Gouvernance, Compliance & Risk Project

Building a Governance, Risk, and Compliance Framework for Gambili Corp's E-Commerce Operations

Lum Rina Ngwan

Role: GRC Analyst

Date: 11th August 2025

Table of Content

Project Scenario

Gambili Corp is a fast-growing e-commerce platform operating across Africa, selling both physical goods (fashion, electronics) and digital products (ebooks, software licenses). The company handles **customer PII**, **payment card data**, and partners with multiple **third-party vendors** for payment processing, logistics, and cloud services.

In the last 12 months, Gambili has experienced an increase in **cybersecurity incidents** such as phishing attempts, fraudulent transactions, and unauthorized account access. With new GDPR and PCI-DSS obligations, Gambili's leadership has tasked the newly formed **GRC Team** to design and implement a **Governance, Risk, and Compliance Framework** to improve security posture.

Project Objectives

The main objectives of this project carried by the GRC team includes:

1. Establishing foundational **Information Security Governance** through clear **security policies**.

2. Identifying, assessing, and recording cybersecurity risks in a **Risk Register**.

3. Developing a **Vendor Risk Assessment Checklist** for evaluating third-party security maturity.

4. Conducting a **Compliance Gap Analysis** against ISO 27001:2022.

5. Communicating the findings to executive management via a concise **Executive Risk Summary Report**.

Phase 1: Governance (Security Policies)

1. **Information Security Policy (ISP)**

Objective and Scope:

Aimed at putting in place Gambili Corp's commitment to protecting company and customer information from unauthorized access, disclosure, alteration, and destruction. This policy applies to all employees, contractors, and vendors with access to Gambili's systems or data.

Roles and Responsibilities:

- **CISO:** Overall information security governance.
- **Data Protection Officer (DPO):** GDPR compliance and data subject rights management.
- **IT Security Team:** Implement technical controls and monitor security events.
- **All Employees:** Adhere to security procedures and report suspicious activities.

Key Security Commitments:

- Protect personal data with encryption and access controls.
- Maintain an incident response process for breach handling.
- Require vendors to follow equivalent security standards.

Policy Review Cycle: Annually or upon major business/technology changes.

2. Data Protection Policy

Objective and Scope:

In order to ensure compliance with GDPR, NDPR, and PCI-DSS when collecting, processing, storing, and disposing of personal and payment card data.

Main Points:

- Collect only necessary personal data for business operations.
- Obtain explicit consent before processing sensitive data.
- Store data in encrypted formats; securely dispose of data after retention period.
- Provide customers the right to access, modify, or delete their data.

Review Cycle: Annual.

3. Acceptable Use Policy (AUP)

Objective and Scope:
Aimed at defining acceptable use of Gambili's IT assets and preventing the misuse that could compromise business operations or security.

Main Points:

- Use company devices and networks only for authorized business activities.
- Prohibit downloading unauthorized software or accessing malicious websites.
- Report phishing attempts and security incidents immediately.

Review Cycle: Annually or post- major incident.

Phase 2: Risk Management (Risk Register Development)

Below is a Risk register table identifying 6 key risks, identifying their asset, threat, vulnerability, likelihood, impact, risk owner, existing controls, recommended mitigation and status.

Risk ID	Asset	Threat	Vulnerability	Likelihood	Impact	Risk Owner	Existing Controls (ISO 27001 Ref.)	Recommended Mitigations	Status
R001	Customer Database	Phishing	Lack of employee awareness	High	High	CISO	Security awareness training (A.7.2.2), Email filtering	Phishing simulations, awareness training	Open
R002	Payment Gateway	Vendor breach	Weak vendor security	Medium	High	DPO	Vendor contracts with security clauses (A.15.1.1)	Quarterly vendor audits, enforce PCI DSS compliance	Open
R003	Admin Portal	Unauthorized access	Weak MFA enforcement	High	Medium	IT Manager	Role-based access control (A.9.1.2)	Enforce MFA, monitor login patterns	Open
R004	Cloud Storage	Data leakage	Misconfigured storage	Medium	High	CISO	Encryption at rest & transit (A.10.1)	Cloud security posture management	Open

R005	Web Application	DDoS attack	Lack of mitigation tools	Medium	High	IT Security	PCI-DSS compliance, tokenization	Deploy WAF and CDN-based DDoS protection	Open
R006	Backups	Ransomware attack	Lack of offline backups	Low	High	IT Manager	IDS/IPS monitoring	Implement offline/immutable backups	Open

Phase 3 : Vendor Risk Management (Assessment checklist)

Gambili Corp – Vendor Risk Assessment Checklist

Vendor Evaluated: PayXpress (Payment Processor)
Assessment Date: 11 Aug 2025
Assessor: GRC Analyst – Gambili Corp

Control Area	Assessment Question	Vendor Response	Evidence Provided	Score (0–2)	Remarks
1. Data Security Practices	Is customer data encrypted in transit using strong protocols (TLS 1.2 or higher)?	Yes	TLS 1.3 configuration screenshot	2	Meets industry standard
	Is sensitive data encrypted at rest (AES-256 or equivalent)?	Yes	Encryption policy document	2	Strong encryption
	Are access controls role-based (RBAC) with periodic reviews?	Yes	Access control logs	2	Quarterly reviews done
2. Regulatory Compliance	Is the vendor PCI-DSS certified?	Yes	Valid PCI-DSS certificate	2	Certification valid until Dec 2025
	Is the vendor GDPR compliant, including DSAR handling?	Partial	GDPR policy but incomplete DSAR logs	1	Needs DSAR process automation
	Compliant with NDPR (Nigeria Data Protection Regulation)?	Yes	NDPR compliance statement	2	–

3. Incident Response & Notification	Does the vendor have a documented incident response plan?	No	None provided	0	Critical gap
	Does the vendor commit to breach notification within regulatory timelines?	No	No documented SLA	0	Needs contractual inclusion
4. Business Continuity & Disaster Recovery (BC/DR)	Does the vendor have a tested BC/DR plan?	Yes	BC/DR report from last drill	2	Annual tests conducted
5. Certifications	Does the vendor hold ISO 27001 certification?	Yes	Certificate copy	2	Valid until Oct 2026
	Does the vendor have a SOC 2 Type II report?	No	None provided	0	Recommend requesting

NB: Scoring Key

- 2 = Fully compliant (Meets/exceeds requirement with evidence)
- 1 = Partially compliant (Some gaps in process or documentation)
- 0 = Non-compliant (No evidence or process in place)

Total Possible Score: 22
Vendor Score: 15 / 22 (68% – Moderate Risk)

Phase 4: Compliance Gap Analysis (ISO 27001/27002)

Objective:

To evaluate Gambili Corp's current information security practices against the requirements of ISO 27001:2022 (and relevant GDPR/PCI DSS requirements) and identify areas needing improvement.

Control Area	ISO 27001/ISO 27002 Reference	Current Status	Gap Identified	Impact	Recommended Remediation
Consent & Data Collection Practices	A.5.10 – Acceptable Use of Information; GDPR Art. 6-7	Partial compliance – Privacy policy exists, but no explicit opt-in for marketing communications.	No formal consent capture mechanism for marketing or optional services.	Medium – Risk of GDPR fines and loss of customer trust.	Implement explicit opt-in checkboxes on all data collection forms; store consent logs in CRM for audit purposes.
Data Retention & Disposal	A.5.12 – Classification & Retention; A.7.4 – Secure Disposal	Partial compliance – Retention schedule not formally documented; old backups retained indefinitely.	No defined retention period for customer PII; insecure disposal of retired hard drives.	High – Non-compliance with GDPR Art. 5(1)(e) & potential data breach.	Create a data retention policy with defined timelines; implement secure data wiping tools for hardware disposal.
Customer Rights Processes (Access, Deletion Requests)	A.5.11 – Rights of Data Subjects; GDPR Art. 15–17	Compliant – DPO handles access and deletion requests within legal timelines.	–	Low – Maintain process.	Continue process; automate ticket tracking for DSAR requests to ensure timely responses.
Incident Response Procedures	A.5.25 – Incident Management; A.5.28 – Lessons Learned	Partial compliance – Incident reporting channels exist, but no detailed playbooks or communication templates.	No formal documented Incident Response Plan (IRP) with defined roles, escalation, and notification timelines.	High – Delayed or incorrect response in a breach scenario could increase damages and penalties.	Develop a formal IRP with severity classification, escalation matrix, and regulator notification templates. Conduct annual incident response drills.
Third-party Data Processing Agreements	A.5.19 – Supplier Security Requirements;	Non-compliant – Vendor contracts lack standard	Missing mandatory GDPR processor clauses and PCI DSS requirements.	High – Vendor breaches may result in legal liability.	Update all vendor contracts to include GDPR processor clauses, PCI DSS compliance commitments, and breach

	GDPR Art. 28	security and breach notification clauses.			notification SLA (e.g., within 72 hours).

Compliance Gap Highlights

- ☐ Data Retention & Disposal: No documented retention periods and insecure disposal methods.
- ☐ Third-party Data Processing Agreements: Missing contractual security clauses for vendors handling PII/payment data**.**

Remediation Priority Table

Gap	Priority	Owner	Target Date
Data Retention & Disposal Policy	High	DPO & IT Security	30 days
Third-party Data Processing Agreements	High	Legal & Procurement	45 days
Incident Response Plan Documentation	Medium	CISO & IRT	60 days
Consent Capture Mechanism	Medium	Marketing & IT	60 days

Impact of Closing Gaps

- Improved regulatory compliance (ISO 27001, GDPR, PCI DSS).
- Reduced risk of regulatory fines.
- Stronger vendor security posture.
- Enhanced customer trust through transparent data practices.

CONCLUSION

In a nutshell, this GRC framework establishes security governance, strengthens risk management, ensures vendor oversight, and identifies compliance gaps that can be

remediated before they cause major business disruptions. By following this plan, Gambili Corp can improve its risk posture, protect customer trust, and maintain regulatory compliance.

RESOURCES

- https://purplesec.us/resources/cyber-security-policy-templates/
- https://www.sans.org/information-security-policy
- Risk Register Template is in the classroom
- https://www.template.net/business/forms/vendor-audit-form/
- https://safetyculture.com/checklists/vendor-due-diligence/
- https://www.scribd.com/document/609114254/PCI-DSS-Security-Controls-Mapping
- https://safestack.io/blog/resources/template-pci-dss-control-list
- Gap Analysis Template
- ISO 27001:2022 Standard Document
- https://www.slideteam.net/top-10-risk-executive-powerpoint-presentation-templates
- https://www.slidegeeks.com/powerpoint/Summary-Of-Risk-Report