netskope

Architecting for Compliance

7 practical ways zero trust and SASE support continuous compliance in financial services.

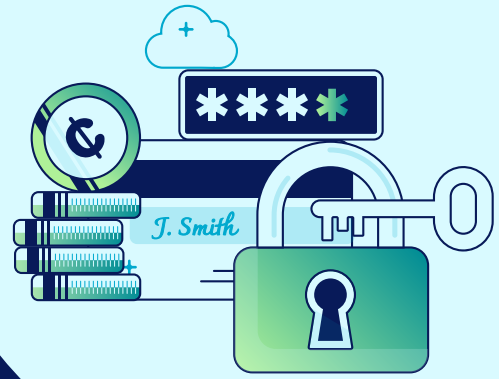


Table of Contents

Introduction

Banking, financial services, and insurance (BFSI) organizations are the lifeblood of the global economy, enabling trade and investment to operate with confidence. They also, as a result, operate at the forefront of global regulation.

From the Digital Operational Resilience Act (DORA) and the NIS2 Directive, to the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS), organizations in the BFSI sector must ensure compliance with some of the most stringent regulatory requirements around. Failure to do so would lead to potentially devastating impacts, both reputationally and financially.

However, the Data Protection Officers (DPOs), Governance, Risk, and Compliance (GRC) teams, and the security and infrastructure teams responsible for validating and implementing the controls to maintain and prove compliance now face a serious problem.

Put simply, current security models are no longer adequate for today's data flows. More specifically, the traditional perimeter-based security approach they've followed for many years has become outdated.

After spending years building infrastructure and enabling modern tools to increase their agility and innovation, most critical financial services organizations now operate with a decentralized environment. A majority have embraced the move to the cloud—rendering legacy security approaches ineffective. More recently, the need to quickly deploy and leverage AI in their businesses has significantly compounded data risks.

Modern best-practice security is built on secure access service edge (SASE) network architecture, with zero trust principles embedded. This cloud-native approach enables consistent enforcement of security controls and optimal performance, providing users with seamless and secure access to applications and data regardless of their location.

For most GRC teams, DPOs, and security architects within BFSI businesses, the question isn't whether to implement a SASE model. The benefits are clear. The question is how to use it for achieving compliance and operational resilience.

In particular, data, security, and infrastructure professionals at BFSI organizations now urgently need to:

- Advance zero trust maturity on a unified, cloud-native platform for consistent policy enforcement for data in use, at rest, and in motion, based upon continuously adapting trust indicators.
- Build scalable, converged security architectures to reduce tool sprawl, simplify operations, and meet regulatory expectations for resilience, availability, and controlled change management.
- Leverage open, interoperable platforms to build tightly integrated security ecosystems, reducing architectural gaps, enriching contextual awareness, and accelerating detection response and resolution across hybrid environments.
- Strengthen data governance, visibility, and AI/ML model oversight through deep inspection, lineage tracking, behavior analytics, and centralized evidence capture—essential to prove compliance during audits and supervisory reviews.

The question isn't *whether* to implement a SASE model. The question is *how* to use it.

This eBook is designed to help answer these challenges and give data, security, and infrastructure professionals seven best practices to support compliance requirements. Each one is underpinned by zero trust principles and achieved with SASE architecture.

Throughout, we consider some of the major regulations and frameworks that BFSI organizations are required to comply with, and we demonstrate how Netskope's security and networking solutions support those endeavors.

The Netskope One platform brings together the full spectrum of security service edge (SSE), SASE, and AI security capabilities within a single, unified platform—including:

- Software-defined wide area networking (SD-WAN)
- Cloud access security broker (CASB)
- Next gen secure web gateway (Next Gen SWG)
- Universal zero trust network access (UZTNA)
- Data security posture management (DSPM)
- Data loss prevention (DLP)
- Remote browser isolation (RBI)
- Enterprise browser
- Firewall as a service (FWaaS)
- Digital experience management (DEM)

This integration provides the architectural consistency and policy enforcement needed for continuous compliance.

Our aim is to show how best practices align with Netskope One's capabilities, and to help teams begin mapping SASE controls to their broader compliance and security frameworks, creating a practical foundation for operationalizing them.

7 compliance challenges facing data and security teams:

1. Enforcing identity and access controls
2. Securing data at rest, in motion, and in use
3. Digital operational resilience and continuity
4. Managing third-party risk
5. Continuous monitoring and response
6. Governance and accountability
7. AI deployments

1. Enforcing strong identity and least-privilege access controls.

Visibility is the essential first step in both control and audit, and so practitioners must build visibility of who (or what) has access to what data—and enable (and prove) least-privilege access. For example, GDPR prioritizes data access limitation, so that the amount of data collected, the time it's stored for, and the purposes for which it's used are only the minimum necessary. Likewise, PCI DSS Requirements 7 and 8 restrict who has access to customer data and require them to be verified to do so.

Solution: Netskope's data-centric SASE

Netskope's SASE platform operationalizes this data-centric approach by mapping its controls directly to common BFSI regulatory frameworks, removing the burden of translating requirements into technical policy:

- **Least-privilege access (PCI DSS 7, 8)**

  ZTNA provides secure, remote access to private apps, enforcing zero trust principles and granular access controls that limit access and privileges. Netskope One DLP uses context-aware policies to secure data across web, cloud apps, and endpoints, ensuring role-based access is enforced, especially during incident response.

- **Data protection by design (GDPR 25, 32)**

  Netskope One DLP, DSPM, and SaaS Security Posture Management (SSPM) continuously monitor SaaS environments to discover and secure personal data and prevent misconfigurations, ensuring data protection measures are implemented from the outset.

1. Enforcing strong identity and least-privilege access controls.

Today, data itself is the perimeter.

- **Continuous monitoring and auditability (PCI DSS 7, 8; GDPR 24, 32)**

  Every user and non-human access attempt is logged and correlated across the platform, producing complete audit trails that simplify supervisory reviews. User and entity behavior analytics (UEBA) provides ongoing risk assessment, detecting anomalies and dynamically tightening controls as conditions change.

By converging these capabilities into an integrated, data-centric SASE platform, Netskope moves beyond traditional “allow/block” controls. Access becomes strictly controlled, continuously verified, adaptive to risk, and fully auditable—meeting the stringent expectations of PCI DSS, GDPR, and the broader regulatory landscape without placing additional operational burden on already stretched security teams.

Strengthen data governance, visibility, and AI/ML model oversight through deep inspection, lineage tracking, behavior analytics, and centralized evidence capture—essential to prove compliance during audits and supervisory reviews.

2. Securing data at rest, in motion, and in use.

Data security is arguably the biggest challenge facing security teams today. Not only is there more data than ever, created and edited in and flowing through more tools and applications, but it's overseen by a growing patchwork of regulations too. Securing data is one of GDPR's core mandates, while PCI DSS Requirement 4 establishes that organizations must protect cardholder data with strong encryption during transmission over public networks.

Solution: Netskope's unified data-centric SASE

Netskope One provides integrated capabilities to ensure data is secure at rest, in motion, and in use.

By unifying DLP, DSPM, and CASB solutions, Netskope enables security teams to operationalize data-centric controls that are already mapped to common BFSI regulatory frameworks:

- **Continuous discovery and protection (GDPR 25; PCI DSS 3)**

  Netskope One DLP and DSPM enable management and protection of sensitive data across AI, cloud, on-premises, and hybrid environments through continuous discovery, classification, and real-time monitoring of structured and unstructured data. Netskope SSPM continuously monitors for misconfigurations that could expose data at rest, enabling teams to prevent compliance drift before it becomes a reportable issue.

- **Encryption in transit and at rest (PCI DSS 4; GDPR 32)**

  Policy-based encryption can be automatically applied to sensitive data moving across web traffic, cloud applications, or endpoints. ZTNA ensures end-to-end encryption for secure remote access to private apps.

2. Securing data at rest, in motion, and in use.

Preventing data sprawl and enabling secure data mobility is crucial in a borderless world.

- **Data residency and sovereignty (GDPR 44-46)**

  Netskope Advanced Analytics provides visibility into cross-border data flows, showing where regulated data lives, how it moves, and who accesses it. Policies can then enforce regional data residency or locality requirements. Netskope NewEdge Network delivers high-performance, in-country processing (including China), so compliance does not compromise user experience.

- **Incident response and audit (PCI DSS 10; GDPR 33)**

  Netskope One logs all data activity, and the cloud ticket orchestrator can automatically open tickets on IT service management and collaboration systems including ServiceNow, Slack, and Jira, helping organizations meet the GDPR's 72-hour breach notification requirement.

By unifying these capabilities, Netskope enables BFSI organizations to protect sensitive data, enforce regional requirements, and meet regulatory expectations without complexity.

All controls in this section are mapped line by line to GDPR and PCI DSS requirements, reducing manual interpretation and accelerating POC validation.

3. Establishing digital operational resilience and continuity.

Operational resilience in the face of digital disruption is a key requirement of modern business. DORA, which applies to all financial entities with EU operations and many critical third-party vendors in the EU, requires the implementation of a comprehensive ICT risk management framework. In addition, DORA and NIS2 set continuity and resilience expectations, meaning security, data, and infrastructure teams must work together to ensure digital systems can withstand, absorb, and recover from attacks or outages.

Solution: The Netskope One platform

By unifying security and network services, Netskope directly supports the resilience mandates defined by DORA and NIS2, and enables teams to jointly protect and recover critical digital services:

- **Risk management and zero trust (DORA pillar I; NIS2)**

  Netskope enforces zero trust principles through the principle of “never trust, always verify,” providing granular, adaptive real-time access control based on both identity and context. This microsegmentation contains threats and minimizes the blast radius.

- **Incident response and reporting (DORA pillar II; NIS2 Article 21)**

  Netskope One SSE capabilities—including NG-SWG, CASB, and ZTNA—deliver real-time visibility across cloud, web, and private apps. Detailed logging and analytics accelerate incident classification and support rapid, accurate reporting of major ICT-related incidents. This enables infrastructure and SOC teams to meet strict regulatory timelines for response, notification, and post-incident review.

3. Establishing digital operational resilience and continuity.

SASE architectures simplify ICT risk management, while containing threats and minimizing their blast radius.

- **Third-party risk and supply chain security (DORA pillar IV; NIS2 supply chain requirements)**

  The Netskope Cloud Confidence Index (CCI) continuously evaluates risk across 85,000+ SaaS and AI applications, giving teams a practical way to assess and govern third-party ICT providers.

- **Resilience, continuity, and recovery (DORA; NIS2 business continuity obligations)**

  Netskope's NewEdge private cloud network delivers a 99.999% availability SLA, providing high availability and supporting recovery methods to minimize downtime.

These resilience controls are fully mapped to DORA articles and NIS2 obligations, removing the first major hurdle for infrastructure, security, and GRC teams.

4. Managing end-to-end supply chain and third-party risk.

As digital ecosystems and supply chains become more interconnected, third parties represent a growing and often opaque source of operational and security risk. Regulations such as DORA and NIS2 now mandate continuous, risk-based oversight of third-party ICT providers, including strict due diligence, monitoring, sub-outsourcing controls, and exit strategies.

Solution: The Netskope One platform

The Netskope SASE platform provides a practical mechanism to meet these requirements, enabling security, procurement, and infrastructure teams to govern third-party relationships with precision

- **Managing third-party ICT risk (DORA pillar IV)**

  Netskope NG-SWG and CASB manage third-party ICT risk by inventorying and categorizing web and cloud apps. This enables organizations to cross-reference data with their Register of Information. Integrations with Governance, Risk, and Compliance (GRC) and inventory tools automatically populate data storage, processing, and GeoIP location details, also helping discover and consolidate unmanaged or redundant services.

- **Due diligence and risk scoring (DORA pillar IV; NIS2 supply chain)**

  Netskope's Cloud Confidence Index (CCI) delivers risk-based assessments of 85,000+ SaaS and AI apps, evaluating security posture, certifications, past breaches, and data handling. This supports due diligence requirements before onboarding critical third-party providers and helps assess supplier security and enterprise readiness throughout their lifecycle.

4. Managing end-to-end supply chain and third-party risk.

Organizations can extend ZTNA to external entities to provide precise access controls and comprehensive monitoring.

- **Monitoring emerging capabilities, including AI (DORA pillar I & IV)**

  CCI continuously tracks changes in SaaS applications—including new AI features or data-processing capabilities—that may introduce compliance or security risks, enabling teams to adjust access and data policies based on dynamic risk scores.

- **Compliance, oversight, and exit planning (DORA articles 28-29)**

  Netskope identifies all SaaS, cloud, and private applications, supporting an accurate Register of Information and enabling teams to identify over-reliance on specific ICT providers. CCI also evaluates factors such as data ownership and data download upon termination to assist in comprehensive exit strategies.

- **Operational resilience testing (DORA article 26)**

  By identifying managed and unmanaged applications and mapping their dependencies, Netskope helps scope and prepare for Threat-Led Penetration Testing (TLPT), ensuring resilience testing captures all critical services.

Netskope provides detailed, line-by-line mapping to DORA's third-party oversight requirements, helping teams skip months of manual compliance translation.

5. Implementing continuous monitoring and rapid incident response.

Cyber incidents are increasing in volume and variety, making monitoring and response a constant challenge for security teams who have to report to regulators quickly when breaches occur. The EU's NIS2 sets a 24-hour "early warning" reporting mandate. The U.S. NIST Cybersecurity Framework sets out Detect, Respond, and Recover functions to which organizations are often expected to align.

Solution: Netskope's SASE for accelerated incident lifecycle

Netskope One provides continuous monitoring and rapid response across the entire ecosystem of web, cloud, and private applications and services.

This capability helps financial institutions move from reactive to proactive detection, spotting subtle patterns or changes that would be impossible to notice otherwise.

- **Continuous monitoring and analytics (NIST DE.CM-01; NIS2 policies)**

  Netskope One provides continuous monitoring across networks, cloud services, and user activity. Advanced Analytics provides visibility into behavioral baselines and identifies anomalies early, such as unusual data movement or deviations from standard access patterns. User and entity behavior analytics (UEBA) detects high-risk behaviors such as bulk downloads, failed logins, and other risky activities indicative of insider threats or compromises.

- **Rapid incident response and containment (NIS2 incident handling; NIST RS.MA)**

  Netskope One applies immediate, policy-driven mitigation controls to limit the impact of an attack—for example, blocking unsanctioned cloud app instances, restricting high-risk user sessions, or isolating web traffic through RBI. Netskope's Cloud Ticket Orchestrator automates incident workflow in systems including ServiceNow and Jira, accelerating triage.

5. Implementing continuous monitoring and rapid incident response.

Netskope One helps organizations move from reactive to proactive detection.

- **Integrated threat intelligence and ecosystem coordination (NIST ID.RA-02)**

  Netskope Cloud Threat Exchange (CTE) integrates with commercial and open-source threat intelligence platforms to collect and leverage intelligence on known malicious domains and IPs, automatically sharing indicators of compromise with deployed defenses, including SIEM and SOAR systems. Netskope Cloud Risk Exchange (CRE) distributes dynamic risk scores for users, devices, and apps to drive adaptive access and data protection policies.

- **Forensics, audit, and recovery (NIST RS.AN; NIS2 reporting requirements)**

  Centralized logging offers a single source of truth for investigations and regulatory reporting. Netskope DLP policies help maintain the log integrity and preserve incident evidence.

6. Architecting for governance and accountability.

With data no longer kept behind well-defined organizational walls, organizations now need to embed governance into the architecture of their data environments. This is especially urgent as senior managers are now held directly accountable under DORA and NIS2 requirements, and are at risk of personal liability if security measures are not sufficiently rigorous.

Solution: Netskope One for embedded governance

Netskope One transforms governance from a static set of documents into a dynamic, continuously enforced framework embedded directly into network and security architecture. By centralizing enforcement and validation, Netskope strengthens policy consistency, auditability, and management accountability.

- **Centralized policy enforcement (DORA article 5; NIS2 article 21)**

  From a single unified console, organizations can define, apply, and enforce security policies across web traffic, cloud applications, private app access, and critical information systems. This ensures governance requirements are implemented uniformly across the ICT estate and directly supports the establishment and maintenance of internal governance frameworks.

- **Security posture management and continuous assurance (DORA article 6; NIS2 security controls)**

  Netskope SSPM continuously validates that SaaS environments adhere to approved configurations and patching standards. By detecting and remediating misconfigurations early, Netskope helps organizations maintain compliance with security baselines—reducing governance drift and closing gaps before they create reportable risks.

6. Architecting for governance and accountability.

Organizations can set governance policies and enforce and validate them in a single location.

- **Accountability, cyber hygiene, and user awareness (DORA articles 5 & 13; NIS2 cyber hygiene requirements)**

  Real-time user coaching notifications reinforce governance policies at the moment of risk. When users attempt unsafe actions, Netskope provides immediate contextual guidance, improving cyber hygiene.

- **Consolidated metrics, reporting, and oversight (DORA article 13; NIS2 expectations)**

  Advanced Analytics and unified dashboards consolidate policy violations, user behavior, threats, and third-party risks. This streamlined reporting helps senior management stay informed, demonstrate accountability, and meet supervisory expectations without manual effort.

By embedding governance directly into the security and network, Netskope turns compliance into continuous, automated enforcement.

These governance controls map directly to DORA and NIS2 accountability requirements, giving senior management immediate clarity without manual cross-referencing.

7. Ensuring trustworthiness and security in AI deployments.

AI has been perhaps the top security challenge for businesses in recent years, and BFSI organizations are no exception. Security teams have been tasked with balancing the company's desire for innovation, product-led growth, and enhanced customer experiences with the need to embed safeguards and meet evolving regulatory standards. Initial regulations, such as the EU AI Act, already establish strict obligations for robustness, accuracy, and data integrity in "high-risk" financial systems.

Solution: Zero trust AI security

AI expands the enterprise attack surface, introducing new risks to data, models, and workflows, especially as organizations begin integrating non-human identities (agents) into core business processes.

Netskope One applies zero trust principles end to end, ensuring that every request is verified, every data flow is monitored, and access is dynamically adjusted based on real-time risk rather than static permissions. These controls allow businesses to securely adopt and scale AI-driven technologies without compromising security or compliance.

- **Risk management and continuous assessment (EU AI Act articles 9 & 15)**

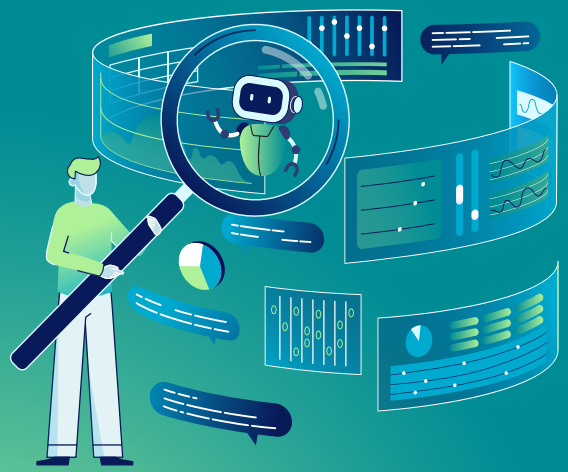
  Netskope provides continuous monitoring and risk scoring across AI systems. Netskope Cloud Confidence Index (CCI) evaluates AI service providers, identifying high-risk systems and informing third-party conformity assessments.

- **Data governance and integrity (EU AI Act article 10)**

  Netskope's DLP and DSPM classify, label, and control sensitive data used to train, tune, and prompt AI models. This prevents inappropriate use of regulated data within AI environments and provides traceability and confidentiality. Policies also ensure that sensitive information is never leaked into model outputs or logged in unsafe environments.

7. Ensuring trustworthiness and security in AI deployments.

Zero trust security strategies are highly effective as AI expands companies' risk surface.



- **Threat protection and model integrity (EU AI Act article 15)**

  The Netskope platform provides granular access controls to systems for authorized personnel, and helps identify vulnerabilities and detect or prevent attempts at data poisoning, model poisoning, or model evasion by monitoring input queries for confidentiality attacks or model flaws.

- **Transparency, auditability, and human oversight (mapped to EU AI Act articles 13 & 14)**

  Comprehensive audit trails capture all human and non-human interactions with AI systems, including data access, prompts, outputs, and policy events. Netskope Advanced Analytics provides visibility into abnormal behavior or misuse, supporting mandated human oversight and demonstrating compliance.

By integrating these capabilities into a unified, zero trust SASE architecture, Netskope ensures data confidentiality, model integrity, and continuous compliance with the EU AI Act, without adding operational complexity.

Conclusion - The architecture is the compliance

Security teams at BFSI organizations need technology infrastructure that builds in security by default, making compliance faster and easier.

This is what a modern SASE platform with zero trust principles delivers. It helps organizations improve resilience and minimize incidents, while also reducing laborious admin.

Why is SASE the best approach for continuous compliance?

Compliance architected in: Zero trust and SASE provide structural, mandatory risk-mitigation frameworks that enforce identity, access, and data-protection requirements at the architectural level.

Unify to simplify: Netskope's unified SASE platform reduces point-solution sprawl, lowering operational risk, cost, and complexity while improving governance.

Continuous compliance: "Never trust, always verify" turns compliance into real-time, adaptive enforcement rather than periodic reviews.

Resilience by default: Converged zero trust and SASE controls support the need for resilience, ensuring availability, rapid containment, and timely reporting during operational disruption.

Download Netskope's compliance guides to map the capabilities of Netskope One to GDPR, NIS2, DORA, and many more. These detailed guides have been designed to save days of time spent mapping controls.

Download compliance guides

About Netskope

Netskope, a leader in modern security and networking, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for people, devices, and data anywhere they go. Thousands of customers, including more than 30 of the Fortune 100, trust the Netskope One platform, its Zero Trust Engine, and its powerful NewEdge network to reduce risk and gain full visibility and control over cloud, AI, SaaS, web, and private applications—providing security and accelerating performance without trade-offs.

Interested in learning more?

Request a demo