Enterprise Cybersecurity Gap Assessment & Response Plan

Executive Summary

An independent security assessment identified material gaps in SAGE Books' cybersecurity governance, regulatory compliance posture, incident response capabilities, and operational resilience.

The organization currently lacks formalized security policies, defined PCI DSS and GDPR controls, dedicated governance resources, and mature incident response and business continuity processes. These deficiencies increase exposure to regulatory penalties, operational disruption, financial loss, and reputational damage.

This report outlines the identified risks and presents a prioritized remediation strategy aligned with NIST guidance, PCI DSS v4.0, and GDPR requirements.

Risk Prioritization Table

Risk Area	Impact	Likelihood	Priority
PCI DSS Noncompliance	High	High	Critical
Incomplete Incident Response	High	Medium	High
Weak Security Training	Medium	High	High
Missing BCP	High	Medium	High

Security Gap Assessment

Governance & Policy Deficiencies

SAGE Books does not maintain a comprehensive security policy framework. Formal documentation is missing for:

- Acceptable Use
- Mobile Device Security
- Password and Authentication Standards
- Protection of Personally Identifiable Information (PII)

The absence of formalized controls creates inconsistent enforcement and increases compliance risk.

Regulatory Noncompliance

PCI DSS Exposure

No standardized processes exist for storing, transmitting, or processing cardholder data (CHD).
This creates elevated risk of payment data compromise and noncompliance penalties.

GDPR Exposure

The organization lacks structured processes to support:

- Lawful data processing
- Data subject rights (access, correction, deletion)
- Documented privacy governance

This exposes the company to significant regulatory fines and reputational harm.

Governance, Risk & Compliance Staffing Gaps

The current security team lacks specialized GRC resources responsible for:

- Regulatory oversight
- Risk assessments
- Control validation
- Compliance reporting

This limits executive visibility into enterprise risk exposure.

Security Awareness Weaknesses

Security training is informal and inconsistently delivered.
Content is not aligned with NIST guidance or PCI DSS requirements.

This increases vulnerability to phishing, credential compromise, and social engineering attacks.

Incident Response Immaturity

The existing Incident Response Plan (IRP) lacks:

- Clearly defined roles and escalation paths
- Standardized response procedures
- Full lifecycle coverage (preparation through post-incident review)

This increases the likelihood of prolonged containment time and business disruption.

Business Continuity Gaps

There is no documented Business Continuity Plan (BCP) addressing operational disruption at high-risk distribution centers located in earthquake- and hurricane-prone regions.

A prolonged outage would significantly impact revenue and customer fulfillment operations.

Remediation Strategy

The following remediation roadmap aligns with PCI DSS v4.0, GDPR, and NIST standards.

Establish Formal Security Governance Framework

- Develop and approve enterprise-wide security policies
- Align policies with PCI DSS, GDPR, and NIST standards
- Implement data classification and access control standards
- Formalize password and authentication requirements (MFA enforcement)

Achieve PCI DSS Compliance

- Define CHD storage, transmission, and processing controls
- Implement encryption and network segmentation
- Maintain annual control reviews
- Establish ongoing compliance monitoring (PCI DSS Requirement 12)

Implement GDPR Data Protection Controls

- Appoint a Data Protection Officer (DPO)
- Implement consent management and subject access workflows
- Document lawful processing activities
- Establish breach notification procedures

Expand Security Staffing

Recommended additions:

Governance, Risk & Compliance (GRC) Analyst

Responsible for compliance monitoring, audits, and risk register management.
NICE Work Role: OV-LGA-001

Data Protection Officer (DPO)

Responsible for GDPR oversight and privacy governance.
NICE Work Role: PR-CDA-001

Security Controls Assessor

Responsible for control testing, vulnerability assessments, and validation reporting.
NICE Work Role: PR-CDA-002

Strengthen Security Awareness Program

Implement a formal training program aligned with NIST SP 800-50:

- Mandatory annual training
- Role-based advanced modules (Finance, IT, HR)

- Quarterly phishing simulations
- Monthly security communications

Participation tracking and reporting should be implemented.

Phased Implementation Roadmap

The following phased implementation plan prioritizes high-risk exposures and establishes a structured path toward regulatory compliance and operational resilience.

Phase 1 – 0–90 Days

- Establish governance framework
- Define PCI DSS controls
- Formalize incident response roles

Phase 2 – 3–6 Months

- Implement GDPR workflows
- Launch awareness program
- Conduct BIA

Phase 3 – 6–12 Months

- Complete compliance audits
- Perform IR simulation
- Conduct DR testing

Incident Response Program Enhancement

The Incident Response Plan should align with NIST SP 800-61r2 and include:

Preparation

- Establish Incident Response Team (IRT)
- Define escalation paths and communication plans
- Maintain response tooling and contact lists

Detection & Analysis

- Deploy centralized logging and SIEM monitoring
- Define severity classification criteria
- Document indicators of compromise (IOCs)

Containment, Eradication & Recovery

- Isolate affected systems
- Remove malicious artifacts
- Patch vulnerabilities
- Restore from validated backups

Post-Incident Activities

- Conduct after-action review
- Update response procedures
- Report to regulators where required

Business Continuity & Disaster Recovery

Business Impact Analysis (BIA)

- Identify critical business processes (order fulfillment, inventory systems)
- Define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
- Quantify potential financial impact of downtime

Continuity Strategy

- Establish geographically redundant recovery sites
- Leverage cloud-based infrastructure for operational resilience
- Formalize vendor contingency agreements
- Conduct semi-annual disaster recovery testing

Physical & Logical Risk Exposure

Physical Risks

- Natural disasters affecting distribution centers
- Theft of hardware containing sensitive data

- Improper disposal of storage devices

Logical Risks

- Unsecured payment processing systems
- Phishing and credential compromise
- Inadequate incident response capability

Conclusion

The current security posture exposes SAGE Books to elevated regulatory, operational, and reputational risk. Immediate action is required to formalize governance structures, align with PCI DSS and GDPR requirements, mature incident response capabilities, and strengthen organizational resilience.

By implementing the recommended remediation roadmap, SAGE Books can significantly reduce enterprise risk exposure and establish a sustainable cybersecurity governance framework.

References

- NIST SP 800-61 Rev. 2 – Computer Security Incident Handling Guide
- NIST SP 800-63B – Digital Identity Guidelines
- NIST SP 800-122 – Protecting the Confidentiality of PII
- NIST SP 800-50 – Security Awareness Training
- NIST SP 800-124 Rev. 2 – Mobile Device Security
- PCI DSS v4.0
- GDPR (EU 2016/679)