Technology Consulting

Making Security Work for SaaS in a Financial Services Environment

High performance. Delivered.
Financial Institutions' Path to Successful SaaS

Financial services organizations are increasingly turning to SaaS technology to help them revamp their CRM, service operations, mobility, HR, and IT operational systems. These SaaS solutions—from Cloud/SaaS providers such as salesforce.com, Workday, and ServiceNow and traditional providers such as Microsoft, Oracle and SAP—are enabling institutions to accelerate the implementation of new and improved capabilities. To help drive growth, they are able to acquire new customers and improve customer insights. To help drive productivity and efficiency they improve customer service and internal and external collaboration, reduce IT cost, and effectively manage talent. SaaS adopters are realizing tangible business benefits, including cost savings, shorter time to market, improved agility and innovation and deeper relationships with their customers.

However, the adoption of such applications—which often include sensitive customer, business, or IT information—has pushed the issue of data protection, regulatory compliance, and security to the forefront of discussions.

Accenture has been a leading SaaS provider for nearly a decade with more than 2,400 skilled SaaS personnel and more than 470 enterprise SaaS implementations across all major industries. Recognized by industry analysts as a leader in salesforce.com implementations, Accenture has a nine-year alliance with salesforce.com and twice the number of salesforce.com-certified professionals than any other company. We collaborate with salesforce.com and other leaders in the cloud, such as NetSuite, ServiceNow and Workday, to help organizations use SaaS to transform their enterprises. Our global experience, innovative methodologies and rapid implementation approach, coupled with our deep understanding of the dynamics of the fast-changing financial services industry, puts us in the unique position to help financial institutions achieve their business objectives while meeting regulatory and security requirements.
Five Key SaaS Concerns—Justified but Addressable

Based on our SaaS experience with numerous companies around the world, we have learned and demonstrated that with the right practices and tools in place, the data used by SaaS applications can be as secure as data handled by on-premise applications.

Accenture understands the concerns about using SaaS for core applications. In our work with financial institutions around the world, we have identified five concerns that are especially prevalent. While these concerns certainly are justified, they can be addressed with the right approach to managing and protecting data.

SaaS providers cannot adequately protect financial account and credit card data.

Today, many SaaS providers are transparent about their security capabilities. Many also carry industry certifications, such as ISO 27001, and have audits, such as SSAE 16 or FISMA. Different SaaS providers have varying degrees of protection available to customers as a contractual or configuration option. A thoughtful due diligence process, tailored to recognize the specific issues of cloud computing, can establish whether or not the SaaS provider can meet the customer's security and regulatory requirements.

I don't know where my data is stored.

While SaaS means the data is not on premise, it does not necessarily mean that the location of data is unknown to its owner. Companies can work with their SaaS provider to include specific residency requirements in their contract. In the case of salesforce.com, contractual arrangements exist to restrict data storage to a particular region or country if required by regulations; data remains in the stated data center and won't move without notice. Bloomberg's Local Vault allows global firms facing stringent cross-border data privacy laws to deploy a cloud-based data archiving and compliance solution locally by leveraging Bloomberg's global infrastructure.

Regulators won’t let me store financial records in the cloud.

Regulators often have not differentiated between on-premise and cloud data. In other words, regulated data typically remains so, on or off the cloud. For example, the US-based Federal Financial Institution Examination Council Agencies (FFIEC) considers cloud computing to be just another form of outsourcing. On the international front, the Monetary Authority of Singapore (MAS) takes a similar position in its June 2012 published guidelines on Technology Risk Management. It is possible for a company to satisfy regulators and auditors that it complies with all applicable regulations by investing in compliance reporting and visibility solutions.

We cannot share data across our branches around the world.

Agreements between countries, such as Safe Harbor, can facilitate the legal cross-border intra-company transfer of data. To complement paper agreements, financial institutions can apply technology to “take back” control and ownership. For example, it is possible to prohibit a cloud service provider from being in the possession of security keys, to protect against a government warrant compelling the vendor to disclose encrypted data. Salesforce.com has field-level tokenization with the ability to localize all data. This can help clients to achieve compliance by demonstrating that access is restricted and data is localized for data residency concerns.

I don’t have control over who can see my data.

Technologies are available that can help a company to retain full control of its data either by extending existing identity and access management infrastructure to the SaaS cloud provider or using the provider’s built-in access management or permissions capabilities. For example, salesforce.com allows customers to use their existing infrastructure to authenticate users in the cloud and manage access to data within the application.
Accenture’s Approach to Security and Compliance in a SaaS Environment

Accenture has worked with a variety of financial institutions to develop SaaS strategies, define the relevant regulatory and control requirements, and design and implement SaaS solutions to handle different types of data. The Accenture SaaS Enterprise Security framework (Figure 1) enables organizations to proceed with their Cloud deployment while addressing regulatory and security requirements. The framework is unique as it recognizes the collaborative nature of implementing cloud controls across the provider(s), vendors, and the organization—and three keys to doing so:

- **Extend** technical controls to the hybrid Cloud
- **Augment** contractual arrangements to address third-party risk in the Cloud
- **Broaden** security operational controls to share responsibilities

The framework can also help companies:

- **Assess** their own data security requirements and the capabilities of prospective SaaS providers;
- **Implement** the appropriate security controls for moving data to the cloud; and
- **Maintain** and monitor the relationship with SaaS providers to continually improve the security profile of data in the cloud.

**Assess**

One step in the process is to identify the risks of moving data to the cloud and fully understand how prospective cloud service providers will protect sensitive data once it is moved to a SaaS application. Accenture helps financial services institutions address these two critical areas.

Using a proprietary algorithm-based tool, Accenture enables decision makers to dissect their company’s data and earmark what can safely be moved to the cloud. With this tool, Accenture looks across all departments and functions to determine—for each type of data—the data’s sensitivity and criticality to the business, the prevailing governing regulations, and the type of security solutions available to protect it. Figure 2 illustrates some of the key types of data that major financial services industry segments consider critical to business and often carefully assess to determine the controls necessary to securely move each to cloud-based applications.

One key is starting with a focus on the data, not the technology used to manage it. It is the data, not the technology, that typically becomes subject to data protection and privacy requirements that drive security. For example, the Gramm-Leach-Bliley Act (GLBA), established before the emergence of SaaS solutions and providers, is technology agnostic and therefore applies whether the data is in the bank’s data center or in the cloud. The FFIEC considers cloud computing to have the same risk characteristics and risk management requirements as traditional forms of outsourcing. The environment in which the data moves may change, but in many cases the controls required to protect the data remain the same. In some cases, there are additional requirements that must be met, such as those prescribed by MAS.

Regardless of the type of data stored by a cloud provider, a financial institution also can benefit from rigorously evaluating its SaaS providers. By taking advantage of the Accenture Cloud Security Evaluation Methodology—developed based on input from the Cloud Security Alliance, ISO 27001, NIST and Accenture’s own detailed assessments of the security posture of the leading cloud service providers—a financial institution can evaluate and rate cloud providers’ security capabilities across security domains such as risk management, data privacy, and security operations. In addition to determining how well providers’ security capabilities stack up, such an evaluation can enable an institution to map its own security and compliance requirements to each vendor’s offerings.
Implement

Once a financial institution has assessed its data and prospective SaaS provider, and is ready to migrate the data to the cloud-based application, Accenture helps institutions with the critical task of creating and implementing the right security framework. This framework typically includes extending technical controls to cloud environments, as well as augmenting contractual controls for third-party risk and shared responsibilities. For example, cloud-specific security solutions such as CipherCloud would be identified that can encrypt sensitive data regardless of where it is stored (on premise or in the cloud) to resolve data residency and privacy considerations.

Extending a financial institution’s existing infrastructure, data and application security architecture to the cloud is critical to segregating the institution’s data from that of other cloud tenants. It can also enable an institution to manage who has access to the data, and to properly secure and maintain its SaaS interface.

Furthermore, generic templates used to guide commercial and outsourcing contracts are insufficient to address data ownership, data location, and regulatory compliance. Thus, Accenture works with financial institutions to create custom agreements that recognize the new landscape of shared responsibilities and liabilities that stem from a multi-tenant environment and multiple stakeholders.

Maintain and Monitor

After it has moved its data to the cloud, a financial institution can benefit from keeping close tabs on the relationship. Accenture has helped many institutions put in place the capabilities to generate insights on how the SaaS applications are performing and what changes the company can make to regularly improve the security of its SaaS-based data to counteract the emergence of new threat sources.

These capabilities typically include compliance monitoring controls designed to align with organizational policies—such as the ability to restrict the hours during which users can connect to the application and the range of IP addresses from which they can connect. They are also designed to provide appropriate access to logs, backups, extracts and other system-level information, and capture and merge log data with threat intelligence to correlate usage reports and track when users are attempting unauthorized access.
Using Accenture’s Software as a Service Capabilities to Harness the Power of the Cloud

Accenture has deep experience using SaaS to help many types of organizations achieve high performance and measurable business results. By identifying which business processes provide competitive advantage and developing an end-state business and IT architecture, Accenture helps organizations use SaaS across the enterprise to avoid stand-alone departmental deployments that can hinder the achievement of impactful results. As part of those efforts, we also address common integration and data challenges often encountered in implementing SaaS for the enterprise. Accenture brings the right people to bear on SaaS engagements at the right time, across 17 industries and many functional domains. Building on more than 30 years of systems integration and data management experience, our professionals have the technology skills critical to implementing enterprise-wide SaaS solutions.

Accenture can be a valuable partner to financial institutions as they consider expanding their use of SaaS. We understand the dynamics of the financial services industry and the security and compliance implications of SaaS in a financial services environment. We have implemented the solutions offered by leading SaaS providers and understand the security capabilities of their applications. And we have a tested, structured approach—incorporating decades of experience with designing and deploying data security solutions—for helping companies determine whether and how they can safely migrate data to the cloud.

In short, Accenture has the skills and experience that financial institutions need to capitalize on the promise of the cloud while securing data, satisfying regulators, and rebuilding trust with their customers.

### Security assets and capabilities

To support the implementation of the Accenture SaaS Enterprise Security Framework, organizations can take advantage of Accenture’s deep Security assets and capabilities including:

<table>
<thead>
<tr>
<th><strong>Cloud Security Assessment Tool</strong></th>
<th>Rates cloud provider’s security capabilities against a set of predefined criteria and allows comparison of providers in selection scenarios.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Sensitivity Scoring Framework</strong></td>
<td>An algorithm-based tool that enables decision makers to dissect their company’s data and earmark what can safely be moved to the cloud.</td>
</tr>
<tr>
<td><strong>Data Privacy and Protection Services</strong></td>
<td>Help organizations achieve effective data protection and privacy compliance for a cloud environment by developing data privacy and protection processes and procedures and by implementing appropriate technology controls.</td>
</tr>
<tr>
<td><strong>Cloud Identity &amp; Access Management (IAM) Solution</strong></td>
<td>Helps organizations develop and implement strategies and solutions for deploying a SaaS-based IAM solution as well as extending the enterprise IAM infrastructure to SaaS providers.</td>
</tr>
<tr>
<td><strong>Secure Integration Gateway Implementation</strong></td>
<td>Accenture brings design and implementation experience for encryption solutions that enable clients to securely connect to and store their data in the cloud thereby satisfying data residency, data encryption, and data protection regulations in different jurisdictions around the world.</td>
</tr>
</tbody>
</table>
Case Examples

**Large Bank**

**Situation:** Implementing Salesforce Sales Cloud and Force.com at a large investment bank to enable the bank to share client details as well as market data on a real-time basis to track the full lifecycle of deals.

**Challenge:** Storing sensitive deal and personal data in Cloud solutions required satisfying data residency, data encryption, and data protection regulations in different jurisdictions around the world, including the European Union, Hong Kong, Singapore, and the United States.

**Solution examples:**
- Deployed CipherCloud to encrypt sensitive information before it left the bank’s network, while keeping encryption keys on premise
- Centralized key management by integrating CipherCloud with an existing enterprise key management system
- Secured storage of salesforce.com attachments by transparently retaining the files on client’s premise in a local file server (tokenization)
- Restricted access to data through permissions assignments, access rights, and restrictions
- Enabled secure mobile access by integrating the solution with an MDM solution

**Financial Institution**

**Situation:** Using an agile app development platform such as Force.com to enable a financial institution to build and deploy social and mobile enterprise apps to enhance collaboration and information sharing across teams.

**Challenge:** Banks are often faced with the temptation to skip the upfront threat analysis and data protection requirements-gathering for new applications. They can also benefit from verifying whether they design and implement security solutions consistent with existing enterprise standards.

**Solution examples:**
- Created and applied profiles to define what actions users can perform on deals (create, view, edit, delete).
- Criteria-based sharing rules are used to share deals with bankers according to their industry or product vertical and based on the lifecycle status of the deal
- Performed security code reviews and designed and implemented secure coding practices
- Extended enterprise authentication and authorization schemes to the cloud solution
- Integrated auditing and logging into the enterprise monitoring infrastructure and processes

**Bank**

**Situation:** Deployed Salesforce Chatter enterprise social collaboration platform at a bank to enable bankers to follow clients and deals they are most interested in, and receive Chatter feed updates when parts of a deal change or a deal is progressing through the lifecycle. Because the bankers work within teams on a deal, they could more easily collaborate on progress and deal updates via chatter groups instead of email.

**Challenge:** Many banks and other financial institutions today are not using Chatter due to compliance reasons—specifically, those related to ownership and portability of data posted on social media if employees leave the organization, and concerns regarding compliance and discovery issues that influence tooling to handle logging, audit, and related controls.

**Solution examples:**
- Enabled real time communications via secure private messaging
- Implemented consistent data retention and e-discovery processes and technology across multiple platforms
- Integrated auditing and logging into the enterprise monitoring infrastructure and processes
In one of the largest enterprise communications migrations undertaken to date, Accenture's internal IT organization moved more than 250,000 mailboxes and nearly 11,300 shared-services sites to the cloud.

Accenture has strict client data protection requirements and procedures. Storing sensitive corporate and client information as well as personal data in the Cloud required satisfying our own information protection requirements in addition to data protection regulations in different jurisdictions around the world.

In addition to the built-in security safeguards and procedures from the cloud providers, Accenture also took the following steps to ensure that the solution met security and data privacy requirements:

- Conducted a detailed risk and security assessment which looked at many aspects of the cloud provider's security, operational practices, and data management standards

- Worked with legal and data privacy teams to identify contractual terms and requirements to support data privacy compliance in all countries and the EU

- Established requirements for third party penetration testing and annual SAS 70 Type II audits/certification.

The successful execution of this massive change effort required strong project management skills and the creation of at-scale migration tools and processes, as well as overcoming technology integration challenges between cloud and on-premise environments.

This initiative earned back its required investment in just one year, and is slated to continue saving Accenture over $10 million per year going forward.
References


For more information

Beth A. Boettcher
Managing Director
Financial Services SaaS Lead
beth.a.boettcher@accenture.com

Stephen M. Murphy
Managing Director
Technology Consulting
Financial Services Industry
stephen.m.murphy@accenture.com

Walid Negm
Senior Director, Security R&D
Accenture Technology Labs
walid.negm@accenture.com

Rudy Bakalov
Senior Manager
Information Risk Privacy & Strategy
rudy.bakalov@accenture.com
About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with approximately 261,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world’s most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$27.9 billion for the fiscal year ended Aug. 31, 2012. Its home page is www.accenture.com.

About Accenture Technology Labs

Accenture Technology Labs, the dedicated technology research and development (R&D) organization within Accenture, has been turning technology innovation into business results for more than 20 years. Our R&D team explores new and emerging technologies to create a vision of how technology will shape the future and invent the next wave of cutting-edge business solutions. Working closely with Accenture’s global network of specialists, Accenture Technology Labs help clients innovate to achieve high performance. The Labs are located in Silicon Valley, California; Sophia Antipolis, France; Arlington, Virginia; Beijing, China and Bangalore, India.

For more information, please visit: www.accenture.com/accenturetechlabs