# The World of Cloud Security, Regulation and AI

**Peter Hainz Global Head of Strategic Initiatives - Cyber Security, Cloud, AI at SmartStream Innovation Lab explains the important role of strong cyber and cloud security measures in keeping on top of compliance requirements**

**In your opinion, are security departments within financial institutions playing a more important role than in the past and if so, do you have any examples?**

We have seen an increase in cybercrime worldwide. The reasons are manifold, ranging from geopolitical tension to remote working, due to the pandemic.

Recently, we had a four-hour cloud security review with one of the largest asset managers in the U.S. After this review, their security department stated that SmartStream's cloud security architecture is the best seen from any vendor. The reason given was that SmartStream is one of the only companies that offers a diverse solution tailored to the individual's unique security and regulatory needs, unlike competitors, which only offers a one size fits all solution. Additionally, we learn from every customer experience, and we put that knowledge to work as we tailor our solution to each client's individual needs.

**What are the best practices that keep you at the forefront of cloud security and architecture?**

A secure software development lifecycle and its architecture are vital elements of a reliable cyber security solution, and a key part of this is the recognition that regulations must be incorporated into any design from the very start.

> "REGULATORS WILL INCREASINGLY INCLUDE SECURITY TOPICS IN THEIR AUDITS AND COMPLIANCE REQUIREMENTS"

To achieve this, it is crucial to get thorough feedback from customers regarding their workflow requirements. Armed with this information we can then have a meaningful collaboration with cloud providers and vendor independent security organisations, like the Cloud Security Alliance and International Information System Security Certification Consortium (ISC2). We then use this gathered information as a basis from which we can more successfully build a client cohesive service to establish a solution that meets the customer's secure architecture needs along regulatory requirements.

As an example, SmartStream has worked with AWS to establish various banking app architectures and encryption workflows. These innovative encryption workflows, published on AWS website under 'Banking Apps Built on AWS: A Deep Dive into SmartStream's SaaS Architecture', illustrate the expertise we uniquely provide.

In an effort to always stay current we regularly meet with experts, such as the AWS cloud team. This ensures we learn about the recent development and forward-looking trends that will affect our offerings. An outcome of one of these recent gatherings was the realisation that we needed to develop a multi-layered architecture along with microservices. This allows for a greater level of defence with controls that are now layered.

Security innovations are important but interoperability and portability in our cloud environment is paramount. This ensures that we avoid vendor lock-in with any cloud providers.

When it comes to monitoring and auditability, the implementation of vendor independent Security Information and

Event Management (SIEM) tools is important. To aid in this, SIEM tools ensure that the operator has an overview of all financial institution clients.

### Security and Usability can be contradicting or not?

Certainly, it is important that the security department and business are closely aligned. SmartStream designed a best-in-class user interface for its Artificial Intelligence Reconciliations (AIR) product, which just recently received the prestigious Red Dot award. Therefore, clients experience a secure user interface, while connecting to a multi-layered microservices architecture.

Moreover, AI enhances the security and user experience. We see the benefits of AI especially in the field of exception management and predictive analytics.

I am working at SmartStream Innovation Lab in Vienna, and we are regularly discussing with the Development and Operations Team 'what if' scenarios. As example, we discuss the unlikely event of a data centre going down. Once we have gone through all the 'what if' scenarios, we input the highest possible resiliency across many geographically dispersed datacentres.

Therefore, security can support usability. User experience heavily improves with a more resilient infrastructure.

### What kind of compliance and security reports are banks asking for from their vendors?

Regulations play a key role in the banking sector – especially when it comes to secure cloud services. Many banks ask for Payment Card Industry Data Security Standard (PCI DSS) requirements, which are not dictated by law but instead by contractual obligation. As we know, PCI DSS governs the security of credit card information. PCI DSS has twelve main requirements like installing and maintaining a firewall configuration and encryption.

Another certification banks ask for is ISO 27001, which is generally considered the most well recognised security program standard globally. ISO 27001 is accepted by a great deal of regulators and jurisdictions as meeting the due care requirements for reducing liability.

Financial institutions also ask for SOC 2 reports. These reports include listings of controls relevant to security, availability, processing integrity, confidentiality or privacy.

Increasingly banks request that vendors complete the Security Questionnaire of the Cloud Security Alliance, called the CAIQ. This CAIQ presents questions that measure a cloud provider's compliance with a Cloud Control Matrix, which is the CSA's cybersecurity control framework for cloud computing.

### What are examples of regulatory topics in the cloud?

Some regulatory considerations related to cloud migration and adoption are:

- **Cybersecurity** – this should be incorporated into every critical workflow.
- **Data privacy** – policies and procedures may need to be amended due to migration to the cloud
- **Business continuity** – this should be regularly tested and documented.
- **Recordkeeping** – the Basel III data retention policies stipulate that banks must archive three to seven years of data history. Therefore, topics like retention periods, format, and media have to be considered in the cloud.

Regulators will increasingly include security topics in their audits and compliance requirements. Therefore, it will be vital for banks to work closely with managed service providers, who have the experience and knowledge in cloud security and regulatory topics. ◆

**Peter Hainz**, Global Head of Strategic Initiatives - Cyber Security, Cloud, AI at SmartStream Innovation Lab– Certified Cloud Security Professional (CCSP) by ISC2