

SISA



CUSTOMER SUCCESS STORY

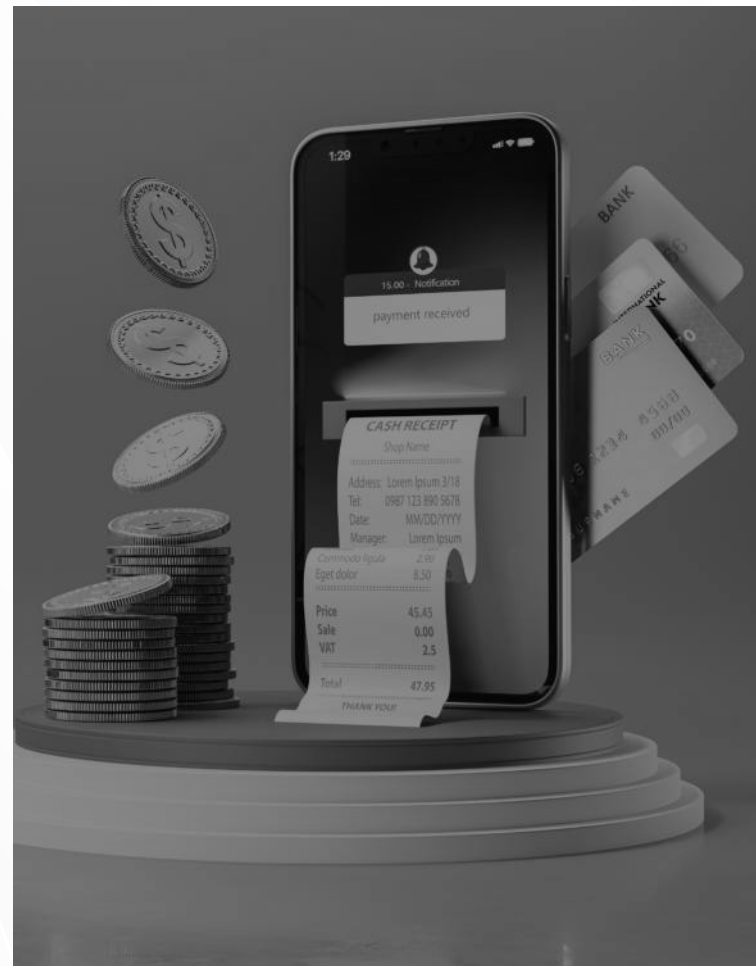
SISA helps a global electronic payment provider strengthen risk management and compliance

ABOUT THE CUSTOMER

Our client, a premier global provider of electronic payment services based in America, offers various electronic financial solutions including ATM, POS systems, credit/debit card services. By operating in three primary segments—Electronic Funds Transfer (EFT) processing, prepaid processing, and money transfer—they have established a vast and geographically diverse financial network. Their platforms and services are designed to tackle the complexities of the financial industry, by leveraging advancements in payment technologies.

THE CHALLENGE

Despite their extensive financial network and advanced platforms, our client faced significant challenges in their risk management practices. They recognized the need for a more effective risk assessment process but were hindered by inadequate audit resources and an outdated information asset inventory. Additionally, they faced challenges in fostering collaboration among internal teams. These issues collectively posed significant risks to the security of sensitive data and the company's ability to prepare for and respond to cyberattacks. With looming threats, it was imperative for our client to align their risk management practices with ISO 27005 standards. To address these concerns, the client sought the expertise of SISA to conduct a comprehensive risk assessment and IS audit.



SOLUTION OFFERED BY SISA

SISA responded to the client's needs with a holistic approach, redesigning the entire risk assessment process in line with ISO 27005 standards. SISA's team undertook the design and implementation of technology and operational risk assessments across 27 departments, using a contemporary risk management framework.

In addition, we placed a significant emphasis on enhancing business continuity planning and disaster recovery measures. This was to ensure that the client could maintain operations even under unforeseen circumstances. A thorough review and audit of the source code was conducted to affirm the security of the client's systems. Following the audit, SISA provided a comprehensive report that prioritized risk ratings and included actionable recommendations for mitigation and compliance. The detailed document empowered the client with insights into security, operational, compliance, and continuity risks, offering clear steps to mitigate them and ensure adherence to regulatory standards.

BUSINESS IMPACT

The implementation of SISA's solutions yielded significant business outcomes for our client. We helped them protect their brand name and prevent significant losses by swiftly identifying and mitigating cyber threats. SISA's expert recommendations resulted in a remarkable 200% improvement in their security posture, building trust among stakeholders. Furthermore, by adhering to ISO 27005 standards and undertaking an IS audit, our client improved their IT governance, paving the way for business expansion into new regions with innovative solutions. Overall, our collaboration enabled our client to manage the complexities of the financial industry with resilience and confidence, resulting in long-term growth and success.



SISA is a global forensics-driven cybersecurity solutions company, trusted by leading organizations for securing their businesses with robust preventive, detective, and corrective cybersecurity solutions. Our problem-first, human-centric approach helps businesses strengthen their cybersecurity posture. Industry recognition by CREST, CERT-In and PCI SSC serves as a testament to our skill, knowledge, and competence. We apply the power of forensic intelligence and advanced technology to offer true security to 2,000+ customers in 40+ countries.

Compliance	Security Testing	Cyber Resilience
<p>Payment Data Security</p> <ul style="list-style-type: none"> • 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 <p>Strategy and Risk</p> <ul style="list-style-type: none"> • CCPA • GDPR • HIPAA • ISO • NIST • SOC 1 • SOC 2 • Cloud Security 	<p>Application Security</p> <ul style="list-style-type: none"> • Application Penetration Testing • CREST/CERT-in Approved Security Testing • API Security Testing • Secure Code Review <p>Network Security</p> <ul style="list-style-type: none"> • Vulnerability Assessment • Penetration Testing • Configuration Review • Red Teaming Exercise • Firewall Rule Review • PCI ASV Scan • Phishing Simulation <p>Hardware and IoT Security Testing</p> <ul style="list-style-type: none"> • Firmware Security Testing • Hardware/Embedded Security Testing • IoT Network Security Testing • IoT/Embedded Application and Management Layer Security Testing 	<p>Managed Detection and Response Solution – SISA ProACT</p> <ul style="list-style-type: none"> • Monitoring • Attack Simulation • Use-case Factory • Advanced Threat Hunting <p>Digital Forensics and Incident Response</p> <ul style="list-style-type: none"> • Incident Response / Compromise Assessment Services • Forensic Readiness Audit • Forensic and Incident Response Retainer Service • Payment Forensics Investigation • Internal Forensics Investigation • Ransomware Simulation

Data Protection and Governance

Data Discovery and Classification Tool – SISA Radar

- Card Data Discovery
- PII (Privacy) Discovery
- Data Classification
- Data Masking/Encryption

Data Security as a Service

SISA Institute

Payment Data Security Training and Certifications

- CPISI
- CPISI Advanced
- CPISI-D (Developers)

Security Incident Detection and Response Programs

- CIDR

Cybersecurity Awareness

Forensic Learning Sessions for Senior Management