SISA

Reimagining compliance

A unified future for a fragmented regulatory world

Table of contents

Compliance challenges in the evolving digital payments landscape

29% of organizations have lost a new business deal because they were missing a compliance certification[1].In the fast-paced world of digital payments, navigating the intricate web of regulatory requirements has become an increasingly daunting task. As financial transactions grow more complex and cross border, the regulatory landscape has transformed into a mesh where companies often find themselves lost.

The challenge of compliance now extends beyond mere adherence to regulations; it requires a deep understanding of the broader implications for risk management, organizational efficiency, and overall business strategy.

The complexity concern

At the heart of the regulatory maze lies a fundamental question: Compliant with what? In a world where regulations are in constant flux, simply checking the boxes is no longer sufficient. Compliance must be viewed as an integral part of a broader risk management strategy that not only ensures adherence to laws but also actively seeks to reduce risk. However, the sheer complexity of the regulatory environment makes this a significantly challenging task. The digital payments sector, the backbone of any economy, is underpinned by about 170 regulations mandating cybersecurity requirements for businesses designed to ensure its stability and integrity[2]. Yet, as these regulations multiply and evolve, organizations are finding it increasingly difficult to keep pace. The fragmentation of compliance programs—particularly in mid-market businesses—creates gaps that are ripe for exploitation, leading to potential security breaches and costly regulatory penalties.

Audit fatigue and its impact

For fintech companies, this regulatory burden manifests in what is commonly referred to as 'audit fatigue.' FinTechs can undergo anywhere from 5 to 25 audits annually, each lasting from one to six months[3]. The result is a significant diversion of resources from critical security functions to the tedious task of demonstrating compliance. This not only increases operational costs but also heightens the risk of non-compliance, which can lead to legal penalties, loss of reputation, and increased regulatory scrutiny.

In a sea of 170+ regulations, the digital payments sector struggles to keep pace, risking security and efficiency.

This proliferation of audits is a symptom of a deeper problem: the lack of coordination and standardization in compliance programs.

Adding to the complexity is the fact that many regulatory frameworks share a significant overlap—between 60% to 80%—in their guidelines[4]. Yet, despite this overlap, companies are often required to approach the same control differently across each framework, leading to a duplication of effort and inefficiency.

The challenge of multi-framework compliance

Nearly 70% of service organizations report the need to demonstrate compliance with at least six different frameworks related to information security and data privacy[5]. Managing compliance across multiple frameworks poses a significant logistical challenge, particularly when navigating the overlapping and sometimes conflicting requirements. Further, as financial transactions increasingly go beyond national borders, the need for a unified approach to compliance becomes more pressing. However, coordinating compliance efforts across multiple regulatory standards is easier said than done. Financial organizations must navigate a patchwork of international regulations and data privacy laws, each with its own set of requirements and enforcement mechanisms.

Nearly 70% of service organizations must comply with six or more frameworks, making it a significant challenge to manage overlapping and conflicting requirements.

The complexity of this task is compounded by the fact that regulatory agencies are ramping up their oversight of cybersecurity practices in the financial sector. Regular audits and assessments are becoming the norm, with non-compliance resulting in significant fines, reputational damage, and legal consequences.

In addition to the issue of regulatory fragmentation is the fact that regulations themselves are constantly evolving. Changes in the market, the threat landscape, and even the introduction of new products can lead to rapid shifts in regulatory requirements. This dynamic environment demands that organizations remain agile, continuously monitoring and adapting to regulatory changes—a task that is further complicated by the ongoing shortage of cybersecurity talent.

The human element: Limited staff resources and cybersecurity skills shortage

In the complex world of regulatory compliance, one of the most significant challenges organizations face is the shortage of staff dedicated to compliance efforts. According to recent data, 21% of organizations lack compliance-focused staff, which significantly hampers their ability to manage the audit process effectively. This shortage is compounded by the fact that 16% of organizations struggle with the tedious and manual collection of evidence required for audits, while 14% face challenges due to budget constraints that limit their ability to invest in necessary resources[6].

These limitations can lead to high turnover rates as compliance teams find themselves overworked and burnt out by the relentless demands of maintaining regulatory adherence. The cybersecurity skills shortage, with approximately 350,000 professionals needed in the digital payments sector according to SISA, further intensifies this issue. The already limited pool of qualified professionals is stretched even thinner, making it increasingly difficult to manage the growing complexity of compliance requirements. This results in a vicious cycle where organizations are unable to retain the necessary talent, leading to gaps in compliance expertise and institutional knowledge.

High turnover rates and a severe cybersecurity skills shortage, particularly in the digital payments sector, create a vicious cycle where overworked compliance teams struggle to manage growing regulatory demands, leading to gaps in expertise and institutional knowledge.

The impact of these challenges is far-reaching. With too few resources, organizations may struggle to keep up with rapidly evolving regulations, risking non-compliance and the associated penalties. Moreover, the lack of adequate staff can slow down the audit process, making it difficult to respond swiftly to regulatory changes or to prepare for multiple, overlapping audits.

In Conclusion, as organizations cope with an increasingly complex regulatory environment, the current efforts to develop and enforce compliance programs often fall short due to a lack of coordination and standardization. This fragmentation deepens the gaps in security and compliance, leaving companies vulnerable to exploitation and regulatory penalties. The rapidly evolving nature of regulations adds another layer of complexity, making it clear that a more strategic, cohesive approach is essential.

To truly untangle the regulatory knot, companies must look beyond piecemeal solutions. The path forward lies in adopting a Unified Compliance Framework (UCF) that not only simplifies adherence to regulations but also strengthens overall risk management and business performance. Such a framework offers the dual benefits of enhancing operational efficiency and providing a competitive edge in a global market where compliance is increasingly a key differentiator.

Unified compliance dashboard: A beacon in the regulatory fog

In response to the increasingly complex and fragmented regulatory landscape, the need for a centralized and streamlined approach to managing compliance becomes critical. unified compliance emerges as a game-changing solution, offering organizations a powerful, single platform that enhances transparency, efficiency, and effectiveness in compliance management. As companies navigate the challenges posed by diverse and evolving regulations, unified compliance provides the foundation necessary to unify their compliance efforts, ensuring a holistic and cohesive strategy.

At the heart of a unified compliance approach is the principle of centralization via a unified platform. A unified compliance dashboard addresses challenges by consolidating all compliance-related data & activities into a single platform. This centralization enhances transparency, providing stakeholders with real-time visibility into the organization's compliance status and facilitating more informed decision-making while also automating manual tasks like data & document gathering. A unified compliance approach comes with advantages that translate to improved business outcomes, making it indispensable to modern organizations.

Figure 1: Key benefits of a unified compliance approach

Centralization & automation

- Single repository for all compliance data.
- Automation reduces manual effort, minimizes errors, and ensures transparency.

Comprehensive reporting

- Real-time insights for informed decision-making.
- Proactive issue resolution and enhanced regulatory alignment.

Cross-framework mapping

- Simplifies compliance by mapping requirements across frameworks.
- Reduces duplication of efforts, improves efficiency, and lowers costs.

Stakeholder engagement

- Facilitates collaboration across departments.
- Streamlined communication ensures consistent compliance.

Customized control implementation

- Tailored controls for precise compliance.
- Avoids pitfalls during audits, ensuring accuracy.

Streamlined data management

- Integrated compliance data for enhanced efficiency.
- Quick adaptation to regulatory changes, maintaining strong compliance posture.

Centralization & automation of compliance data for enhanced transparency & efficacy

A single central repository for all compliance-related information and documents, enables organizations to track and manage their compliance obligations across various frameworks and jurisdictions. This centralization ensures that all stakeholders have access to the most up-to-date and accurate information, reducing the risk of compliance gaps and oversights. By leveraging automation, a unified compliance approach can drastically reduce manual effort. From tracking regulatory changes to generating compliance reports, automation streamlines the compliance process, reducing the burden on compliance teams and minimizing the risk of human error.

Comprehensive reporting capabilities for informed decision-making

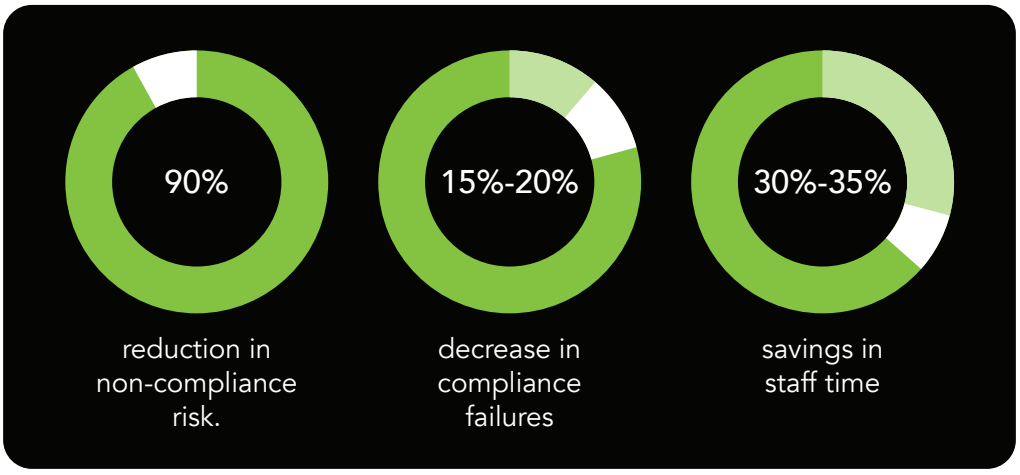
One of the key features of a unified compliance approach is enabling informed decision-making. This platform allow organizations to generate detailed reports on compliance status, risk assessments, and regulatory changes, so the burden of proof during compliance audits is drastically reduced. A single dashboard empowers decision-makers with a holistic view to take proactive steps, addressing potential issues before they escalate, improving regulatory alignment. Real-time insight into compliance metrics supports a trustworthy financial and regulatory environment, ultimately boosting investor confidence and aligning with global standards.

Cross-framework mapping for simplified compliance

A powerful feature that is unlocked by the centralization of a unified compliance platform is the ability to map compliance requirements across multiple regulatory frameworks. The UCF provides structured content and comprehensive guidance, allowing organizations to implement common controls that are mapped across standards, frameworks, and regulations. Compliance overlaps are highlighted, allowing organizations to address multiple compliance obligations simultaneously, thereby reducing duplication of efforts thus improving efficiency & reducing costs.

These standardized frameworks, help companies to manage their compliance programs more efficiently, ensuring that they remain aligned with both global and local regulations. The UCF also ensures that organizations stay updated with changes across multiple frameworks by providing updated mappings for new framework versions, allowing for quick identification of new controls that need to be implemented.

Figure 2: Practical benefits for organizations adopting a unified compliance approach in digital payments



Stakeholder engagement and communication for collaborative compliance

Effective compliance management requires collaboration among various stakeholders, including legal, finance, IT, and operational teams. A unified compliance dashboard facilitates this collaboration by providing a platform for seamless communication and information sharing. Stakeholders can easily access the information they need, communicate and coordinate their efforts to ensure that the organization remains compliant with all relevant regulations. This consolidates visibility throughout the organization, removing the impediment of a fragmented compliance approach and siloed departments.

Customized control implementation for precision compliance

UC offers the flexibility to customize control implementation, ensuring that compliance efforts are tailored to the specific needs of an organization. This customization ensures that all locations, systems, and processes are adequately covered, reducing the risk of false assertions about compliance posture. By tailoring the UCF to their specific scope, organizations can avoid potential pitfalls in external audits or examinations, ensuring that compliance efforts are both accurate and effective.

Streamlined compliance data management for enhanced efficiency

Unified compliance also excels in streamlining compliance data management, making it easier for organizations to maintain a robust and responsive compliance framework. By developing a comprehensive risk and control register within a unified dashboard, UC enables organizations to systematically update compliance controls in line with regulatory changes. This process ensures that all compliance data sources are integrated effectively, reducing data silos and enhancing the ability to conduct deep analytical reviews. The streamlined management of compliance data not only improves operational efficiency but also ensures that organizations can quickly adapt to ongoing regulatory challenges, maintaining a strong compliance posture in an ever-evolving landscape.

Figure 3: Understanding the overlap: Percentage comparison of different compliance standards

		If you want		
		PCI	SOC2	ISO
If you have	ISO	**60-70%**	**35-45%**	
	SOC2	**25-35%**		**25-35%**
	PCI		**30-40%**	**60-70%**

Percentage Overlap of Compliance Standards

Amplifying unified compliance with automation & AI: A strategic imperative

The cost of manual compliance: A growing burden

67% of businesses are under increasing pressure from customers, investors, and suppliers to provide stronger security and compliance proof. However, despite this critical need, only 9% of an organization's IT budget is typically allocated to security, with 40% of that already limited budget consumed by compliance efforts. Much of this expense and effort is wasted on outdated, manual processes that involve reconciling competing, redundant, and inefficient tasks. This reliance on manual methods not only aggravates resource gaps but also turns compliance into an administrative burden, leaving organizations struggling to keep pace with rapidly changing regulations and effectively protect against cyber threats.

Traditional, manual approaches to compliance are no longer sufficient in today's rapidly evolving regulatory landscape. These outdated methods drain resources, introduce human error, and create significant vulnerabilities. With 21% of organizations lacking dedicated compliance staff, 16% overwhelmed by manual evidence collection, and 14% constrained by budget limitations, the risks are clear: organizations are not just at risk of regulatory penalties, but also cyberattacks that could have been prevented through more efficient, automated processes.

The role of automation in transforming compliance

To address these challenges, organizations are increasingly turning to automation to streamline and enhance their compliance efforts. Automation offers a powerful solution by replacing manual, error-prone processes with efficient, accurate, and scalable workflows. For instance, automated compliance tools can handle a wide range of tasks that would otherwise consume significant human resources, including self-assessment, corrective action planning, controls analysis and testing, regulatory horizon scanning, evidence collection, centralizing compliance data, and monitoring security controls. By automating these processes, organizations can save hundreds of hours typically spent on manual tasks, such as responding to requests for proposals and security questionnaires. This not only streamlines compliance efforts but also allows teams to focus on more strategic, high-value activities.

According to Gartner, by 2025, 60% of organizations will have adopted continuous compliance practices powered by automation, allowing them to manage and mitigate cybersecurity risks more effectively.

Figure 4: The impact of automation on compliance

Efficiency and accuracy

Automation ensures that organizations adhere to standards more accurately and efficiently, resulting in a lowered risk of compliance failure by 15-20%.

Efficiency boost

Automation helps optimize resource utilization by up to 35%, freeing up your team for strategic initiatives.

Risk reduction

Automation helps minimize compliance failures by 15-20% through proactive monitoring.

Enhancing automation with intelligence

While automation addresses many of the inefficiencies in traditional compliance processes, Artificial Intelligence (AI) brings an additional layer of intelligence that can further enhance these efforts. AI excels in areas such as risk assessment, remediation, and data analysis, where it can process vast amounts of information and generate insights that would be difficult, if not impossible, for humans to achieve alone.

For example, AI can be used to calculate inherent risk scores, develop tailored remediation strategies, and produce residual risk scores, thereby improving an organization's ability to manage and respond to risks. AI also plays a crucial role in augmenting human expertise by providing actionable recommendations based on real-time data from compliance systems.

SISA's research indicates that an increase in automation can lead to a 30% decrease in compliance costs highlighting the cost-effectiveness of these technologies.

In addition, AI-driven automation enhances evidence review and report generation by providing instant feedback for straightforward cases, where evidence is clearly acceptable or rejectable. AI facilitates the automatic acceptance or rejection of evidence and generates reports for various regulatory modules with minimal manual input, significantly improving resource utilization and process efficiency. For more complex cases, where evidence falls into a grey area or is partially acceptable, AI suggests corrective actions, with human intervention required for final decisions. This approach allows organizations to perform evidence reviews more accurately, with manual oversight as needed.

The auto-generation of reports is another key benefit, ensuring high-quality and consistent outputs that are not dependent on the consultants' command of English. Instead, reports are tailored to the specific language and requirements of auditors, improving accuracy and relevance. AI helps standardize these activities, reducing variability and subjectivity in the review and reporting processes. This not only enhances the overall quality but also significantly reduces the time needed to complete these tasks.

Organizations that have extensively adopted AI and automation in their compliance processes have seen significant benefits. A study found that such organizations can identify and contain data breaches 108 days faster on average and save nearly $1.8 million compared to those that do not use these tools.[7]

The strategic advantages of integrating automation and AI into a unified compliance framework are obvious. Automation, when combined with AI, not only streamlines compliance processes but also reduces costs and enhances an organization's ability to respond quickly to new threats and regulatory changes.

As AI continues to evolve, its role in compliance will only grow, enabling organizations to proactively manage risks, improve their compliance posture, and maintain the trust of their customers and partners. The future of compliance lies in continuous, tech-enabled strategies that leverage the best of automation and AI to create a resilient, future-ready compliance environment.

Figure 5: Unified compliance framework: Strategic AI use cases for future-ready organizations

Risk management and mitigation

- Vulnerability Management
- Third-Party Risk Management

Governance and accountability

- Compliance Monitoring and Reporting
- Audit and Control Testing
- Policy Enforcement

Innovation and growth enablement

- Proactive Compliance Strategy
- Data Protection and Privacy Management

Transparency and reporting

- Regulatory Engagement and Communication
- Enhanced Metrics and Analytics
- Non-compliance Monitoring

Future-proofing compliance: Towards a new unified compliance paradigm

Cultivating competence and ongoing development

For most businesses, the biggest cybersecurity risk isn't just the technology—it's the people. A single compromised password, a successful phishing attack, or an accidental download can quickly lead to a costly data breach. This is why security frameworks stress the importance of regular security awareness training, ensuring that all employees are well-versed in the latest threats and best practices. Frameworks like PCI DSS and HIPAA even mandate specialized training on topics such as secure coding practices and the handling of sensitive data. However, managing and tracking training for an entire workforce can be a daunting task, especially as the organization grows, new employees join, and annual training requirements approach.

In today's fast-paced digital world, the ability to scale training efforts without sacrificing quality is crucial. A unified compliance platform streamlines the entire training process—from assigning and tracking training to updating content and reporting completion. This scalability allows organizations to maintain rigorous compliance standards while efficiently managing the ongoing education of their workforce, all within the ever-changing landscape of cybersecurity threats. Instead of manually scheduling sessions, sending reminders, and tracking completions, an automated tool handles everything.

Training modules are rolled out at regular intervals, employees receive timely reminders to complete their training, and detailed reports offer insight into who is up to date and who still needs to finish. This ensures that training is consistently delivered on schedule, without the need to chase down participants.

Moreover, updating training materials becomes seamless. As the threat landscape evolves rapidly, staying current is crucial. Automated updates across the platform ensure that every employee receives the most up-to-date information, keeping your team equipped with the latest knowledge.

A unified compliance platform also allows organizations to assign, track, and follow up on security, privacy, and compliance training from one centralized location. Whether it's employees or contractors, everyone can access their required training directly within the platform. Specialized training modules can be assigned based on roles, ensuring that each group receives the specific education they need. Checklists within the platform make it easy to assign only the necessary training, optimizing both time and resources. The ability to segment training for different groups not only increases relevance but also enhances engagement and retention of information.

Additionally, the platform facilitates the seamless integration of additional modules, such as AI Risk, Secure Coding, Insider Threat, and Social Engineering, into the organization's training program. By automating training assignments and updates, organizations can ensure that all employees are consistently equipped with up-to-date security and privacy knowledge, making the most of their training efforts in a dynamic threat environment.

Ensuring operational integrity and enhanced security posture

A unified compliance paradigm elevates organizations from merely meeting regulatory requirements to proactively safeguarding against emerging threats, thereby building a foundation that supports long-term security and success.

As regulatory frameworks increasingly incentivize threat prevention and risk mitigation, a unified compliance approach will drive organizations to adopt best practices such as continuous penetration testing, vulnerability management (including vulnerability prioritization techniques), and continuous security monitoring. These practices are not just about ticking boxes; they are integral to continuously monitoring and identifying compliance gaps, enabling organizations to implement improvements that enhance their overall security posture. This proactive approach ensures that potential vulnerabilities are addressed before they can be exploited, keeping the organization resilient against new threats.

To effectively manage and demonstrate the health of their security capabilities, companies require reliable and insightful metrics and reporting. This includes security compliance, risk metrics, and vulnerability tracking—elements that are critical not only for internal governance but also for assuring regulators that an organization's cybersecurity measures are robust. As regulations evolve, they will increasingly underscore and precipitate the need for enhanced reporting, greater transparency, and stronger governance of cybersecurity risk. A unified compliance paradigm will facilitate this by integrating advanced metrics and reporting capabilities into the compliance framework. This integration allows organizations to measure risks accurately and provide clear, actionable insights to both internal stakeholders and external regulators. It will enable a set of evolved controls that are essential for identifying strengths and weaknesses in an organization's security posture, enabling gaps to be addressed before they escalate into significant issues.

Moreover, the growing emphasis on third-party risk management will play a critical role in this enhanced security posture. As regulatory frameworks begin holding organizations accountable for the security practices of their vendors and suppliers, robust vendor risk assessments will become essential. A unified compliance framework will ensure that third-party vendors adhere to the same high standards as the organization itself, digging deeper into their security practices and maintaining vigilance over who is allowed into the digital ecosystem. This heightened scrutiny will help prevent security breaches that could arise from weak links in the supply chain, further strengthening the organization's defenses.

Further in a unified compliance paradigm, resilience and adaptability are key. The framework will ensure that compliance processes are not static but continuously evolving in response to new challenges. By keeping compliance frameworks robust and adaptable, organizations can stay ahead of potential vulnerabilities, ensuring that their defenses are as dynamic as the threats they face. This ongoing commitment to improvement will position organizations to thrive in an environment where regulatory demands and security threats are ever-changing, securing their future in the digital landscape.

Driving business performance for value creation

Unified compliance will ensure that organizations reach the next level of business value by transforming compliance from a mere regulatory necessity into a strategic driver of growth and innovation. While traditional compliance has been essential for building trust, safeguarding data, and protecting revenue, UC will take these benefits further, creating a future where compliance plays a pivotal role in business success.

Unified compliance will drive optimization of key economic value drivers by streamlining processes and enhancing resource utilization. This approach will improve asset efficiency, boost operating margins, and accelerate revenue growth, turning compliance from a cost centre into a significant contributor to overall business performance. As organizations look to maximize their financial outcomes, unified compliance will be the engine that powers these improvements.

By providing a structured framework, unified compliance ensures that organizations can explore new business opportunities while maintaining strong compliance controls with responsible governance. This balance between innovation and governance will allow companies to push boundaries confidently, knowing that their compliance foundation is secure. UC will enable organizations to transform compliance into a catalyst for innovation, rather than a barrier.

As businesses aim for long-term sustainability, unified compliance will help establish the robust, stable processes needed to support these goals. Comprehensive compliance controls within a UC framework will ensure that products and services are not only secure but also sustainable, maximizing revenue and profitability while mitigating operational risks.

In essence, as organizations look to future-proof their operations, unified compliance will be the key to unlocking enhanced economic value, driving innovation, and ensuring long-term sustainability. unified compliance will redefine compliance as a strategic advantage, delivering unparalleled value across all facets of the business and positioning organizations for continued success in a challenging and evolving landscape.

SISA Assistant 3.0 – AI-driven unified compliance solution for the digital payment industry

In an increasingly complex regulatory landscape, maintaining a strong compliance posture while optimizing resource allocation and improving the speed of compliance cycles is critical. SISA Assistant 3.0, a cutting-edge, cloud-based compliance management platform is designed to equip businesses to do just that. It equips digital payment organizations with the tools necessary to navigate the ever-evolving landscape of critical compliance and security standards. This innovative tool is engineered to reduce manual effort through automation, enhance efficiency with cross-framework mapping, and provide a streamlined approach to managing compliance activities.

SISA Assistant 3.0 is a comprehensive solution that leverages AI-driven automation to simplify the complexities of frameworks like PCI DSS, SWIFT, ISO27001, SOC2, GDPR, HIPAA, and HITRUST. By integrating AI-powered automation with SISA's forensics expertise, SISA Assistant 3.0 helps digital payment organizations achieve and maintain compliance with greater ease and efficiency.

The platform is built around three core components that work together to deliver a holistic compliance management experience:

1. A unified compliance platform
2. Assessment Services
3. SISA Co-Pilot

Figure 6: Key benefits of SISA Assistant 3.0 for digital payment organizations

Efficiency boost

Optimize resource utilization by up to **35%**, freeing up your team for strategic initiatives.

Faster compliance

Accelerate compliance cycles by **20-30%** with streamlined workflows.

Risk reduction

Minimize compliance failures by **15-20%** through proactive monitoring.

Improved collaboration

Enhance team communication and collaboration by **20-30%**.

Cost optimization

Reduce manual reporting by saving **20-25%** on operational costs.

Complete visibility with a unified audit platform

SISA Assistant 3.0's Unified Audit Platform is designed to centralize and streamline compliance activities, allowing organizations to efficiently manage and track their obligations across multiple regulatory frameworks from a single, user-friendly dashboard.

This centralized approach provides all stakeholders with comprehensive visibility into the status and progress of compliance efforts, ensuring that everyone is informed and aligned.

The platform's ability to map compliance activities across different regulatory modules allows executive leadership visibility into compliance levels for multiple frameworks, with the system automatically updating compliance statuses for all relevant modules. This real-time update empowers executive leadership and internal teams to make informed, strategic decisions without delay. Additionally, when a customer opts to certify against a specific standard, the platform highlights the percentage of completion for other overlapping standards. This allows organizations to make swift decisions on pursuing additional certifications, saving both time and cost. This feature also incentivizes organizations to comply with multiple standards, thereby enhancing overall compliance integrity and security posture.

In addition, SISA Assistant's intuitive dashboard highlights compliance activities that require immediate attention, ensuring that critical tasks are prioritized and addressed promptly. This proactive approach helps organizations stay on top of their compliance requirements, reducing the risk of oversights and ensuring a more efficient, cohesive compliance management process.

Once compliance is achieved the platform's 24/7 Audit Readiness feature keeps compliance documentation and reports continuously updated. This helps organizations minimize the stress and disruption that can accompany unexpected audits, keeping the compliance posture of organizations in an upward trajectory.

Assessment services: Expert guidance with SISA Assistant 3.0

SISA Assistant 3.0 goes beyond technological solutions by integrating SISA's expert forensics-driven assessment services, offering organizations tailored guidance to meet and exceed the highest standards of security and regulatory compliance.

Throughout the compliance lifecycle, from initial assessments and gap analysis to remediation and reporting, the partnership between our compliance experts and technology ensures that compliance is deeply integrated into an organization's operations. SISA Assistant 3.0 enables auditors to deliver personalized guidance, making the compliance process seamless and effective. This collaboration coupled with a wealth of experience spanning various regulatory frameworks, including PCI DSS, GDPR, HIPAA, ISO 27001, SOC 2, HITRUST and more, our compliance experts are well-equipped to guide organizations through the intricacies of maintaining a robust compliance posture.

Our compliance experts are essential in providing contextual understanding and informed decision-making. AI may flag potential issues, but it is the auditor's deep industry knowledge and ability to interpret findings within the broader organizational context that ensures compliance efforts are truly effective. This nuanced understanding allows our experts to translate complex regulatory requirements into actionable steps that are tailored to the unique needs of each organization.

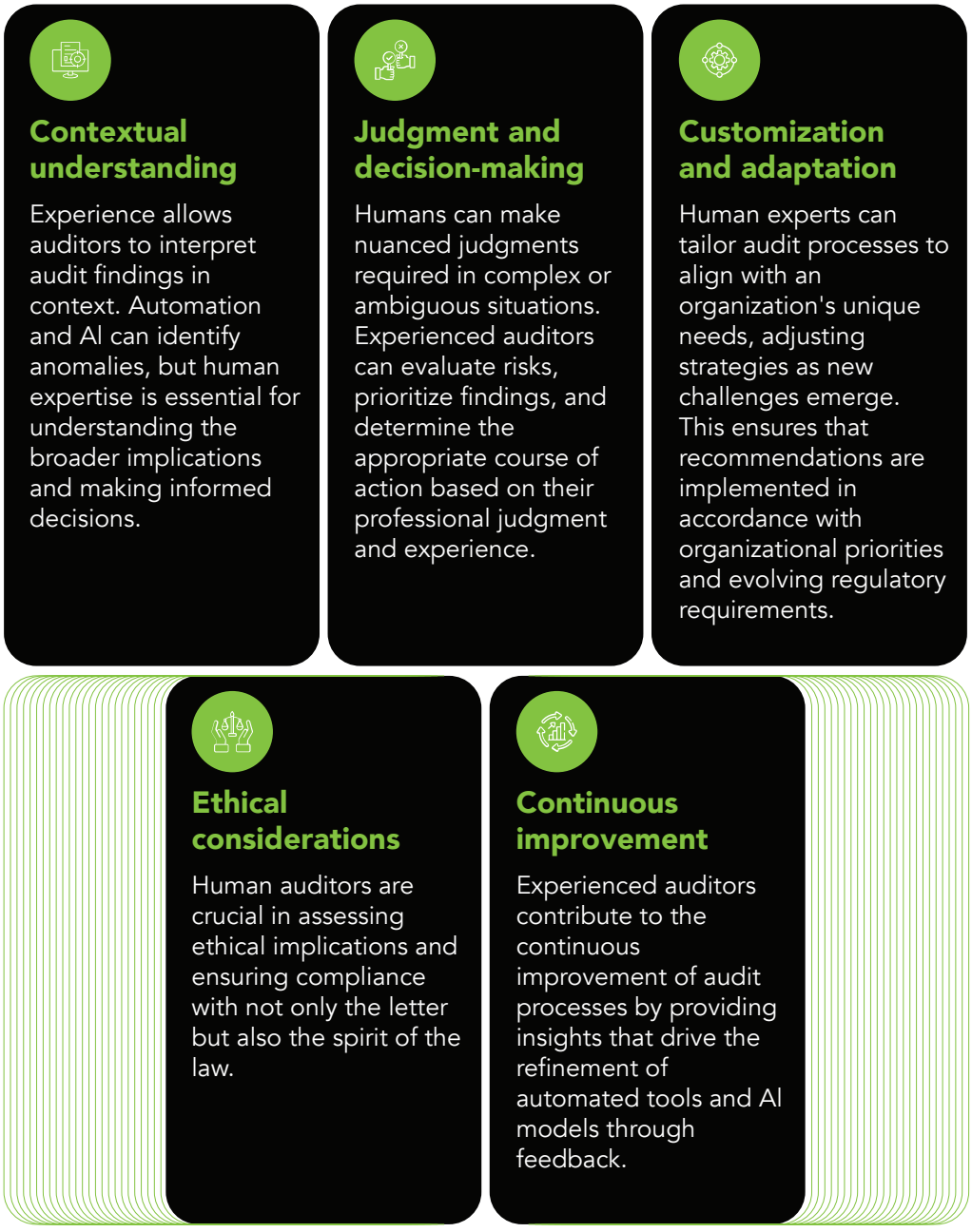
Moreover, the ability to make sound judgments in complex or ambiguous situations is something that technology alone cannot replicate. SISA's experienced auditors evaluate risks, prioritize findings, and determine the most appropriate course of action based on their professional experience. This human insight is crucial for navigating the intricacies of compliance, particularly when faced with challenges that require more than a straightforward, rules-based approach.

Every organization faces unique challenges, and compliance strategies must be tailored to fit these specific needs. We bring the flexibility needed to adapt audit processes as new challenges emerge or as the regulatory environment shifts. This ensures that compliance efforts remain aligned with organizational priorities and up to date with the latest standards.

Ethical considerations further highlight the indispensable role that our compliance expert plays. Beyond merely adhering to regulations, these experts assess the ethical implications of business practices, ensuring that organizations not only comply with the letter of the law but also uphold its spirit. This focus on ethical compliance fosters a culture of integrity within the organization.

We also focus on continuous improvement in compliance processes. Our experienced auditors provide valuable insights that help refine automated tools and AI models. This ongoing feedback loop ensures that technology evolves in ways that better serve the organization's needs, enhancing both the efficiency and effectiveness of compliance efforts.

Figure 7: The irreplaceable role of human expertise in auditing



The SISA Co-Pilot factor

The SISA Co-Pilot is an innovative AI-driven feature within the SISA Assistant platform, designed to revolutionize compliance management by automating key processes and providing real-time insights.

Real-time project insights

Track project progress, view project timelines and milestones and identify potential delays or roadblocks.

Compliance status updates

Identify vulnerabilities and action points and monitor compliance status for various security frameworks (PCI DSS, SOC 2, etc.).

Evidence management

Track the number of evidence uploaded for each project and monitor the review status of uploaded evidence (approved, rejected, with comments).

Proactive risk management

Identify compliance gaps and receive tailored recommendations, fostering proactive risk mitigation strategies.

Simplified communications

Streamline communications with SISA Co-Pilot by accessing crucial project information readily.

User workload and status

View assigned tasks for individual users and their current completion status. Identify potential bottlenecks or resource constraints within project teams.

Audit readiness assessment

Evaluate the project's readiness for audits within specific frameworks.

Figure 8: Benefits of SISA Co-Pilot

Enhanced transparency and control

Gain real-time project visibility, facilitating informed and proactive decision-making.

Improved efficiency

Utilize self-service capabilities to reduce reliance on support for basic inquiries, streamlining overall project management.

Data-driven decisions

Leverage insightful data to optimize resource allocation and project management, driving better outcomes.

Effortless compliance

Achieve and maintain comprehensive compliance with proactive risk management, ensuring a robust security posture.

Streamlined communication

Improve communication with quicker access to project information, enhancing collaboration between clients and teams.

Future-proof security

Build a strong security foundation that supports long-term success and resilience.

SISA Assistant 3.0 – AI-driven unified compliance solution for the digital payment industry

10 reasons that make SISA Assistant 3.0 indispensable for digital payments

AI-powered compliance efficiency for end-to-end compliance

SISA Assistant 3.0 is an AI-enabled compliance solution that seamlessly integrates automation with the nuanced expertise of SISA's seasoned compliance professionals. This unique combination delivers a 20-30% acceleration in compliance cycles and optimizes resource utilization by up to 35%, freeing up teams to focus on strategic initiatives.

Unified audit framework

SISA Assistant 3.0 provides a comprehensive solution that allows organizations to conduct a unified audit across various multiple regulations such as PCI DSS, ISO 27001, HIPAA, SOC2, SWIFT, HITRUST, etc. The centralized dashboard offers a single-pane view that significantly reduces the effort required by IT, Security, and Compliance Managers to gather evidence and map controls effectively across different frameworks. This reduces operational costs by 20-25%, leading to significant cost savings and better resource allocation.

Enhanced collaboration

The SISA Assistant 3.0 platform improves team communication and collaboration by 20-30%, ensuring all stakeholders are aligned, and processes are streamlined.

Reducing compliance risks with real-time evidence review

Unlike traditional compliance practices that rely on batch-based evidence reviews, SISA Assistant 3.0 enables organizations to conduct real-time reviews of their compliance evidence. This shift drastically reduces delays associated with validating evidence and responding to auditors, thereby lowering the risk of compliance errors during final reviews.

Comprehensive task management

The tool also facilitates comprehensive management of tasks such as Project Tracking, Vulnerability and Action Point Management, Compliance Status checks, Report Availability, Audit Readiness Assessment, and User Workload and Status tracking. This holistic approach ensures that potential bottlenecks and resource constraints are identified and addressed promptly.

Bridging the automation gap with human expertise

SISA's compliance experts bring a deep understanding of industry standards and organizational contexts, filling in the gaps where automation alone may fall short. The platform unlocks direct access to over 500 cybersecurity specialists within SISA, including 90+ certified penetration testers with certifications like CISSP, CISA, ISO 27001, OSCP, CPSA, ASV, eJPT, CRTP, CEH, ECSA, etc. These specialists bring unparalleled insights into the assessment of fintech products, underpinned by a profound understanding of the payments domain.

Proactive monitoring

The integration of human expertise with AI-driven processes helps minimize compliance failures by 15-20%, offering organizations a proactive approach to managing compliance risks and maintaining robust security postures.

Proprietary payment industry check lists for tailored assessments

SISA Assistant 3.0 offers proprietary checklists specifically designed for the payment industry, derived from detailed threat modeling of payment systems such as Card Management Systems (CMS), Payment Gateways (PG), and others. These checklists are meticulously aligned with regional regulatory requirements and guidelines, ensuring that your compliance assessments are thorough, accurate, and tailored to the specific needs of the payments sector.

Red team assessments for proactive risk mistigation

SISA Assistant 3.0 enhances your security posture through red team assessments powered by real-world attack scenarios and Tactics, Techniques, and Procedures (TTPs) gleaned from SISA's extensive forensic investigations. These simulations provide a proactive approach to identifying and mitigating potential threats, ensuring that your defenses are robust against the latest tactics used by cyber adversaries.

Bug bounty hall of fame mentions

SISA's deep expertise in cybersecurity is recognized across the industry, with multiple mentions in prestigious Bug Bounty Hall of Fames. This recognition underscores SISA's commitment to identifying and addressing security vulnerabilities, further solidifying the credibility and effectiveness of SISA Assistant 3.0 as an indispensable tool for digital payments security.

Why choose SISA

Payment data security professionals

In addition to being ANAB accredited security professionals (CPISI), our team specializes in the digital payment industry. This expertise gives us a deeper understanding of your business needs.

18 years of payment industry expertise

Deep experience in compliance, uncovering security vulnerabilities, and strategizing remediations.

Global recognition and accreditation

SISA stands out as a leading global PFI recognized by PCI SSC, VISA, Mastercard, AmEx, and Discover, an empaneled CERT-In auditor, CREST accredited VAPT service provider, SWIFT accredited assessment provider, and PCI Approved Scanning Vendor (ASV).

Proven PCI compliance excellence

With 2000+ PCI audits completed and a perfect track record of zero breaches, SISA leads the pack with a proven track record of compliance excellence.

Forensics expertise

As a leading forensic investigator in the financial services industry, learnings from breach investigations are leveraged into all solutions. SISA's problem-first, human-centric approach combines the power of forensic intelligence with advanced technology to improve customers compliance and security posture.

Diverse regulatory expertise

With deep compliance expertise on global regulations like PCI DSS, ISO27K, SOC2, SWIFT, HIPAA, HITRUST, GDPR & CCPA, SISA Assistant 3.0 combines and platformizes our compliance expertise for better business outcomes.

References

1. https://go.a-lign.com/benchmarkreport2023?_ga=2.54619182.406184446.1709584867-1681479690.1709584867
2. https://www.techtarget.com/searchcio/news/366585204/CIOs-play-a-role-in-responding-to-cybersecurity-regulations
3. https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/regusense-by-scrut-automation-the-unified-compliance-framework-for-indian-fintechs/100069711
4. https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/regusense-by-scrut-automation-the-unified-compliance-framework-for-indian-fintechs/100069711
5. https://coalfire.com/insights/resources/reports/securealities-report-2023-compliance
6. https://go.a-lign.com/benchmarkreport2023?_ga=2.54619182.406184446.1709584867-1681479690.1709584867
7. IBM, Cost of a Data Breach Report 2024

About SISA

SISA is a global forensics-driven cybersecurity solutions company for the digital payment industry, 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. We apply the power of forensic intelligence and advanced technology to offer true security to 2,000+ customers across 40+ countries.

SISA is one of the leading global forensic investigators for the digital payments industry.

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 compliance management

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

Hardware and IoT Security Testing

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

Cyber Resilience

Managed Extended Detection and Response Solution - SISA ProACT

- Monitoring
- Attack Simulation
- Use-case Factory
- Advanced Threat Hunting

Digital Forensics and Incident Response

- Incident Response / Compromise Assessment Services
- Forensic Readiness Audit
- Forensic and Incident Response Retainer Service
- Payment Forensics Investigation
- Internal Forensics Investigation
- Ransomware Simulation

Data Protection & Governance

Data Discovery and Classification Tool - SISA Radar

- PCI/PII/PHI Data Discovery
- Data Classification in Endpoint (Windows, Linux)
- Data Classification in 0365, Metadata
- Dynamic Masking, Redact, Truncation
- Integration to DRM, DLP, SIEM
- Deployment and Implementation Support
- Product support
- Demos and PoC in the client's environment
- Training and KT

Data Protection and Governance Managed & Shared Services

- Data Security Assessment & Recommendations
- Consultation & Data Risk Assessment support

SISA Institute

Payment Data Security Implementation Training and Certifications

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

Cybersecurity Awareness

Forensic Learning Sessions for Senior Management

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**