SISA

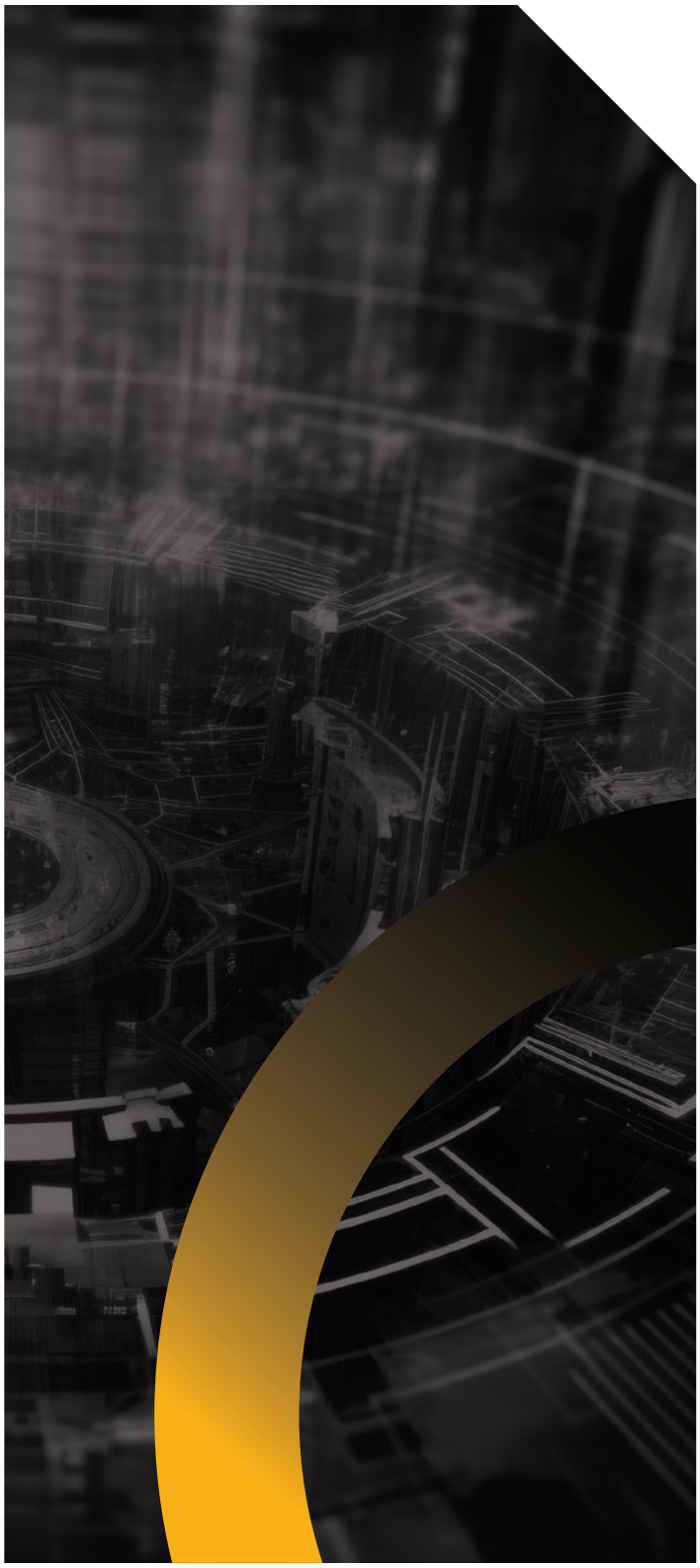
SISA CANVAS

CYBERSECURITY CONVERSATIONS FOR A SAFER TOMORROW.

EDITION 3

Optimizing Data Governance Strategies to Navigate Compliance in the Digital Payments Landscape

Table of Contents



01

Foreword

In today's digital age, the sheer volume of data generated and collected by organizations is staggering. The digital payments industry is experiencing a data explosion with the market size expected to reach USD 399 billion by 2031. This exponential growth in data has turned it into a core asset that fuels innovation and competitive differentiation in the digital payments industry. However, with great data comes great responsibility.

The true value of data emerges only when it is managed with precision and foresight, especially in light of the growing consumer demand for privacy and the stringent regulatory frameworks now in place globally.

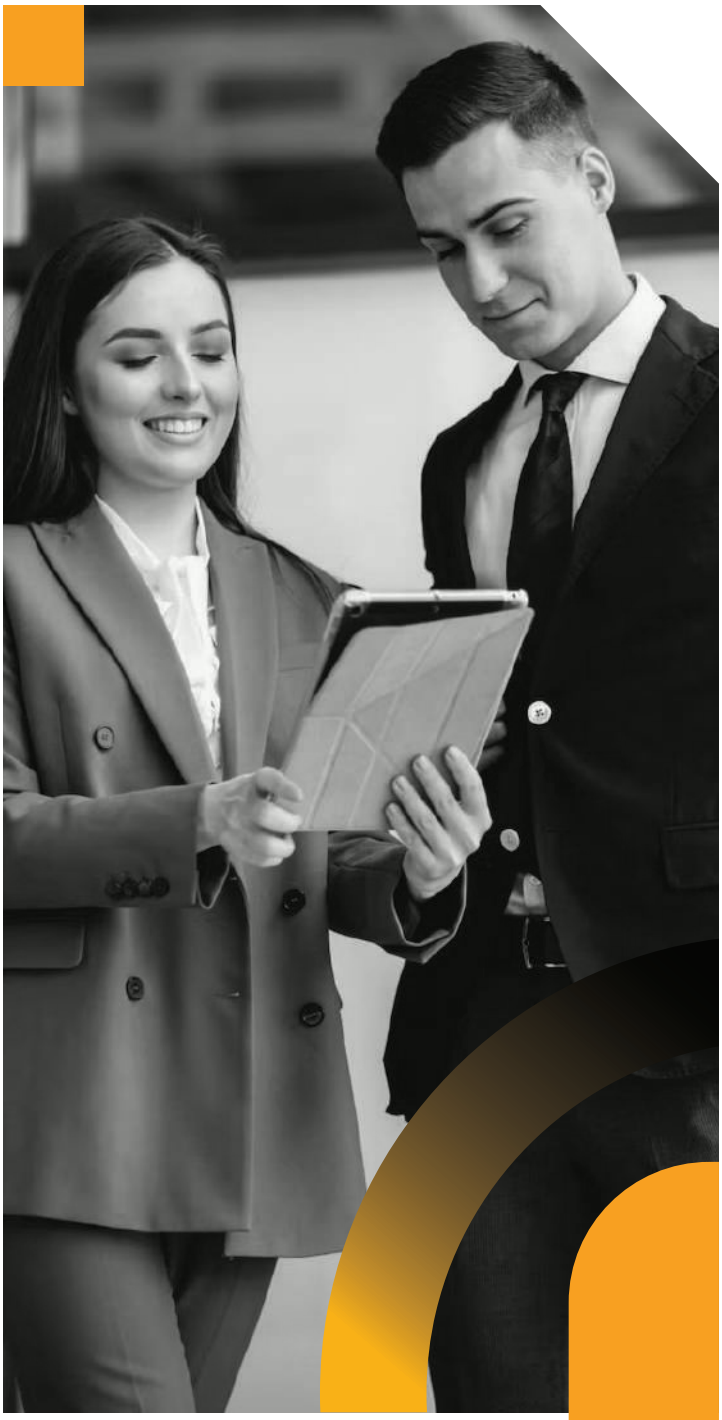
The prevalent issue of data sprawl has obscured visibility and diminished control over data distributed across multiple environments. The 2023 Cost of a Data Breach Report highlights a significant concern: 39% of breached data was dispersed across diverse settings, not only elevating the cost of these breaches but also complicating their management and containment

This dispersion of data highlights the need for a robust data governance framework that transcends basic compliance to integrate fully with organizational goals. Effective data governance must be dynamic, scalable, and deeply embedded into the company's operations, ensuring responsible management of data from creation to disposal. It's essential to develop a framework that not only meets regulations like GDPR or CCPA but also adapts to customer preferences, maintaining trust and integrity.

At the foundation of solid data governance are data discovery and classification processes, which enhance visibility and aid in the protection of sensitive information. Understanding where data is stored and how it is utilized allows organizations to set precise controls and proactively manage risks. Moreover, effective data governance requires a cultural shift within the organization, promoting a mindset that places a high priority on data security across all levels.

As we look ahead, the role of data governance is set to become more central to organizational strategy. The evolving digital landscape, marked by rapid technological advancements and shifting regulatory frameworks, demands a proactive and preemptive approach to data management. Organizations must continuously refine their data governance practices to not only comply with current regulations but also anticipate future trends and challenges.

At the core of our strategy at SISA is the commitment to ensure that our customers are not merely reactive to changes but are well-prepared to leverage data securely and effectively. By integrating rigorous data governance frameworks, we empower businesses to safeguard their most valuable assets, foster innovation, and maintain trust with their customers, thus securing their position at the forefront of the digital payments industry. As the landscape evolves, so too will our strategies, continually adapting to meet the challenges of tomorrow and ensuring our clients always remain one step ahead.



02

Conversations with Industry Experts

With over a decade of executive experience leading global technology and risk management teams, Farhan Chaudry is a proven cybersecurity, governance, and compliance leader. As the VP of Cyber Security, Governance, Risk & Compliance, and Aircraft Cyber Security at Qatar Airways, he leverages his extensive expertise and qualifications, including an Executive MSc in Technology Management and a BSc in Computer Science, to drive innovation and mitigate complex risks. Farhan's impressive credentials, which include MBCS, Security Clearance, Six Sigma, PRINCE2, and ITIL certifications, make him a trusted authority in his field.

Farhan Chaudhry

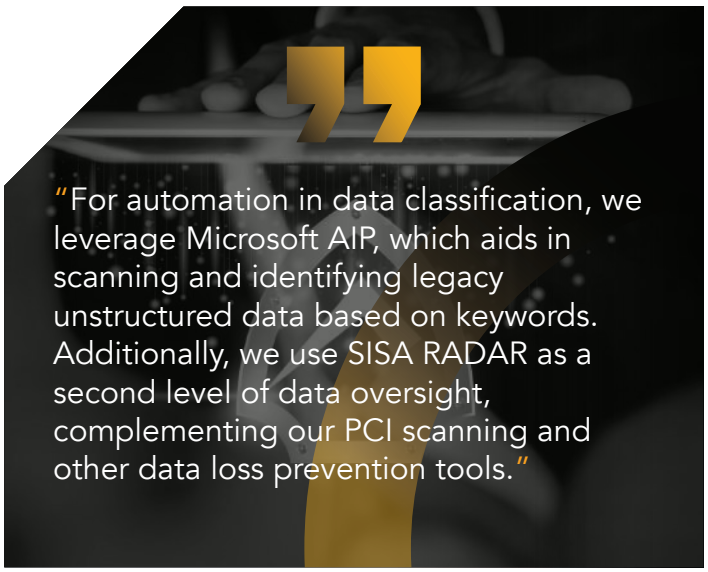
VP of Governance, Risk & Compliance, and Aircraft Cyber Security, Qatar Airways

As you handle the security strategy for a leading global airline, what are the emerging trends in data privacy and compliance across various regions?

The primary emerging trend in data privacy and compliance focuses on the foundational controls we have known for years, particularly in the context of new technologies like artificial intelligence. It's crucial to maintain our focus on data classification, ensure access is on a minimum rights principle, and protect the integrity of our data through rigorous governance frameworks. This approach involves treating AI and machine learning technologies with the same stringent controls we apply to robotic process automation and human interventions. It's about sticking to basics, ensuring our controls are well-architected to map to regulations, and understanding the lineage of our data through its lifecycle.

Given the global operations of your airline, how do you manage compliance with varying data policies across different countries?

Managing compliance across different jurisdictions involves a judicial manner of 'defense in depth', which incorporates multiple layers of controls across people, processes, and technology. At the foundation, we ensure all employees understand the policies around data classification and the treatment of sensitive data, including personally identifiable information (PII), payment card information (PCI), and commercially sensitive data.



Furthermore, we conduct regular data classification reviews, understand our data lineage, and perform data privacy impact assessments and processing activity records. These efforts are crucial as they help us blend our operational strategies with compliance requirements, especially as we shift more workloads to the cloud. In designing our cloud environments, we focus on landing zone configurations, encryption, and key management processes, which are critical for maintaining data security in transit, in use, and at rest. Our commitment to zero trust principles involves setting up information barriers and mitigating insider risks, aligning our strategy with broader cybersecurity themes. These include a mix of preventative and detective controls, designed to minimize risks to an acceptable level.

Finally, our journey towards compliance is underscored by our adherence to international standards such as ISO certifications, and PCI DSS v4, which provide a structured pathway for maintaining and demonstrating compliance.

As we migrate more systems onto the cloud, we also align our practices with **ISO 27018** to ensure that our cloud operations remain secure and compliant.

This comprehensive strategy allows us to effectively manage the myriad of data policies we encounter across the globe, ensuring that our data governance practices are robust, compliant, and capable of adapting to the evolving regulatory landscape.

How critical is data classification in your data governance journey?

Data classification is the essence of our data governance strategy. It's not just about compliance but ensuring the confidentiality, integrity, and availability of data across the organization. By establishing robust defense-in-depth strategies, we aim to centralize data governance, involving data protection officers and information security teams while ensuring that the business units that own the data are actively engaged in the governance process. There's also a crucial educational aspect, ensuring all parts of the organization understand and own the risks associated with data they handle.

With respect to effective data classification and governance, what role does AI play? Can AI be used broadly across data governance initiatives, and what impacts do you foresee?

AI is increasingly integral to our data governance strategies, particularly in data classification tasks. At its core, AI functions by identifying specific keywords we define and then automatically classifying data based on these keywords. This automation is a fundamental application of AI in data governance, streamlining processes that were traditionally manual and time-consuming.

However, the role of AI extends beyond mere automation. We are exploring generative AI and other advanced forms of AI that can assist in humanizing knowledge and supporting decision-making processes. These AI systems can potentially operate independently in the future, but currently, we are cautious about fully automating decisions without human oversight. The reason for this cautious approach is partly due to the variability in organizational risk tolerance and appetite regarding decisions made by AI.

We need to ensure that the business is brought along in this journey, understanding and aligning with the AI's role in our governance framework. At Qatar Airways, we treat AI similar to any other workload in the cloud. This means applying strict data classifications, ensuring robust security measures, and maintaining processing integrity. Our governance of AI follows the trust criteria established by SOC 2 and ISO standards, focusing on maintaining the confidentiality, integrity, and availability (CIA) of data. This structured approach ensures that while we leverage AI to enhance our data governance capabilities, we also maintain strict controls and oversight to prevent any misuse or errors in the AI's operations.

What considerations are paramount when transitioning data from legacy systems to the cloud?

When moving from legacy systems to the cloud, it's vital not to inherit outdated governance practices. Instead, establish strong operational checks during the transformation. This involves ensuring that data handled during the migration meets our stringent governance standards before it's integrated into new systems. The approach is about maintaining data integrity from legacy environments to cloud platforms, avoiding the transfer of any governance debts.

For SaaS providers, what data governance strategies do you deem necessary?

Data governance for SaaS providers hinges on the assurance of control effectiveness that aligns with industry standards, such as SOC 2 compliance. It's critical to map out data flows, understand where data resides, and ensure that encryption and security measures are robust. The organization must own these governance processes, regardless of the controls applied by third-party vendors.

What qualifications and trainings are ideal for personnel managing data governance?

For teams responsible for data governance, the qualifications go beyond formal certifications; they involve a deep understanding of the organization's culture and the ability to foster a sense of ownership and responsibility for data across all levels. Everyone in the organization should view themselves as a data owner, steward, or champion. This is crucial because the strength of our data protection is as good as our weakest link.

From a training perspective, we implement a comprehensive approach starting from induction into more specialized sessions. We strongly recommend certifications focused on cybersecurity aspects, such as Certified Information Security Manager (CISM) courses, which are valuable for those directly involved in data governance.

Moreover, we organize workshops that cover various topics around data management, which help in understanding the implications of data breaches, integrity issues, and the potential reputational damage from cyber incidents. These sessions are designed to make theoretical knowledge applicable in practical, operational contexts.

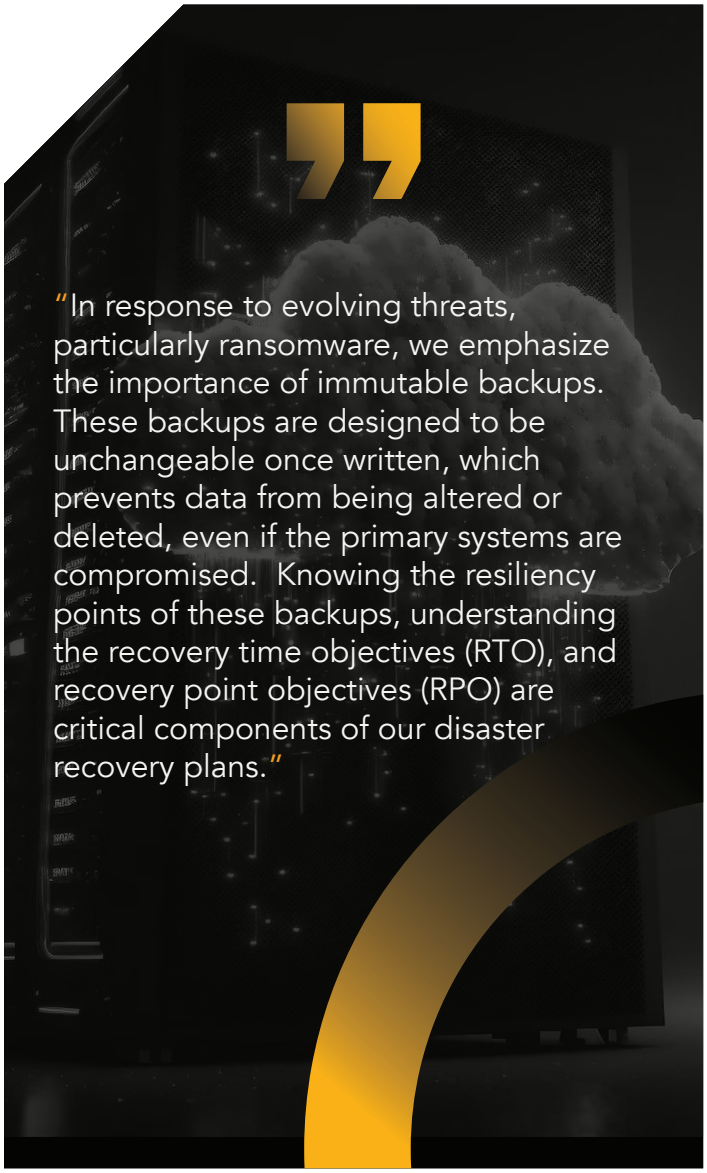
We also believe in targeted training that considers the unique roles within the organization. For example, our cabin crew might receive different data governance training compared to our pilots or ground services staff, who interact directly with customers and handle bookings. Each group is trained according to the specific data risks and responsibilities associated with their roles.

Ultimately, the goal is to tailor the training and qualifications to meet the needs of different areas within the organization, ensuring that those who govern the data and those who enforce the governance controls are well-equipped. This tailored approach helps in creating a robust data governance framework that is understood and upheld across the entire organization.

Considering that sensitive data might also reside in backups, which are often less protected, are there specific compliance mandates that classify and protect data in backups?

Indeed, sensitive data in backups is a critical area that requires rigorous protection, often overlooked in broader data security strategies. Standard IT and Information and Business Technology Risk Management (IBTRM) controls derived from banking regulations provide clear mandates on handling backups. These mandates emphasize the need for segregation of duties—this is a fundamental control to prevent risks like man-in-the-middle attacks, where a production administrator should not have the ability to modify or delete backups, thus preserving the integrity and auditability of the data.

Additionally, our backup strategy is tightly integrated with privileged access management controls. This involves stringent monitoring of who accesses the backup data and ensuring that access is strictly on a need-to-know basis. These practices are essential to prevent unauthorized access and potential data breaches.



Furthermore, we ensure that all backups are encrypted, adhering to industry best practices and compliance requirements. This encryption is crucial in maintaining the confidentiality and security of the data, even in backup form.

In many organizations, including ours, backups are treated with the same level of security as live production environments. This means that any control we apply in production, such as access controls, encryption, and monitoring, is equally applied to backups. This comprehensive approach ensures that our backups are not only compliant with regulatory mandates but also provide a robust defense against potential data security threats.

How do you ensure uniform data classification standards across regions with varying compliance demands?

We apply our data classification standards uniformly, regardless of regional compliance variations. This involves consistent policies, regular audits, and a strong culture of compliance across all regions. We strive to maintain high standards of data governance to ensure that all data is managed securely and in accordance with the strictest regulations.

How do you integrate new technologies with traditional security practices in your strategic planning?

Integrating new technologies involves a careful balance of innovation and adherence to established security practices. We continuously evaluate and update our security strategies to incorporate new technological advances, ensuring that they complement and enhance our foundational security measures without compromising on governance or integrity.

Throughout his nearly 15-year career, Rajesh has consistently demonstrated exceptional proficiency in navigating intricate information security challenges. As the current head of the information security function at one of the reputed UAE banks, he shoulders the responsibility of safeguarding the institution's invaluable information assets across on-premises and cloud environments, addressing threats from both external and internal sources. In his previous roles, Rajesh's expertise spans crucial responsibilities, notably establishing information security functions and overseeing global information security compliance across 12 branches spanning the Gulf, Europe, Asia, and America. Demonstrating a deep understanding of business dynamics, he positioned information security as a business enabler by effectively safeguarding critical assets.

Rajesh Yadla

Executive Manager Information Security, Leading Bank in the UAE

As you handle the security strategy for a leading bank in UAE that operates in almost every country, what are the emerging trends in data privacy and compliance across these regions?

From a banking industry perspective, the first emerging trend is the importance of understanding how we protect customer data. This involves implementing best practices for data security within organizations. An emerging trend in data privacy regulations can be seen in countries like the UAE and Bahrain, which were pioneers in introducing such laws. Other GCC countries are following suit, emphasizing the need for robust data privacy frameworks.

Could you elaborate on the specific trends in data governance that you are observing?

The first significant trend is data minimization and consent. Organizations are increasingly adopting the principle of collecting only the necessary data from customers to provide services. Furthermore, obtaining explicit consent from customers on how their data will be processed, stored, and protected is becoming standard practice. This ensures transparency and builds trust, informing customers that their data is used strictly for defined purposes.

Another critical trend is enhancing the understanding of data subject rights. Data privacy laws are empowering customers with several rights, including accessing their data, restricting how it is used by the organization, and data portability—allowing customers to request a comprehensive copy of their data stored by the organization.

Additionally, compliance requirements are becoming more stringent. Regulators are vigilant about the activities banks undertake with customer data, imposing hefty fines for non-compliance. There's also a shift towards greater accountability within organizations regarding data privacy and security. Many organizations are now developing dedicated data privacy functions, recruiting data privacy officers who work alongside Chief Information Security Officers (CISOs) to develop and implement comprehensive data security and governance programs. This trend reflects an increased organizational commitment to safeguarding customer data and enhancing overall data governance frameworks.

Given that your bank operates across multiple countries with varying local laws and regulations, how does your organization handle these diverse data policies?

Handling diverse data policies across different jurisdictions is indeed challenging for any bank, especially when regulated by central banks and local authorities within each country, as well as international regulatory bodies. Our approach begins with a thorough identification and inventory of all relevant regulatory requirements in each country where we operate. For example, in the UAE, we adhere to data privacy laws, the Central Bank's Consumer Protection Standards, and outsourcing regulations that dictate how we can outsource services and handle data sharing with third parties.

Could you explain the processes involved in ensuring compliance with these diverse regulations?

Once we have a clear understanding of the regulations, we perform a comprehensive gap assessment to pinpoint where our current policies might not fully align with regulatory requirements. This assessment helps us identify specific areas that need improvement from a policy standpoint.

Following this, we focus on gap remediation, which we address through two main strategies: technological innovations and process enhancements. From a technology standpoint, we might implement solutions like data classification technologies. These tools are invaluable for discovering and classifying legacy data that otherwise would be challenging and resource-intensive to manage manually.

On the process enhancement side, we deploy Data Protection Impact Assessments (DPIAs) and Records of Processing Activities (ROPAs). These tools help us identify privacy requirements and the gaps related to them, allowing us to implement necessary process changes and security controls to meet regulatory standards.

How do you ensure that frontline staff are compliant with these data protection practices?

Frontline staff are essentially the ambassadors of our organization's data security principles. It's crucial that they are equipped with the right information and training to implement these principles effectively. We ensure they have comprehensive awareness of how to handle customer data securely and communicate to customers that their data is used solely for authorized purposes. This not only protects the customer's data but also enhances customer trust in our services.

Overall, our approach to dealing with diverse data regulations involves a balanced mix of leveraging cutting-edge technology, refining our processes, and ensuring our staff are well-trained. This comprehensive strategy allows us to align our operations with both local and international data protection regulations effectively.

Considering that data classification is mandatory in some regions like Qatar but not universally required, how important do you believe data classification is in the overall data governance journey?

I'd like to emphasize its critical importance in three specific ways. First, data classification is vital for controlling access based on the data's criticality. This practice ensures that sensitive data can only be accessed by authorized personnel, which is fundamental for maintaining security within the organization.

Second, data classification significantly enhances the effectiveness of Data Loss Prevention (DLP) solutions. These solutions rely on the predefined criticality of data to prevent sensitive information from unauthorized export out of the organization. Without proper classification, DLP systems may fail to protect crucial data adequately.

Third, from an operational efficiency perspective, it's important to avoid classifying all data as critical. Over-classification leads to unnecessary overhead costs related to data protection, data retention, and the resources required to manage this data. Efficiently classifying data ensures that resources are allocated appropriately, reducing costs and optimizing operational performance.

Considering the capabilities of AI, what role do you see it playing in data classification and broader data governance initiatives?

It's crucial to understand AI's capabilities and the ethical frameworks required for its implementation. Theoretically, AI has significant potential to transform data governance through automation and enhanced efficiency. One of the primary roles AI can play is in automating data classification and data discovery processes. By training AI systems to recognize the types of data that are critical to an organization and incorporating these criteria into the AI's functionality, we can streamline the identification and classification of sensitive data, which is a substantial benefit.

Additionally, AI can be incredibly effective in the area of data anonymization. This is particularly relevant in scenarios where businesses need to analyze large datasets to derive actionable insights without compromising sensitive information. Properly trained AI systems can anonymize data in a way that both complies with regulatory and privacy standards and supports robust business analysis. This dual capability of AI not only enhances compliance with data protection regulations but also provides significant business advantages by enabling safe and effective data utilization for strategic decision-making.

In summary, if we navigate the ethical considerations and train AI systems appropriately, they can play a transformative role in data governance by automating complex processes such as data classification and anonymization, thereby increasing efficiency and compliance while reducing potential human error.

Often challenges exist during data migration from legacy systems to the cloud. What steps would you recommend to ensure that automation adheres to compliance requirements?

The migration of data from legacy systems to the cloud is a critical challenge, particularly for banks that often face inherent risks due to the outdated nature of these systems. It's important to acknowledge that legacy systems frequently lack the flexibility to implement new controls or receive updates from vendors to meet modern requirements.

When planning a migration to the cloud, the strategy must be carefully considered. There are generally two approaches: one is to simply 'lift and shift' the existing infrastructure to the cloud (IaaS), and the other is to modernize the application stack during the migration.

The 'lift and shift' method may not offer significant benefits in terms of compliance and control implementation, as it essentially replicates existing environments with all their inherent limitations. However, modernizing the application stack provides a substantial advantage. It allows an organization to address and rectify the inherent issues of legacy systems by implementing more advanced systems that are capable of integrating enhanced controls in the cloud. This approach not only facilitates better compliance but also leverages the cloud's native solutions for effective data management and governance.

Specifically, for audiences in the UAE, there are additional regulatory requirements concerning what data can be hosted in the cloud and where these cloud services are located. For instance, transaction-related data from banks must be hosted within the UAE as per central bank regulations. These regulatory needs must be factored into the cloud migration strategy to ensure compliance.

Is there a particular data governance framework you recommend, regardless of the region?

While I'm cautious about making broad recommendations, it's clear that most data privacy regulations, such as GDPR in Europe or data protection standards in the UAE, provide a comprehensive list of control requirements. Organizations typically perform a gap assessment to align their practices with these guidelines.

Unlike legal compliance that is usually verified through external audits without certification, ISO **27701** allows organizations to be officially certified. This certification serves as a credible testament to an organization's adherence to data privacy and governance standards, which can be communicated to customers and partners. Thus, for those looking for a standardized approach to data governance that is recognized globally, ISO **27701** provides a solid foundation, encompassing a blend of international data regulatory and governance requirements.

What qualifications or certifications would you recommend for someone managing or overseeing data governance?

Addressing data governance effectively requires a deep understanding of the criticality of your organization's data. While certifications like Certified Information Privacy Professional (CIPP) or Certified Data Privacy Solutions Engineer (CDPSE) are beneficial, they are most effective when combined with a thorough understanding of your organization's specific data needs.

A good data governance professional doesn't just aim to protect all data uniformly; instead, they focus on governing the data that is crucial for the core business operations. So, while certifications provide a theoretical foundation, the ability to apply these principles practically within the context of your business is what truly enhances data governance. Tools and platforms like Google and chatbots can offer insights into best governance practices, but adapting these to fit your organizational needs is key to effective data governance.

03

Executive Viewpoint

Dharshan Shanthamurthy is a cybersecurity veteran specializing in digital payments for over two decades. As the Founder and CEO of SISA, he leads one of the fastest-growing cybersecurity companies, working with 6 of the top 10 digital payment companies in India. Dharshan has served as a payment security assessor, a core payment forensic investigator, and a lead contributor to numerous digital payment security standards globally. His extensive expertise and contributions have been instrumental in shaping the landscape of digital payment security. Born in Mysore, Dharshan is a chartered accountant who fell in love with cybersecurity in the early 2000s. He has been recognized for his contributions to the industry with various accolades and continues to be a thought leader in the field of cybersecurity.

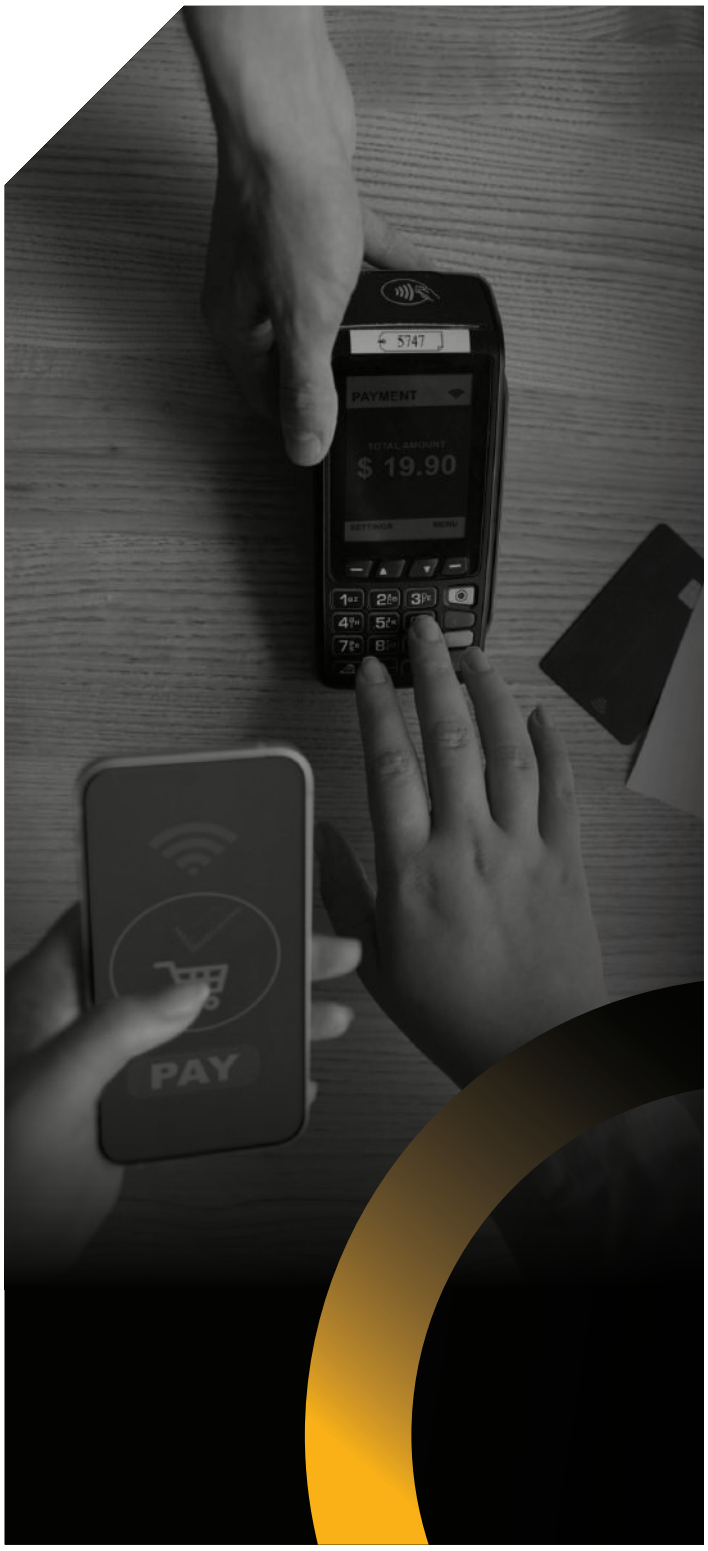
Dharshan Shanthamurthy

Founder & CEO, SISA

From a solution provider's perspective in the digital payments industry, can you discuss whether there's a universal solution or approach to data governance that can be implemented across various regions?

Addressing the idea of a universal solution in data governance, it's important to note that there isn't a one-size-fits-all solution or a magical "silver bullet" that can address all challenges. Solutions tend to be more standalone, catering to specific needs such as protection and privacy. The best approach, from my perspective, is to integrate the strongest elements from these various solutions.

"Combining robust data retention policies with advanced encryption and backup strategies forms a comprehensive framework that supports both data privacy and security. This integration allows for a more versatile and effective governance strategy that can adapt to different regulatory environments."



With your extensive experience, how should organizations handle varying data policies across different countries, especially considering the complexities of local and international regulations?

The approach starts with thoroughly understanding and discovering the data landscape, which is crucial as it allows for proper classification and application of relevant security controls. This is particularly important in regions like India, where regulatory frameworks are rapidly evolving. Knowing your data and assessing its security needs are fundamental steps.

In regions like Qatar where data classification is mandatory, how crucial do you believe data classification is to the data governance journey overall?

Data classification serves as a cornerstone of effective data governance. It's essential not just for compliance but for operational efficiency as well. Understanding which data is sensitive and needs more stringent protection helps in focusing resources and security measures appropriately. This prioritization is critical as it ensures that sensitive data, such as personal identifiers, is adequately protected against breaches, thereby safeguarding the organization's reputation and compliance status. Additionally, proper data classification supports the implementation of data retention and archival policies, aligning them with legal and regulatory requirements which may vary significantly across different jurisdictions.

Regarding the often-discussed topic of migrating from legacy systems to the cloud, what steps do you recommend ensuring that automations and operations adhere to compliance requirements during this transition?

The transition from legacy systems to the cloud must be strategically planned, focusing on the type of security controls needed based on the sensitivity of the data involved. It's not just about moving data; it's about modernizing the infrastructure so that new security controls can be effectively implemented in the cloud environment. This modernization process should include evaluating the ROI of migrating specific data sets and considering whether certain data should remain on-premises based on compliance and security requirements.

How can organizations engage all the employees to take data security seriously and understand the importance of stringent controls without overwhelming them?

Security awareness should start at the individual level, recognizing that every employee plays a crucial role in safeguarding the organization's data. To make security training more engaging and effective, incorporating interactive elements such as gamification, quizzes, and even using familiar cartoon characters in learning modules can significantly enhance participation and retention of information. Regular phishing exercises and security drills can also help maintain security awareness in a manner that is both educational and enjoyable. By making security a part of the organizational culture in an engaging way, employees are more likely to recognize their role in the security ecosystem and act accordingly.

04

SISA Perspective

Strategic Integration of AI and Foundational Controls: Navigating Data Governance in the Middle East

As the regulatory landscape of data privacy evolves across the globe, organizations in the Middle East find themselves at a crossroads of traditional governance and the burgeoning field of Artificial Intelligence (AI). The integration of these elements forms a critical pivot for enhancing data governance, ensuring compliance, and maintaining operational resilience. This perspective dives deeper into the complexities and strategies discussed by industry experts, illustrating a comprehensive approach to modern data governance.

Reinforcing Foundational Controls with AI Enhancements

Foundational controls, such as robust data classification, strict access rights management, and stringent data integrity protocols, remain the cornerstone of effective data governance. These controls are crucial for ensuring that sensitive data, including personally identifiable information (PII) and payment card information (PCI), is protected across varying jurisdictions, especially in regions with rigorous data privacy laws like the Middle East.

Integrating AI into these foundational practices offers transformative potential. AI can automate and enhance the accuracy of data classification, rapidly identifying and categorizing sensitive data. This capability not only streamlines processes but also reduces the potential for human error, thus strengthening compliance efforts. For example, leveraging technologies like Microsoft AIP for automated data tagging and classification or utilizing advanced AI algorithms for predictive data privacy impact assessments can significantly enhance the governance framework.

Strategic AI Integration for Predictive Compliance and Enhanced Privacy

The predictive capabilities of AI are invaluable for foreseeing potential compliance issues before they arise. By analyzing patterns and trends in data, AI can alert organizations to possible breaches or non-compliance scenarios, allowing for proactive remediation. This aspect of AI is particularly beneficial in regions like the Middle East, where data privacy regulations are stringent and evolving.

Moreover, AI's role in data anonymization represents a critical advancement in maintaining privacy while utilizing data for business analytics. By effectively anonymizing data, AI ensures that the extracted insights comply with privacy standards without compromising the utility of the data. This balancing act is crucial for organizations looking to leverage big data while adhering to GDPR, UAE's data protection standards, or other regional regulations.

Holistic Governance Frameworks: From Cloud Migration to Continuous Compliance

As organizations transition from legacy systems to cloud-based infrastructures, the importance of a holistic governance framework becomes evident. The shift often involves a strategic choice between merely lifting and shifting existing data or modernizing the application stack to leverage cloud-native security features. This decision is pivotal in maintaining compliance and data security during and after the migration.

The journey involves rigorous gap assessments to align with legal standards and implementing robust encryption and data handling protocols as data moves to the cloud. For example, ensuring data residency requirements are met as per local regulations, such as data transaction records within the UAE, is a critical compliance aspect.

Empowering Organizations Through Training and Engagement

Training and continuous education of staff play a pivotal role in the successful implementation of advanced data governance strategies. Employees must understand the complexities of AI tools and cloud systems to utilize these technologies effectively. Furthermore, fostering a culture of security awareness through regular training sessions, interactive learning modules, and phishing exercises can enhance the organization's overall data protection posture.

Navigating Compliance with Global and Regional Standards

Aligning with international standards such as ISO 27701 provides organizations with a structured pathway to demonstrate compliance credibly. These certifications are not merely regulatory checkboxes but strategic tools that enhance trust with partners and customers, showcasing the organization's commitment to robust data governance.

Conclusion

The strategic integration of AI into traditional data governance frameworks offers a forward-looking approach that addresses both current and emerging challenges in the field of data privacy and security. By adopting these advanced technologies in a thoughtful, structured manner, organizations in the Middle East can navigate the complexities of compliance, safeguard their operations against regulatory risks, and foster a culture of innovation and security. This comprehensive approach ensures that organizations not only meet the demands of today's digital landscape but are also prepared for future challenges in an increasingly interconnected world.

About SISA

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. We apply the power of forensic intelligence and advanced technology to offer true security to 2,000+ customers in 40+ countries.

SISA is one of the leading global forensic investigators for the 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
- IDeployment 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**