ATLASSIAN

Evaluating Vendor Risk Management:

A quick guide to a streamlined security evaluation process

Why it's important to have a standard cloud vendor evaluation

In a recent survey by McAfee, researchers found that organizations use a staggering number of unique cloud services–nearly 2000 on average–though most believe they only use about 30.

Given the potential risks of storing sensitive data in the cloud, conducting a thorough security evaluation of each service is both critical–and can also be overwhelmingly time-consuming.

According to the Cloud Security Alliance, IT professionals reported that they receive more than 10 requests each month for new cloud services. Some of those requests may be from different teams–but for the same service, potentially creating duplication of efforts. Sifting through these requests and manually assessing the security practices of each cloud vendor can require tens of hours of work per person, making IT a bottleneck to productivity and innovation.

In order to relieve your team of this time burden, you can design a standard, repeatable cloud vendor security evaluation checklist that streamlines the process while ensuring your security requirements are covered.

> There are many ways to assess risk, ranging from an in-depth, matrixed approach favored by some enterprises, to a simpler 'low-medium-high' risk-scoring model.

Establish security risk criteria and a scoring system

Every organization will have its own security priorities and definitions of risk for the purpose of determining who should have access to data and services–and what protections must be put into place. Factored into these priorities are the industry and security standards the organization has to meet, as well as applicable laws.

As you design your evaluation process, you can include a risk score that helps you prioritize vendor security features and practices. There are many ways to assess risk, ranging from an in-depth, matrixed approach favored by some enterprises, to a simpler "low-medium-high" risk-scoring model. However you approach your assessment, in general, it should include:

1. Defined categories of risk, scored based on the impact of a breach

2. Likelihood or probability that a particular risk will occur

Here is a sample list of data security risk categories, organized by the severity of impact, should a breach occur:

SECURITY RISK CRITERIA

 **LOW RISK**	• The data is public, or could be made public, without impact. • The loss of data or system integrity or availability would not have a significant impact.
 **MODERATE RISK**	• The data is generally not available to the public, and there are no plans to release it publically. • The loss of data or system integrity or availability could have a negative impact, but would likely be recoverable.
 **HIGH RISK**	• A law or regulation requires the protection of the data, and it's required to report or give notice if the data or system is breached. • The loss of data or system integrity or availability could have a significant adverse impact. • The vendor will store or come into contact with sensitive data, including trade secrets, source code, or customer data. • Personally identifiable data (PII) is stored in the application. • If the cloud service were to go down it would have a significant impact on business operations.

Cloud Security Evaluation Criteria

What you ask of your cloud vendors depends on how you're using their products, your organization's standards, and your security and change compliance needs. Here are the most common categories of inquiry you should consider as you evaluate SaaS vendors:

CLOUD ARCHITECTURE

Speed, scalability, and reliability: Is the SaaS application hosted in an environment architected to automatically distribute processing functions, reducing latency, and maximize speed and data accessibility?

Investigate the architecture of the cloud vendor–even if the application is hosted in a public cloud, such as AWS, Microsoft Azure, or Google Cloud. As organizations grow–especially those with globally distributed teams–so does the volume of content and data they work with. Look for vendors that incorporate edge computing with centralized cloud computing for maximum flexibility in computing power and data availability.

AUTHENTICATION AND IDENTITY

Multi-factor authentication: What types of authentication does the vendor support (SMS, phone token, one-time PIN, authenticator app, etc.)?

Two-step verification adds a second login step for user accounts, usually requiring them to enter a code in addition to their password when they log in. The second step helps keep user accounts secure, even if the password is compromised.

Identity federation method: Which single sign-on (SSO) methods does the vendor support?

SAML SSO, an open standard, is the predominant means by which you can enable the secure communication of identities between organizations through authentication and authorization functions. It is most often used to gain SSO functionality between an Identity Provider (IDP) and a Service Provider (SP). This capability can provide more complete audits, by capturing all of a user's actions after they log in.

Enterprise identity: Does the vendor support integration with enterprise directories, such as Active Directory or cloud identity providers?

You may already use an on-premises solution like Active Directory to manage user accounts. As you integrate SaaS products into your application ecosystem, consider the need to centralize identity management and automate user provisioning with a cloud identity provider. Look for cloud applications that enable these types of integrations.

Application- and feature-level security: Can you control application access or access to specific types of data and content beyond each user's role?

When you control access based on risk factors including location, network, device restrictions, type of request, and timing, you go beyond simple role-based access. This allows you to comply with regulatory and statutory requirements for confidentiality and privacy, decreasing the risk of security breaches and data leakage.

DATA SECURITY

Sensitive customer data: What access controls are in place?

In some cases, even cloud application administrators should have limited access to customer data. Ensure the vendor has a process in place to explicitly request access to customer data, as in the case of support activities, for example.

Encryption for data at rest: Does the vendor encrypt data at rest in databases, file systems, or the virtual machine layer?

Data encryption at rest ensures data is continuously encrypted, even while resting in one product or app. Look for cloud application vendors that use the standard Advanced Encryption Standard (AES) encryption.

Encryption for data in transit: What modes of secure socket layer (SSL) or transport layer security (TLS) does the vendor support for protecting data in motion?

Know which protocols the vendor uses to provide communication security to protect data from unauthorized disclosure or modification over public networks.

APPLICATION SECURITY

Secure coding practices: Are applications developed using verified secure coding practices?

Many SaaS products release new features and updates on a frequent basis. Understand what measures the vendor takes to ensure privacy and security best practices are implemented in the application lifecycle management process.

Penetration testing: Does the vendor have a report of past pen tests, and do they perform them regularly?

Penetration testing, or the intentional hacking of a system, network, or application is a part of holistic security strategy. Ask for reports of past pen tests, and follow up with any concerns about weaknesses or failures.

Response to externally reported threats: Does the vendor have a process by which users can report vulnerabilities or bugs?

Look for a vendor that has an ongoing vulnerability reporting program. Instead of relying on a single

"moment in time" for security testing, programs like a public bug bounty can enhance the ongoing security of cloud applications.

INTERNAL CONTROLS

Data center protections: What protections are in place to secure physical data centers?

Many cloud application vendors employ public data center hosting partners, and those partners are responsible for the physical security of the data center. In cases where the vendor hosts the application in its own data center, confirm it limits access to only authorized personnel, and ask for verification of secure access methods.

User activity logging: Does the provider offer logs of user activities? Can you review, access, or synchronize logs with your own logging and alerting applications? Does the vendor log key user login and authentication, data access, and account management activities?

In the event of a security incident, logs and audit trails are required to investigate and understand how an application was exploited. Ensure you can migrate log files for storage and analysis.

TRANSPARENT SECURITY MANAGEMENT PROGRAM

Documented security practices: Does the vendor have a publically available security management program?

Look for a vendor that makes available detailed security and privacy practices. This should include the application development process, operational practices, compliance certifications, and what to expect in the event of a security incident.

Known breaches: Has the vendor reported any data security breaches in the past?

Security incidents are common, so be wary of any vendor that claims they don't have any. Look for postmortem reports on how the company handled past incidents.

Uptime and SLAs: Does the vendor commit to uptime, with verification? Does the vendor provide real-time uptime portals, and is the vendor transparent about maintenance or downtime windows?

Look for evidence of adherence to uptime policies and a public-facing source of information about scheduled maintenance, incidents, and outages, with transparency about how long it takes to resolve an issue.

ASSOCIATIONS AND CERTIFICATIONS

Certifications: Which compliance certifications does the cloud service provider have?

Depending on your industry, the sensitivity of your customer data, and if and how your organization is subject to government regulations, you may have specific security requirements. In general, your vendor should have standard security and technical certifications, such as Service Organization Controls (SOC1 or SOC2) and security management certifications, like ISO27001.

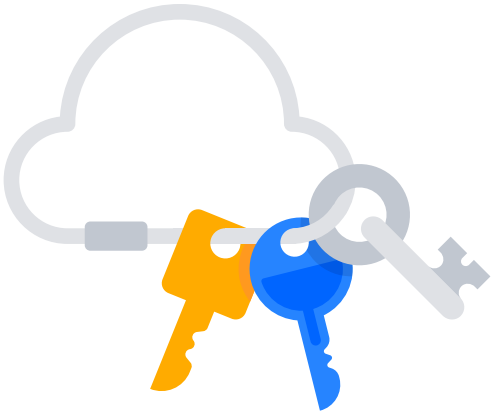
Cloud Security Alliance (CSA): Is the vendor engaged in the cloud security community and a member of associations like CSA?

The CSA is a research organization that determines the best practices for secure cloud computing and authors one of the best-known cloud service frameworks and standards. Look for a vendor that has submitted completed security questionnaires with the CSA Security, Trust and Assurance Registry (STAR) of cloud service providers.

When you finalize your standard evaluation criteria for your cloud vendors, document it and make it available to the people in your organization involved in the sourcing and procurement of cloud services. With a standardized process, you can make sure that each vendor is thoroughly vetted–and that members of your IT team don't have to jump in and run every evaluation process.

Next steps

Learn more about how to scale and govern your Atlassian cloud products with this 10-step plan, designed for both the seasoned SaaS administrator and those just beginning their cloud journey. In this presentation, Dave Meyer, Principal Product Manager at Atlassian, will share his top recommendations for governance, user management, and security for Atlassian's cloud products.



ATLASSIAN