The Shadow IT Governance Framework: 5 key elements

THE ITAM REVIEW

Torii

Written by AJ Witt

Executive Summary

For over twenty years, IT managers have struggled with the challenge of managing an IT estate which is no longer under their direct control. In this whitepaper we explore approaches to this problem and advocate new methods for managing your estate in the context of accelerating digital transformation and employee-led innovation. Rather than being a problem, we conclude that having the right processes and tools in place to manage shadow IT in the form of SaaS will result in a source of competitive advantage for your business.

Shadow IT in context

Much has been written about Shadow IT over the years, always framing it as a source of risk an unnecessary cost. We're all aware of that narrative and indeed those risks and costs are real. Shadow IT predates SaaS, as anyone who struggled to support and manage unofficial, unsanctioned employee-developed solutions can attest. I'm sure I'm not the only one to work in an organization where a critical business service and source of revenue was underpinned by an undocumented database written by a long since left employee.

The continuing growth of SaaS means that despite IT's best efforts Shadow IT also continues to grow. This trajectory will not change. Innovative tools become available all the time and our workforces are increasingly technology proficient. Tools such as Zapier and Slack mean almost anyone in your organization can build a process, for free, and with zero oversight from IT and other governance functions.

The problem this presents for IT is that rather than be expected to manage all the technology in use – AWS or Azure are doing much of that – they remain on the hook from a governance perspective. IT teams are the ones who need to ensure that an organization's use of technology complies with legal and regulatory requirements.

The result of this disconnect between control and governance demands was IT being slowly transformed into the department of "No", the ones who got in the way of innovation and prevented employees from using the tools they want to use to get their jobs done. IT departments decided which tools should be deployed and put controls in place, such as removal of administration rights, to enforce that.

The outcome was an increasing disconnect between IT and "the business" at the exact time when for most organizations IT was becoming the business. Even non-tech companies now rely heavily on IT to directly deliver value to their customers and thereby generate profits. IT became slow and cumbersome, tied up innovation in red tape, and constantly fought to justify why technology should be controlled centrally.

Meanwhile, whilst that battle for control was being fought at C & D-level, employees were getting on with innovating and using the tools they preferred to use, rather than some legacy corporate standard. Shadow IT grew, the influence of IT waned, and departments started taking official control of their IT stack. In my experience this started in niche areas such as Engineering and Data Science but then spread to Finance, Marketing, and Sales. Shadow IT became Departmental IT. IT leaders rightly remained concerned about it, but its use became legitimized.

IT, transformed

Come 2020, and IT stepped up to deliver during their organization's COVID response. Almost overnight they transformed their in-office estates into a modern hybrid "work anywhere" environment. IT enabled businesses to keep functioning and indeed growing in '20/'21 by finding ways to innovate faster than ever before. It's likely that corners were cut, procedures ignored, and governance standards slipped. For example, CISOs report that securing remote work is their top priority and source of stress in 2022. Furthermore, 69% of IT professionals report that Shadow IT is a top security concern.

This increased pace of innovation is now increasingly expected of IT. Organizations are committing to a fresh wave of digital transformation, and much of that transformation is being led by departments and employees. It's a necessity – IT can't deliver everything when potentially an entire way of working is being transformed.

So, that's where we are in context. SaaS usage is continuing to grow, and increasingly departments are managing their own IT. Does this mean that Shadow IT is no longer a problem? The answer to that question lies in the approach you take to managing innovation in your organization.

Approaches to Shadow IT Governance

IT are now faced with a conundrum. Do they try to continue to apply centralized control to a business which has embraced democratized innovation? Do they stick their collective heads in the sand and ignore it? Or is there a middle way where IT becomes creates a safe space for innovation to thrive and succeed?

Central Control

A degree of central technology control remains necessary for any business. Some systems such as collaboration tools, ERP, and financial applications need to be enterprise-wide for the business to function correctly. Compatibility between systems needs to be considered, even in the age of APIs that allow almost any app to be connected to any other. Pre-SaaS IT achieved this control by taking business requirements and providing systems to meet those requirements.

IT then went on to manage those systems end-to-end and exerted full control over them. IT was therefore also responsible for ensuring that those systems were available, safe, fit-for-purpose, and met legal and regulatory requirements. The result was a monolithic slow-to-change stack of applications which in part is responsible for that other great challenge for modern CIOs – technical debt.

To apply centralized control to SaaS requires strong enforceable policies along with technical measures to prevent unauthorized use of applications. Centralized control also requires greater headcount in IT, as innovation will become IT's remit. More business analysts, more project managers, more implementation experts, more support staff. And if that centralized new application investment doesn't give ROI, IT are also on the hook for the fallout from that.

The result of such tight centralized control will be slower innovation. IT simply can't be staffed to deliver change at the pace modern businesses require. IT also can't recruit the necessary experts in increasingly narrow specialisms such as data science and engineering. The ongoing focus on outsourcing IT Operations, either to cloud providers or to managed services shows that CIOs are moving away from wishing to provision everything in-house.

Even with strong centralized control, it is inevitable that some shadow IT will slip through the net. Without a SaaS Management toolset, it becomes challenging for organizations to detect Shadow and Departmental IT. Typically on first deployment of a SaaS Management tool IT finds 3x the amount of SaaS that they were expecting to find. This presents a particular danger. IT teams who think that they have watertight control can become complacent and overly-confident of what they think is running in their IT estate.

To summarise, maintaining centralized control requires IT to be more highly staffed, the pace of innovation is slowed, and the company is likely to discover that they're less secure than perhaps they thought they were.

Free rein

In the face of demands for accelerating innovation and in recognition of the difficulty in centrally controlling SaaS using their current processes and tools IT might choose to adopt a "light touch" approach to technology governance. Typically, this is seen in smaller organizations, or perhaps those running in "startup mode". In this approach to SaaS management there are no specific SaaS Management policies and potentially no tooling to detect and manage SaaS usage. The organization may still retain a list of officially supported applications but employees and departments are given free rein to select and support their own application stacks.

This approach presents several issues. Inevitably there will be duplication, compatibility problems, unnecessary costs, reduced productivity, and a general lack of governance. Almost universally there are laws and regulations which apply to an organization's use of technology. Not having technology governance in place can therefore directly affect an organization's ability to do business. In practical terms this means that a free rein approach cannot be sustained long-term. Inevitably the day will come when organizations taking a laissez-faire approach to technology innovation will need to rein in that innovation. However, in doing so, it likely won't be possible to move to centralized control approach as that simply won't fit the company culture.

The solution is to adopt a middle way whereby individuals and departments continue to innovate but governance teams are enabled to carry out necessary due diligence in accordance with the organization's appetite for risk management and technology governance.

Democratized Innovation

As we've highlighted so far, there is limited opportunity or desire for IT to exert strong centralized control over modern IT estates and workplaces. Along with that, companies are also faced with increasing technology regulation, particularly in the areas of data privacy.

How should governance teams approach this conundrum? The answer lies in deploying a set of key tools and processes designed to detect SaaS usage, categorize it, optimize it, and secure it. With automated detection of existing and new SaaS usage governance teams can engage with “citizen” innovators to assess new solutions and bring them into a governance framework. In time, as the organization matures, policies can be devised and communicated to give end users and departments a toolkit to ensure that they innovate safely, cost-effectively, and derive maximum business benefit from the solutions they devise.

At the center of this empowering framework is a SaaS Management toolset and a set of processes.

Process and tools for effective SaaS Management

Comprehensive Discovery

SaaS Management tools start by solving the most fundamental management problem, that of discovery. Without comprehensive, automated discovery we're unable to effectively manage our SaaS estates.

To get that comprehensive and automated discovery, tools must utilize a variety of methods. At a minimum, API connections to sources of record, such as administration portals, must be used. These are the "gold standard" and most reliable method of managing larger SaaS applications such as Microsoft 365 and Salesforce. Alongside API connections integration with Enterprise Single Sign On applications are a valuable source of discovery data, particularly for applications which perhaps are not deployed enterprise-wide.

Combining SSO & API discovery sources will get many organizations a long way towards comprehensive discovery. But what about those applications which aren't onboarded into SSO, or don't have an API? In order to discover those SaaS managers need further tools in their toolbox. One particularly effective approach is to use a browser agent. Browser agents are added as extensions to the common internet browsers and will capture all traffic travelling over typical browser protocols. This data is then filtered and analyzed by the SaaS Management toolset, making use of a SaaS software library in the same way that traditional installed applications are detected by a conventional SAM solution. Finally for discovery, it's also important to look at expenditure and entitlements. Integration with reseller portals can provide information on what's been purchased. Integrations with accounts and expense systems capture entitlements for paid-for SaaS applications.

The outcome of a comprehensive discovery strategy driven by a SaaS Management tool is a rich, detailed, complete and trustworthy data source which unlocks the door to effective SaaS and innovation governance.

Engage with Innovators

With comprehensive discovery deployed, what can we do with that rich data we now have about our technology landscape?

One of the key early activities should be for governance teams to engage with the users of newly detected SaaS applications. It's important to do this early to head off any potential risky applications before they become embedded. Comprehensive discovery captures user information enabling SaaS Management teams to directly engage with the person responsible for first bringing a new SaaS application into the organization. How you engage with that person depends on your policies and approach to application governance.

At a minimum, however, by knowing who deployed the application you can reach out to them quickly and discover their intentions for using it. And, with full visibility of the applications already in use in the organization, you may guide them to select a different application, perhaps the one that's used by more individuals, or the one that we have preferential pricing in place for, or the one where we have spare licenses ready to deploy.

Set Minimum Standards

Innovators may not consider the outcomes of their actions, and probably aren't experts in technology governance. However, they're also unlikely to be setting out to put the organization at risk. This is where a comprehensive set of standards is essential in empowering individuals to innovate safely. Ground rules, guard rails, operational envelope, whatever you wish to call it the desired outcome is the same – a safe framework in which to drive forward innovation in your organization.

SaaS Management tools help here by leveraging rich discovery data and automated workflows. For example, when a new application is detected a ticket can be generated for your Security team to carry out an assessment. And, if your discovery data includes the compliance status for an application – for example GDPR or SOC2 compliance – it's possible to permit or block future use of that application based on that compliance status. A further minimum standard you may wish to enforce would be to ensure that two-factor authentication is used, that data is hosted (or not hosted) in specific jurisdictions, and that the application can be enrolled in your enterprise Single Sign On application.

Onboard Innovations

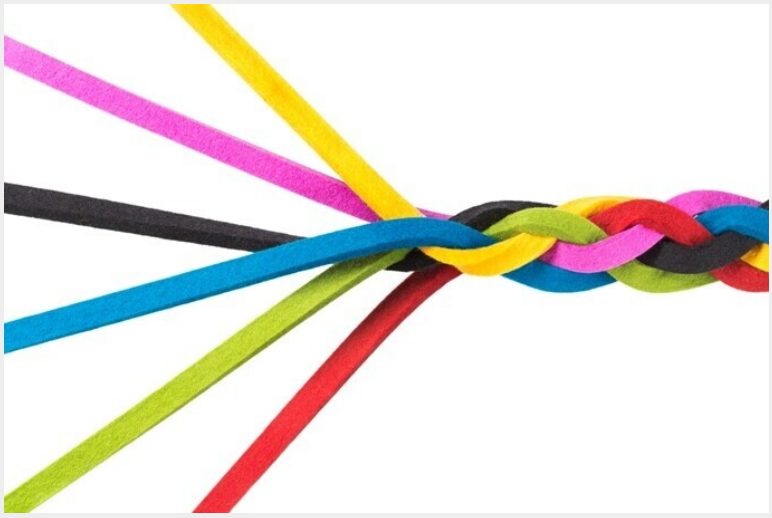
In time you may choose to onboard new applications into formal SaaS governance, kicking off workflows to get approvals for its use, and even negotiating with the vendor to receive preferential pricing. It's even possible to use SaaS Management to perform adoption tracking, which is particularly important in the early stages of application deployment, in order to ensure that the application is embedding, and that the business is deriving expected value from it. In this way we transform shadow IT into approved IT. Departments can still retain operational independence in its use but within a safe framework whereby IT and other teams such as Procurement provide services to ensure safe use and cost management.

Track Progress

Linked with the process of onboarding applications is tracking progress of application usage in general. We know that SaaS application turnover is more rapid than it was for perpetual software. Each application category provides multiple solutions at your fingertips, all promising a new way of solving a pressing business problem. Swapping from Dropbox to OneDrive is a matter of a few clicks.

As IT Asset Managers we're used to working on 1–3-year timeframes for software renewals so it is vital that your SaaS Management toolset provides easily accessible usage trend information. When it comes to renewing that application, you need to know whether usage is increasing or decreasing in order to ensure that your renewal reflects current and future demand. It makes sense to lock in preferential pricing if you know that your usage is increasing, or that an increase in headcount is just around the corner.

Summary



The Shadow IT Governance Framework presented in this whitepaper enables organizations to unlock innovation and empower their employees. IT are able to use SaaS Management to provide effective governance and a set of guidelines to ensure that grassroots innovation doesn't put the organization at risk or incur unnecessary cost. With the world of work changing, and employees expecting more of their employers, the Shadow IT Governance Framework is also a vital tool in unlocking competitive advantage and attracting and retaining the best talent.

For more on this subject see the On Demand Webinar presented in association with Torii - Unlock Innovation through SaaS Management