



Guide to Controlling SaaS Costs and Risk

Implementing a SaaS Management Lifecycle

Software-as-a-service (SaaS) is overtaking business software environments.

Projected to capture more than \$116 billion in revenue in 2020—a 17% increase year over year—SaaS tools are used by more businesses, more than ever before.

In its annual State of the Cloud report, Bessemer Venture Partners states that “the cloud is eating software” and projects that by 2025, more than half of all enterprise software environments will be cloud-based. The majority of these applications will be SaaS.

But for many organizations, the growing use of SaaS-based business tools presents enormous challenges. Even though SaaS technology has existed for more than two decades, many organizations and teams struggle to manage this category of software effectively.

Specifically, businesses frequently struggle to define the total cost of their organization’s investment in SaaS and to mitigate its risks.

Based on the experience from implementing SaaS Management in more than 100 companies, Zylo has developed a SaaS Management Lifecycle that establishes an open framework and continuous process for identifying, optimizing, planning, and governing SaaS within a large organization. The Lifecycle creates the ability to immediately address controlling SaaS costs and risks while also providing a plan for secure and optimized SaaS growth.

Projected to capture more than \$116 billion in revenue in 2020, SaaS tools are used by more businesses, more than ever before.

Source: Gartner

Why SaaS Management Matters Now

It's impossible to account for what you cannot see, and rogue SaaS spending has grown to become a massive blind spot for many businesses due to several factors:

Shifts in IT spending to business units

Software purchases on behalf of the business used to be managed exclusively by the IT team. Enterprise software was built to enable entire organizations and required technical expertise to deploy, as well as hardware-based assets such as servers to host the software.

In the early 2000s, software spending began to shift towards individual business units as software publishers began creating business-unit specific products. Salesforce creating software exclusively for sales teams, Adobe marketing tools to creative teams, and so on.

Today, IT controls 42% of SaaS spend, but manages just 25% of SaaS applications, which increases organizational costs and risk.

Product-led growth

In the early 2010s, software spending underwent another shift - this time towards individual teams and employees. With the rise of product-led growth strategies leveraged by software makers such as Slack, Zoom, and Box, SaaS applications have increasingly become acquired not by IT or specific business units, but teams and employees.

The products then spread organically across the organization, often creating enterprise-wide deployments. This trend has also been called the end user era of software because the end user, aka the employee, now selects and acquires software, not IT and not specifically business units.

Shadow IT

An unfortunate outcome of the end user era is the corollary growth of shadow IT: when tools and applications enter an organization's IT environment unbeknownst to IT.

Shadow IT can lead to increased risks and compromised security as applications unknown to IT or IT security teams go unvetted for risk or vulnerabilities that could lead to data breaches or other issues, which carry significant consequences and costs. According to an IBM-Ponemon Institute cybersecurity study, **the average data breach in the United States costs more than \$8 million.**

A company's compliance with regulations that protect personally identifiable information (PII), such as the European Union's GDPR or the United States' HIPAA, can also be put at risk due to shadow IT.

Finally, Shadow IT creates unmanaged costs beyond the initial purchase price as free trials convert to paid subscriptions and multiple purchases of the same application increase license numbers and per unit costs.

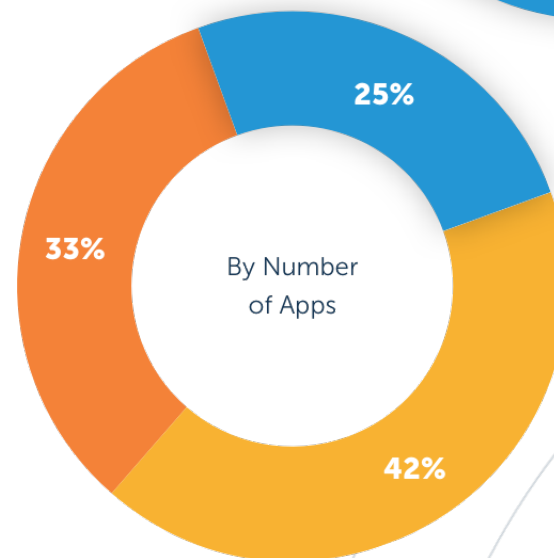
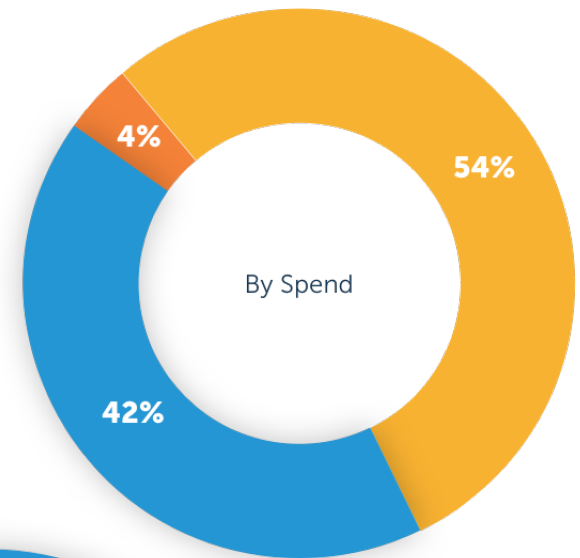


*Shadow
IT Grows
in the End
User Era*

*IT controls 42% of SaaS spend, but manages just 25% of SaaS applications, **which increases organizational costs and risk.***


Source: Zylo

- Business Units
- Employees
- IT





How to Start Managing SaaS



As organizations increasingly recognize the urgency to control costs and manage risks associated with SaaS applications, a logical next step is to ask, how?

Based on these common themes and its experience helping hundreds of businesses incorporate SaaS management into their existing technology management processes,

Zylo has developed a SaaS Management Lifecycle to enable SaaS management.

Every organization's technology profile carries unique challenges; this is especially true with the use of SaaS. However, many organizations face the same problems:

- ✓ **Poor management of SaaS licenses**
- ✓ **Lack of visibility into how SaaS applications are being purchased**
- ✓ **Lack of spend or utilization data about SaaS**
- ✓ **Little to no planning for SaaS renewals**
- ✓ **Lack of monitoring of new incoming applications**
- ✓ **No framework for managing SaaS across an organization**
- ✓ **No central system of record for SaaS applications**

The Zylo SaaS Management Lifecycle

The SaaS Management Lifecycle represents an open, flexible framework that any company can immediately use to start managing SaaS applications more effectively.

Organizations can begin the Lifecycle in any phase, then work towards developing a more mature SaaS management process as short-term needs are met.

The objective of the SaaS Management Lifecycle is to create both immediate and long-term actions to control spending and reduce risk.





Discover

Identify every SaaS application within the organization

For many organizations, discovering the entire inventory represents the first step in developing SaaS management processes. Most organizations underestimate the number of applications operating within their environment. Zylo data shows that a large organization (1,000 employees or more) maintains about 600 applications.

However, companies consistently underestimate the quantity of applications used by their organization.

Large organizations maintain on average 600 SaaS applications, only 25% of which are managed by IT.

Multiple methods exist for discovering and inventorying SaaS applications and their attributes.

✓ **Manual spreadsheet inventory**

Technology-owning teams may survey their organization, requesting teams and employees to self-report their SaaS application uses. This approach can be problematic for larger organizations due to the length of time it takes to collect the information, the high likelihood of inaccuracies in reporting, and the lack of continuous monitoring needed to keep an up-to-date inventory.

✓ **Cloud access security broker (CASB)**

CASBs are primarily designed as security tools intended to be installed on hardware, monitoring data that flows between the company and cloud-based data centers. However, if end users access applications on a personal device, that data will not be reported, making the ability to discover all SaaS limited.

✓ **Web browser plugins**

Browser plugins can help sniff out SaaS tools. These plugins are installed on company-managed devices and capture details about application usage based on browser activity. This approach is relatively affordable and straightforward to implement. However, it can be somewhat easy to circumvent. If an end user bypasses traditional web browsing by enabling private or incognito mode, usage data regarding SaaS applications will go uncollected which can increase costs and risk.

✓ **Single sign-on (SSO)**

SSO tools can significantly improve SaaS application management. With one set of login credentials, users can access a wide variety of applications. However, as a discovery tool, SSO is a partial solution at best, as only IT-managed applications are typically added to an SSO platform. The use of personal devices to access SaaS applications or circumventing SSO with a manual sign-on can prevent full discovery.

✓ **Financial analysis**

Finance-based SaaS discovery involves analyzing financial records to uncover any SaaS purchases. By analyzing Accounts Payable and expense reimbursement records, SaaS spend through IT, business unit, and end user accounts can easily be tracked and inventoried.

By tracking the money, an organization can identify all SaaS tools being utilized, regardless of the procurement process. This approach is also feasible from a compliance perspective as no PII is necessary to uncover all applications. For some organizations, providing the needed access to financial data prohibits the use of finance-based discovery.



Build a system of record for SaaS applications

When completing a discovery process, it's of crucial importance to record multiple characteristics for each application. This ensures that SaaS applications and their metrics can be compared apples to apples.

These data fields can and will form a system of record that allows technology managers to make informed decisions about the ongoing use of each application, as well as opportunities to reduce costs and optimize future spending.

A system of record can take the form of an actively managed spreadsheet or an automatically updated inventory provided by a SaaS management platform like Zylo.

Ideal SaaS application attributes to capture in a system of record:

- **Total spend on each application**
- **AP vs. Expensed purchases**
- **Ownership (business unit, team, employee)**
- **Categorization, function**
- **# of licenses/seats/users**
- **Compliance status (if applicable)**
- **Security profile**
- **Contract terms**
- **Renewal date, notification period**

Monitor the environment for new incoming SaaS applications

Once the discovery process has established the current state of SaaS inventory, it's essential to monitor the environment for new incoming applications continually and update the system of record. Zylo data shows that an average large company may see as many as ten new SaaS applications enter their environments every 30 days. Without an ongoing process that discovers and monitors these new applications, the inventory becomes out of date quickly and shadow IT may once again grow.

Other factors also signal the need to monitor and update the SaaS application inventory continually. Employee attrition is a prime example of why managing SaaS on an active basis is a vital safeguard against risk.

When an employee leaves the organization, all access to their SaaS-based applications should be terminated to prevent potential data leaks or breaches. More than half of all data breaches are due to malicious or criminal attacks, according to IBM and the Ponemon Institute's 2019 data breach study, and these attacks have been known to be instigated by disgruntled former employees. Unsecured and unmonitored SaaS applications represent a vulnerability to these types of attacks.



An average large company may see as many as ten new SaaS applications enter their environment every 30 days.



Optimize

Identify ways to control SaaS spend and increase efficiencies

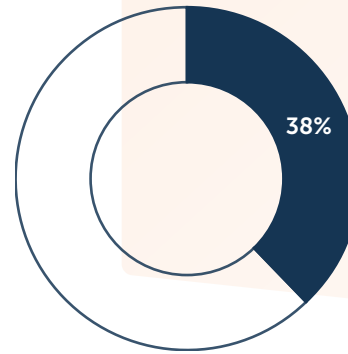
According to Zylo data, it costs about \$4,000 per employee per year to provide SaaS tools and services needed to be effective at their job. However, with a reliable SaaS management program in place, organizations can quickly reduce costs, both short term and long term.

*It costs about **\$4,000**
per employee per year
to provide SaaS tools
and services.*

Reduce underutilization of SaaS licenses

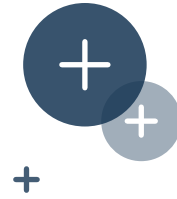
Zylo data shows that 38% of all SaaS licenses go unused in a 30-day period, meaning that more than \$1,500 of each employee's SaaS spend is potentially wasted. Effective SaaS license management represents an opportunity to reduce costs and increase value.

An underutilized SaaS license can be traced back to its assignee, who can then be queried about their need (or lack of need) for the license. If the license is genuinely unnecessary, it can be deployed to another user or eliminated to reduce costs.



*But **38% of all SaaS licenses** go unused in a 30-day period*

*Meaning that **more than \$1,500** of each employee's SaaS spend is potentially wasted.*



*Up to **12% of all SaaS applications** in a large organization are the result of duplicated purchases.*

Consolidate duplicated SaaS applications, overlapping functionality

According to Zylo data, up to 12% of all SaaS applications in a large organization are the result of duplicated purchases. For example, a Marketing team requires a project management application and acquires an application like Asana. In another part of the organization, and unbeknownst to Marketing, an HR team also needs a collaboration tool and also purchases Asana.

In this scenario, the teams are not combining their purchasing power, as SaaS products typically cost less per user as more users are added.

Most Common Categories for Overlapping Applications

- Project Management
- Web Conferencing
- Sales Intelligence
- Team Collaboration
- File Storage and Sharing

Another common inefficiency occurs when multiple applications are purchased to perform the same function.

To reduce costs when overlaps are identified, a technology manager should identify the functional overlap, then propose standardizing both teams (or the entire organization) on a single tool. This standardization on a single tool would consolidate maximum purchase power and ensure uniform functionality and access to data across all teams.

However, note that teams and individuals may establish different requirements for tools, and legitimate reasons may exist for having a variety of tools to complete the same function.

*A SaaS application approval process can help **prevent rogue spending and Shadow IT***



Prevent shadow IT to reduce cost and risk

Reducing shadow IT and preventing inefficient SaaS purchases can be accomplished by rethinking the SaaS acquisition process.

One in three employees in a typical large organization has purchased a SaaS application using expense reimbursement, according to Zylo data.

One of the ways organizations have stymied this activity and its resulting contribution to shadow IT growth is by prohibiting expense reimbursement for SaaS applications or defining expense reimbursement thresholds.

Create a SaaS application approval process

Another avenue to prevent rogue spending is the establishment of an approval process for any new SaaS application. One such option is a software review board that must green-light any new tool acquisition. Instead of an outright purchase, a team or employee submits a request to purchase an application and defines its use case.

The review board, composed of stakeholders from teams such as Legal, Finance, IT, IT Security, Sourcing/Procurement, reviews each request and checks the request against the current inventory of in-use applications.

This process may take more time but can prevent unnecessary spending and risks in the future.



Plan

Forecast future SaaS spend with utilization data

One side effect of SaaS creating shadow IT within organizations is that it impedes the ability for CIOs and CFOs to forecast future spend accurately. Without a continually updated view of all apps across the organization—IT managed, department managed, and individually purchased—forecasting spend is nearly impossible.

However, a discovery process that continually updates and identifies utilization data and stores it systematically unlocks the ability to forecast future SaaS spend based on historical data and usage trends.



Pro tip: Notification periods can range from 30 to 365 days, so make sure you plan your renewals well in advance.

*Large organizations experience as many as **two SaaS application renewals every business day.***

Proactively manage renewals with data-driven insights

Reactive renewals can impact the bottom line by not providing technology managing teams with adequate time to prepare for an upcoming renewal.

Zylo data shows that **large organizations experience as many as two renewals every business day**. An essential objective of any SaaS management program is to capture all information about agreement renewal dates and notification periods (the original agreement or purchase contract is the best source) and document this information into a SaaS renewal calendar.

With a SaaS renewal calendar in place, technology managers can work with business units, teams, or employees to proactively plan renewals, including the creation of automatic alerts for upcoming notification periods and renewal dates.

With sufficient early warning, these groups can partner with technology managers (and other stakeholders) to evaluate current utilization, spending, and other characteristics for a given application, then make an informed decision regarding renewal or non-renewal. If the data supports the decision to renew, the company can also negotiate better terms with SaaS vendors based on utilization.



*With a SaaS renewal calendar and automatic alerts in place, **technology managers can proactively plan renewals.***



Govern

Establish a process to manage SaaS apps actively

One reason SaaS applications create uncontrolled costs and increased risks is the lack of framework or process for governing SaaS in larger organizations. The SaaS Management Lifecycle helps each organization create a plan that reflects their unique business needs and priorities.

No two business or technology environments are alike. That said, SaaS governance models can be adapted to fit individual needs. One such model is a tiered approach to managing SaaS that distributes management throughout the organization.

Levels of Governance with Distributed SaaS Management

✓ IT Managed Applications

SaaS applications are widely deployed throughout the organization

✓ IT Supported Applications

SaaS applications that IT can or will support during implementation or troubleshooting

✓ Unmanaged Applications

SaaS applications that are neither directly managed nor supported by the IT team

✓ IT Managed Applications

IT managed SaaS applications represent tools and services essential for keeping a business in operation. These mission-critical tools typically require more complex configuration and support, as well as more robust security requirements.

SaaS applications that are widely deployed throughout the organization, such as office tool suites such as Microsoft 365 or Google Suite, also typically remain under IT's direct day-to-day control. Often, these applications are managed within the IT budget.



✓ IT Supported Applications

The next layer of governance focuses on applications that IT can or will support in terms of initial implementation, issue troubleshooting, and other tasks. However, the day-to-day control remains the responsibility of the business unit, team, or employee deemed the owner of the application.

By supporting these applications, but not directly managing them, the IT team can focus its finite time and resources on mission-critical applications. While IT supports these applications, their budget generally comes from a Line of Business. They are sometimes referred to as Line of Business applications.

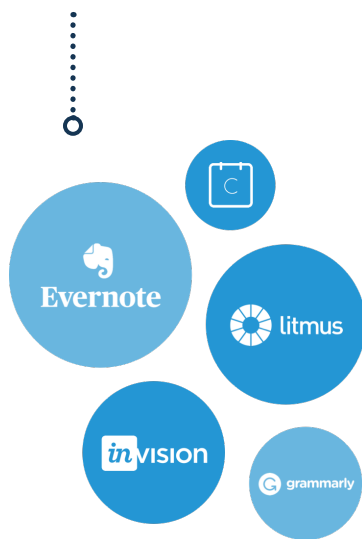
In this scenario, all applications must remain visible to the IT team via a robust continual discovery process, as well as any new applications entering the environment. If and when applications are discovered or enter the system, they undergo vetting and review to ensure that they receive an appropriate amount of governance.



***IT must
continually
discover
and vet new
applications***

✓ Unmanaged Applications

The last level of distributed management for SaaS includes applications that are neither directly managed nor supported by the IT team. These applications are typically tools for smaller teams or individual employees.



Unmanaged applications fall into two major categories:

Shadow IT, when IT has not approved the application for security, compliance, or risk, and the cost of the application is often expensed by individuals.

Approved applications, which have been vetted for information security, but are not managed or funded by IT. Spend for these applications may fall under Line of Business budgets or may be expensed by individuals.

As with applications that receive IT support but not direct management, it's critical that IT retains visibility and documentation on unmanaged applications, including initial vetting, spending, or security review, so that these applications do not contribute to increased spending or risk associated with Shadow IT.

With a distributed management approach for SaaS, IT (or the technology managing team) can provide business units, teams, and employees freedom within a framework that allows the business to adopt new tools and technologies quickly while balancing requirements for spending control and risk management.

As with other portions of SaaS Management Lifecycle, establishing distributed management requires a robust discovery process, a tested method for onboarding new applications (such as a software review and approval process), and ongoing monitoring to ensure all applications receive an appropriate level of management.

It is critical that IT maintains visibility and documentation so that unmanaged applications do not contribute to increased spending or risk associated with Shadow IT.

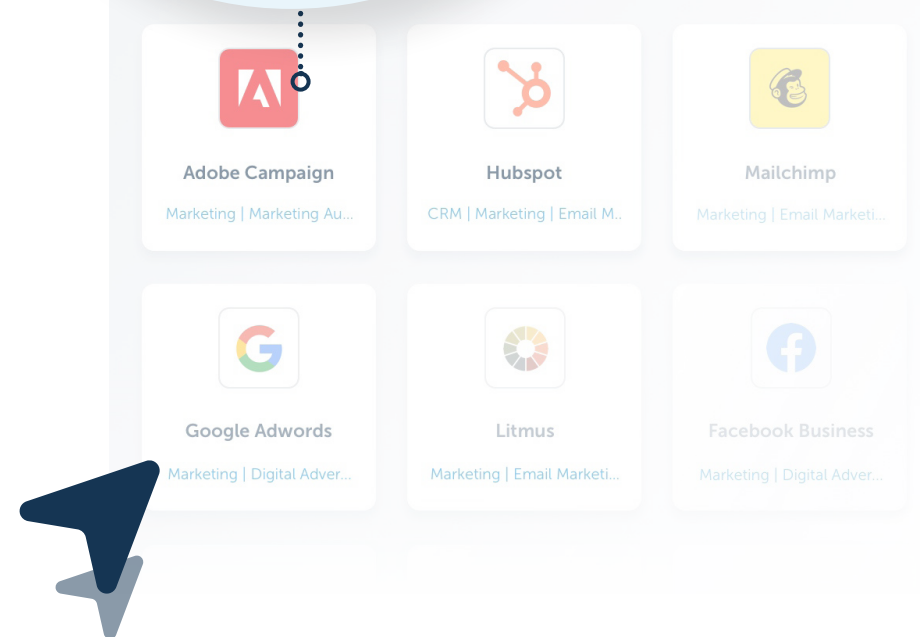
Create a self-service SaaS catalog

Innovative organizations that have deployed SaaS management have benefited not only from bringing transparency and accountability to their SaaS inventory, but also by creating new approaches to preventing shadow IT, controlling costs, and reducing risks.

These benefits are multiplied when technology managing teams can make the available catalog of SaaS applications accessible to employees and other internal customers.

An application catalog not only consolidates and standardizes the SaaS application inventory, it represents the next phase of SaaS adoption, where organizations have the right tools at the ready when teams and employees need them.

An application catalog enables organizations to have the right tools at the ready when teams and employees need them.



It's Time to Manage SaaS

SaaS will only continue to grow and displace traditional on-premise software and it's incumbent on CIOs and other technology leaders to address the challenge this evolution in software represents. Only with a strong process that emphasizes the discovery, optimization, planning, and governance needed for managing SaaS can businesses embrace the significant benefits of SaaS and mitigate the challenges it represents.

It's up to technology leaders to recognize the need for SaaS management and provide new avenues for business units, teams, and employees to consume and utilize SaaS - such as distributed management of SaaS and self-service application catalogs, or be relegated to a default posture of reaction, unmanaged risk, and unnecessary costs.

With a SaaS Management Lifecycle as part of the SaaS management process, organizations can start managing SaaS applications more effectively immediately with discovery and optimization, and then move into evolving their organizations.





To see how the practice of SaaS management and the SaaS Management Lifecycle can be applied for your organization, **request a complimentary demo of Zylo's SaaS management platform today.**

[ZYLO.COM/DEMO](https://zylo.com/demo)