**Botium Toys Audit Results:**

Review the controls assessment and compliance checklist you completed in “Conduct a security audit, part 1” and consider the following, before moving on to the next step:

**What were the audit scope and goals?**

Botium Toys is undergoing an audit of its cybersecurity program with the following scope and goals:

**Scope:**

* The audit will encompass the entire security program at Botium Toys, including all assets, internal processes, and procedures.
* Specific areas to be assessed include user permissions in accounting, endpoint detection, firewalls, intrusion detection systems, and security information and event management (SIEM) tools.
* The audit will also evaluate implemented controls and procedures in these systems.
* Compliance requirements will be reviewed to ensure that current user permissions, controls, procedures, and protocols align with necessary standards.
* The audit will account for the organization's current technology, including hardware and system access.

**Goals:**

* Adherence to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).
* Establishing a more robust process to ensure compliance within Botium Toys' systems.
* Strengthening system controls to enhance the overall security posture.
* Implementing the concept of least permissions for user credential management.
* Establishing policies, procedures, and playbooks for the organization.
* Ensuring compliance with relevant requirements.

The desired outcomes of the audit are a report on the current security posture of Botium Toys, recommendations for improving security, and justification for hiring additional cybersecurity personnel.

**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)?**

Based on the provided information, the controls and policies can be listed from most critical to implement now to lower priority are as follows:

1. Least Privilege
2. Disaster Recovery Plans
3. Password Policies
4. Access Control Policies
5. Account Management Policies
6. Separation of Duties
7. Intrusion Detection System (IDS)
8. Encryption
9. Backups
10. Password Management System
11. Antivirus (AV) Software
12. Manual Monitoring, Maintenance, and Intervention
13. Locking Cabinets
14. Closed-Circuit Television (CCTV) Surveillance
15. Locks
16. Fire Detection and Prevention
17. Time-Controlled Safe
18. Adequate Lighting
19. Signage Indicating Alarm Service Provider

Here they are again categorized:

**Administrative Controls:**

* Least Privilege: Implement measures to ensure that vendors and non-authorized staff only have access to the assets and data necessary for their job functions.
* Disaster Recovery Plans: Establish plans to ensure business continuity and minimize productivity downtime in the event of an incident or system failure.
* Password Policies: Implement rules and guidelines for password strength to enhance security and reduce the risk of account compromise.
* Access Control Policies: Develop policies to increase the confidentiality and integrity of data by controlling access to sensitive information.
* Account Management Policies: Implement measures to reduce the attack surface and mitigate the potential impact of disgruntled or former employees.
* Separation of Duties: Ensure that no individual has excessive access privileges that could be exploited for personal gain.

**Technical Controls:**

* Intrusion Detection System (IDS): Implement an IDS to quickly identify and respond to possible intrusions or anomalous network traffic.
* Encryption: Apply encryption measures to protect confidential information and enhance data security, especially for website payment transactions.
* Backups: Establish regular data backups to support ongoing productivity and align with the disaster recovery plan.
* Password Management System: Implement a system for password recovery, reset, and lockout notifications to enhance password security.
* Antivirus (AV) Software: Deploy AV software to detect and quarantine known threats to the organization's systems.
* Manual Monitoring, Maintenance, and Intervention: Provide necessary resources for the manual monitoring and maintenance of legacy systems to identify and mitigate potential threats and vulnerabilities.

**Physical Controls:**

* Time-Controlled Safe: Implement a safe with time-controlled access to minimize the impact of physical threats.
* Adequate Lighting: Ensure sufficient lighting in the premises to discourage potential threats and provide a safer environment.
* Closed-Circuit Television (CCTV) Surveillance: Install CCTV cameras for preventative and detective purposes to reduce the risk of incidents and aid in post-event investigations.
* Locking Cabinets: Use locking cabinets to prevent unauthorized access or modifications to network infrastructure equipment.
* Signage Indicating Alarm Service Provider: Display signage indicating the presence of an alarm service provider to deter potential attacks.
* Locks: Implement physical locks to enhance the security of both physical and digital assets.
* Fire Detection and Prevention: Install fire detection and prevention systems such as fire alarms and sprinkler systems to safeguard inventory, servers, and other critical assets.

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

**Based on the information provided, the findings and controls/policies that need to be addressed in the future are as follows:**

**Administrative Controls:**

* Access Control Policies: Develop and implement access control policies to increase the confidentiality and integrity of data within the organization.
* Account Management Policies: Establish and enforce policies for managing user accounts to reduce the attack surface and minimize the impact of disgruntled or former employees.
* Separation of Duties: Implement measures to ensure that no individual has excessive access privileges that could be exploited for personal gain.

**Technical Controls:**

* Intrusion Detection System (IDS): Implement an IDS to quickly identify possible intrusions and anomalous network traffic for proactive threat detection.
* Encryption: Implement encryption measures to protect confidential information, particularly for website payment transactions.
* Backups: Establish a regular backup strategy to support ongoing productivity and ensure data integrity in case of system failures or incidents.
* Password Management System: Implement a password management system to facilitate password recovery, resets, and lockout notifications for enhanced password security.
* Antivirus (AV) Software: Deploy AV software to detect and quarantine known threats, reducing the risk of malware infections and system compromises.
* Manual Monitoring, Maintenance, and Intervention: Ensure appropriate resources and processes are in place for manual monitoring and maintenance of legacy systems to mitigate potential threats and vulnerabilities.

**Physical Controls:**

* Time-Controlled Safe: Implement a safe with time-controlled access to minimize the impact of physical threats and unauthorized access.
* Adequate Lighting: Ensure proper lighting in the premises to deter potential threats and provide a safer environment.
* Closed-Circuit Television (CCTV) Surveillance: Install CCTV cameras for preventative and detective purposes, aiding in the reduction of security incidents and assisting in investigations.
* Locking Cabinets: Utilize locking cabinets to prevent unauthorized access and modifications to network infrastructure equipment.
* Signage Indicating Alarm Service Provider: Display signage indicating the presence of an alarm service provider to deter potential attacks.
* Locks: Implement physical locks to enhance the security of both physical and digital assets.
* Fire Detection and Prevention: Install fire detection and prevention systems, such as fire alarms and sprinkler systems, to safeguard inventory, servers, and critical assets.
* These findings highlight areas where controls and policies can be implemented or strengthened to enhance the overall security posture of Botium Toys. It is important for the organization to prioritize and address these findings in the future to mitigate potential risks and protect its assets and data.

How can you summarize your recommendations clearly and concisely to stakeholders?

**Assessment and Recommendation of Controls:**

**Critical Controls:** The most critical controls include implementing the principle of least privilege, establishing disaster recovery plans, enforcing strong password policies, and defining access control policies. These controls minimize the risk of unauthorized access, data breaches, and system vulnerabilities. It is essential to prioritize these controls to ensure the company's security and compliance.

**Important Controls**: Additional controls that are important to implement include account management policies, separation of duties, intrusion detection systems (IDS), encryption, and regular backups. These controls address critical aspects such as user account management, preventing internal fraud, detecting and responding to network intrusions, protecting data confidentiality, and ensuring data availability and recovery. By implementing these controls, the company can enhance its overall security posture and safeguard critical assets.

It is crucial for the company's stakeholders to prioritize and effectively implement these controls in their security framework. By doing so, they can mitigate risks, protect sensitive data, ensure compliance with

**Assessment and Recommendation of Regulation and Compliance Standards:**

To ensure compliance and regulatory adherence, the company should prioritize the following recommendations. Firstly, if the company plans to expand internationally, particularly into the European Union (EU), it must comply with the General Data Protection Regulation (GDPR). This involves transparently handling consumer data and promptly notifying EU citizens in the event of a data breach. Secondly, for secure handling of credit card information, the company must adhere to the Payment Card Industry Data Security Standard (PCI DSS). Failure to meet PCI DSS requirements could lead to legal and financial consequences, while compliance allows for smooth credit card transactions. Lastly, implementing System and Organizations Controls (SOC type 1, SOC type 2) reports is crucial. These reports assess financial compliance, risk levels, and data safety, ensuring user access policies are established and control failures are minimized. By following these recommendations, the company can manage assets, maintain compliance, mitigate risks, and safeguard data effectively.