Executive Summary

It’s all about the data. Or so it seems from the viewpoint of an information technology executive. Databases, data warehouses, data mining, data transformation, and Big Data—data integration binds all of an enterprise’s disparate applications together. One of the IT manager’s primary responsibilities is to ensure data security; many cloud experts and providers rank security as the top priority (note this importance detailed in “Salesforce.com Service Delivery”). With today’s movement to cloud-based software as a service (SaaS) applications, platforms, and infrastructure, data integration can become even more complex. Although data integration has existed in various forms for more than a decade, in the past few years data integration software has also moved to the cloud—sometimes called middleware as a service or simply cloud integration. This white paper discusses this top priority. It identifies a five-item checklist covering security-related topics that need to be addressed when choosing a cloud integration solution. The paper concludes with a series of key questions to ask when selecting a cloud integration provider.

Architectural Overview

As Figure 1 depicts, there are many levels of cloud computing. The top level, SaaS, includes vendors such as salesforce.com and NetSuite. These are line-of-business software applications that many end users within the corporation access. The next level is platform as a service (PaaS). Cloud integration solutions can reside at both of these levels. The lowest level of the “cloud stack” is infrastructure as a service (IaaS). Vendors such as Amazon and Microsoft offer virtual machine environments that IT departments can provision as needed. These lower levels need a fair amount of “assembly required” (maintaining operating systems and DBMS and building custom applications, for example).
When implementing a cloud-based integration project—such as building an interface between on-premise SAP Financials and Salesforce CRM—data will be exposed outside of the corporate firewall. The IT manager’s challenge is to reduce and mitigate any exposure as much as possible. There are certain information management practices that cloud computing vendors should follow to ensure the confidentiality, integrity, and availability of customers’ data. The issues of end-to-end security, privacy, and continuity are of greater complexity in a cloud computing world than in a single, on-premises data center. For example, enterprise data can be in any of these locations:

- Local storage of the virtual machine (i.e., processing engine): data is tied to the virtual machine location and state
- Persistent data store (i.e., Amazon EBS or S3, Azure SQL, etc.): data is independent of virtual machine location and state
- In transit on the wire (the focus of this paper)
Cloud Integration Security Checklist

This paper provides a checklist to address the most common issues when implementing cloud based security.

- Establishing a solid data governance policy for both on premise and cloud systems
- Identifying a vendor with a solid data center
- Being able to transmit data securely
- Complying with various data and privacy standards
- Verifying the cloud vendor’s audit results

Data Governance

Governance can be a wide-ranging topic, but the focus for this paper is on authentication and authorization. IT managers need to understand how users are authenticated in the integration application and what they are authorized to do. Items to address include:

- **Weak credential-reset mechanisms.** In the past, password-recovery mechanisms have proven particularly weak.
- **Insufficient or faulty authorization checks.** Missing authorization checks can be the root cause of URL guessing attacks. In such attacks, users modify URLs to display information of other user accounts.
- **Coarse authorization control.** Cloud services’ interfaces are particularly prone to offering authorization control models that are too coarse. For example, requiring system administration-level authority for API use is too general to be an effective control. A best practice would be for the cloud integration to support granular role-based permission management to minimize unauthorized access.
- Insufficient logging and monitoring facilities.
Using a cloud environment does not relieve an IT department of its responsibility to ensure that proper security measures are in place for both data and applications. This becomes a joint responsibility with cloud service providers. Additional concerns will arise:

- Who has jurisdiction over data as it flows across borders?
- Can governments access that information as it changes jurisdiction?
- Is there more risk in storing personal information in data centers that belong to a single entity rather than in multiple data centers?

Cloud provider transparency can help IT managers determine whether their service is trustworthy based on profiles and security assurances. The cloud provider should document self-test or simulated attack results that inform enterprises about the provider’s strengths and weaknesses and reveal how their security policies would be addressed. Enterprises can then determine whether they need additional security to tackle any vulnerabilities they see in the cloud.

Insufficient authorization can be addressed via multifactor authentication—whether through the use of one-time password (OTP) tokens, certificates, USB tokens, or smart cards. Possible solutions for identity and access management include IP restrictions (a “white list” of allowable computer access points), strong authentication standards (HOTP, OCRA, TOTP), and entitlement management (XACML) support.

Another key governance issue is privacy. The cloud provider should publish its privacy policy. The IT manager can check to see if this is a “living document”—updated over time or stagnant. And the manager should determine the scope of the privacy policy (apply to all of the cloud provider’s services, or varying policies for separate services). Lastly, if the cloud vendor uses other providers’ services bundled within its own service, does it have a bilateral agreement to hold the other providers to the same standard?

**Data Center Security**

Because the SaaS model is typically provided as a Web-based client or a set of Web services, most of the potential attack vectors are pushed to the provider. This situation implies that the cloud provider handles almost all threat mitigation. Cloud providers typically implement one security model, but have many customers with different demands. Ideally, the provider should attempt to furnish configurable security mechanisms with the following layers and seen in Figure 2:

- **Facility** — Controlling and monitoring physical access to the hardware are high priorities. Surveillance should include closed-circuit cameras and patrolling security guards. In addition to following best practices in separation of privileges/least privilege, you need to have alarm systems, employee codes of conduct, confidentiality agreements, background checks, and restricted visitor access.
• **Network** – Firewalls, dynamic firewalls, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), and network proxies are the basic network devices for protecting the network border.

• **Hardware** – Because the IT department interacts only with a virtualized environment, the provider is responsible for maintaining and monitoring the hardware. Look for hardware audit results that verify configurations have not been tampered with.

• **Physical Operating System** – The cloud provider should deploy a master pared-down OS throughout its cloud. It can then monitor these systems’ images for any changes (and safeguard against the eventuality of malicious customers and intentional attempts to compromise the OS through the customer’s Virtual Machine).

**Provider relationships**

Many cloud application providers do not run their own data centers. The IT manager needs to verify the relationship and strength of the underlying collocation data center. To ensure data confidentiality, integrity, and availability (CIA), the storage provider must offer capabilities that include a tested encryption schema to guarantee that the shared storage environment safeguards all data.

Ideally, the cloud integration solution will not store any enterprise data in the data center. Only metadata that is needed for processing and transforming data should be saved in the data center. Actual customer data would be saved at source and destination targets. An example of this approach is the Informatica® Cloud Secure Agent, which establishes direct connections between enterprise source and target applications.

**Disaster recovery**

Business continuity and uptime are important issues for any enterprise moving to a cloud computing environment. Downtime of the cloud would hinder integration transactions between critical applications, possibly impacting the bottom line. Cloud integration vendors should provide data backup to an offsite location and maintain a resilient incident response model to ensure business continuity for their customers. Additionally, contract provisions might call for service-level assurance details, regulatory compliance, and specification of security policies and terms. The data center should have a comprehensive continuity-of-operations plan, preferably conforming to U.S. Federal Emergency Management Agency standards. The current status of the data center needs to be published on the cloud provider’s trust site. (Informatica offers a cloud integration trust site with real-time visibility: http://trust.informaticacloud.com/status)
Data Transmission Security

The “inside/outside the firewall” paradigm doesn’t work when the enterprise and its competitors and customers are all hosting data, applications, and identity in the same data store (assuming a multitenant implementation). So, security must extend beyond infrastructure and into an integration structure. Most cloud integration solutions provide an agent or gateway that runs on premise (or can be hosted by the provider in an IaaS environment). This component manages the communication and security for the cloud’s entry and exit points.

Gateway security architecture responsibilities fall into five main categories.

- Communication channel security services include transport encryption, transport authentication, proxy services, and protocol bridging. The agent should be able to validate and issue security access to the integrated applications (such as logging in to salesforce.com from the cloud integration system or using XML Signature standards).
- Message security services include integrity (making the message tamper-proof via hashing messages) and message-level encryption—for example, using XML Encryption.
- Message processing includes message transformation and content validation. Ability to support real time versus batch processing. Provide full support of an Integration lifecycle management (frequency and duration of integration task; workflow procedures in a business process).
- Threat protection includes input validation, protection against escaping data, XML denial of service (XDoS) protection, output encoding, and virus protection.
- Threat detection includes systems logging and monitoring, administrative interfaces, and testing through systems management.

Figure 3. Informatica Cloud Secure Agent performs data transfer orchestration and is run locally behind the firewall or can be hosted in the cloud. No data passes through or resides on Informatica servers.
Establishing trust in cloud computing requires identity and data privacy through encryption. It will also require data integrity, which security techniques such as digital signatures and access control can accomplish. Ideally, any enterprise data that is transmitted across the wire is fully encrypted and not decrypted until arriving at the destination.

Data Standards and Connectivity

For many organizations, the prospect of leveraging elastic, pay-as-you-go services for transmitting their expanding volumes of digital assets represents a significant opportunity. But for those that must meet regulatory mandates, security risks posed by keeping information in multitenant cloud storage servers can impose a large hurdle. Depending on the industry, enterprises need to verify that their cloud integration provider can support standards such as HIPAA HL7 and Payment Card Industry (PCI). PCI requires high levels of data protection. Therefore, complying with PCI from an integration perspective will be easiest where data is not stored anywhere in the cloud integration architecture. In some cases, cloud integrators provide pay-as-you-go services, which require PCI-compliant billing processes. Look for connectivity to B2B standards as well (EDI, SWIFT, ACORD, etc.).

Of course, the cloud integration solution must provide secure connectivity to line-of-business data formats (from SAP, PeopleSoft, salesforce.com, etc.). Data must be transformed into standards-based XML format, without compromising firewall security—for example, additional port exposure—plus securing the data envelope as discussed in the previous section. To successfully mitigate application-level threats, the IT manager needs to understand the applications being integrated. Proper training on the application programming interfaces (APIs) and security features provided is critical to successful mitigation. Look for prebuilt process-centric connectivity templates. Many cloud integration vendors also provide a marketplace of prebuilt connectors to various applications and cloud services. These connectors need to be certified and remain supported (see https://community.informatica.com/community/marketplace/informatica_cloud_mall).

Data Audit Results

Wrapping all these items together, data audits encompass the overall reliability of the cloud provider. The IT executive must review and drill down into audit results of the cloud integration environment. Two main compliance vehicles apply to cloud-based integration systems: SAS 70 and ISO 27001. In addition, most experts recommend a mix of the following methods to supplement or serve as an alternative to the standard audits for security in the cloud: background and reference checks; vendor self-assessment and attached evidence (evidence could include PCI security assessments, self-testing, and records from other external audits); on-site audit by the enterprise’s own internal auditors and application of direct controls on the services provider (for example, having vendor employees undertake the organization’s ethics training and sign off on the code-of-conduct policy).

1 The Health Level Seven (HL7) standard addresses complex healthcare information sharing processes.
**Statement on Auditing Standards Number 70 (SAS 70)**

Intended for use by the cloud provider’s auditor, the result of a SAS 70 certification is either a Type I attestation that the processes as documented are sufficient to meet specific control objectives, or a Type II attestation, which additionally includes an on-site evaluation to determine whether the processes and controls actually function as anticipated. SAS 70 is only a generic guideline for the preparation, procedure, and format of an auditing report. It places the onus on the service recipient to ensure that all controls relevant to the recipient’s requirements are examined.

Type II audits include an examination of controls that have been placed in operation and testing of operating effectiveness. Testing of controls is required for Type II audits, with a testing period ranging from 4 to 10 months (usually at least 6 months). Testing is conducted throughout various predetermined timeframes throughout the evaluation period and in a manner that significantly mitigates any type of business interruption.

The IT manager needs to be careful about the use of the terms “SAS 70 certified” or “SAS 70 compliant,” which may imply guarantees or the meeting of statutory or regulatory requirements that don’t exist. A vendor voluntarily engages an auditor to prepare the report, and there may be no specific criteria for its content. Simply having a report doesn’t mean the audit was rigorous; no auditor uses words like all and always (which imply a guarantee); and auditors’ SAS 70 opinion letters explicitly note that they make no forward-looking representations. Further, the services auditor makes one overall evaluation rather than expounding on the environment control by control.

Most basically, a cloud vendor must show corporate procurement and finance officers that it has controls over the integration process entrusted to it in place. We recommend that at least the Type II certification is in place and up to date. Here is an example of this type of transparency: [http://trust.informaticacloud.com/security](http://trust.informaticacloud.com/security). Also, maintaining the SAS 70 compliance needs to be written into service-level agreements between enterprises and outsourcing organizations.

**ISO 27001 Standard**

ISO/IEC 27001 specifies requirements for the establishment, implementation, monitoring and review, maintenance, and improvement of a management system—an overall management and control framework—to handle an organization’s information security risks. It does not mandate specific information security controls. The standard covers all types of organizations (e.g., commercial enterprises, government agencies, and nonprofit organizations) and all sizes from micro-businesses to huge multinationals.
ISO 27001 encourages sustainable, directed, and continuous improvement security control. This standard incorporates several plan-do-check-act (PDCA) cycles: for example, information security controls are not merely specified and implemented as a one-off activity but are continually reviewed and adjusted to take account of changes in the security threats, vulnerabilities, and impacts of information security failures, using review and improvement activities specified within the management system.

Again, the IT manager needs to verify the depth of the ISO 27001 compliance document with the cloud provider. When was the last time the audit was completed? Review the “Key Findings” and recommendations report. And then drill down on these issues for satisfactory resolution.

**Recommendations**

This paper provides five key checklist items that IT organizations need to assess when implementing cloud-based integration. The cloud integration solution must provide more than a bunch of connectors and data encryption. IT managers need to modify the enterprise’s data governance policies to incorporate cloud-based data transmission; verify that the underlying data centers are secure; make sure that the provider complies with standards that are important to IT; and drill down on the audit reports delivered by the cloud service. Here are some key questions to address when evaluating cloud integration providers:

- Does the cloud integration solution provide a granular level of access control?
- Has the data center employed standard employee checks and surveillance practices?
- Are the various connectors important to your business supported?
- Is data encrypted from end to end during transmission?
- Has the provider passed both SAS 70 Type II and ISO 27001 audits? Verify the results.

Security controls in cloud computing are, for the most part, no different from security controls in any IT environment. However, because of the cloud service models, the operational models, and the technologies used to enable cloud services, cloud computing may present different risks to an organization than traditional IT solutions. Leveraging cloud integration can empower line-of-business divisions with self-service capabilities while ensuring strong operational data governance.
About Informatica

Informatica Corporation (NASDAQ: INFA) is the world’s number one independent provider of data integration software. Organizations around the world gain a competitive advantage in today’s global information economy with timely, relevant and trustworthy data for their top business imperatives. Worldwide, over 4,280 enterprises rely on Informatica to access, integrate and trust their information assets held in the traditional enterprise, off premise and in the cloud. For more information, call +1 650-385-5000 (1-800-345-4639 in the United States), or visit www.InformaticaCloud.com.

About Mercury Consulting

Mercury (http://www.mercuryinthecloud.com/) is your trusted cloud technology advisor, specializing in integration services. We make your adoption of cloud services easier by bringing our deep expertise to design your cloud enterprise and provide unbiased guidance on cloud vendors and their SaaS solutions.