IS YOUR SHADOW IT COMPROMISING YOUR GROWTH AND COMPLIANCE?
By Joe Galletta, Sales Manager – Americas, ClusterSeven

With the financial crisis behind us and the much-debated rollback of some Dodd-Frank Act regulations underway, the focus of many financial institutions has finally shifted from managing compliance to managing the business. Issues such as cost management, optimizing business performance and the need for innovation have once again come to the fore.

The emphasis now is firmly on building the business across areas such as portfolio management, risk management and product development. Central to these goals are the models banks use to manage their business, and the technology they use to deliver the output of these models – typically spreadsheets, databases and visualization tools.

Regulators are “on the case”
Of course, the wide and varied use of models – together with the tools, calculators and the technology infrastructure that supports them – brings its own challenges. Unmonitored and uncontrolled, models can themselves pose risk factors that regulators are increasingly noting. The Current Expected Credit Losses (CECL) accounting standard is one such example where model management is a fundamental requirement for which institutions need to demonstrate full control and transparency. The FDIC too has its model risk management framework for financial institutions with assets over $1 billion, affecting around 700 banks in the U.S.

Hence, while financial institutions are keen to focus on developing and driving the business forward, effective compliance management remains an imperative. And judging by historical events, compliance appears to be a moving goal post.

Shadow IT a risk
Shadow IT (e.g., databases, development environments, management information systems and spreadsheets) today is extensively used to manage numerous business processes, in parallel with and integrated with corporate IT applications. In fact, these applications, especially spreadsheets, are often the preferred business and regulatory compliance modelling tool due to their ease of use and flexibility. They are powerful enough to run complex calculations and are easy to connect so that data seamlessly flows between the various models, tools and calculators, as well as the processes they support. Perhaps this is why these applications often start as a tactical fix for a business issue, and eventually become so embedded into a business-critical process that they can't be easily removed.

Regulators are increasingly recognizing the importance of shadow IT to key business processes at banks and credit unions. There is nothing wrong with this as such, but it does mean that institutions need to have suitable visibility and controls in place. Without these controls, there's no getting away from the operational, regulatory and reputational risks the unfettered use of these tools pose.

For example, a fat-fingered data entry can cause outcomes to be skewed. A lack of version control means that there can be multiple versions of the same file or spreadsheet in use at the same time, which can seriously impair decision-making and critical reporting. This can be exacerbated if these applications are linked to other applications, replicating the same problems across the business almost instantaneously.
From a compliance standpoint, such situations can cause inadvertent misreporting, resulting in severe regulatory fines. Recently, a regulator in the UK imposed a $37 million fine on UBS for a decade of transaction misreporting errors, serving as a reminder of the potential risks involved – and a fine like this doesn’t begin to quantify the reputational risk involved.

From a business perspective, the impact can be equally serious. Poor quality information can lead to missed opportunities, or give an unrealistic view of potential returns on an investment. It can also expose an institution to contractual breaches or other issues that drive reputational risk.

A risk-sensitive approach to managing shadow IT

These shadow IT challenges can be overcome by taking a risk management led approach to its usage. At its core, it requires establishing a framework for “business as usual” shadow IT management, which should include:

1. **Visibility**
   - Creating a comprehensive inventory of the shadow IT tools and processes is an obvious place to start.

2. **Risk-based tiering**
   - Not all the tools and processes will be equally materially important to the business. Based on a defined criteria and the institution’s appetite for risk, tiering the shadow IT processes and models helps identify the ones that pose the most operational, regulatory, compliance and reputational risk to the business.

3. **Understanding the data connections**
   - Especially for high-risk processes, identifying and understanding the data linkages and lineages across the landscape is crucial to ensuring data quality and accuracy – and thereby integrity – of the processes and models.

4. **Managing and monitoring**
   - Based on a shadow IT user policy, the business-critical models and processes can then be monitored and managed for version and change control, as well as review, approvals and authorizations, to ensure that the data is accurate and can hold up to scrutiny at all times.

Institutions often resort to manual processes to govern their shadow IT estate, but despite the best will in the world, they’re fighting a losing battle due to the vast expanse and complexity involved. Achieving full transparency for an estate (to the stringent requirements of auditors and regulators) that is complex and grows organically due to lack of controls is next to impossible to achieve manually.

Therefore, automation is often the preferred solution for taking care of everything end-to-end. From scanning the IT infrastructure to locate the spreadsheets and other files to exposing the underlying data sources and relationships across the landscape to risk-checking the critical files and models, automation can help to provide continuous monitoring and control without being a drain on resources. In doing so, it also presents a reliable and demonstrable way to assure stakeholders – including senior management, auditors and regulators – that the institution’s shadow IT is subject to the same level of scrutiny that its enterprise IT is.

*Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the official policy or position of the Financial Managers Society.*

**ABOUT THE AUTHOR**

Joe Galletta has over three decades of experience in business development and partner management, with extensive work with financial services organizations, banks, asset managers and insurers.