SISA

CUSTOMER SUCCESS STORY

How SISA's Approach to Multi-Framework Compliance Helped a Leading BPO Provider Achieve Scalable Audit and Operational Savings

ABOUT THE CUSTOMER

The Client is a global business process outsourcing (BPO) leader founded in 1995, providing omnichannel customer experience solutions across contact centres, back-office operations, and AI-enabled customer engagement services. Headquartered in Michigan, with approximately 13,500 employees across multiple continents and operations spanning the United States, Mexico, Philippines, Guyana, and Costa Rica, it serves Fortune 500 clients in healthcare, insurance, and technology sectors.

BUSINESS CHALLENGE

With operations spanning multiple geographies and diverse regulatory landscapes, the Client required to demonstrate stringent adherence to HIPAA, PCI-DSS, and SOC frameworks. Further, rapid growth trajectory and acquisition strategy demanded a unified compliance framework to maintain competitive advantage in highly regulated industries. However, challenges stemming from operational and technical fronts, created roadblocks in achieving regulatory compliance and enforcing cybersecurity policies.

Challenges of a Decentralized Audit Approach

1

Critical gaps in internal audit capabilities

Severe audit fatigue from managing four simultaneous compliance audits (HIPAA, PCI-DSS, SOC 2, Cyber Security Risk Assessment (CSRA)) with overlapping timelines and redundant documentation requests hurt business-as-usual activities.

2

Lack of skilled resources

Insufficient in-house qualified security assessors (QSAs) and limited technical knowledge to interpret complex regulatory requirements across multiple jurisdictions led to inefficient artifact collection, delays, miscommunications, and incomplete submissions.

3

Absence of centralized audit management system

Decentralized audit approach required 16 weekly coordination meetings over a projected 4-month timeline, consuming approximately 256 hours of senior management time resulting in fragmented artifact collection processes and inconsistent stakeholder engagement.

4

Disjointed approach to evidence gathering

Fragmented communication channels created bottlenecks in evidence gathering, with artifacts scattered across disparate systems, email threads, and shared drives without version control, resulting in inconsistent quality standards.

These capability gaps exposed the Client to significant compliance risks, potential regulatory penalties, and reputational damage in industries where trust and data security serve as competitive differentiators.

SISA's SOLUTION

To streamline and strengthen the Client's compliance posture across multiple regulatory frameworks, SISA deployed a comprehensive and customized engagement strategy. This initiative focused on integrating diverse compliance requirements into a unified audit methodology, enhancing assessment efficiency, and accelerating remediation efforts.

The following key actions outline the strategic approach adopted during the four-phase engagement.

01 Deployed customized Unified Audit Approach, consolidating all four compliance frameworks (HIPAA, PCI, SOC, CSRA) under single integrated assessment methodology with shared control mapping.

02 Onboarded certified Qualified Security Assessors (QSAs) with multi-framework expertise, conducting comprehensive readiness assessments that identified 47 critical gaps requiring immediate remediation.

03 Developed and implemented proprietary SISA Assistant Portal featuring multi-factor authentication, role-based access controls, and automated artifact collection workflows tailored to Client's organizational structure.

04 Executed proactive gap remediation strategies including customized remediation plans, prioritized action items with clear ownership assignments, and continuous monitoring throughout audit lifecycle.

SISA's integrated approach eliminated redundant control testing, streamlined evidence collection through centralized repository, and provided real-time visibility into audit progress for predictive risk management.

BUSINESS IMPACT

SISA Assistant Portal with MFA-enabled artifact management reduced document collection time by 68%, eliminating email-based exchanges and manual follow-ups across global teams.

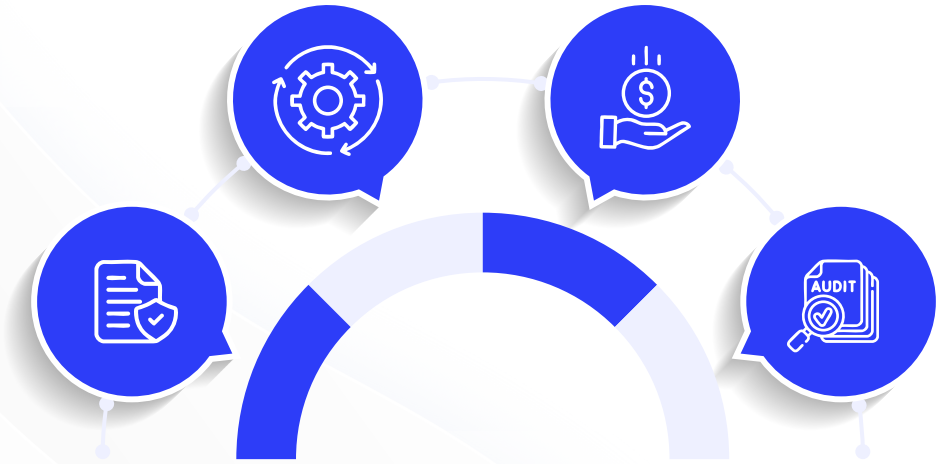
Key Benefits

Reduction in operational overhead

Weekly stakeholder coordination meetings decreased from 16 sessions to 13 sessions, representing 19% reduction in meeting burden and saving 48+ senior management hours.

Cost efficiency

Unified approach generated tangible cost savings through eliminated duplicate testing, reduced consultant hours, and minimized internal resource allocation disruptions.



Faster compliance

Total audit timeline compressed from projected 4 months to 3 months, delivering 25% faster compliance achievement and enabling earlier certification.

Scalable audit framework

All four compliance certifications (HIPAA, PCI-DSS, SOC 2, CSRA) delivered on schedule with zero major non-conformities, strengthening competitive positioning, enhancing client confidence, and establishing scalable compliance framework for future growth.

CONCLUSION

Overall, SISA's integrated compliance strategy delivered substantial operational, financial, and strategic benefits. By unifying audit processes, automating evidence collection, and proactively addressing gaps, the engagement accelerated certification timelines, reduced resource strain, and enhanced audit readiness. The scalable framework not only ensured timely delivery of all four compliance certifications with zero major non-conformities but also positioned the Client for sustained regulatory success and future growth.

About SISA

SISA is a Global Leader in Cybersecurity Solutions for the Digital Payment Industry. As a Global Payment Forensic Investigator of the PCI Security Standards Council, we leverage forensics insights into preventive, detective, and corrective security solutions, protecting 1,000+ organizations across 40+ countries from evolving cyberthreats. Our suite of solutions from AI-driven compliance, advanced security testing, agentic detection/ response and learner focused-training has been honored with prestigious awards, including from Financial Express, DSCI-NASSCOM and The Economic Times. With commitment to innovation, and pioneering advancements in Quantum Security, Hardware Security, and Cybersecurity for AI, SISA is shaping the future of cybersecurity through cutting-edge forensics research.

Compliance

Payment Data Security
- PCI DSS
- PCI PIN
- PCI 3DS
- PCI P2PE
- PCI S3
- PCI S-SLC
- PCI CP (Card Production)
- Facilitated PCI SAQ
- Quarterly Health Check-ups
- Central Bank Compliance
- SWIFT

Strategy and Risk
- CCPA
- GDPR
- HIPAA
- ISO
- NIST
- SOC 1
- SOC 2
- Cloud Security
- HITRUST

Unified Audits

Managed Compliance

Security Testing

Application Security
- Application Penetration Testing
- CREST/CERT-in Approved Security Testing
- API Security Testing
- Secure Code Review

Network Security
- Vulnerability Assessment
- Penetration Testing
- Configuration Review
- Firewall Rule Review
- PCI ASV Scan

Phishing Simulation

Red Teaming Exercise
- Layer Security Testing

Cyber Defense

Managed Extended Detection and Response Solution - SISA ProACT
- 24x7 Monitoring
- UEBA
- Threat Intel
- Advanced Threat Hunting
- Breach & Attack Simulation
- SOAR
- Use-case Factory

Digital Forensics and Incident Response
- Incident Response / Compromise Assessment Services
- Forensic Readiness Audit
- Forensic and Incident Response Retainer Service
- PCI Forensic Investigation (PCI)
- Internal Forensic Investigation (IFI)
- Ransomware Simulation

Data Protection & Governance

Data Discovery and Classification
- PCI/PII/PHI Data Discovery
- Data Classification in Endpoint (Windows, Linux)
- Data Classification in O365, Metadata
- Dynamic Masking, Redact, Truncation
- Integration to DRM, DLP, SIEM

Data Privacy Professional Services
- Assessments (Unified Privacy Maturity, DPIA, 3rd Party Risk)
- Data Inventory, Mapping and Process flow, RoPA
- Data Privacy Framework - Policy, Notice, SoPs
- Consent and Notice Management framework
- Data Breach and Management
- Principal management
- Privacy by Design implementation guide
- Define Data Retention Guidelines and processes
- Technical/Organization measures
- Privacy Training/Awareness

Trainings & Certifications

Payment Data Security Training and ANAB Accredited Certification
- CPISI (2 Day Program
- CPISI (3 Day Program)
- CPISI- Advanced (3 Day Program)
- CPISI-D (Developers)
- CPISI Hybrid (4 Weeks)

Certification Program in Cybersecurity for AI – CSPAI
- CSPAI

Forensic Briefing Sessions for Senior Management

Leading Tech Security

PRISM
- PRISM LLM Vulnerability Scanner Solution
- AI Risk Management and Governance Solution Framework
- AI Compliance and Governance Consulting Service

Hardware and IoT Security Testing
- Firmware Security Testing
- Hardware/Embedded Security Testing
- IoT Network Security Testing
- IoT/Embedded Application and Management Layer Security Testing
- MPOC/ PCI PTS

Quantum Security
- Quantum Cryptographic Consulting
- Quantum Security Risk Assessment
- Quantum Security Standards Compliance

SISA is a Global Leader in Cybersecurity Solutions for the Digital Payment Industry

USA | Canada | UK | Bahrain | Saudi Arabia | UAE | Qatar | India | Singapore | Malaysia | Australia

To learn more about SISA's offerings visit us at **www.sisainfosec.com** or
Contact your SISA sales representative at **contact@sisainfosec.com**