

MITR/TECH

THE NEW SPREADSHEET RISK MANAGEMENT ISSUES OF SARBANES OXLEY

ClusterSeven



INTRODUCTION

The Sarbanes-Oxley Act of 2002 (SOX) has been in place for many years, and US-listed companies are very experienced in complying with it. This reflects the declining cost and effort of SOX compliance in recent years, as it has become 'business as usual.'

However, in recent years, the cost and effort of SOX compliance has started to increase again. A Protiviti 2017 report entitled 'Fine-tuning SOX Costs, Hours and Controls', stated that for two out of three companies, SOX compliance hours have increased by more than 10 percent since 2016. Much of this additional effort has come from the recognition

that spreadsheets continue to play a key role in many of the business systems and processes that underpin SOX reporting. Auditors and management are increasingly applying the same standards of auditability, governance and accuracy to their business-critical spreadsheet estate as are applied to their SOX-compliant corporate IT systems and processes.

This whitepaper explores the challenges that this presents organizations subject to SOX and a best practice approach to addressing these issues. It also proposes a solution that allows businesses to retain the power and flexibility of spreadsheets, while also ensuring that their use does not compromise SOX compliance.



SPREADSHEET RISK AND SOX

The most significant driver for the enhanced scrutiny of spreadsheets under the SOX compliance regime has been the US Public Company Accounting Oversight Board (PCAOB) becoming much stricter in how they oversee the US audit community, especially over audit failures and violations of the Board's quality standards. Faced with potential million plus dollar fines, auditors are redoubling their efforts in reviewing their clients' internal audit controls, which are central to SOX. Consequently, auditors are extending their audit scope to cover business processes that are extensively underpinned by spreadsheets.

In the past, SOX compliance has encouraged organizations to make use of centralized IT systems, where the SOX compliance controls for business processes are available 'out-of-the-box'. Auditors have reviewed these controls and outputs as part of their audits. CEOs and CFOs have used these reports and controls to sign-off on shareholder reports that comply with the regulations, and so head off the potentially onerous penalties for non-compliance.

Auditors are now extending client audits to cover their spreadsheet estates, as they recognize how pervasive spreadsheets are in many key SOX-related business processes.

This reflects how spreadsheet have remained vital to many key business processes - despite the widespread use of complex corporate IT systems. Users often wish to leverage the power and flexibility of spreadsheets to bridge the gap between what the business needs now and what IT can provide in a timely way. This is also reflected in the Protiviti report, which found that 64% of their respondents had experienced increased focus on their deficiencies by their auditors.



THE SPREADSHEET CHALLENGES OF SOX

Spreadsheets remain an invaluable resource for businesses, because their ease of use, flexibility and powerful functionality. Spreadsheets help them remain agile, generate new insights, model the development of their business, as well as provide accurate and timely reports.

Under SOX, this power and flexibility can be a source of issues, if the key spreadsheet estate is not managed effectively. It works in two ways.

Firstly the flexibility of spreadsheets, and lack of controls means that errors can quickly emerge, which can significantly affect the accuracy of the results. Spreadsheet risk is especially likely if complex formulas or macros are used, or if a spreadsheet is linked to other spreadsheets, other applications or external data sources.

In the SOX framework, these results can easily create reporting errors that can compromise the quality of financial results and reports. Many businesses have had to restate their earnings through calculation errors in their quarterly or annual reports. This can cause a range of reputational, regulatory,

commercial and legal headaches.

Another issue is that the lack of data governance and management controls in Excel estates prevent Corporate Officers from being able to sign-off the results as being an accurate picture of the company's results. This can potentially expose them to the significant sanctions available under the legislation.

Under SOX, organizations need to ensure that their spreadsheet-based business processes have the same level of management control as found in their highly controlled and maintained enterprise systems – without removing any of the valuable capabilities, flexibility and sheer business value that spreadsheets give to users and the business alike. An enterprise strength spreadsheet risk management capability can help them square this circle, by retaining this operational flexibility, whilst fully complying with SOX. As well as helping to deliver this capability cost effectively, it also addresses the issue that in many case companies are applying manual controls that will unlikely stand up to the enhanced scrutiny that SOX related spreadsheets are now be exposed to.



MANAGING SPREADSHEET RISK & GOVERNANCE IN SOX – AN OPTIMAL APPROACH

While spreadsheet risk might be a new area of focus of SOX, its key principles remain unchanged. The quarterly and annuals results reported by US-listed companies must be a fair reflection of the underlying business, and senior management, typically the CEO and CFO, must be willing to attest to that.

This means that the same level of management control, transparency, and auditability needs to be applied to the newly significant spreadsheet environment, as are applied to the corporate IT environment that underpins the rest of the SOX environment.

Given the challenges of managing spreadsheet risk under SOX, and the significance of the results, institutions need to think carefully about how best to leverage the power of spreadsheets, while also mitigating the risks associated with them. They need to assure the data governance that management, auditors and regulators expect.

For these spreadsheet processes organizations need to demonstrate the following:

- Visibility of the end-to-end data flow
- Clear segregation of duties
- Exception -based management
- Access control
- Documentation
- Speed of resolution

Based on the experience of helping a wide range of businesses address spreadsheet risk management under a range of compliance regimes, this is a best practice approach managing spreadsheet risk in SOX.



MANAGING SPREADSHEET RISK & GOVERNANCE IN SOX – AN OPTIMAL APPROACH

1 Confirm the SOX Spreadsheet Estate

Effective SOX reporting depends on having proper foundations, and confirming which spreadsheets form part of the SOX processes is essential. These spreadsheets may cover a range of business areas and functions: revenue management processes, cost management models, amortization models, revenue recognition models, contract records, or order management for example. Spreadsheets also feature significantly in consolidation models and final mile reporting. These, combined, with data from a range of corporate systems, deliver the final SOX results that need to be attested to.

Most, if not all these spreadsheets will be known to the business. From a SOX perspective the key is being able to demonstrate this 'completeness' to compliance and auditors. It also provides a solid foundation for managing the spreadsheet risks that could compromise the SOX results and their integrity.

Given that these spreadsheets will be located in different departments, business units and even countries, with different versions, formats and definitions used throughout business, there is ample scope for the emergence of spreadsheet risk.

2 Risk Assess your SOX Spreadsheets

In a SOX framework that utilizes spreadsheets, the spreadsheets will be of varying significance. Identifying these key spreadsheets is not straightforward. The significance of a spreadsheet may, for example, depend on how many other spreadsheets are linked to it, how many formulas and worksheets it contains and the complexity of its formulas and macros. While a useful yardstick, other, much simpler spreadsheets, may be equally critical to SOX reporting.

Having a systematic risk assessment model for SOX compliance allows people across the business to agree objectively which are the spreadsheets that require the closest scrutiny. This can form the basis of an effective SOX spreadsheet management project implementation model, as well as serving to enhance the audit and governance framework that SOX requires.

It also ensures that the risk management focus is targeted at the right areas, rather than having the effort dissipated through assessing too many of the wrong spreadsheets.



MANAGING SPREADSHEET RISK & GOVERNANCE IN SOX – AN OPTIMAL APPROACH

3 Auditing your SOX Spreadsheets

The final stage is to provide the audit capabilities of your SOX-related spreadsheets, to drive the end-to-end auditability of the results, as well as the ability for senior managers to verify the final SOX results.

In reality this means proactively monitoring the key SOX spreadsheets for changes, whether it be data, formulas, calculations, or additional worksheets for example, anything that can have a material impact on the accuracy and quality of the final SOX results. This change data can be used to provide the evidence that underpins the end-to-end audit model that SOX demands.

Under SOX, it is essential that these in-scope files are proactively monitored, in the same way as the systems are in by the corporate IT function. The reality is that often they are not, or else, it is completed manually, at great expense in time, resource and money, and often accuracy.

It is this inability for firms to systematically collect this audit data that lies at the heart of the growth in the SOX workload highlighted earlier. Rather than simply generating a report detailing all the changes in the estate, for further analysis, staff are finding that they are having to respond to enquiries from auditors by reviewing multiple spreadsheets, to identify the relevant changes and then find out who made them and who authorized them. As well as being very time consuming, this ad-hoc approach does not fully meet the requirements of SOX and exposes the business to significant issues in the future.

The scale, complexity and relentless change of US listed businesses means that a manual spreadsheet audit and review model is impractical and places them in danger of a material breach of the regulations. The optimal approach demands an automated, systematic and scalable spreadsheet management framework that fully meets the needs of the business and the regulations.



THE SOLUTION: INTEGRATED DISCOVERY, INVENTORY MANAGEMENT AND SPREADSHEET MONITORING

It is clear that spreadsheets present a significant challenge to maintaining SOX compliance and reporting. However approached the right way, and armed with the right capabilities, it possible for businesses to meet and overcome these challenges.

Applying the best practice principles highlighted above, it is possible to design a solution that utilizes proven technologies to automate these processes that delivers an effective SOX compliance framework for mission-critical spreadsheets, meeting the needs for accuracy, auditability and cost effectiveness.

Discovery

The discovery process is the foundation of the core SOX audit process. As well as helping to identify the spreadsheets in the core business processes, it can also demonstrate full discovery of the estate to auditors and management.

This process can be completed manually, but will be time consuming, expensive and error-prone. Discovery can be very problematic, as very often there will be multiple versions of the same spreadsheets, multiple formats and multiple definitions. Identifying which of the spreadsheets matter to the SOX regime will be very difficult to set up, let alone maintain, with plenty of scope to unwittingly breach the regulations.

Discovery lends itself well to automation, given the need for speed and efficiency, as well as often broad distribution of spreadsheets across an environment.

As well as finding relevant spreadsheets, powerful discovery tools can drill down deeply into spreadsheets, even down to cell level. This enables the process that drives exception-based alerting for changes, errors and omissions that drive the proactive monitoring of the most significant spreadsheets, as well as the evidence of change needed by auditors and management.

These powerful discovery tools also allow companies to identify the links between spreadsheets – the data lineage – that that provide much of the power and flexibility found in spreadsheets, where a user changes one variable, which is then propagated through multiple spreadsheets. It also means that errors or omissions can be propagated easily, compromising the processes demanded by SOX.



THE SOLUTION: INTEGRATED DISCOVERY, INVENTORY MANAGEMENT AND SPREADSHEET MONITORING

Inventory Management

With the scope and complexity of the SOX spreadsheet estate fully defined, the next step is to

introduce the first level of management control, by checking all the relevant spreadsheets into an inventory management system. This both defines those spreadsheets that need to be considered under SOX, and allows the SOX compliance team to risk assess the spreadsheets as low, medium and high risk.

The twin drivers of systematic risk management and business efficiency means that automation is the optimal model for managing this process.

A risk assessment model allows organizations to agree which spreadsheets are the most significant for their SOX compliance. There is no hard and fast rule for deciding which spreadsheets are significant, and which are less so. Complexity may well be significant, and the extent to which they are interlinked. Materiality – the significance of a spreadsheet to the SOX process – will also be important.

Criteria, reflecting these points, can be applied to the SOX spreadsheet estate, to systematically categorize the SOX spreadsheet estate into low, medium and high risk to the SOX compliance and reporting. SOX compliance teams can triage their efforts and focus their main efforts on making sure that their most critical spreadsheets are proactively monitored.

This inventory model has the benefit of creating a framework that can provide periodic attestation capability that auditors seek when determining whether the SOX results are a fair reflection of the position of the business.

Monitoring and Auditing

Once the highest risk, and most critical spreadsheets have been identified, a framework to proactively monitor them is the next step. This process can again be delivered manually, but the numbers of spreadsheets, their likely complexity means that manual processes is impractical. Equally the importance of getting the right result, and being able to provide a complete audit trail of these changes is vital, and too important to leave open to the errors and mistakes in achieving this manually.

The structured nature of many of the spreadsheets used in SOX lends itself well to automation. This eliminates the chance of potentially serious spreadsheet risk issues being missed, efficiently and effectively. The power and flexibility of a spreadsheet, especially in a SOX context means that a diverse set of spreadsheet functions will be used in business processes underpinned by SOX. This will require a powerful, functionally rich search model to capture these functions and any changes that will drive the critical audit trail that is central to SOX compliance. This model will need to be able to capture, at the very least, changes to macros, functions, data as well as highlight stale data or missing data as well as new or broken spreadsheet links, cell errors, changes to the number of worksheets to name a few.

Proactive alerting to potential spreadsheet risk issues also helps to keep the SOX compliance on track. In a complex SOX spreadsheet environment, it is likely that a large number of alerts will be generated, so it will be useful to have an alert filtering process that makes analyzing the alerts practical.

THE SOLUTION: INTEGRATED DISCOVERY, INVENTORY MANAGEMENT AND SPREADSHEET MONITORING

It should be possible to filter from multiple perspectives, including by business unit, by formula type, by macro, and by links, for example. This capability provides the ability to identify and address issues swiftly, helping to maintain compliance at a reducing cost.

Reporting capabilities will also be essential, to provide timely reporting for management, as well as to provide the foundations for the documentation and auditing requirements that will be a feature of SOX compliance. As well as enabling the segregation of duties, identifying who has made changes and seeing the requisite approval of these, this capability also provides scope for potentially reducing the cost and effort involved in auditing.

Integration

Each phase – the discovery, inventory management and monitoring – can each be delivered using a range of toolsets and applications.

However, there is value in delivering them as an integrated whole, as it ensures that the critical spreadsheet risk data is fully captured through each phase. This end-to-end spreadsheet risk management approach ensures all the critical spreadsheet risk information is consolidated into one environment, with reduced scope for errors and omissions. It also assure the comprehensive audit trail required under SOX. This reduces compliance risk and provides the most effective framework for auditing the spreadsheet estate in SOX reporting. A unified approach also offers the greatest scope for costing savings too.

CONCLUSION

Spreadsheets almost certainly form a significant part of any SOX compliance process. The complexity of the spreadsheets, the SOX results, and need for data integration provides ample scope for spreadsheet risk to develop undetected. This can expose an institution to significant regulatory, reputational, commercial and legal impact, should the ultimate SOX results be flawed or unauditible.

However, approached in a logical and systematic way, and recognizing the significance and value of spreadsheets to the SOX reporting process, there are options that allow SOX filers to make use of spreadsheets as part of their day-to-day SOX compliance. It is perfectly possible to use spreadsheets as part of a SOX process, to deliver compliance on time and on budget while also retaining the level of management control and auditability that banks are accustomed to in their corporate IT environment.

**For more information about ClusterSeven,
please visit www.Mitrates.com**

ABOUT MITRATECH

Mitratech is a proven global technology partner for corporate legal, risk, and compliance professionals seeking to maximize productivity, control expense, and mitigate risk by deepening organizational alignment, increasing visibility and spurring collaboration across the enterprise.

With Mitratech's proven portfolio of end-to-end solutions, enterprises worldwide are able to implement best practices and standardize processes throughout their organizations and realize fast time-to-value.

Serving 1,200 organizations of all sizes worldwide, Mitratech works with almost 40% of the Fortune 500 and over 500,000 users in over 160 countries.

For more info, visit: www.mitratech.com

MITRATECH

info@mitratech.com

www.mitratech.com

© 2020 Mitratech Holdings, Inc. All rights reserved.