Stakeholder memorandum

Complete each section of the stakeholder memorandum template to communicate your audit results and recommendations to stakeholders:

- *Scope*
- *Goals*
- *Critical findings (must be addressed immediately)*
- *Findings (should be addressed, but no immediate need)*
- *Summary/Recommendations*

Use information from the following documents:

- *Botium Toys: Audit scope and goals*
- *Controls assessment (completed in "Conduct a security audit, part 1")*
- *Compliance checklist (completed in "Conduct a security audit, part 1")*

TO: IT Manager, Stakeholders
FROM: Erick Tafel
DATE: 7/17/2023
SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

I would like to share the findings from the recent internal audit conducted at Botium Toys. Below is a summary of the audit scope, goals, critical findings, and recommendations:

Scope:

- Current user permissions set in accounting, endpoint detection, firewalls, intrusion detection system, and SIEM tool
- Current implemented controls in accounting, endpoint detection, firewalls, intrusion detection system, and SIEM tool
- Current procedures and protocols set for accounting, endpoint detection, firewall, intrusion detection system, and SIEM tool
- Alignment of user permissions, controls, procedures, and protocols with compliance requirements

- Accounting for current technology, including hardware and system access

Goals:

- Adherence to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- Establishing a robust process for compliance
- Strengthening system controls
- Implementing least privilege concept in user credential management
- Establishing policies, procedures, and playbooks
- Ensuring compliance requirements are met

Critical Findings:

1. **Immediate implementation of least privilege access control measures:** It is crucial for Botium Toys to restrict user permissions to only necessary levels to mitigate the risk of unauthorized access and potential misuse of resources.
2. **Development of comprehensive disaster recovery plans:** Botium Toys should establish robust plans to ensure business continuity in the event of incidents, minimizing downtime and ensuring the availability of critical systems and data.
3. **Strengthening password policies:** The company needs to enforce stronger password rules, including complexity requirements and regular password changes, to enhance security and reduce the likelihood of password-based attacks.
4. **Implementation of access control and account management policies:** Botium Toys should implement strict access control measures and effective account management procedures to prevent unauthorized access and minimize the impact of insider threats.
5. **Separation of duties for enhanced security:** The company should establish clear segregation of duties to ensure that no individual has excessive access privileges, reducing the risk of fraudulent activities and unauthorized system modifications.
6. **Development and implementation of policies** to ensure compliance with PCI DSS, GDPR, and SOC1/SOC2 guidelines regarding user access policies and data safety.

Other Findings:

1. **Ongoing monitoring, maintenance, and intervention for legacy systems:** It is essential to dedicate resources to monitor and maintain legacy systems to identify and mitigate potential vulnerabilities, threats, and risks.
2. **Strengthening intrusion detection capabilities:** Botium Toys should enhance its intrusion detection system to quickly identify and respond to anomalous network traffic and potential security breaches.

3. **Encryption for sensitive data:** Implementing encryption mechanisms for sensitive data, such as payment transactions, will add an extra layer of protection against unauthorized access and ensure confidentiality.
4. **Robust backup strategies:** The company should establish comprehensive backup strategies to regularly and securely back up critical data, enabling efficient restoration in case of data loss or system failures.
5. **Effective password management system:** Deploying a reliable password management system will streamline password-related operations, including recovery, resets, and lockouts, ensuring secure access management.
6. **Antivirus software implementation:** Botium Toys should deploy and regularly update antivirus software to detect and quarantine known threats, reducing the risk of malware infections.

Controls to consider implementing when appropriate:

- Time-controlled safes
- Adequate lighting measures
- Locking cabinets for securing network gear
- Signage indicating the alarm service provider

Summary/Recommendations:

In order to effectively address the critical findings resulting from the security audit, it is strongly advised that Botium Toys prioritizes the following actions: adherence to the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS) to safeguard data privacy and maintain legal and ethical standards. With global operations and the collection of personal information worldwide, these measures ensure the mitigation of data breach risks. Furthermore, implementing a comprehensive user access control policy based on System Organization Controls (SOC1/SOC2) guidance is crucial to protect data from unauthorized access. Immediate implementation of least privilege access controls, development of comprehensive disaster recovery plans, and strengthening password policies are essential steps to be taken. Moreover, Botium Toys should focus on implementing access control and account management policies, ensuring separation of duties, and enhancing intrusion detection capabilities. Ongoing monitoring and maintenance for legacy systems, encryption for sensitive data, robust backups, and effective password management should also be addressed. Lastly, it is recommended to consider implementing time-controlled safes, adequate lighting measures, locking cabinets for securing network gear, and signage indicating the alarm service provider. By implementing these recommendations, Botium Toys will strengthen its security posture, align with compliance requirements, and mitigate potential risks.