Gaining Control Over End User Computing

*Increased Pressure to Control Spreadsheets and Documents*
Table of Contents

Pervasiveness of End User Computing Brings Risk.......................................................... 4
  Specific Challenges and Risks in the Use of Spreadsheets........................................5

Increased Pressure to Gain Control over End User Computing ............................. 10

GRC 20/20’s Final Perspective .................................................................................. 12

About GRC 20/20 Research, LLC .......................................................................... 14

Research Methodology ........................................................................................... 14

TALK TO US . . .

We look forward to hearing from you and learning what you think about GRC 20/20 research. GRC 20/20 is eager to answer inquiries from organizations looking to improve GRC related processes and utilize technology to drive GRC efficiency, effectiveness, and agility.
Gaining Control Over End User Computing

Increased Pressure to Control Spreadsheets and Documents

Pervasiveness of End User Computing Brings Risk

Use of end user computing applications such as spreadsheets, emails, and other document types has revolutionized how technology creates value for organizations. However, this brings a significant challenge to govern and control information and technology in a distributed and dynamic environment. Organizations are facing increased pressures from regulators and auditors to ensure that they have adequate controls over end user computing applications, particularly spreadsheets used in accounting and finance processes. This specifically has caught the attention of the Public Company Accounting Oversight Board (PCAOB) and external auditors. This scrutiny is leading to new SOX failings for companies that had previously had no such failings.

How does the organization take advantage of the wealth of benefits that end user computing solutions such as documents and spreadsheets deliver while avoiding the compromise of confidentiality, integrity, availability, and auditability of critical business information, increased risk exposure, and potential legal and regulatory actions?

End user computing applications are pervasive in the enterprise. This increases productivity and gives organizations agility that helps them succeed in a complex, dynamic, and distributed business environment. At the same time, risk and compliance issues are compounded by the extensive nature of collaboration and unstructured data. Individuals and departments can quickly set up online collaboration portals and share documents inside and outside the organization, increasing the number of people who can misuse them and simultaneously decreasing the organizations control over them. Consider that information comes in various forms:

- **Structured data** is found in databases and consists of master data and transactions. Structured data can expose the organization to significant risk and compliance concerns but is contained within database structures and is to a degree easier to control, monitor, and secure. However, pathways to export data and access to structured data is a concern to organizations when it is exported and manipulated in spreadsheets and documents.

- **Unstructured data** is pervasive and quickly gets out of control. It consists of documents, emails, spreadsheets, as well as communication and collaboration technologies. Data is easily copied, disseminated, and manipulated. In the distribution process, different versions evolve and can conflict with each other. Business critical data is often stored within spreadsheets and communications subjecting the organization to risk and compliance exposure.
- **Dark data** that is data that the organization has no clue about or control over. What should have been destroyed still lives on in remote corners of the organization and beyond. An older version of a spreadsheet that relies on bygone assumptions may still be accessed and used resulting in poor business decisions and faulty analytics.

- **Rogue data** that is easy to manipulate and present out of context. What is legitimate information may be unintentionally or maliciously altered to present a different story out of context.

- **Duplicated data** in which the organization may have understanding and control of areas where information exists, but is not aware how it has been copied and distributed. When the data changes, those changes are not reflected across areas where it has been copied, referenced, and used.

- **Pervasive data** that has no boundaries — unless controlled. Employees quickly use social sharing, collaboration portals, and mobile devices to access information from wherever they are, whenever they want it with little thought to risk and compliance.

There is no doubt about it – end user computing applications are a strategic and critical business application. End user computing applications, particularly spreadsheets, represent an essential and strategic application to business, but also are a significant risk if left uncontrolled.

**Specific Challenges and Risks in the Use of Spreadsheets**

Organizations face a challenge: spreadsheets are a strategic, useful, and flexible business application but require significant amounts of checking and review to mitigate errors and risk. It is not the spreadsheet’s fault; it is the users’ fault. Organizations need to control spreadsheets so that they can in the end control or avoid the problems users introduce in their use – both inadvertent and malicious.

Organizations that have failed to manage and control spreadsheets have faced significant loss as the result of bad decisions from unreliable data. Lack of control can introduce significant loss to the organization: spreadsheets are prone to breaking because of user error in their configuration, values, use, and calculations. The organization, without proper end user computing controls, does not know that spreadsheets are broken and ends up relying on data that is faulty. Bad spreadsheets do not tell you they are broken; they just spit out bad information. Organizations need to have a defined process to ensure the control over end user computing applications used in critical business processes. This includes understanding:

- **Business criticality of end user computing applications**. Spreadsheets and documents are business-critical applications. They offer advanced analytics and modeling of numbers, finance, and statistics. They are flexible, used, and cherished by many users. Spreadsheets and documents are here to stay, and the organization must figure out how to control them.
- **Pervasiveness of spreadsheets and documents.** Spreadsheets and documents are everywhere; every workstation typically has them installed as a standard application. They electronically breed and multiply by users adapting them for different purposes. They are copied and modified with no accountability or documentation of their use. Little thought has gone into their development and they often have a host of inaccuracies.

- **Complexity and integrity of spreadsheets and documents.** Spreadsheets, while a tool in everyone’s electronic toolbox, are often highly complex with bewildering math, configuration, and calculations spanning multiple worksheets. Complexity makes integrity a challenge. The data quality and integrity of spreadsheets is critical, and the more complex they are, the more control, oversight, and diligence is required.

- **Simple mistakes introduce significant errors.** Spreadsheet issues resulting in loss and bad decisions come about through simple user error, miscalculations, and manual processes such as copying and pasting data. When spreadsheets and documents are not controlled or vetted, it can be quite some time before the organization realizes the loss, and in the meantime, it has grown exponentially. It is the exponential loss that finally brings attention to the fact that a simple error in a spreadsheet caused it. Organizations also struggle with the fact that as spreadsheets were developed or changed, no testing was done to provide assurance that they functioned correctly.

- **No audit trail, change control, or versioning.** Changes to spreadsheets are typically not monitored, and the organization could not tell you who did what, when, how, and why. It is not a difficult task for miscreants to come in and modify numbers to cover a trail and protect themselves. Further, the data in spreadsheets can often be a mystery with no way to trace where it came from. Organizations struggle with versioning and archiving of spreadsheets because of modifications and cannot fall back to a reliable version should an error be found as there is no reliable version available.

- **Lack of accountability and ownership.** In general, spreadsheets and documents are unsecured and unmonitored tools. A spreadsheet is developed and then proliferated throughout the enterprise. It may be modified, and calculations changed. Multiple versions end up existing with no single person responsible for their integrity and use. Someone may access a spreadsheet and never realize it was modified and perhaps functions in a different way or has errors in calculations and/or values.

- **Compliance and audit challenges.** Organizations are under the microscope from regulators and external auditors to improve control and assurance over the data in their spreadsheets, comply with regulatory requirements, and conform to auditor expectations. Further, the internal control and audit process is cumbersome as it involves manual processes that require significant time to manually check spreadsheet integrity and function - time that constrained resources in internal audit and control staff do not have. They need an
automated and reliable approach to meet expectations and requirements while minimizing risk and loss to the business.

Despite these challenges and risks, many organizations lack a thorough understanding of end-user computing solutions that present a risk to an organization’s financial reports. In a recent GRC 20/20 survey of 109 organizations, nearly half of organizations responding (49%) state they do not have a grasp on end user computing risks and controls in their environment impacting financial reporting.

*Does your organization have a thorough understanding of end-user computing solutions (e.g., spreadsheets, desktop databases) that might present a risk to your financial reports?*

- **51%** Yes
- **49%** No

This unpreparedness to address end user computing risks is even greater when organizations were asked specifically if they had identified and built an inventory of spreadsheets and desktop databases where material misstatements could arise. In the survey, 53% of respondents stated they lacked this inventory and are thus unprepared to even understand the scope of this risk let alone address it.
Have you identified the spreadsheets and desktop databases where material misstatements could arise?

47% Yes  
53% No

Most organizations are unprepared to address the risk in end user computing applications. Just over half (51%) of organizations indicate that they do not have controls around end user computing (see Figure). Those that do have controls to address end user computing risks are largely dependent on manual controls (49%) with only a small minority of organizations (20%) indicating that they have technology in place to automate control of end user computing (see Figure). Manual processes are prone to inefficiency, ineffectiveness, and lack agility to the demands of a dynamic and distributed business environment.
Do you have controls around end user computing solutions – in particular spreadsheets and desktop databases?

- **Yes**: 51%
- **No**: 49%

If so, what types of controls?

- **Manual Controls & Processes**: 49%
- **Solutions to Automate Controls**: 20%
- **Unsure**: 31%
Increased Pressure to Gain Control over End User Computing

The information within documents and spreadsheets faces a bombardment of risk and compliance challenges from every direction. New methods of collaborating through pervasive access to data introduce serious risk and compliance concerns. Documents shared inside, as well as outside, the organization may not be adequately protected. How does the organization take advantage of the wealth of benefits that end user computing and pervasive access to information promises? While at the same time avoiding the compromise of confidentiality, integrity, and availability of critical business information, increased risk exposure, legal actions, and regulatory actions? With an onslaught of regulations and enforcement actions, the concern of information governance, risk management, and compliance continues to grow.

The creation, integration, consumption, and analysis of information in various forms drives the products, services, operations, and finances of the organization, determines strategy, and impacts operations of organizations. A challenge to organizations is to govern information and use in end user computing applications like word processes and spreadsheets. This requires managing the uncertainty and exposure to risk that documents and spreadsheet use brings to the organization.

Spreadsheets are too often not in the purview of internal control programs, though they support and are an important part of critical business processes. Thus, they often fall below the radar of internal control, oversight, and audit with little to no governance and data standards. This is something the PCAOB and external auditors are focused on rectifying. Organizations are facing increased pressures from regulators and auditors to ensure that they have adequate controls over end user computing applications, particularly spreadsheets used in accounting and finance processes. The PCAOB specifically has requested auditors to increase their focus on ‘System Generated Data and Reports’ driving the application of so-called ‘enhanced audits’ of Sarbanes Oxley (SOX) control processes which often involve a predominant and pervasive use of end user computing applications. In the survey, 78% of organizations state that their external auditors are applying tougher standards in the application of PCAOB pressure on end user computing controls, with only 22% of organizations stating they have not seen this increased pressure (see Figure).
Are your external auditors applying tougher standards in the application of this PCAOB Guidance?

- 22% None
- 31% Somewhat
- 25% Moderately
- 22% Extreme

This scrutiny is leading to new SOX failings for companies that had previously had no such failings. Enhanced audits are exposing the role of spreadsheets in context of Internal Control over Financial Reporting (ICFR) and the fact that spreadsheets are often open to manual manipulation.

In context of this increased pressure from tougher audit standards, most organizations (60%) responding to the survey state they are undertaking new process and technology improvements to address end user computing controls. This indicates significant changes within organizations to gain control over spreadsheets and documents that are used in financial and accounting processes.
Is your organization undertaking any new process or technology improvements in the area of system generated data and reports to meet tougher audit standards?

- 60% Yes
- 40% No

GRC 20/20’s Final Perspective . . .

Organizations have a clear need to ensure that information access and collaboration is controlled and secured. GRC roles have often been in reactive mode to an onslaught of regulations and risk and have failed to develop a sufficient strategy to govern how end user computing is used across the organization. It is the responsibility of an internal control team to work in tandem with GRC functions across areas of IT, security, legal, compliance, risk management, and audit. Together these roles have the responsibility to provide a clear strategy for end user computing controls. In that context they need to clearly define classification, policy, and control of unstructured information, and use of end user computing solutions. This is not the responsibility of one department, but is a cooperative effort across functions. These collaborative roles need to clearly define the appropriate use of end user computing applications in policies and provide for automated controls needed to govern end user computing applications. GRC technologies that discover, monitor, and enforce control of end user computing solutions are a key component of how to address this growing need.

Information governance is not information restriction. The goal is not to inhibit business, but to protect the business. There is a legitimate need for the access to information and collaboration with others inside and outside the organization using end user computing solutions. It is the role of GRC professionals to provide this control and governance so that those who need it in the context of regulatory boundaries and risk mitigation can access information.

A GRC strategy for end user computing controls helps organizations to:
- **Ensure** that ownership and accountability of information governance and collaboration through end user computing technologies is clearly established and enforced.

- **Manage** ongoing business impact of risk exposure in the context of end user computing.

- **Integrate** intelligence that establishes workflows and tasks when issues arise that impacts the organization in context of improper use of end user computing solutions.

- **Monitor** the organization’s environment for the dissemination, access, and control of information across end user computing solutions.

- **Identify** changes in risk, compliance, and control profiles spreadsheets that expose information to issues of integrity, confidentiality, availability, and auditability.

- **Visualize** the impact of a change on the organization’s processes and operations in the context of information and end user computing use.
About GRC 20/20 Research, LLC

GRC 20/20 Research, LLC (GRC 20/20) provides clarity of insight into governance, risk management, and compliance (GRC) solutions and strategies through objective market research, benchmarking, training, and analysis. We provide objective insight into GRC market dynamics; technology trends; competitive landscape; market sizing; expenditure priorities; and mergers and acquisitions. GRC 20/20 advises the entire ecosystem of GRC solution buyers, professional service firms, and solution providers. Our research clarity is delivered through analysts with real-world expertise, independence, creativity, and objectivity that understand GRC challenges and how to solve them practically and not just theoretically. Our clients include Fortune 1000 companies, major professional service firms, and the breadth of GRC solution providers.

Research Methodology

GRC 20/20 research reports are written by experienced analysts with experience selecting and implementing GRC solutions. GRC 20/20 evaluates all GRC solution providers using consistent and objective criteria, regardless of whether or not they are a GRC 20/20 client. The findings and analysis in GRC 20/20 research reports reflect analyst experience, opinions, research into market trends, participants, expenditure patterns, and best practices. Research facts and representations are verified with client references to validate accuracy. GRC solution providers are given the opportunity to correct factual errors, but cannot influence GRC 20/20 opinion.