White Paper

rillion™

# Bank Security Standards

## A deep dive into the security framework for Secure Cloud SAAS

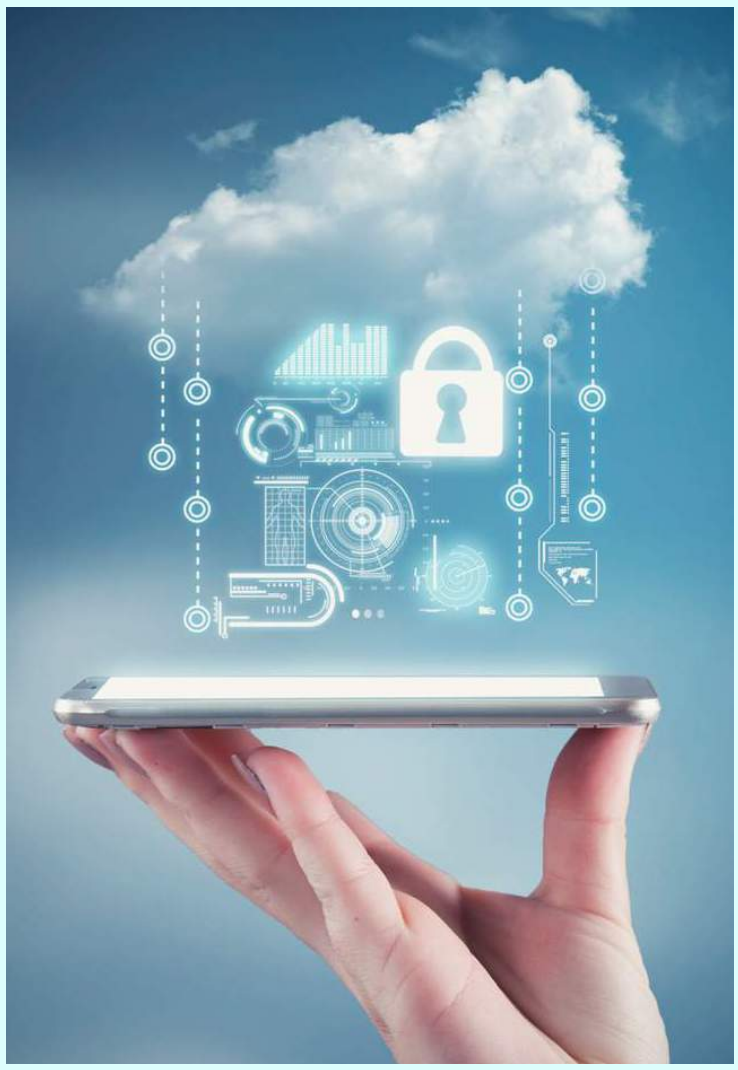
PROJECT HOSTS™
Security Compliant Clouds

White Paper

**Bank Security Standards**

# Introduction

New technologies are driving innovation and disrupting financial services faster than ever before. In the face of FinTech start-ups encroaching upon established markets, executives are demanding more from their IT departments. Increased efficiency driven by game-changing innovation is not an option—it's a must.



Meanwhile, financial services clients have had their expectations set by other industries. They're demanding better services, more value for money, and seamless, omnichannel experiences.

Regulators are also demanding more from the industry, adopting new technologies to revolutionize data collection and analytics.

And it's all happening in the cloud!

**Rillion** and **Project Hosts** have made available **Rillion White Label**, an ultra-secure white label Purchase to Pay Cloud service for banks and financial institutions.

The two companies came together in 2017 to design and deploy both private and public cloud environments offering unparalleled uptime, infrastructure, security, compliance, and support.

# Mitigate threats, ensure compliance AND protect the enterprise

Although confidence in public cloud has increased, institutions opting to leverage FinTech solutions to gain cost and operational advantages over the competition face additional security concerns.

According to EY Global Information Security Survey 2018–19, “77% of organizations are still operating with only limited cybersecurity and resilience,” and “only 6% of financial services companies say their information security function currently meets their organization’s needs.”

The PwC report referred to above states that while 65% of financial services institutions claim to have implemented cloud-based security, 69% of CEOs in the segment say that “they are either somewhat or extremely concerned about cyber-threats.”

These cyber-threats are escalating because of the proliferation of complex, rapidly evolving technologies including increased mobility and the Internet of Things (IoT).

Integration with expansive networks of third-party vendors and cross-border data exchanges only adds to the challenge of managing information security threats.

However, while there are no regulations that prevent financial institutions moving to cloud, there are approaches to running in the cloud that mitigate risk and ensure regulatory compliance.

# Minimize risk with a shared security model

Robust security in the public cloud depends on both cloud service providers and clients committing to a shared security model.

While considering the use of cloud, financial institutions need to assess the adequacy of a cloud service provider's processes and controls to assure the availability, confidentiality, and integrity of data stored in the cloud.

Data privacy and integrity is only as good as the layers of security, governance technologies, operational practices, and compliance policies that the cloud provider puts in place.

Leading cloud platforms—such as Microsoft Azure—comply with regulations such as Center for Financial Industry Information Systems (FISC), Payment Card Industry Data Security Standards (PCI DSS), and Service Organization Controls (SOC) 1, 2 and 3.

Leveraging decades of experience building enterprise software, Microsoft has incorporated security-aware software development, operational management, and threat-mitigation best practices into Microsoft Azure. The result is a secure public cloud platform that can be even more secure than on-premise, private cloud installations.

But that's only one piece of the piece of the puzzle. While Microsoft Azure secures an organization's overall global cloud infrastructure, each Azure client still needs to deploy the layers of security required to secure their own applications, content, and customer data.

Shared security requires the implementation of a comprehensive set of operating procedures and best practices based on internationally accepted standards including ISO, NIST, PCI, and HIPAA.

# Secure your Purchase to Pay process with 16 operating procedures and best practices every bank requires

Following a risk-based approach with multiple layers of security and best practices, the Rillion host environment for banks encompasses a set of 16 necessary operating procedures and practices that continuously evolve according to industry trends and regulatory policies.

| Operating procedure/Best Practice | Impact Description |
|---|---|
| AC: Access Control Policy | Ensures that the appropriate levels of controls are defined and implemented throughout the environment. |
| AT: Awareness and Training | Ensures that all employees and contractors receive up-to-date security awareness training when hired and annually. |
| AU: Audit and Accountability | Ensures the implementation and management of audit trail controls in line with legal requirements for full accountability. |
| CA: Security Assessment and Authorization | Ensures annual compliance reviews are conducted and appropriate actions taken for non-compliance. |
| CM: Configuration Management | Ensures all assets are recorded in an up-to-date inventory for the rapid identification and removal of unauthorized assets. |
| CP: Contingency Planning | Ensures regular maintenance of a detailed contingency and business continuity plan, including roles and responsibilities. |
| IA: Identification and Authentication | Ensures verification of employees when hired and users when issued with multifactor authentication. |
| IR: Incident Response | Ensures the establishment of a formal security incident response program for the handling of security breaches or events. |
| MP: Media Protection | Ensures the registration and limits of laptop usage and the encryption of removable media. |
| PE: Physical and Environmental Protection | Ensures monitoring and management of physical access, adherence to fire regulations, and correct disposal of media. |
| PL: Planning | Ensures all networks are correctly configured, secured, maintained, and documented. |
| PS: Personnel Security | Ensures user security roles and responsibilities are clearly defined, communicated, and sanctioned as required. |
| RA: Risk Assessment | Ensures up-to-date maintenance of a formal, comprehensive risk management program for the use of information assets. |
| SA: System and Services Acquisition | Ensures a standardized process for procuring, authorizing, auditing, and managing external services. |
| SC: System and Communications Protection | Ensures multi-layered security protocols are in place for managing data, gateways, firewalls, whitelists, and exceptions. |
| SI: System and Information Integrity | Ensures the protection of all systems with proven, up-to-date anti-virus and malware solutions. |

White Paper

# Bank Security Standards

## About Rillion Software

Rillion Software is a market-leading vendor of financial process automation for domestic and global corporations.

Rillion solutions automate the connecting and matching of purchase orders, invoices and contracts, on-premise or in the cloud.

Customers experience significant and measurable cost savings, productivity gains and operational excellence. Rillion solutions are GDPR compliant and optimize financial management for more than 4,000 customers in 50+ countries.

With 25 years of experience, Rillion and its partners offer automation solutions for organizations of all sizes worldwide.

**rillion.com**

## About Project Hosts

Project Hosts implements security and compliance on Microsoft Azure for the US Federal government, healthcare organizations, financial institutions and commercial enterprise. Project Hosts' pre-audited environments give organizations turnkey compliance for their applications, removing a key barrier to migration from on-premise deployments into Azure.

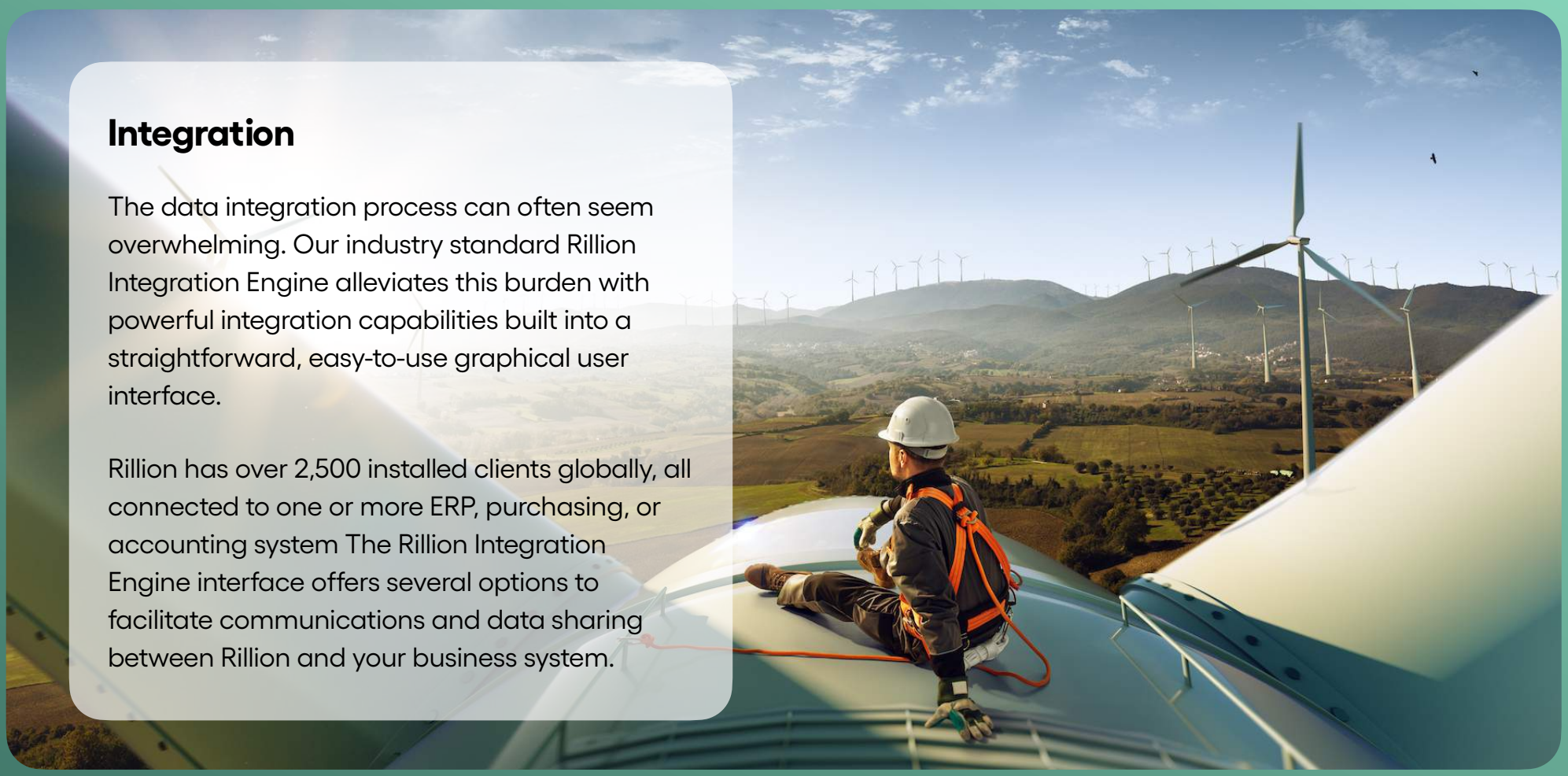
Project Hosts environments hold certifications and authorizations from ISO 27001, HIPAA, HITRUST, FedRAMP, and the DoD, including a DoD IL5 PATO. Project Hosts is just 1 out of 7 companies to achieve this authorization.

Healthcare organizations, federal, state and local government agencies, financial institutions and commercial enterprises rely on Project Hosts to ensure they have a cloud solution that meets their business needs, their budget and most importantly, protects their organization, employees and data from unauthorized access or theft.

**projecthosts.com**

White Paper

# Bank Security Standards



## Integration

The data integration process can often seem overwhelming. Our industry standard Rillion Integration Engine alleviates this burden with powerful integration capabilities built into a straightforward, easy-to-use graphical user interface.

Rillion has over 2,500 installed clients globally, all connected to one or more ERP, purchasing, or accounting system The Rillion Integration Engine interface offers several options to facilitate communications and data sharing between Rillion and your business system.


**Schedule a Consultation**

★★★★★

*"Easy to Use."*

Ap Automation with Rillion saves time, lowers costs and improves efficiency for over 3,000 clients worldwide.

**96%**

**User Satisfaction Ratings**

To learn more, visit

rillion.com

AP Automation for your peace of mind - we got this!