Student:	Email:
Bradley Adams	badams10@my.athens.edu

Time on Task:	Progress:
	100%

Report Generated: Tuesday, March 18, 2025 at 2:58 PM

Guided Exercises

Part 1: Research Security Awareness Policies

2. For the sample security awareness training policy that you reviewed in the step above, **discuss** the policy's main components. You should focus on the need for a security awareness program and its key elements.

The Security Education, Training, and Awareness (SETA) policy in the North Carolina Department of Health and Human Services (DHHS) Information Security Manual highlights critical components for establishing a strong security culture. The need for a SETA program arises from the understanding that technological security controls are lacking when used alone. Workforce awareness, vigilance, and proper training are critical to defend against ever-evolving security threats.

The policy emphasizes developing a customized SETA program that aligns with organizational missions and business needs. A key component includes performing a thorough needs assessment to determine workforce skills gaps, evaluate existing knowledge, and uncover the specific requirements of different organizational roles. Various information-gathering methods, such as interviews, surveys, resource reviews, and trend analyses, assist in the design of a tailored training program.

The strategy development phase merges the assessment insights into actionable plans. It clearly outlines objectives, target audiences, specific topics, roles and responsibilities, resource needs, delivery methods, and methods for evaluating training effectiveness. Establishing training priorities ensures that SETA activities focus on the areas with the most significant impact and urgency.

Material development considers both awareness and training aspects. While awareness materials provide short, high-level messages for broad dissemination, training materials involve detailed, targeted, role-specific content. The policy advises that materials should account for various learning types, such as visual, auditory, and tactile. Adult learning preferences should focus on behavioral reinforcement and skills application, which will maximize engagement and effectiveness.

Measurement and evaluation of the program are critical. The policy requires straightforward, actionable, meaningful, accessible, and repeatable metrics to demonstrate compliance, gauge effectiveness, and encourage continuous improvement. These metrics include implementation measures and impact measures.

Content is delivered using diverse methods, including electronic formats such as emails, pop-ups, and webinars and physical formats such as pamphlets, posters, and seminars, to cater to varying contexts and workforce needs. Accountability and ease of access are critical in these delivery means.

Professional development is encouraged, promoting workforce engagement in security-oriented certifications, memberships, and continuous learning and reinforcing organizational capabilities. Organized documentation of completed training, awareness, and professional development activities must be maintained, aligning with regulatory requirements for audit and accountability.

The policy's approach assures a comprehensive security education, encouraging a security-aware culture critical to protecting sensitive data.

Part 2: Create a Security Awareness Policy

Policy Statement
Define your policy verbiage.

Bankwise Credit Union Security Awareness Policy

Policy Statement

Bankwise Credit Union is dedicated to safeguarding customer information, complying with the Gramm-Leach-Bliley Act (GLBA), and following IT security best practices. All employees, contractors, and third-party vendors with access to the organization's systems must adhere to strict security awareness guidelines to protect sensitive financial data, prevent cyber threats, and ensure the integrity of organizational IT assets.

Bankwise mandates a comprehensive security awareness training program for all new hires and existing employees, with annual refresher courses. The training will cover GLBA compliance, customer privacy protection, cybersecurity risks, acceptable use policies, and incident reporting procedures.

The use of organization-owned IT assets is strictly for business purposes. Personal use of company systems, including email and internet access, is prohibited. Bankwise will enforce content filtering, email security controls, and system monitoring to prevent unauthorized access and mitigate risks. Employees are required to report security incidents or suspicious activities immediately.

Failure to comply with this policy may result in disciplinary action, including termination. The IT security team will review this policy annually and update it when necessary to address current security threats and regulatory requirements.

Purpose/Objectives

Define the policy's purpose as well as its objectives.

Purpose

This security Awareness Policy seeks to establish a strong security culture at Bankwise Credit Union. It assures all employees, contractors, and third-party vendors that they understand their responsibilities in protecting customer financial data, adhering to Gramm-Leach-Bliley Act (GLBA) regulations, and following IT security best practices. Bankwise seeks to minimize security risks, prevent cyber threats, and uphold customer trust by implementing and enforcing a structured security awareness training program.

Policy Objectives

Assure Compliance – Align employee security practices with GLBA and other regulatory requirements governing customer data protection.
Enhance Security Awareness – Educate employees on phishing, social engineering, malware, insider threats, and other cyber risks through mandatory training sessions.
Protect Customer Information – Reinforce secure handling, storage, and transmission of personally identifiable information (PII) and financial data to prevent unauthorized access or breaches.
Define Acceptable Use – Restrict personal use of company IT assets, enforce content filtering, and enforce email security controls to reduce exposure to security threats.
Improve Incident Response – Train employees to promptly recognize and report security incidents, suspicious activities, or policy violations.
Promote Ongoing Education – Require annual security awareness training to reinforce best practices and inform employees of emerging threats.

Scope

Define whom this policy covers and its scope. What elements, IT assets, or organization-owned assets are within this policy's scope?

Scope

This Security Awareness Policy applies to all employees, contractors, third-party vendors, and individuals accessing Bankwise Credit Union's IT systems, networks, and sensitive customer information. Compliance is mandatory for all personnel, regardless of job role or location, to secure the confidentiality, integrity, and availability of Bankwise Credit Union's ecosystem.

The scope of this policy includes, but is not limited to, the following IT assets and resources:
*Workstations, laptops, and mobile devices owned or managed by Bankwise Credit Union.
*Network infrastructure, including wired and wireless connections, firewalls, VPNs, and cloud-based services.
*Online banking platforms, internal applications, and customer databases containing sensitive financial data.
*Email systems, including corporate email accounts and messaging services, are subject to monitoring and security controls.
*Content filtering regulates Internet access to prevent unauthorized use and mitigate cybersecurity threats.
*Removable storage devices, including USB and external hard drives, are restricted to prevent data leakage.
*Third-party access includes vendors and service providers interacting with Bankwise's systems and customer data.

This policy covers the use, access, and security of IT assets to ensure compliance with Gramm-Leach-Bliley Act (GLBA) regulations and protect customer privacy. All personnel must follow security awareness training mandates and adhere to all acceptable use guidelines. Non-compliance shall result in disciplinary action, including termination and, if applicable, legal action.

Standards

Does the policy statement point to any hardware, software, or configuration standards? If so, list them here and explain the relationship of this policy to these standards.

Standards

This Security Awareness Policy aligns with industry best practices, regulatory requirements, and internal IT security standards to protect Bankwise Credit Union's data, systems, and customers. It sets a baseline for security awareness by requiring compliance with the following hardware, software, and configuration standards:

Regulatory Standards: Compliance with the Gramm-Leach-Bliley Act (GLBA), National Institute of Standards and Technology (NIST) Cybersecurity Framework, and ISO/IEC 27001 for data protection, access controls, and security training.
Access Control Standards: Enforcement of least privilege access, multi-factor authentication (MFA), and role-based access controls (RBAC) for all users accessing sensitive systems and data.
Endpoint Security Standards: Antivirus, endpoint detection and response (EDR) solutions, and automated security patching.
Network Security Standards: To protect against unauthorized access, firewalls, intrusion detection/prevention systems (IDS/IPS), VPN encryption, and network segmentation will be implmented.
Email Security Standards: Deployment of email filtering, phishing detection, and encryption to prevent malware, phishing, and unauthorized data transmission.
Acceptable Use Standards: Prohibition of personal use of company IT assets, enforcement of content filtering for internet browsing, and strict controls over removable media and external storage devices.
Security Awareness Training Standards: Mandatory annual security training for all employees, including phishing simulations, social engineering awareness, and secure customer data handling.

Procedures

Explain how you intend to implement this policy for the entire organization.

Procedures

This policy will implement the following procedures:

Security Awareness Training
All new hires must complete mandatory security awareness training before being granted access to company IT systems.
All employees are required to attend annual refresher training to stay informed about emerging threats, regulatory updates, and security best practices. Training will be provided and tailored to specific departments and high-risk roles such as customer service, information technology, and finance. This tailored training will address unique security concerns.

Acceptable Use Enforcement
Employees must sign an acknowledgment agreeing to the Acceptable Use Policy, which prohibits personal use of company IT assets.
Content filtering will be applied to block access to unauthorized or high-risk websites.
Email security controls will prevent the sending or receiving of unencrypted sensitive data and detect phishing attempts.

Monitoring and Compliance
IT security teams will monitor network activity, system logs, and user behavior for potential security incidents.
Simulated phishing campaigns will regularly test employee vigilance and provide corrective training.
Employees are required to report security incidents immediately via the Bankwise Security Hotline or IT helpdesk.

Policy Enforcement and Consequences
Failure to comply with this policy shall result in disciplinary action, including revoked access privileges, written warnings, termination, or legal action.
The IT security team will review this policy annually to confirm it agrees with new security threats, regulations, and industry standards.

Guidelines

Explain any roadblocks or implementation issues that you must overcome in this section and how you will surmount them per defined guidelines. Any disputes or gaps in the definition and separation of duties responsibility may need to be addressed in this section.

Guidelines

Implementing the Bankwise Credit Union Security Awareness Policy may present several challenges, including employee resistance, lack of technical expertise, and enforcement consistency. The following guidelines will provide for a successful rollout and ongoing compliance:

Overcome Employee Resistance
Employees may perceive security training as unnecessary or time-consuming. Training will be interactive, engaging, and role-specific, focusing on real-world threats like phishing, social engineering, and financial fraud. A rewards program will be introduced to incentivize participation and knowledge retention.

Technical Challenges and Accessibility
Employees with limited technical knowledge may struggle to understand complex security concepts. The training materials will be provided in multiple formats (videos, quizzes, hands-on simulations). This diversified training will assist in accommodating different learning types. Employees will have 24/7 access to an internal security knowledge base for self-paced learning.

Consistent Enforcement
Managers and supervisors will be held accountable for confirming that their teams have completed training and are following acceptable use policies. The IT security team will conduct random audits and security compliance checks to verify compliance with security controls, including email security, content filtering, and access management.

Role-Based Security Gaps
Due to their access to sensitive data, employees with privileged access (IT, finance, customer service) will undergo enhanced security training and additional monitoring. Third-party vendors must comply with Bankwise's security policies before being granted access to internal systems.

Challenge Exercise

Identify three security awareness training software providers.

KnowBe4 https://www.knowbe4.com/

Guardey https://www.guardey.com/

Hook Security https://www.hooksecurity.co/

Identify 10 questions that you would include in your RFI.

Can training content be customized to align with eChef's specific industry risks and policies?

Do you provide metrics on user participation and improvement over time?

Does your platform support customizable phishing simulations?

How does your training align with industry standards such as PCI-DSS and provide compliance tracking and auditing?

Can your platform integrate with eChef's existing Microsoft Active Directory?

What types of reporting and analytics dashboards are available to track progress?

Do you offer flexible scheduling and self-paced learning options?

Does your system provide immediate remedial training if an employee fails a phishing test?

Do you undergo regular third-party security audits or penetration testing to secure the CIA of user data?

What levels of customer support do you offer (dedicated account manager, 24/7 help desk, live chat)?