, awareness, and protocols for physical and cybersecurity.

Physical security

During my visit to the School Name campus, I observed several vulnerabilities with physical security. In addition to the physical security, I did not gain access to any documentation regarding the use of physical security systems in the case of an emergency or an intruder.

With the door systems I noticed that it was mostly manual locks. Doors were locked in some buildings, but mostly open and accessible throughout my visit. In most cases, I did not have trouble accessing any building during the school day. What's more, there was no record of me being there throughout the day.

Systems are just one part of the security process. Physical security systems and technology, even the best implemented, is worth nothing if the users do not understand how to leverage it in various emergency situations. During my visit and interviews, I got the sense that there were limited conversations and understanding amongst the IT team and administration.

Recommendations

- Upgrade physical security systems for IT assets and ensure regular maintenance.

- Look into installing a cloud-based card swipe system that can be used for door access and managed centrally. Verkada is one example out there.
- Lock doors during school hours and update or refresh visitor policy and procedure documentation.
- Coordinate an incident response team that meets regularly (once a month) to discuss new and planned system upgrades and technology hardware upgrades needed, train team and users on systems and engage in tabletop exercises for IRT members. These training and meeting minutes should be documented and shared with the community.
- Coordinate with local authorities or a third-party organization to gain training resources for the incident response team and help train and provide resources to faculty and staff, students, and the community.

Conclusion

The IT department at School Name faces significant challenges in terms of structure, communication, operational efficiency, governance, integration, and security. Addressing these concerns through strategic planning, restructuring, training, and improved security measures will be crucial for enhancing the department's effectiveness and aligning its operations with the school's overall objectives. Implementing these recommendations will not only streamline IT operations but also ensure a more secure, efficient, and integrated technological environment conducive to the school's educational mission.