Student:	Email:
Bradley Adams	badams10@my.athens.edu
Time on Task:	Progress:
	100%

Report Generated: Wednesday, February 26, 2025 at 11:17 AM

Guided Exercises

Part 1: Research Security Policy Frameworks

3. **Summarize** the Policy Development Guide's recommendations for organizing a policy hierarchy and selecting policy topics.

The guide recommends a structured hierarchy for security policies to provide clarity and effectiveness. This hierarchy has three levels.

1. The Governing Policy is a high-level document outlining core security principles. It defines the security philosophy, concepts, and expected employee behavior. The policy should align with human resources policies and address the 'what' of security policies.

2. Technical Policies provide more details that define security controls for specific systems or technologies and cover particular requirements, such as Windows security or Oracle database policies. Technicians primarily use technical policies and should address the who, what, when, and where of security controls.

3. Job Aids or Guidelines are step-by-step procedures. They include hardening procedures, coding guidelines, and user manuals. They focus on the 'how' of policy implementation.

The guide recommends prioritizing policy topics based on legal requirements, business criticality, and security risks. The legal and compliance requirements identify policies that address compliance. Policies should map to legal requirements. Any critical business information, such as data for decision-making, financial, and customer data, should be protected. Any critical business information should include data classification, risk assessments, and privacy. Policies should be developed for the organization's different operating systems, applications, and network devices. Acceptable use policies should define how employees interact with resources. Policies should define physical access controls and encryption standards.

The guide recommends beginning with foundational policies and evolving as the organization matures in security governance. The phased approach provides incremental adoption and compliance while allowing for future improvements.

5. **Describe** the core principles and objectives of COBIT 2019.

There are approximately six core principles for COBIT 2019. The core principles start with a distinction between governance and management, then apply COBIT enterprise-wide, align COBIT with business goals, integrate any other standards, COBIT focus on performance and maturity, and have a risk-based approach. Governance and management address differences between organizational direction and stakeholder needs to the daily running and monitoring of information technology. Enterprise-wide means the COBIT applies to the entire enterprise, not just a single department. Business goals are aligned with IT processes and business objectives to reduce risk. COBIT's designed to work with other frameworks and standards, making COBIT flexible. COBIT focuses on maturity models and performance indicators to assess and improve processes over time. COBIT provides risk management to guide security, compliance, and risk decisions.

There are also approximately six objectives. The objectives are cost-effectiveness, an overall holistic approach, meeting compliance, supporting efficient resource usage, strengthening risk management, and allowing for future technologies. COBIT sets up an environment for investment in information technology and processes to create benefits while supporting cost-effectiveness. COBIT considers how processes flow and the impact on business operations. COBIT helps meet compliance through a structured framework. COBIT supports efficient IT resource utilization for effective management. COBIT identifies and mitigates risk with integrated risk management. COBIT allows for emerging technology for growing and/ or changing organizations.

Part 2: Define a Security Policy Framework

2. For each risk, threat, or vulnerability in the list above, **select** an appropriate security policy that might help mitigate it. You can select one of the SANS policies or choose one from the following list.

Unauthorized access from public Internet maps to an Access Control Policy, Internet Ingress/Egress Traffic Policy, and Remote Access Policy.

Hacker penetrates IT infrastructure maps to Access Control Policy, Vulnerability Management and Vulnerability Window Policy,Mandated Security Awareness Training Policy

Communication circuit outages maps to Business Continuity and Disaster Recovery Policy and Wide Area Network (WAN) Service Availability Policy

Workstation operating system (OS) has a known software vulnerability maps to Vulnerability Management and Vulnerability Window Policy

Unauthorized access to organization-owned data maps Access Control Policy maps to Data Classification Standard and Encryption Policy

Denial of service attack on organization’s e-mail maps to Internet Ingress/Egress Traffic Policy and Business Continuity—Business Impact Analysis (BIA) Policy

Remote communications from home office maps to Remote Access Policy and VPN Tunneling Policy

Workstation browser has software vulnerability maps to Vulnerability Management and Vulnerability Window Policy

Weak ingress/egress traffic-filtering degrades performance maps to Internet Ingress/Egress Traffic Policy

Wireless Local Area Network (WLAN) access points are needed for LAN connectivity within a warehouse maps to Access Control Policy and Remote Access Policy

User destroys data in application, deletes all files, and gains access to internal network maps to Access Control Policy, Mandated Security Awareness Training Policy, and Production Data Backup Policy

Fire destroys primary data center maps to Business Continuity and Disaster Recovery Policy and Production Data Backup Policy

Intraoffice employee romance gone bad maps to Acceptable Use Policy

Loss of production data maps to Production Data Backup Policy and Business Continuity and Disaster Recovery Policy

Need to prevent rogue users from unauthorized WLAN access maps to Access Control Policy and Mandated Security Awareness Training Policy

LAN server OS has a known software vulnerability maps to Vulnerability Management and Vulnerability Window Policy

User downloads an unknown e-mail attachment Mandated Security Awareness Training Policy and Internet Ingress/Egress Traffic Policy

Service provider has a major network outage maps to Wide Area Network (WAN) Service Availability Policy

User inserts a USB hard drive with personal photos, music, and videos on organization-owned computers maps to Acceptable Use Policy

Virtual Private Network (VPN) tunneling between the remote computer and ingress/egress router maps to Remote Access Policy

3. **Organize** the security policies you selected so that they can be used as part of an overall framework for a layered security strategy.

A Layered Security Strategy starts at the perimeter with network and access controls. This layer should prevent unauthorized external access to internal systems and create secure communications. An access control policy will restrict unauthorized access. Internet ingress/Egress traffic policy will define controls to filter network traffic. A remote access policy will allow for secure access for remote users, and a wide area network service availability policy will create a reliable network through redundancy and failover.

The next layer is device and workstation protection and endpoint security. The organization must secure devices from unauthorized use and exploitation at this layer. An acceptable use policy will define the safe use of company devices. A vulnerability management and vulnerability window policy will implement patch management and vulnerability remediation timelines. A mandated security awareness training policy will educate employees on security threats.

The next layer is to protect sensitive data and services. At this layer, sensitive information should be protected, and unauthorized access and data loss should be prevented. A data classification standard and encryption policy will define how sensitive data is classified and encrypted at rest and in transit. An access control policy ensures proper authentication and authorization. A production data backup policy ensures regular backups.

The next layer ensures resilience for operational security and business continuity. This layer will maintain ‘best practices’ in cyber security during incidents. A business continuity and disaster recovery policy outlines procedures for keeping operations going and the recovery of IT systems. A business continuity-business impact analysis policy assesses risks and maps those risks to business functions to help prioritize recovery efforts. A service provider network outage policy will ensure contingency plans for third-party network outages.

The last layer for this implementation is for insider threats and unauthorized activities in the form of an internal threat management layer. This layer will prevent malicious or accidental internal actors from causing security incidents. An acceptable use policy will limit unauthorized use of company IT resources. An access control policy will mandate role-based access control, limiting user privileges. A mandated security awareness training policy will educate employees on internal threats.

Challenge Exercise

Identify at least two appropriate policies that should be in place to define this type of behavior and the consequences thereof.

Two policies will address the unauthorized use of network resources. The first is an Acceptable Use Policy (AUP), which will define how employees use IT resources, including network access, computers, and software. Clear guidelines will establish what is acceptable and unacceptable behavior. The Policy should prohibit downloading, sharing, or distributing unauthorized or illegal content. It will define limits on personal use of company resources and clarify that using the company's network to bypass security measures is not allowed. It will state that violations of this Policy may result in disciplinary action, up to and including termination. The consequences for violations can be on a tier-style system, such as a verbal or written warning for a first-time offense and further disciplinary action, up to and including termination.

The second is a Data Classification Standard and Encryption Policy that defines how data is classified, accessed, and transferred. This Policy will prevent the unauthorized transfer of company-related or illegal content to devices such as USB drives. It will also define categories of confidential, internal, and public data and rules on how each type of data is accessed and shared. This Policy will implement technical controls to restrict unauthorized access to USB drives. This Policy will mandate encryption for data stored on removable media and make authorization mandatory before transferring sensitive data. The Policy will implement security controls for monitoring and auditing file transfers. It will state that violations of this Policy may result in disciplinary action, up to and including termination. The consequences for violations will result in a first-time offense of restricted use of removable media. The consequences for violations can be on a tier-style system, such as a prohibited use of removable media and a written warning for a first-time offense. For subsequent violations, further disciplinary action, including termination.

Write a brief overview for C-level executives explaining which policies should be added to the company's overall security policy framework, why they should be added, and how those policies could protect the company.

Due to a recent unauthorized action regarding the misuse of company network resources to download torrent files from the Internet, Digital Innovation Products must strengthen its security policy framework. Implementing additional security policies will mitigate equivalent risks in the future, guard our digital assets, and secure compliance with legal and regulatory standards.

Digital Innovation Products should add an Acceptable Use Policy (AUP) and a Data Classification Standard and Encryption Policy to the security policy framework. These two policies will further mitigate risk, strengthen our security posture, enhance employee accountability, and support regulatory compliance. Both will reduce the risk of legal and financial liabilities that accommodate unauthorized network activity, data breaches, and /or intellectual property theft. Both will address external and internal threats and promote responsible use of company resources using guidelines and training. Both will support compliance with industry regulations and best practices.

The AUP will define acceptable and unacceptable behavior when employees use company-owned IT resources. Digital Innovation Products should implement this policy to establish clear guidelines to reduce the risk of unauthorized activities like downloading torrents. An AUP will protect the company by preventing the misuse of company IT resources, which have legal ramifications. An AUP establishes employee accountability by clearly outlining prohibited activities and the consequences of non-compliance with the policy.

The Data Classification Standard and Encryption Policy will define how data is classified, accessed, stored, and transferred. This policy will prevent unauthorized data movement and/ or misuse and create safeguards for transferring and storing sensitive information, such as USB drives. This policy will protect the company by preventing unauthorized data transfers that may lead to data breaches, intellectual property loss/theft, or reputation damage. I will strengthen our controls around data access, storage, and encryption, reducing the risk of data leakage. This policy will adhere to industry regulations and best practices.

Digital Innovation Products will improve its ability to detect and prevent unauthorized activities, protect its digital assets, and encourage a culture of security awareness, responsibility, and accountability.