Fast-track to PCI compliance

A case study

How BSI helped an industry-leading airline retail service provider to embrace 'compliance-by-design' and enhance its cloud security posture

In 2004, Retail inMotion (RiM) was created by a small group of individuals with brilliant ideas powered by strong ambitions. Sixteen years later, the promising start-up has evolved into a well-structured organization with over 300 employees and offices located across three different continents.

The challenge

Retail inMotion works alongside airline companies worldwide, assisting their clients with a wide variety of services, covering the development and procurement of onboard retail products and end-to-end IT support, including payment processing through proprietary software solutions. As often happens with organizations facing rapid growth, speed of delivery and being first to market is key to grow the business. In this way, securing Retail inMotion and their clients' information and maintaining PCI DSS Level 1 Service Provider status was paramount.

Such rapid pace of development can often lead to an overly complex IT infrastructure and increased technical debt, as new services and products are released. In facing these challenges, Retail inMotion was operating in two forked environments, one in Europe and one in North America, maintained by the same Infrastructure team but on different application and security stacks. This approach meant an effective doubling up of effort from compliance, governance and financial perspective.

The journey

As Retail inMotion matured as an organization, a project was initiated to migrate all instances to AWS. As with any such transformation project, the key to a successful migration was the retention of a secure baseline to maintain the security of the environment and associated compliance obligations.

BSI worked with Retail inMotion to ensure a compliance-by-design approach for both the PCI DSS and ISO 27001 standards without affecting their certifications. This cooperation ensured that the most efficient approach to compliance was achieved while always keeping security top of mind. The designed solution optimized resource use and ensured scalability, security and availability.

The approach

BSI worked with Retail inMotion to understand their proposed approach through continuous close collaboration. When engaged, BSI were able to inform RiM of the potential benefits and pitfalls of adopting one specific approach over another.

Key actions:

- Adoption of a single identity provider across the two regions
- Restricting user access and permissions by enforcing the 'least privilege' principle
- Reviewing AWS Network Security Groups and slimming down network ports to what is necessary
- Identification of network segmentation requirements
- Confirmation of security solution options chosen, providing confidence of effectiveness and efficiency in achieving PCI DSS compliance. [Configuration management, effective encryption implementation, logging and monitoring, IPDS and vulnerability management solutions]
- All the above leveraging demarcation of duties and compliance obligations assigned to AWS

The solution

BSI's Qualified Security Assessor's (QSA) possess broad experience in designing and verifying the effectiveness of AWS Cloud solutions from design stage through to secure implementation while utilizing industry configuration benchmarks and penetration testing techniques.

By engaging BSI QSAs at the early stages of the project, Retal inMotion gained assurance around the design and implementation of all security controls within the environment.

BSI and Retail inMotion's strong collaboration produced a standardized infrastructure with shared security services supporting standardised procedures and automated processes in both Europe and North America.

PCI compliance was achieved by Retail inMotion in 2020 with the newly deployed AWS environment, certified by BSI following a thorough assessment to ensure that the security of cardholder data is maintained as instructed by the PCI Council.

While PCI DSS forms one aspect of good cloud security governance, there is a wider cloud security perspective to be considered which is summarised in BSI's high-level methodology below.

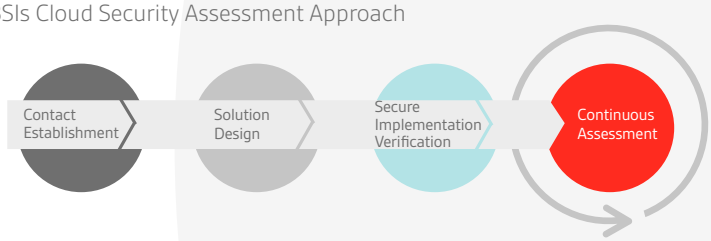
Today, BSI continue to support Retail inMotion, providing consultancy in information security,penetration testing regular PCI DSS health checks to ensure ongoing compliance is maintained.

BSI's Cloud Security Advisory Services

BSI can assist organizations using AWS with a wide range of cloud security services:

- PCI scope definition and reduction options
- Network security – Amazon VPC, Firewall, API Gateway
- Event logging and monitoring – including Amazon CloudWatch and CloudFront, GuardDuty
- Infrastructure service management – Amazon EC2 and S3
- Encryption key management – Amazon KMS
- Security of serverless environments – Lambda, RDS and DynamoDB
- PCI-compliant DevOps procedures
- ASV and penetration testing

BSIs Cloud Security Assessment Approach



Determine

Business Requirement Security Requirements Compliance Requirements whether PCI DSS, SOC2, ISO 27001, ISO 27701, Privacy (GDPR,HIPAA, CCPA, IPPA +)

Assess & Collaborate

On the Proposed Solution Design and verify requirements are met in the most effective and efficient manner:

Verify

The implementation has achieved the proposed and agreed design requirements as set out in previous stages through configuration review and benchmarking, and penetration testing

Continuous

Verification of the state of compliance through audit, quarterly health-checks benchmarking, Vulnerability Scanning and Penetration Testing

The benefits

With AWS cloud products, Retail inMotion's infrastructure and services had immediate benefits:

- Security and compliance by design;
- "Near real-time" visibility into security and compliance issues;
- Facilitated automated evidence generation;
- DevOps processes compliant with related PCI requirements.

Some of the advantages brought by the new environment consisted of offloading security responsibilities to AWS which are covered by their PCI Attestation of Compliance. According to the standard, service providers are responsible for demonstrating their compliance to their clients by providing relevant PCI DSS documentation.

By leveraging IaaS, PaaS and SaaS best in class solutions in AWS, Retail inMotion were able to reduce their overall PCI responsibilities with native security built-in features resulting in a holistic view and control of data and flows processes by the organization.

"A very special thanks to BSI for the professional and thorough execution of our PCI audit."

Cillian Smyth
Information Security Analyst / Data Protection Coordinator

About PCI

Organizations that store, process, or transmit payment card information are mandated by the Payment Card industry to meet the security requirements included in the Payment Card Industry Data Security Standard (PCI DSS).

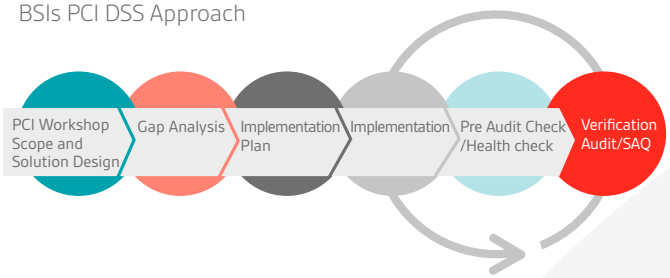
With our team of security experts and certified PCI QSAs, BSI can help by ensuring that PCI compliance requirements are implemented by your organization professionally and effectively. BSI provide consultancy services from the very early stage of the compliance roadmap (for instance defining the scope of the requirements) to validating them with a formal PCI Assessment and issuing the Attestation of Compliance.

Retail inMotion

Client: Retail inMotion
www.retailinmotion.com

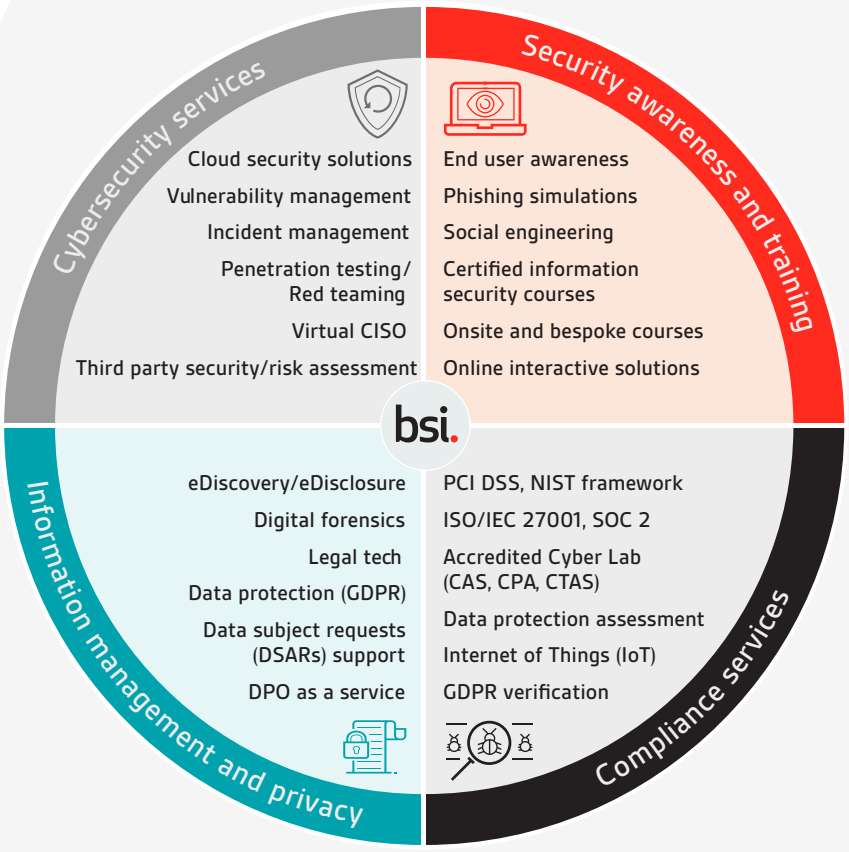
Additional resources
www.bsigroup.com/en-GB/our-services/Cybersecurity-Information-Resilience/Resources/Case-Studies

BSIs PCI DSS Approach



BSI Cybersecurity and Information Resilience

BSI Cybersecurity and Information Resilience helps you address your information challenges. We enable organizations to secure information, data and critical infrastructure from the changing threats that affect your people, processes and systems; strengthening your information governance and assuring resilience. Our cyber, information security and data management professionals are experts in:



Find out more

EMEA
Call: +353 1 210 1711
Email: cyber.ie@bsigroup.com
Visit: bsigroup.com/cyber-ie

UK
+44 345 222 1711
cyber@bsigroup.com
bsigroup.com/cyber-uk

US
+1 800 862 4977
cyber.us@bsigroup.com
bsigroup.com/cyber-us

bsi.