Making Shadow IT Work for You: What Financial Companies Can Do to Bring Grassroots IT Solutions Into the Fold

**Issue**

Among the many concerns of information technology (IT) departments is a phenomenon known somewhat alarmingly as “shadow IT.” Depending on your role at work, shadow IT can either be a cause for worry and suspicion or a way you get your job done. Luckily, this mysterious entity isn’t something that lurks inside a server room ready to attack. Simply put, shadow IT is any IT solution used within an organization without the formal approval of the organization. It can be a singular solution to an IT problem or a widespread “grassroots” technology shortcut; it’s just not part of what the IT department has officially approved.

Shadow IT has existed since the dawn of IT, often created and perpetuated by tech-savvy employees, and it is reasonable to believe that it will continue to exist – even flourish – into the future. Lest you think of it as a trivial concern, consider that CIOs globally estimate that shadow IT represents an additional 20 percent of IT investment above and beyond official IT budgets, while a recent study by CEB pegged this figure as high as 40 percent. This unsanctioned portion of IT can appear in the form of a souped-up desktop underneath someone’s desk hosting an unauthorized-yet-critical database; as a custom application developed on weekends at home; as end user-created databases or spreadsheets outside of the main database; as workflows cobbled together with tools available to users; or – more recently – as cloud services procured outside of normal IT channels. Because these solutions typically are developed to solve a very specific pain point, they often have a surprisingly positive impact on productivity and a passionate user base.

Organizations uncover shadow IT in various ways, including leadership changes, regulatory examinations, business process reviews or technology audits. When discovered, shadow IT is often correlated with control gaps in the “usual suspect” areas, such as access control, business continuity management and technical vulnerability management, to name a few. It is well established that gaps in these areas, if left unmitigated, can expose the organization to severe monetary and reputational losses and will certainly capture the attention of regulators. In other words, while shadow IT may often represent a viable solution to a business problem, the fact that it is not part of the standardized control structure can lead to additional financial, regulatory and IT security risks, all of which should be carefully evaluated when determining an appropriate response.

---

Challenges and Opportunities

All companies face shadow IT concerns, but financial services institutions are affected especially because of the intense regulatory scrutiny placed on the industry. In addition, financial services companies often have fragmented infrastructure and a traditional IT focus on compliance, not users. These factors create an environment in which user groups are frustrated by the cost and pace of output from traditional IT groups. This frustration drives demand for alternative, or shadow IT, solutions to compensate for traditional IT’s expense and/or lack of responsiveness.

From a regulatory standpoint, shadow IT presents risk to an organization due to the absence of controls in areas such as access control, disaster recovery, change management, data security and privacy, and data governance. Shadow IT is often discovered through audits or compliance reviews, which flag the shadow IT applications for not having these types of controls. Subsequently, traditional IT groups are tasked with implementing the necessary controls – often without the budget or headcount to do so. As the regulatory environment continues to evolve and become more complex, and nontraditional IT solutions more easily attainable, shadow IT will continue to loom on technology executives’ list of concerns.

Given the risks, many financial institutions take a firm hand to these exceptions when they are discovered. More innovative companies, however, realize that shadow IT can also present opportunities. Employees today are heavily incentivized to accomplish their jobs effectively, and over the past twenty years many of them have become increasingly proficient in the use of technology, while the tools available to them have become more powerful. As the average user becomes more adept at understanding and utilizing technology, shadow IT deployed by such users potentially can be adopted, even enabled, as a business driver.

In this paper we discuss different approaches to managing shadow IT; we also offer examples of opportunities presented by shadow IT that were successfully incorporated or converted to productivity enablers.

Our Point of View

Three Approaches to Managing Shadow IT

Because the nature of shadow IT varies so greatly, there isn’t a single best way to deal with it. A successful strategy relies on capturing and capitalizing on users’ creativity and drive, while ensuring the effectiveness of the control environment and the fulfillment of regulatory and compliance objectives.

- **Eradication and enforcement.** The traditional approach to dealing with shadow IT is to establish a strict set of technical standards and enforce them. This approach is driven by a “search-and-destroy” mentality, shutting down rogue solutions when they are discovered and vigilantly rooting them out. Naturally, this encourages employees to develop workarounds in utilizing their illegitimate “brainchild,” further hiding it in the shadows. For this reason alone, eradication may be difficult, even in organizations where a highly controlled environment makes this an appropriate approach.

  To be successful, the eradication and enforcement approach requires each business unit to be reviewed periodically and its most critical tools and data inventoried, labeled and audited. Anything found to be outside of compliance should then be removed from the network and business processes. If the shadow IT in question is critical to operations, the IT department could work with the business partners to find alternative solutions that comply with the policies and standards of the organization.
• **Sandboxing.** Sandboxing isn’t new, especially for companies that focus on innovation and development; for other companies, it’s an approach that can be put in use to harness the ingenuity of innovation-focused “rogue developers.” Establishing virtual network segments and test environments dedicated to developing solutions outside of the IT department can coax shadow IT out of the shadows and provide room for experimentation. Sandboxing allows organizations to implement controls that fit the target user base and ensure that the less formal development processes are still secure. By allowing normal business users to develop in this sandbox, organizations can maintain (and also demonstrate to their regulators) an appropriate level of controls to protect data and systems. Optimally, IT executives retain oversight and the ability to review the best and most creative solutions to the most challenging problems and take appropriate steps to convert that creativity to value. Eventually, concepts that prove successful within the sandbox can be moved to the standard IT control environment.

• **Enablement.** Enablement of solutions born “in the shadows” is an emerging approach to dealing with shadow IT that is quickly becoming a trend. With enablement, IT leaders not only have awareness of each and every custom spreadsheet and server but even allow and encourage their development. In the most innovative teams, IT leaders will actively offer opportunities for users to deploy shadow IT. This “blue sky” approach is attractive: Most startups tell stories about their founding in a setting of boundless imagination and can-do attitude. For established companies, lifting burdensome restrictions certainly can enable employees to seek more effective ways to complete their jobs and quickly develop better service offerings. However, an organization should consider carefully its risk appetite and the regulatory environment in which it operates before embracing this approach.

**Financial Services: Which Is the Right Approach?**

There is no one-size-fits-all approach to shadow IT; companies should adopt the approach or combination of approaches that best fits the situation. Eradication, sandboxing and controlled enablement are all appropriate solutions depending on the nature of the application. In situations where shadow IT is embraced, organizations should ensure the necessary controls are implemented. Many of the new tools – Microsoft SharePoint and cloud solutions, for example – have capabilities that allow an organization to address the control points more effectively than shadow IT solutions of the past (e.g., local Microsoft Access databases or custom solutions that sit in environments outside of IT’s control).

**How We Help Companies Succeed**

Protiviti helps financial services companies, as well as clients in other industries, decide what types of information systems should be under full control of IT, placed in a sandbox, or enabled. The ideal strategy allows an organization to strike a balance between managing the downside risk while realizing the upside benefits of enabling shadow IT. Regardless of the maturity of your IT organization, Protiviti is positioned to help you develop and implement a customized strategy for managing shadow IT. We regularly partner with financial services clients to resolve their shadow IT issues and realize the most benefit from them.

Protiviti employs experienced professionals across an array of solution groups to help organizations manage and enable technology solutions born outside of the official IT system. Our expertise includes IT risk management, asset management, end user application risk management, spreadsheet risk management, and software services. By bringing an interdisciplinary team of consultants, subject-matter experts, developers and architects, we can work with you in a collaborative fashion to harness the ingenuity of your human capital while keeping IT solutions “in-bounds.”
Bringing Shadow IT Into the Open: Examples

Technology Asset Governance
A large financial institution was under regulatory pressure to place controls around applications developed by various business units outside of the sanctioned development process. A majority of these applications were complex spreadsheets and Microsoft Access databases used for board reporting and financial modeling. Protiviti helped the institution by developing a governance framework using a combination of the three approaches described in this paper. The framework modified existing asset management tools to incorporate a database for tracking these applications, including critical attributes and links to other databases, and instituted an auditable process for maintaining the currency of the asset management system. This enabled the institution to reduce information risk and strengthen data integrity by effectively identifying, inventoried and governed applications not directly managed by IT.

Integrating Rogue Applications
A large brokerage firm needed assistance in managing a “rogue” application hosted at a third-party cloud services provider. The application was developed independently by a business unit with a focus on researching and creating competitive advantages for brokers. The group had created its own development team that could react to the needs of brokers faster than the IT organization. After reviewing some audit findings, a newly appointed leader within the business unit realized the high information security risk profile of the application due to a lack of general IT controls and sought to transition responsibility to IT. Before IT assumed responsibility for the application, Protiviti was asked to help remediate short-term risks and develop a long-term integration strategy to bring the application in-house and recreate the functionality into the primary brokerage dashboard. Resources from Protiviti’s IT Consulting and Software Services practice helped the firm accomplish these goals as well as manage development resources during the transition. Our work enabled the organization to retain a valuable brokerage application by reducing its risk profile and avoiding the disruption of end-user activities.

Retaining & Securing Intellectual Capital
Numerous corporations have approached Protiviti for help with solving a growing problem with knowledge capital being stored outside of the companies on third-party, cloud-based file share systems. In addition to potential security implications, information stored that way represented for these companies a corporate asset that was being underutilized. With reduced access and an inability to tag information, the enterprises were unable to search, find and make decisions based upon this information. Protiviti’s SharePoint business consulting group helped these organizations reclaim their valuable resources and related workflows by bringing them in-house where they could be utilized better. Our work allowed our clients to improve business functionality by streamlining information requests, meeting document retention objectives and reducing security exposure.

Bringing IT and Compliance Together
A multinational financial services corporation found itself in a typical dilemma with central IT and corporate compliance at odds over an outsourced service. The central IT organization was not able to support specific departmental needs, and while the business line had unique requirements that necessitated an outside vendor, the outsourced service also needed to be aligned with the long-term IT strategy of the company. Protiviti’s SharePoint business consulting team was brought in to resolve the dilemma. We custom-built a SharePoint application that satisfied the business need and was “inside the box” from a corporate IT perspective, removing the friction and resolving the compliance concerns. In this
example, the solution created a greater alliance between IT and end user groups, allowing IT to maintain necessary controls, while giving the end-user groups the ability to solve “local” problems without the overhead of traditional IT. Effectively, both groups won.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 40 percent of FORTUNE 1000® and FORTUNE Global 500® companies. Protiviti and its independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index

Contacts

**Tom Andreesen**
+1.312.476.6318
thomas.andreesen@protiviti.com

**Doug Sellers**
+1.312.476.6099
douglas.sellers@protiviti.com

**Ed Page**
+1.312.476.6093
ed.page@protiviti.com

**Andrew Retrum**
+1.312.476.6353
andrew.retrum@protiviti.com