**Brenner Financial Services: Audit scope and goals**

**Summary:** Perform an audit of Brenner Financial Services’ cybersecurity program. The audit needs to align current business practices with industry standards and best practices. The audit is meant to provide mitigation recommendations for vulnerabilities found that are classified as “high risk,” and present an overall strategy for improving the security posture of the organization. The audit team needs to document their findings, provide remediation plans and efforts, and communicate with stakeholders.

**Scope:** (*To understand the audit scope, review the security audit reading. Note that the scope is not constant from audit to audit. However, once the scope of the audit is clearly defined, only items within scope should be audited. In this scenario, the scope is defined as the entire security program at Botium Toys. This means all assets need to be assessed alongside internal processes and procedures*).

Brenner Financial Services Internal IT audit will assess the following:

* Security Controls:
* Network Security: Assess the security measures in place to protect the organization's network infrastructure from unauthorized access, data breaches, and cyber threats.
* Endpoint Security: Evaluate the security of end-user devices (computers, laptops, mobile devices) to ensure they are protected against malware, unauthorized access, and other security threats.
* Firewalls and Intrusion Detection/Prevention Systems: Review the configuration and effectiveness of firewalls and systems designed to detect and prevent unauthorized access.
* Data Protection:
* Data Encryption: Assess the use of encryption to protect sensitive data during transmission and storage.
* Data Backup and Recovery: Evaluate the organization's data backup and recovery processes to ensure the ability to restore critical data in case of a disaster or data loss.
* Access Controls:
* User Access Management: Review the processes for granting and revoking user access to systems and data.
* Authentication and Authorization: Assess the effectiveness of authentication mechanisms (e.g., passwords, multi-factor authentication) and authorization processes to control access to systems and sensitive information.
* IT Governance:
* Policies and Procedures: Evaluate the existence and adherence to IT policies and procedures that ensure compliance with regulatory requirements and industry best practices.
* Risk Management: Assess the organization's risk management processes related to IT, including identification, assessment, and mitigation of IT-related risks.
* Compliance:
* Regulatory Compliance: Ensure that IT systems and processes comply with relevant financial regulations, industry standards, and legal requirements.
* Internal Policy Compliance: Evaluate adherence to internal policies governing IT security, data handling, and other relevant areas.
* Incident Response and Management:
* Incident Response Plan: Review and test the organization's incident response plan to ensure preparedness for handling and mitigating cybersecurity incidents.
* Logging and Monitoring: Assess the effectiveness of logging and monitoring systems to detect and respond to security incidents in a timely manner.
* Vendor Management:
* Third-Party Risk Management: Evaluate the processes in place for assessing and managing the cybersecurity risks associated with third-party vendors and service providers.
* Infrastructure and Technology Architecture:
* System Configuration: Review the configuration of servers, databases, and other critical infrastructure components for security and efficiency.
* Software Development Practices: Assess the security of software development processes and applications to identify and mitigate potential vulnerabilities.
* Training and Awareness:
* Employee Training: Evaluate the effectiveness of training programs to educate employees about cybersecurity best practices and security policies.
* Physical Security:
* Data Center Security: If applicable, assess the physical security measures in place to protect data centers and other critical IT infrastructure..

**Goals:** (*The goal of an audit is the desired deliverables or outcomes. The goal of an audit can be to achieve compliance, to identify weaknesses or vulnerabilities within an organization, and/or to understand failures in processes and procedures and correct them. In this scenario, the IT manager set the goals. He is expecting a report of the current security posture of the organization and recommendations for improving the security posture of the organization, as well as justification to hire additional cybersecurity personnel.)*

The goals for Brenner Financial Services’ internal IT audit are:

* Security Assurance:
* Ensure the confidentiality, integrity, and availability of sensitive financial and customer data.
* Assess the effectiveness of security controls to protect against cyber threats, unauthorized access, and data breaches.
* Regulatory Compliance:
* Verify compliance with relevant financial regulations, such as those set forth by financial regulatory bodies (e.g., SEC, FINRA), data protection laws (e.g., GDPR, CCPA), and other applicable regulations.
* Ensure that IT practices align with industry standards and best practices.
* Risk Management:
* Identify and assess IT-related risks that could impact the organization's financial operations.
* Evaluate the adequacy of risk mitigation measures and controls in place.
* Operational Efficiency:
* Assess the efficiency of IT processes and systems in supporting the financial services operations.
* Identify areas for improvement in terms of technology utilization and workflow optimization.
* Data Protection and Privacy:
* Ensure proper measures are in place to protect sensitive customer information and financial data.
* Evaluate data encryption, access controls, and data handling practices.
* Business Continuity and Disaster Recovery:
* Verify the effectiveness of business continuity and disaster recovery plans to ensure the organization's ability to continue critical operations in case of disruptions.
* Vendor Management:
* Assess the cybersecurity risks associated with third-party vendors and service providers.
* Ensure that vendor management practices align with industry standards and regulatory requirements.
* Incident Response Readiness:
* Evaluate the organization's preparedness to respond to and recover from cybersecurity incidents.
* Test the incident response plan and identify areas for improvement.
* Technology Governance:
* Review and ensure the alignment of IT strategies with overall business objectives.
* Evaluate IT governance practices, policies, and procedures.
* Training and Awareness:
* Assess the effectiveness of employee training programs related to cybersecurity and IT policies.
* Enhance awareness of security practices and potential risks among employees.
* Audit Trail and Monitoring:
* Ensure the existence and effectiveness of audit trails for monitoring and investigating security incidents.
* Evaluate the organization's ability to detect and respond to security events in real-time.
* Comprehensive Policy Review:
* Review and update IT security policies to address emerging threats and changes in the regulatory landscape.
* Ensure that policies are communicated and enforced throughout the organization.