- What were the audit scope and goals?

  This audit's scope is the entire security program for Botium Toys. The internal IT audit will review and assess all assets and internal processes and procedures.

  The scope includes:

  1. User Permission Settings
  2. Implementation of security controls
  3. Procedures and protocols
  4. Ascertain that all current technology is accounted for

  The audit's goals are to review and improve the current security posture of the organizations as well as suggestions on how to improve it. The IT manager would also like grounds to hire new cybersecurity personnel.

  The goals include:

  1. Compliance to the National Institute of Standards and Technology Cybersecurity Framework (NIST CISF)
  2. Create better process for systems to ensure compliance
  3. Fortify system controls
  4. Improve credential management by implementing concept of least permissions
  5. Establish policies and procedures, including playbooks
  6. Ensure that they are meeting compliance requirements

- What were the *critical findings* of the audit that need to be addressed immediately (i.e., What controls and/or policies need to be implemented immediately)?

Some of the critical controls/policies that need to be implemented immediately include:

1. Principle of Least Privilege:
   a. Currently not implemented. Limits access to only those with a need-to-know basis. Reduces risk of parties accessing data or information that they are not authorized to access.
2. Disaster Recovery Plans:
   a. Highly important, ensures business continuity in the case of an incident. Ensures that when an event does occur, that an organization is able to recover systems back to regular functioning with minimal disruption to productivity.
3. Access Control Policies:

    a. Similar to principle of least privilege, it is the set of policies that define the criteria for whether or not a party should be authorized to access something. It increases confidentiality and integrity of data.
4. Locking Cabinets (For Network Gear) & Locks
    a. High priority since it prevents unauthorized parties from accessing/modifying network infrastructure gear.
    b. Can also prevent unauthorized access to other physical assets.
5. Backups
6. Intrusion Detection Systems
7. Fire Detection and Prevention

Some policies should also be addressed such as:
- Adherence to the Payment Card Industry Data Security Standard (PCI DSS) so that they can conduct credit card transactions in a secure manner.

- They should also adhere to System and Organizational Control regulations (SOC type 1 and 2) so that they may better manage their access policies and minimize risk and improve financial compliance.

- What were the *findings* (i.e., What controls and/or policies that need to be addressed in the future).

Some controls/policies that should be addressed in the future are:

Policy: General Data Protection Regulation (GDPR)

This regulation details and articulates the rights of E.U. citizens and their data. Botium Toys must be compliant as they wish to conduct business worldwide.

Controls: Password policies, Account Management Policies, Separation of Duties, Encryption, Password Management System, Antivirus Software, Manual monitoring, CCTV surveillance