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

Time on Task:	Progress:
	100%

Report Generated: Wednesday, March 12, 2025 at 1:22 PM

Guided Exercises

Part 1: Research Separation of Duties Policies

2. **Write** a **brief summary** of the article. In your summary, focus on the need for a Separation of Duties policy and its key elements.

The research paper explores the dynamic enforcement of Separation-of-Duty (SoD) policies. This fundamental security principle is designed to prevent fraud and errors in access control. SoD policies assure that no single individual has the necessary permissions to complete a sensitive task alone, requiring cooperation among multiple users.

The article distinguishes between Static SoD (SSoD) and Dynamic SoD (DSoD) policies:
Static SoD (SSoD): Enforces role restrictions at the initial access control setup.
Dynamic SoD (DSoD): Enforces constraints during task execution by tracking user actions.

The paper introduces the Dynamic Safety Checking Problem (DSCP), which determines whether an access control state complies with a given SSoD policy. The authors prove that DSCP is computationally intractable (NP-complete), making direct enforcement difficult.

To address this, the authors offer an improvement algorithm for DSCP enforcement using preprocessing, which reduces the number of users and permissions considered, and static pruning, which filters user sets to eliminate redundant checks.

Experiments indicate that the optimized algorithm significantly improves efficiency compared to a straightforward approach.

Key Takeaways
*The need for SoD policies is essential in business, government, and industry to minimize risk, assure compliance, and prevent unauthorized actions.
*Static enforcement is often infeasible due to computational complexity.
*A dynamic approach requires tracking and verifying user actions in real time.
*The proposed solution uses preprocessing and pruning techniques to enhance enforcement efficiency.

This research spotlights the need for dynamic enforcement mechanisms for SoD policies in complex access control while addressing computational restrictions.

Part 2: Create a Separation of Duties Policy

Policy Statement
(Define your policy verbiage.)

Bankwise Credit Union
Separation of Duties Policy

Policy Statement
Bankwise Credit Union is committed to safeguarding its information systems and ensuring compliance with the Gramm-Leach-Bliley Act (GLBA) and industry best practices. This Separation of Duties (SoD) policy is created to reduce risks related to unauthorized access, fraud, data breaches, and internal misuse of information technology (IT) resources.

This policy establishes explicit role-based access controls (RBAC) and enforces the division of responsibilities between different departments and personnel to maintain operational integrity and compliance. No single employee or team shall have unreasonable authority over critical business functions, particularly system security, online banking, customer data, and IT infrastructure management.

This policy prevents conflicts of interest, improves accountability, and provides a strong security posture by defining responsibilities and restricting overlapping privileges. The Information Security Officer (ISO), IT Department, Compliance Team, Internal Audit, and Executive Leadership will work together to implement and enforce this policy.

This policy applies to all employees, contractors, and third-party vendors accessing Bankwise Credit Union's IT systems. Violations shall result in disciplinary action, up to and including termination.

Purpose/Objectives
(Define the policy’s purpose as well as its objectives.)

Purpose and Objectives

The purpose of this policy is to enforce security best practices by confirming that no individual controls critical IT functions excessively. It mitigates risks associated with fraud, insider threats, unauthorized system modifications, and data breaches while assuring regulatory compliance.

This policy's objectives are to provide the following:
*Prevent employee conflicts of interest by segregating critical security and business functions.
*Assure compliance with the GLBA by maintaining strict access controls.
*Monitor and enforce Internet and e-mail usage restrictions to prevent unauthorized activities.
*Protect customer financial data and IT assets from unauthorized access and data manipulation.
*Implement role-based access control (RBAC) to confirm that employees have only the minimum access required for their roles.
*Harden internal controls and auditing processes to detect and stop security violations.
*Annual security awareness training is conducted to verify that all employees understand their responsibilities.

Scope

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

Scope

The scope of this policy applies to all Bankwise Credit Union employees, contractors, and third-party service providers interacting with Bankwise Credit Union IT systems and processes. The scope of this policy includes all IT assets owned and operated by Bankwise Credit Union, such as:
*Online banking systems
*Customer databases
*Internal applications
*Workstations, servers, and cloud infrastructure
*E-mail and Internet systems
*Network security and monitoring tools

All security-related processes to include:
*User access and deactivation
*Network security administration
*Incident response and auditing
*Data access and encryption management

This policy does not include end-user devices not owned by the organization. This policy shall mandate compliance to access Bankwise Credit Union's systems.

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

The Separation of Duties (SoD) policy aligns with the following standards:

Regulatory Compliance Standards

*Gramm-Leach-Bliley Act (GLBA) to enforce data protection and customer privacy.
*National Institute of Standards and Technology (NIST) 800-53 to define access control and security best practices.
*ISO/IEC 27001 shall provide a framework for information security management.

Technical Standards

*Role-Based Access Control (RBAC) will confirm access is granted based on job roles and responsibilities.
*The Least Privilege Principle mandates that employees shall have only the access necessary to perform their jobs.
*Network Security Standards will mandate firewalls, VPNs, and content filtering to restrict Internet usage.
*E-Mail Security Standards implements encryption, spam filtering, and data loss prevention (DLP) controls.

Procedures

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

Procedures

User Account Access Management
*The HR Department is responsible for beginning access requests during onboarding.
*The IT Department creates accounts but cannot approve access requests.
*The Information Security Officer (ISO) reviews and approves all access requests.
*The Internal Audit Team performs quarterly access reviews.

Internet and E-Mail Security Enforcement
*The Network Security Team will configure and enforce content filtering policies to block non-business-related sites.
*The Security Operations Center (SOC) will monitor and log Internet activity for policy violations.
*The E-Mail Security Team will enforce anti-spam, encryption, and phishing protection policies.

System and Database Management
*Database Administrators can read and modify customer records but cannot access security logs.
*The Security Team will have log monitoring privileges but cannot alter system data.
*The Finance Team will process financial transactions but cannot modify database configurations.

Incident Response and Monitoring
*The Security Incident Response Team will investigate and respond to security incidents.
*The Compliance Team will conduct independent audits and report findings to executive leadership.
*The IT Department will implement security patches and system updates.

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

Challenges and Implementation Issues

*Implementing separation of duties may increase labor costs.
  *Solution: Automate security controls where possible.
*Employees may resist restrictions on Internet and e-mail use.
  *Solution: Provide training on cybersecurity risks and enforce policies gradually.
*Employees may feel Internet and e-mail monitoring invades privacy.
  *Solution: Communicate that monitoring is for security purposes only and aligns with legal requirements.

Dispute Resolution and Policy Gaps

The Information Security Officer may review any disputes regarding access controls or responsibility overlaps and escalate them to Executive Leadership.

If an employee requires an exception to this policy, they must submit a formal request to the Compliance Team for review and approval.

This policy will be reevaluated and updated annually to provide compliance with regulatory changes and evolving security threats.

Challenge Exercise

Discuss how a separation of duties policy would help to resolve the issues at Bankwise Credit Union, as discussed in this case study. Assume your audience is the CEO and Board of Bankwise Credit Union.

Enhancing Security at Bankwise Credit Union through Separation of Duties

Threat Overview
A lack of Separation of Duties (SoD) can lead to insider threats, as presented in a case study of ABS Banking Corporation, where an employee exploited job function conflicts to commit fraud. These same risks are at Bankwise Credit Union (BCU). Employees at BCU with overlapping access rights could manipulate financial transactions, vendor payments, or customer data.

To mitigate these risks and comply with Gramm-Leach-Bliley Act (GLBA) regulations, BCU must implement a structured SoD framework that guarantees no single individual has excessive control over any single critical process.

Solution: Implement a Separation of Duties Policy
*Role-Based Access Controls (RBAC) and Privilege Restrictions
*Employees must only have the minimum necessary access to perform their job functions.
*Critical functions shall be separated across multiple employees.
*Quarterly audits will review role assignments to detect unauthorized access changes and fraud.

Segregation of Duties
*Financial Transactions: The Finance Team processes payments but cannot modify customer accounts.
*Vendor and Procurement Management: Only authorized personnel create vendors. Separate payment approvals shall be required.
*Customer Data Access: Customer service can view but not edit account details. BCU shall require dual approval for modifications.
*IT Security: System administrators cannot audit their own actions. A separate compliance team must monitor security logs.

Automated Monitoring and Detection
Real-time conflict detection software will flag employees attempting to perform conflicting duties. Comprehensive audit logs will track all financial and IT security actions to detect anomalies.

Employee Training and Compliance
Annual security training will educate employees on SoD best practices and insider threat risks. Employees must acknowledge security policies. This acknowledgment will strengthen accountability.

Expected Outcomes
By implementing a structured SoD framework, Bankwise will prevent insider fraud and unauthorized financial transactions, enhance regulatory compliance with GLBA and industry standards, strengthen IT security by enforcing role-based restrictions, protect customer data, and maintain trust with the public.