Establish Effective SaaS Governance in Your Organization

Published 16 December 2020 - ID G00738421 - 11 min read
By Analysts Jay Heiser

Initiatives: Security of Applications and Data; Technology, Information and Resilience Risk

Organizations require a comprehensive and continuous approach for the controlled use of software as a service. Executive leaders should enable the adoption of an effective SaaS governance approach to meet their business goals and prevent unnecessary losses or incidents.

Overview

Key Challenges

- The best practices for the control of SaaS are still evolving, with only a partial consensus on standards, approaches, policies, staffing or tooling.

- Organizations using SaaS often fail to capture their operational requirements and, consequently, fail to anticipate the governance shortcomings of SaaS offerings.

- Organizations that govern their use of SaaS can significantly reduce unnecessary security, compliance and financial risks.

- Inattention to SaaS governance leads to ad hoc controls and incomplete visibility over SaaS use. This makes it impossible for most organizations to determine, report on and reduce exposure to security, compliance and vendor risk.

Recommendations

Executive leaders looking to adopt a strategic approach to SaaS governance should:

- Collaborate with the IT function to establish a foundational directive on acceptable uses for SaaS, how it should be controlled and who should be explicitly responsible for enforcing policy.

- Enable cost-effective, productive, legal and regulatory compliant, and secure use of public cloud applications by supporting a SaaS “competency center.”

- Facilitate the assessment of the optimal level of oversight for each SaaS application by adopting a life cycle approach to SaaS governance.
Introduction

This research is adapted from How to Develop a SaaS Governance Framework, which enables CIOs to work with other business leaders in establishing an effective SaaS governance framework.

The procurement and use of SaaS outside the IT function’s visibility often represents an acceptable level of risk. However, it should not be automatically assumed that a particular service is appropriate for use, or that it is being used beneficially. Governance addresses how risk acceptance decisions and control needs are embedded in policy and applied in practice. Explicit attention to the governance of SaaS use ensures that corporate goals are set, control tasks are assigned, outcomes are tracked and status is reported.

This research introduces an outline for a life cycle approach to effective, secure and compliant SaaS use, based on people, policies, processes and products.

Analysis

SaaS Governance Approach

The lack of explicit control of SaaS use risks the creation of countless unconnected channels that are difficult to detect and more expensive to administer and protect. Each SaaS application in use becomes an identity and a data island that must be managed separately, with isolated manual provisioning processes often introducing security gaps and exponentially complicating activity monitoring. SaaS applications that lack IT assistance may never fully meet business unit (BU) needs for sharing content with other applications or business partners. They may be out of compliance with the contractual requirements that customers impose on the organization.

Organizations that have installed technology to track SaaS use consistently find their employees storing regulated and sensitive data in their personal cloud-based accounts. This raises concerns about both security and regulatory compliance.

A SaaS application is not just a one-time project. It requires ongoing management to a degree commensurate with the relative significance of its use case. As illustrated in Figure 1, SaaS governance requires a complete life cycle approach. Unfortunately, most organizations concentrate on only the bare minimum effort needed to initiate the use of a SaaS service.
As shown in the lower right-hand box in Figure 1, most organizations focus on analyzing the immediate requirements across functions, ignoring the longer-term issues of management and capability augmentation. Even when a risk acceptance process is conducted, it ends up being based on an incomplete analysis of requirements. Once they've been provisioned, most SaaS applications are on their own, without a great deal of overt attention. While many low-criticality SaaS applications need little further oversight, those that are of critical importance, or that contain sensitive or regulated data, should receive explicitly defined levels of control, proportional to data criticality, across the remaining phases of their life cycles.

A growing number of organizations are creating new multidisciplinary teaming arrangements for SaaS life cycle governance. These typically include application specialists, vendor managers, business architects or strategists, and security or compliance professionals.

Executive leaders should ensure that this sort of new function has adequate resources and that it has the power to enforce SaaS selection and use rules. Large BUs increasingly have their own application...
specialists, with full or partial responsibility for ensuring the successful use of SaaS.

Create SaaS Governance Policy, Define SaaS Use Process and Identify Risk Owners

No effective governance is possible without some form of written directive to set the rules and provide a basis for enforcement. At a minimum, executive leaders should work with the IT leadership to establish three basic SaaS control policies: approve SaaS use through a defined process, identify SaaS risk owners and ensure a cloud application inventory is maintained.

Approving SaaS use through a defined process does not necessarily mean approaching IT to veto every request to use SaaS. Instead, executive leaders should engage their direct reports with IT to create a flexible and practical process for how they can work together to acquire new SaaS capabilities.

If the IT function is not maintaining responsibility for a particular SaaS application, then the owner is typically a BU manager or department head. For larger organizations, it may be necessary to track multiple defined roles:

- **Risk Acceptor**: This is typically the department head who pays for the service. This person agrees to enforce relevant policies on use and explicitly agrees to “accept” the residual risk, including responsibility for security or continuity failures.

- **User Administrator**: If a service is not explicitly administered by IT, then a specific individual (and backup) must be responsible for account creation, maintenance and deletion. This individual should coordinate with the risk acceptor to determine the disposition of data from deleted accounts.

- **Other Privileged Accounts**: The greater the number of users, the more important it is to have multiple privileged users or administrators who can reset passwords or provide other forms of support. However, an excess of privileged accounts presents unnecessary risk. An effective balance is often between two and four accounts, with additional levels of administrative access.

- **Support**: This involves someone who provides the first level of support and is responsible for escalating problems to IT or the SaaS vendor. A more sophisticated level of support might also include a second tier of support that provides customization or even integration.

Executive leaders should also ensure the defined approval and responsibility acceptance processes include a formal registration of SaaS use with IT. If more than a few dozen SaaS services are in use, then it is usually necessary to formally track them. At a minimum, the tracked information should include:

- The name and type of SaaS service
- The owner (and other roles, if used) — for example, user administration, support, vendor liaison and so on
- Data sensitivity or significance — for example, confidentiality, integrity, availability/mission criticality and regulatory compliance
Analyze Control Requirements

Every stage in the SaaS governance life cycle could imply specific features, functions or service levels. Without a defined SaaS requirements collection process, they may fail to fully specify needs for control mechanisms, interoperability and monitoring. Thus, executive leaders should ask IT to prepare a list of preapproved SaaS products, along with guidelines on their appropriate use, in order to reduce the need for a full requirements analysis for every SaaS buy.

It is not always necessary to acquire application services that include all desired control and integration features. Most organizations are using some combination of third-party control products to add additional controls or functionality to SaaS services.

In many cases, even with add-on control tools, it will be impractical to find a SaaS service that meets all requirements for activity or data governability. This doesn't mean they can't be used; however, if the use case is sensitive, the executive leader should formally acknowledge and accept the residual risks (often referred to as “risk ownership”). As departments become more free to make decisions on the use of SaaS services, executive leaders should also ensure the IT function monitors how the service is used and what data is stored in it.

Prioritize Risk Assessment to Select Your SaaS Provider

Organizations typically use a wide variety of externally provisioned services, representing different control challenges (see Figure 2). Different public cloud use cases will represent different forms and levels of risk exposure.

---

**Figure 2. The Spectrum of Cloud Applications**

<table>
<thead>
<tr>
<th>Spectrum of Cloud Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Most Similar to On-Premises Governance</strong></td>
</tr>
<tr>
<td>IT-Sponsored for Entire Enterprise</td>
</tr>
<tr>
<td>- IaaS and PaaS</td>
</tr>
<tr>
<td>- Cloud Office and Collaboration</td>
</tr>
<tr>
<td><strong>Department-Sponsored</strong></td>
</tr>
<tr>
<td>- Strategic Services Administered by IT</td>
</tr>
<tr>
<td>- Strategic Services Administered by BU</td>
</tr>
<tr>
<td>- Nonstrategic Services Supported by BU</td>
</tr>
<tr>
<td><strong>Individual Decision</strong></td>
</tr>
<tr>
<td>- Collaboration, Social Networking, Other</td>
</tr>
<tr>
<td><strong>Partner-Imposed</strong></td>
</tr>
<tr>
<td>- Collaboration, Other</td>
</tr>
</tbody>
</table>

Source: Gartner (February 2020)
ID: 382961_C
The risk assessment and supplier decision should be based on the expected ability to meet functional and risk control requirements using the SaaS application in the context of SaaS control processes, as well as the organization's SaaS governance technical capability. The variety in SaaS circumstances, in addition to the sheer number of SaaS applications in use, means that one-size-fits-all approaches to SaaS approval cannot scale to cloud needs. Approaches that can optimize SaaS usage requests include:

- Variable levels of risk assessment rigor, in which the level of effort is proportional to the data or use-case criticality. This risk-based and pragmatic approach will ensure that strategically important use cases are well-analyzed, without unnecessarily reducing the flexibility to quickly deploy SaaS on a departmental basis. It facilitates the use of noncritical SaaS applications, without wasting time on unnecessary levels of review. This approach can succeed only if it is clearly enshrined in policy and supported by the executive team.

- A self-service questionnaire that provides an initial risk score based on the type of data, number of users, need for external access and so on. Low scores can be automatically approved; higher scores require assessment by a security architect and/or approval by a governance team.

- List of SaaS services that are preapproved for specific uses, or forms of data without the need for additional assessment.

**Be Cautious of Free SaaS**

Services offered for free are never an appropriate place to store sensitive data. Free services may reserve the right to look at their client's data for marketing or research and, in a few cases, may even claim ownership of user data. Cloud access security broker (CASB) tools can help monitor and control the use of all forms of externally provisioned applications, including free SaaS and social networking. The SaaS governance approach, including policy and technical controls, should take into account the ubiquity of free services.

**Initiate SaaS Service**

Once a decision has been made to use a SaaS service, the time and difficulty of startup vary widely. A relatively simple application used by a small number of people can be productively used within days, or even minutes. However, a more strategically important application intended to be used by the entire organization can take almost as long to implement as traditional in-house alternatives. Major governance tasks during the implementation phase include:

- **a. Purchase**
  The price and any desired contract terms should be agreed on before fully committing to the use of the service. SaaS vendors are rarely flexible about substantive contract provisions, and smaller vendors can have cash-flow problems that affect their future ability to live up to their agreements.

- **b. Implementation**
Many simple SaaS services used on a casual basis have minimal implementation needs. Applications with a significant impact on the organization, especially systems of record, can require a significant level of effort to begin operation. This may involve a multiyear process of data migration, software optimizations, changes and integrations. SaaS can reduce some of the effort involved in implementing business applications; however, some tasks require the same level of attention and time as on-premises or hosted deployments. Integration, configuration and extensions increase the cost of SaaS implementation, support and maintenance, which must be kept in check.

c. User Provisioning
If the new service can be integrated with the existing corporate directory service (and existing multifactor authentication mechanisms, if desired), then the provisioning of user accounts is relatively simple. If user federation or synchronization is not possible, then someone (usually not in IT) must be responsible for manually creating and maintaining user accounts.

d. Data Migration
An entirely new form of service that hasn't been used by the organization before requires no data migration. However, a change in a form of application that is already in use may require an extensive migration process.

e. Contingency Planning
No SaaS application should be used before the service owner formally states the business objectives for recovery time and completeness. If the data or processes in the service are not mission-critical, then there may be no need for a formal contingency plan. If the data is considered critical, a plan should be created that specifies how the data will be recovered in case of a provider business or technology failure and how it will be repurposed in some other service. SaaS contingency planning is not a mature practice area, and, in many cases, protecting against provider failure will not be practical. When contingencies cannot be directly mitigated, higher levels of continuous vendor monitoring are indicated.

Enable Continuous Management
Executive leaders should enable IT to provide continuous management and support for every anticipated activity and possible contingency. This includes routine periodic tasks and response tasks when a failure or unplanned event takes place.

Otherwise, executive leaders need to ensure that people in their own departments are aware of their roles and have the resources to perform them. We are increasingly seeing this function fulfilled by centralized SaaS support or cloud competency centers run by IT, as well as an increase in BU SaaS application specialists.

Manage End of Life (Planned and Unplanned)
The final phase of SaaS control activities involves the closing down of a service and safely deprovisioning it before the vendor is no longer contractually obligated to maintain your data.

Exit
strategies are usually not maintained for all applications in the in-house portfolio. However, if a SaaS vendor provides short notice of change or shutdown, or worse, ceases operation without warning, it can leave customers without recourse. Executive leaders should facilitate some level of exit planning before it’s actually needed. Some of the critical exit activities include data migration and redeployment, and data destruction and/or archiving.

Recommended by the Author

What to Include in Your SaaS Security Policy

Embrace Vendor and Asset Management to Effectively Manage SaaS Applications

Align Your Cloud Strategy With the Organizational Strategic Plans

4 Steps to Successful SaaS Negotiations and Vendor Lock-In Prevention