Guided Practice Quick Review -

**What is a key strategy for maintaining**

**What is a key beneusing security**

**t of**

**What action is essential for**

**How can organizations ensure eective**

**cybersecurity**

**con**

**guration**

**organizations to**

**security compliance?**

**compliance in large organizations?**

Implementing manual checks for compliance

**management tools in organizations?**

They encrypt all data stored on systems.

**achieve security compliance?**

Ignoring regulatory

requirements

Implementing manual controls Ignoring security baselines

Ignoring low-level cybersecurity

They identify miscon

gurations

incidents

and monitor critical changes.

Focusing only on internal

Automate security controls

Focusing only on IT department involvement

They automatically vulnerabilities.

x all

standards

and continuous monitoring

Automating security controls for compliance

Submit

● Loading...

They prevent all malware infections.

Submit

● Loading...

Implementing controls and processes

Submit

● Loading...

Only tracking past incidents

Submit

● Loading...

**Answer the following quick Review Questions Above.**

**Answer here...........**

**Research and Case Evaluation on Auditing**

fi

**I. Case Study Role of Audit**

**Objective:** Students will research real-world cases involving security auditing and evaluate how auditing policies helped or could have helped resolve or prevent security incidents.

**Instructions**:

Research: Choose at least two recent cybersecurity incidents *from news articles, academic case* fi

*studies, or official reports that involved security breaches, unauthorized access, or data tampering*. Focus on cases where auditing played a role.

**Evaluate**: For each case, answer the following questions:

What was the nature of the security incident?

How did auditing (e.g., log analysis, event tracking) contribute to identifying or resolving the issue? What audit policies or procedures could have prevented or mitigated the incident? What lessons can be learned about implementing effective audit policies?

**Presentation**: Summarize your findings in a brief report or presentation (3-5 paragraphs or a slide deck). **Screenshot your Incident, provide the source. below the screenshot, use Word Document**

**Outcome**: Students will develop a deeper understanding of the practical application of security auditing and critical thinking skills in evaluating real-world scenarios.

**II. Audit Case Analysis**

**fi**

Objective: Students will analyze a given simulated audit report or event log and identify potential security issues.

Instructions:

Review the provided sample audit log (can be a simplified version or based on an actual audit event

**fi**

IDs from page ).

Identify and list any suspicious activities or anomalies based on the log entries. Suggest possible actions or policies to address the identified issues.



Assessment Criteria:

Correct identification of anomalies

Proper explanation of why these activities are suspicious..

Suggested corrective measures aligned with audit policies..

CompuSkill

**Seatwork 2 (Assessment): Self-Reflection and Application**

**Objective**: Students will reflect on the importance of security auditing based on their research and analysis.

**Instructions**:

Write a reflection paragraph (about 150-200 words) on how auditing procedures can enhance the security of information systems.

Describe how you would implement basic audit policies in your own future organization or personal system.

Include at least one insight from their research or activity case evaluations.

**Outcome**: Students develop personal insights on the significance of auditing and practical application skills.