GOVERNANCE, RISK & COMPLIANCE ASSESSMENT FOR GAMBILI LLC

EXECUTIVE SUMMARY

Gambili LLC is a rapidly growing e-commerce company that processes sensitive customer data and financial transactions. Recent security incidents—including data theft, ransomware-driven service outages, and regulatory warnings—highlight critical gaps in its governance, risk management, and compliance (GRC) posture. The CEO has engaged a cybersecurity analyst to evaluate existing exposures, prioritize risks, and recommend treatments grounded in internationally recognized standards. This assignment focuses on identifying three residual risks, prescribing ISO/IEC 27002:2022-aligned controls to mitigate them, and defining how the effectiveness of those controls will be assessed. The approach embeds principles of risk-based decision making, continuous improvement, and alignment with compliance obligations such as ISO/IEC 27001.

METHODOLOGY

The risk treatment process follows a structured GRC risk management approach as implied in the case study, consistent with ISO 27005 and ISO/IEC 27001 principles: asset identification, threat and vulnerability analysis, likelihood and impact estimation, risk prioritization, control selection, and monitoring. Stakeholder involvement, continuous monitoring, and validation (through tools like SIEM and scanners) are emphasized to ensure effectiveness.

Risk identification draws on critical asset and threat definitions provided: customer data, source code, and employee information as assets; threats include unauthorized access, malware in development environments, and phishing. Existing baseline controls (password policies, antivirus, periodic awareness training) are acknowledged but identified as insufficient to manage deeper systemic risks.

Risk Identification and Prioritization

From the case study, three residual, high-consequence risks were selected that would still materially threaten Gambili if unaddressed:

Risk 1: Lateral movement and privilege escalation due to insufficient network segmentation.

An attacker gaining initial foothold (e.g., via phishing or credential compromise) can traverse the internal network unimpeded if segmentation is weak, leading to broader data theft or ransomware propagation.

Risk 2: Ineffective detection and response capabilities

While tools like logging and alerting are mentioned, without formalized incident response planning, preparation, and continuous monitoring, detection latency and inconsistent responses will hinder timely containment and recovery from security incidents.

Risk 3: Poorly managed privileged access and lack of separation of duties

Excessive or improperly governed privileged access increases the chance of insider abuse, unauthorized escalation, and misuse of high-impact credentials. Absence of lifecycle controls and segregation creates opportunities for conflict of interest and undetected misuse.

Risk Treatment: ISO/IEC 27002:2022-Aligned Controls

For each identified risk, three specific controls from ISO/IEC 27002:2022 are proposed, with rationale and brief implementation guidance.

Risk 1: Lateral Movement

Control 8.22 – Segregation of networks

- **Rationale:** Divides the network into security domains to limit the spread of an intrusion, making lateral movement harder.
- **Implementation note:** Define and enforce network zones (e.g., separation between customer data storage, development systems, and administrative consoles) with firewalls or virtual LANs controlling cross-domain traffic.

Control 8.21 – Security of network services

- **Rationale:** Ensures only authorized services are exposed, and communication between zones is controlled and protected.
- **Implementation note:** Harden network services, restrict unnecessary ports, apply access rules, and monitor service usage.

Control 8.20 – Network security

- **Rationale:** Implements both preventive and detective measures (e.g., traffic filtering, IDS/IPS) to protect the network fabric.
- **Implementation note:** Deploy intrusion detection, limit broadcast domains, and apply anomaly detection on inter-zone traffic.

Risk 2: Detection and Response Gaps

Control 5.24 – Information security incident management planning and preparation

- **Rationale:** Establishes a formal incident response capability (roles, playbooks, communication plans).
- **Implementation note:** Develop and test an incident response plan, define escalation paths, and conduct tabletop exercises.

Control 8.15 – Logging

- **Rationale:** Captures security-relevant events for detection, correlation, and forensic analysis.
- **Implementation note:** Ensure logs from critical systems (authentication, access, system changes) are centralized, immutable, and retained per policy.

Control 8.16 – Monitoring activities

- **Rationale:** Continuously observes system state to surface anomalies and feed alerts to the response mechanism.
- **Implementation note:** Tune monitoring tools to threshold anomalies, integrate with SIEM (e.g., Wazuh/Splunk), and establish alert-to-action workflows.

Risk 3: Privileged Access Mismanagement

Control 8.2 – Privileged access rights management

- **Rationale:** Controls the grant and use of elevated privileges to prevent misuse.
- **Implementation note:** Enforce least-privilege, use just-in-time elevation, log privileged sessions, and restrict break-glass scenarios to documented and audited use
- **Control 5.18 – Access rights provisioning, review, and segregation of duties**

- **Rationale:** Establishes a lifecycle for access rights and prevents role conflicts.
- **Implementation note:** Regularly review access rights, enforce separation (e.g., approval vs execution), and revoke stale privileges.

Control 8.3 – Information access restriction / least privilege

- **Rationale:** Ensures users (including privileged) only access what's necessary.
- **Implementation note:** Implement role-based access, context-aware restrictions, and dynamic access management where appropriate.

MEASURING CONTROL EFFECTIVENESS (MONITORING & VALIDATION)

Risk 1 Indicators

- **Segmentation compliance reports** showing network flows only occur per defined policy.
- **Internal penetration test results** demonstrating blocked lateral attempts.
- **Alerts on unauthorized inter-zone traffic.**

Risk 2 Indicators

- **Incident response drill outcomes** evaluating readiness and time-to-contain.
- **Log coverage audits** confirming that required sources emit and retain logs appropriately.
- **Alert efficacy metrics** (mean time to detect/respond, false-positive rates) from continuous monitoring.

Risk 3 Indicators

- **Privileged access review logs** verifying that elevated rights are justified and time-bounded.
- **Audit trails of privileged operations** showing consistent logging and detection of anomalous use.
- **Separation-of-duties enforcement evidence** ensuring no single individual holds conflicting privileges.

Recommendations

1. **Formalize and enforce network segmentation policies** with technical implementation (firewalls, ACLs) and periodic validation.
2. **Institutionalize an incident response program** with planned exercises, integrated logging, and pathways from detection to remediation.
3. **Implement strong privileged access governance**, including least-privilege, dynamic access controls, and regular reviews to prevent insider risk and escalations.
4. **Integrate these into a continuous improvement cycle**, regular reassessment, stakeholder-involved risk reviews, and leveraging tools (SIEM/vulnerability scanners).

CONCLUSION

Gambili LLC's current baseline controls provide initial defense-in-depth, but critical structural and governance deficiencies remain. By targeting lateral movement, response capability, and privileged access through calibrated ISO/IEC 27002:2022 controls, the organization can sharply reduce its exposure to advanced threats and misuse. Success will depend not only on implementing controls, but on embedding them within a risk-aware culture, supported by continuous monitoring, recurring validation, and a clear governance feedback loop. These measures collectively align Gambili's security posture with compliance objectives and strengthen its trustworthiness to customers and regulators.

REFERENCES

ISO/IEC. (2022). *ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Code of practice for information security controls*. International Organization for Standardization.

Gambili LLC Case Study. (2025). *GRC Case Study: Implementing Governance and Compliance Frameworks*. Provided document.