

Specialization: *Governance, Risk and Compliance*

Business Focus: *Governance and Compliance*

Tool: Frameworks and Docs

The Gambili LLC Case Study: Implementing Governance and Compliance Frameworks

Project Learning Opportunities

See how a GRC and Cybersecurity Specialist helps organizations achieve compliance with regulatory bodies by identifying and assessing their assets and their accompanying risks, and providing compliance-based recommendations.

Tools and Technology to be Used

*ISO 27001:2022 Standards document
NIST 800-53, NIST CSF
Google Docs
Microsoft Word*

Case Study Overview

Scenario Overview

Company: Gambili LLC, a fast-growing online store

They sell digital and physical products. As more customers shop on their website, they store personal data like names, emails, addresses, and payment information.

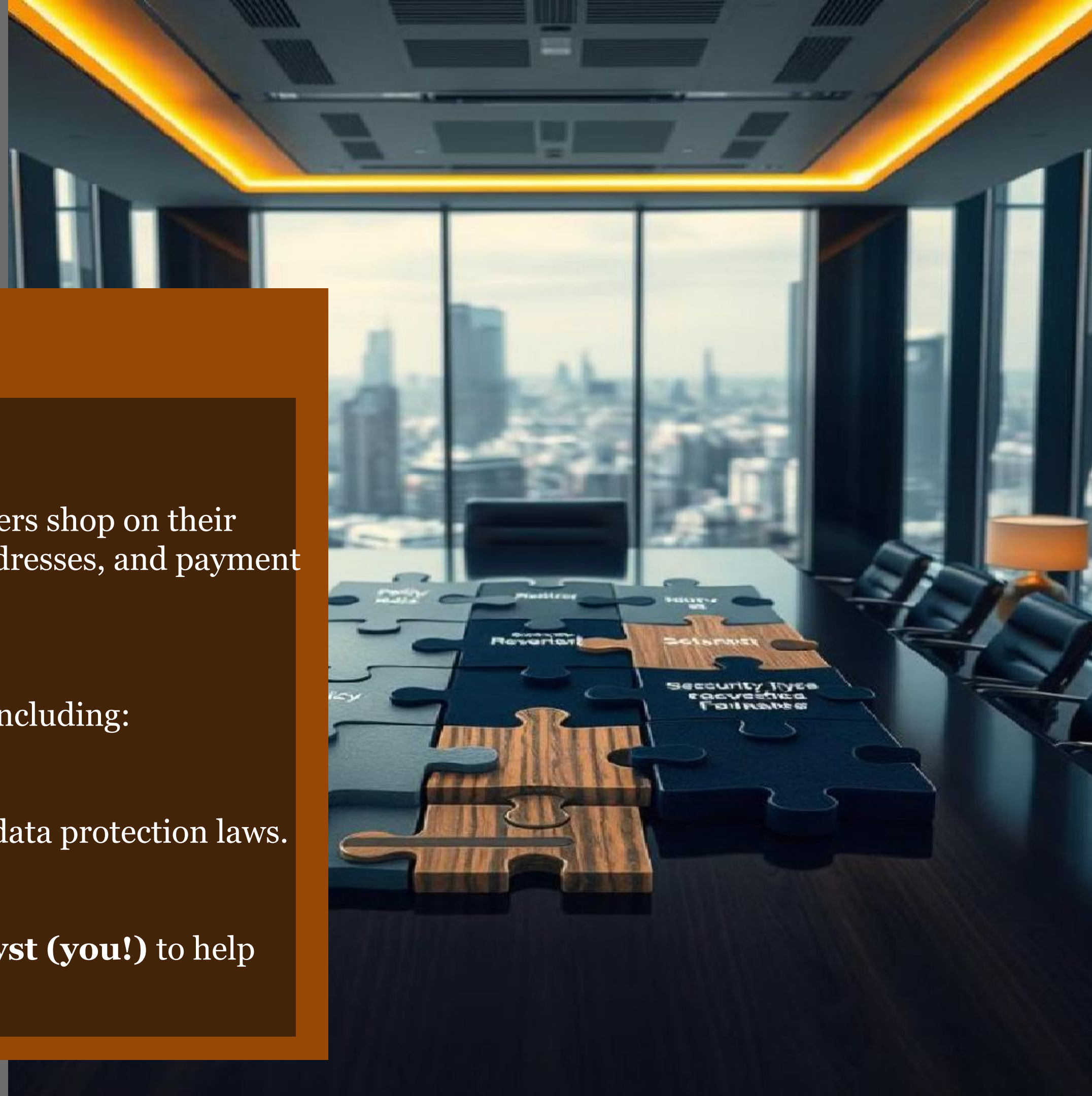
Challenges

Recently, Gambili suffered a few **security incidents**, including:

- A hacker stole some customer data.
- Their website was shut down by a ransomware attack.
- They got warnings from regulators about not following data protection laws.

Your Role:

The CEO has now hired a **junior cybersecurity analyst (you!)** to help ensure they become a safer and more trusted platform.



Case Study Overview

Problem Statement

Gambili LLC is a rapidly growing **e-commerce company** headquartered in Nigeria, with a global customer base. The company provides a wide array of digital and physical products through its online platform and **processes thousands of financial transactions daily**. As the business expands, so does its attack surface and responsibility for safeguarding customer data.

Gambili LLC has **experienced several security incidents** in the past, resulting in **data breaches** and **financial losses**. The company realizes that it needs to implement a **robust governance and compliance framework** to ensure the security of its systems and data.

Rationale for the Project

(What is the Importance of the project to the business)

1.

Data Protection

- Secure PII, payment info, and browsing history across databases and APIs.
- Implement encryption-at-rest and in-transit policies.
- Ensure the confidentiality, integrity, and availability of customer data.



2.

Regulatory Compliance

- Align with **GDPR** (for EU users), **NDPR**, **PCI-DSS**, and **ISO/IEC 27001** standards.
- Maintain audit-ready documentation and data processing registers.



3.

Risk Management

- Identify business-critical assets and map risk levels.
- Apply a risk treatment plan and control ownership.
- Identify and mitigate potential cybersecurity risks to the business.



Governance & Compliance Framework

To drive sustainable improvements, Gambili LLC will implement the following governance frameworks:

What Is Governance and Compliance?

Governance is about planning and making rules for how to protect information.

Compliance means following laws and industry standards to stay out of trouble.

What is ISO/IEC 27001:2022?

International standard: ISO/IEC 27001:2022 is an international standard that helps organizations manage information security risks.

Information Security Management System (ISMS): It provides a framework for establishing, implementing, maintaining, and continually improving an ISMS.

Key Components of ISO/IEC 27001:2022

1. Context: Understand the organization's context, including its internal and external environment.
2. Stakeholders: Identify stakeholders and their needs.
3. Risk management: Identify, assess, and mitigate information security risks.
4. Security objectives: Establish security objectives and plans to achieve them.
5. Controls: Implement security controls to mitigate risks.

What is NIST 800-53?

Security controls framework: NIST 800-53 is a framework that provides a set of security controls for federal information systems.

Risk-based approach: It helps organizations identify and manage security risks.

Key Components of NIST 800-53

1. Security controls: NIST 800-53 provides a catalog of security controls that can be applied to information systems.
2. Control families: The security controls are organized into families, such as:
 - Access control: Controls that manage access to information systems.
 - Incident response: Controls that help respond to security incidents.
3. Control baselines: NIST 800-53 provides control baselines that can be tailored to meet specific security requirements.

Key details about Gambili LLC

1

Critical Assets

Customer data, proprietary source code, and employee information.

2

Key Threats

- Unauthorized access to customer data.
- Malware targeting software development environments.
- Phishing attacks aimed at employees.

3

Existing Controls

- Password policies for account management.
- Basic antivirus software on all systems.
- Periodic training on cybersecurity awareness.

4

Goals

Identify risks, assess their likelihood and impact, and implement necessary controls to mitigate them effectively.



1. Identify threats, vulnerabilities, and potential impacts based off the assets.

2. Assess the likelihood and impact of identified risks.

4. Propose mitigation controls.

Questions

1

Approach for risk assessment

What approach should Gambili use for its risk assessment?

2

Risk prioritization

How should Gambili prioritize identified risks?

3

Additional controls

What additional controls could Gambili implement to mitigate risks?

4

Ensuring effectiveness

How can Gambili ensure that the risk assessment process is effective?

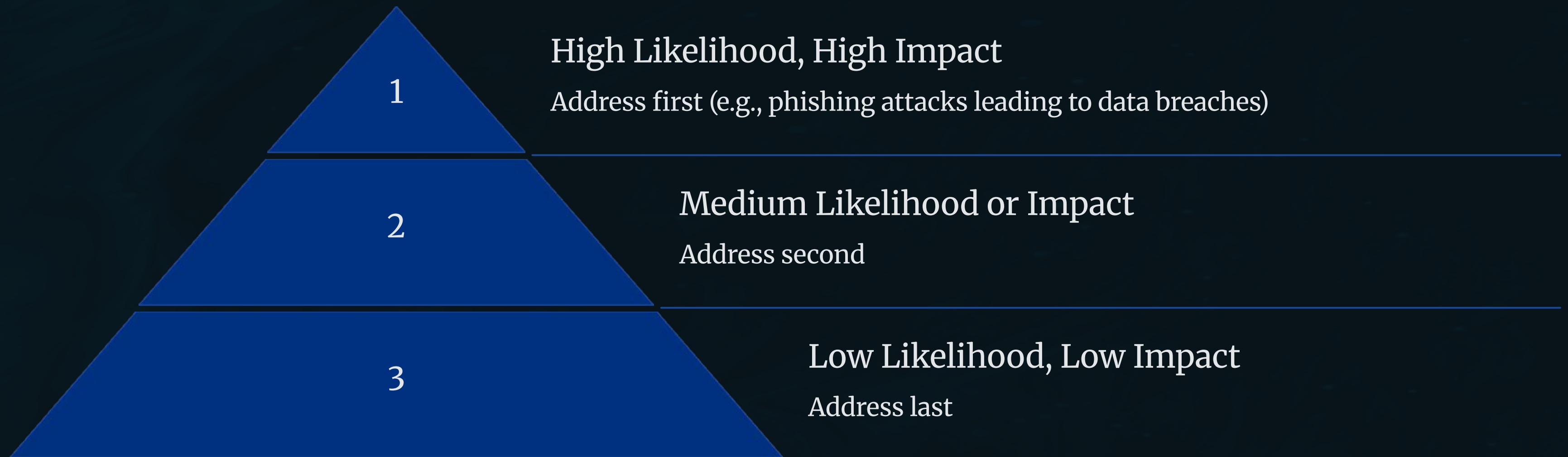
Answers

1. What approach should Gambili use for its risk assessment?

Gambili should use a structured approach, such as the ISO 27005 risk assessment methodology, which includes:

- Identifying assets, threats, and vulnerabilities.
- Estimating the likelihood of threat exploitation.
- Calculating the impact of potential security incidents.
- Documenting findings in a risk assessment report.

Risk Prioritization



2. How should Gambili prioritize identified risks?

Risks should be prioritized based on a risk matrix that considers:

- Likelihood: High, medium, or low probability of occurrence.
- Impact: High, medium, or low severity of consequences.

Additional Controls



Unauthorized Access

Implement multi-factor authentication (MFA) and role-based access controls.



Malware

Use advanced endpoint detection and response (EDR) tools and network segmentation.



Phishing

Conduct regular simulated phishing campaigns and enforce email filtering solutions.

3. What additional controls could Gambili implement to mitigate risks?

Ensuring Effectiveness

Regular Assessments

Conduct risk assessments regularly and whenever significant changes occur.

Validation Tools

Use tools like vulnerability scanners and security information and event management (SIEM) systems to validate findings.



Stakeholder Involvement

Involve all stakeholders, including IT, HR, and legal teams, in the risk assessment process.

Continuous Monitoring

Continuously monitor and review the effectiveness of implemented controls.

4. How can Gambili ensure that the risk assessment process is effective?

Ensuring Effectiveness

Regular Assessments

Conduct risk assessments regularly and whenever significant changes occur.

Validation Tools

Use tools like vulnerability scanners and security information and event management (SIEM) systems to validate findings.



Stakeholder Involvement

Involve all stakeholders, including IT, HR, and legal teams, in the risk assessment process.

Continuous Monitoring

Continuously monitor and review the effectiveness of implemented controls.

4. How can Gambili ensure that the risk assessment process is effective?

RECOMMENDATIONS FOR GAMBILI

Recommendation 1: Create a Cybersecurity Team

- A **Security Manager** makes the rules.
- An **IT Engineer** helps set up technical tools.
- A **Data Privacy Officer** makes sure laws are followed.

Recommendation 2: Look for Risks (Risk Assessment)

- Check which parts of the system are most valuable (like the customer database).
- Find out how hackers might try to break in (using tools like Nessus or even Google Dorks).
- Rate the risks from low to high.

Recommendation 3: Apply Security Controls

- Add strong passwords and **two-factor login (MFA)**.
- Use **firewalls** to block attacks.
- Turn on **logging** to track who does what on the network.
- Encrypt data so hackers can't read it, even if they steal it.

Recommendation 4: Monitor & Improve

- Watch for alerts using tools like **Wazuh** or **Splunk**.
- Review logs weekly.
- Test systems monthly and report progress.

Additional Questions based off the Phases of a Governance and Compliance Audit.

Phase 1: Risk Assessment

Question: What could go wrong, and how bad would it be?

 **Scenario:**

Gambili stores customer credit card data in plain text on their servers. A hacker could easily steal it. That's a big risk.

 **Exercise:**

Write down three other risks Gambili might face. Using this questions as a guide:

- What if a staff member uses a weak password?
- What happens if a backup is not created regularly?
- What if a developer uses outdated software?

Phase 3: Monitor and Review


Question: How to check if the controls are working?

 **Scenario:**

You set up weekly log reviews, system alerts, and quarterly audits to monitor everything.


Quiz :

1. Why is it important to monitor controls?
 - a) Just for fun
 - b) To know when they stop working
 - c) So we can turn them off

 Answer: _____

2. What does a “log review” mean?

- a) Reading social media
- b) Checking security events recorded by systems
- c) Watching CCTV cameras

 Answer: _____

Phase 2: Implementing Security Controls

Question: How do we fix the problems found in Phase 1?

Scenario:

You recommend solutions to Gambili, explain why you chose each of these recommendations:

- Encrypts customer data.
- Sets up multi-factor authentication (MFA) for admin logins.
- Applies software updates weekly.

 **Exercise:**

Match each risk with the best control:

2. **Risk:** Weak staff passwords

Control Options:

- a) Regular training
- b) Data encryption
- c) Access logs

 Answer: _____

3. **Risk:** Unpatched software

Control Options:

- a) MFA
- b) Apply regular updates
- c) Use firewalls

 Answer: _____

ASSIGNMENT

Gambili LLC is preparing for a security audit next week. You've been asked to:

1. List **3 risks** they might still have.
2. Suggest **3 controls** to fix them.
3. Explain how you'd know the controls are working (monitoring).

