December 2019

Q Software

Managing Risk & Controls in Multiple ERP Environments

SOLUTION***PERSPECTIVE***

Governance, Risk Management & Compliance Insight

Table of Contents

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.

Q Software

Managing Risk & Controls in Multiple ERP Environments

Monitoring and Managing Access Controls Effectively

Agility Required in Access Control & Segregation of Duties

Organizations fail to monitor and manage controls effectively in an environment that demands agility. Too often internal control management is a periodic exercise that provides incomplete visibility into the organization's people, processes, and systems, particularly across multiple ERP systems.

Gone are the years of simplicity in business operations. Exponential growth and change in risks, regulations, globalization, employees, distributed operations, competitive velocity, technology, and business data encumbers organizations of all sizes. Keeping this risk, complexity, and change in sync is a significant challenge throughout all levels of the business. This challenge is even greater when internal control management and automation is done in manual processes or silos and is not an ongoing and monitored process across business systems. Organizations need to understand how to design effective controls, implement them, and review whether the risks they were designed to control are effectively mitigated on a continuous and ongoing basis across business systems and applications.

Business is impacted by constant change. Change is the single greatest governance, risk management, and compliance (GRC) challenge today. Today's organization is in a continuous state of change with shifting employees: new ones are hired, others change roles, while others leave or are terminated. Business processes and technology change at a rapid pace. In the context of change, internal controls over financial reporting, regulatory requirements (e.g., SOX), internal and external auditors, and fraud risk put increased pressure on corporations to ensure all ERP and critical business systems are secure and access control risks are managed across a dynamic and distributed business environment.

Corporate governance and organizational culture have largely been based on trust. In this context the organization trusts their employees, contractors, and other third parties working on its behalf. It is understood that these individuals will follow policies and procedures. The reality is that people are human. They make mistakes, they cut corners, and their own motives and goals may not align with the organization's. This is further confounded when management undermines controls they find bothersome. Keeping up with controls in a changing workforce environment as regulations, risks, applications, priorities, and business processes change is challenging. There is a greater need to define and automate the breadth of internal controls to bring real-time insight into what

individuals are actually doing across the enterprise to mitigate user access and process risks.

Internal control management in the modern organization is:

- **Distributed.** Even the smallest of organizations can have distributed operations complicated by a web of interrelated transactions, systems access, processes, and relationships. The traditional brick and mortar business with physical buildings and conventional employees has been replaced with an interconnected mesh of relationships and interactions which define the organization. Complexity grows as these interconnected roles, relationships, and processes move to an increasing number of systems and ERP moves to the Cloud.

- **Dynamic.** Organizations are in a constant state of change as distributed operations and systems grow and evolve. At the same time, the organization is trying to remain competitive with shifting employees, business strategies, technologies, partners, and processes while also keeping pace with change to risk environments that impact internal controls. Managing internal controls and business change on numerous fronts has buried the organization when done in manual processes or siloed point solutions.

- **Disrupted.** The explosion of data in organizations has brought on the era of "Big Data." Organizations are attempting to manage high volumes of access across multiple systems, transactions, processes, roles, and relationships to see the big picture of risk and controls. The velocity, variety, veracity, and volume of control data is overwhelming – disrupting the organization and slowing it down at a time when it needs to be agile and fast.

- **Accountable.** There is growing awareness among executives and directors that internal control management needs to be taken seriously. It is part of their fiduciary obligations to oversee controls, and their intersection with risk and compliance, as an integrated part of business strategy and execution. Furthermore, regulations that are increasing personal liability within these roles put an emphasis on business leaders taking greater interest and accountability for risk, control, and compliance.

Understanding the Interrelationship of Access Controls

Access control management and automation is often misunderstood, misapplied, and misinterpreted as a result of scattered and uncoordinated approaches. This is particularly true when access controls are a set of manual processes encumbered by documents, spreadsheets, and emails when it could be continuously monitored and enforced not only in one business system, but across business systems. Managing segregation of duties (SoD), inherited rights, critical and super user access, and changes to roles in manual processes is a losing battle. The challenge of managing access control in the ERP environment is burdensome when done with manual and document centric approaches.

The management of internal controls has become increasingly challenging as the organization has:

- *Multiple lines of businesses operating globally* across many jurisdictions and systems.
- *Workforce that is constantly changing* with access into systems and processes. Over time there are significant gaps and rights issues as the average user has access into a dozen systems or more.
- *Web of third-party relationships* of contractors, consultants, temporary workers, service providers, and outsourcers that have access to data, systems, and processes.
- *Mergers and acquisitions that exponentially grows* the systems, processes, and controls in the organization if not properly integrated.
- *Migration of applications to the Cloud* that provides further challenges to monitoring controls.
- *Millions of dollars in transactions* that flow through business systems in the digital economy that need controls.

For some organizations, access control management is done in silos and does not truly provide an enterprise view of controls across roles, processes, and operations. Completing a control assessment process and ticking the box has got in the way of true access control analysis and understanding.

Internal access control silos — where distributed systems and processes maintain their own controls, data, and analytics — pose a major challenge to achieving this. Documents and spreadsheets are not equipped to capture the complex interrelationships that span systems, operations, transactions, lines of business, and processes. When an organization approaches internal controls in scattered silos without acknowledging interrelationships across silos, there is little opportunity to be intelligent about risk and control. This is because processes intersect, compound, and interrelate to create a larger risk exposure than each silo is independently aware of. A siloed approach to internal controls fails to deliver insight as well as context and renders making a connection between controls and risk management, objectives, and performance nearly impossible.

Surprisingly, many organizations still use these manual processes to manage access control and SoD risk. This is primarily done through spreadsheets, word processing documents, and email. Not only are these approaches inefficient and ineffective, causing the business to slow down, but they introduce greater exposure to risk and non-compliance, as it is nearly impossible to keep up with the pace of change in employees and access across business systems. The inefficient, ineffective, and non-agile organization runs a combination of security and access reports, and compiles access information into documents and spreadsheets that are sent out via email (used as an improvised workflow tool) for review and analysis. At the end of the day, significant time

is spent running reports - compiling and integrating that information into documents and spreadsheets to send out for review. This ends up costing the organization in wasted resources, errors in manual reporting, and audit time drilling into configurations and testing access controls in the ERP environment. Organizations often miss things, as there is no structure of accountability with audit trails. This approach is not scalable and becomes unmanageable over time. It leads to a false sense of control due to reliance on inaccurate and misleading results from errors produced by manual access control processes.

Manual processes and document-centric approaches to SoD, inherited rights, as well as critical and super user access is time-consuming, prone to mistakes and errors, and leaves the business exposed. By automating access controls, organizations take a proactive approach to avoiding risk while cutting down the cost and time required to maintain controls, be compliant, and mitigate risk.

Making sense of access control management and its varying factions across operational risks can be bewildering. An access control management strategy that is siloed and myopic makes risk management a challenge. This is exponentially compounded when risk velocity is considered: when risk materializes into an event it moves very quickly and controls are missing. Are organizations agile enough to react?

The bottom line: Technology for access control management, automation, and continuous monitoring now enables organizations to achieve a real-time, integrated view of enterprise access controls and risks in business systems, applications, processes, and roles. This not only enables an enterprise perspective of access risk, but also allows the organization to increase efficiency, effectiveness, and agility in internal control management and automation.

Q Software

Managing Risk & Controls in Multiple ERP Environments

Q Software is a GRC solution provider that GRC 20/20 has researched, evaluated, and reviewed with organizations that are using it in complex, distributed, and dynamic business environments. Q Software delivers a new breed of intuitive automated access controls and SoD across a range of ERP systems. The solution delivers significant business value and brings a contextual understanding of access controls across an organization's distributed ERP environment.

Customers use Q Software to assess SoD and critical access, provide audit trails on key data in their application, and enable a single-source location to request and approve access requests. GRC 20/20 finds that Q Software is a solution that can grow and expand with the organization and adapt as the organization and its environments change.

Q Software started in 1996 and has grown to over 300 customers across 58 countries. They specialize in solutions for security management, segregation of duties, auditing, and compliance reporting tools for users of:

- JD Edwards EnterpriseOne
- JD Edwards World
- Oracle E-Business Suite
- Oracle ERP Cloud.

GRC 20/20's evaluation, research, and interactions with Q Software clients have revealed the following:

- **Before Q Software.** Typical clients struggled with manual processes for access management in their ERP environment(s) that were encumbered by documents, spreadsheets, and emails. No one had complete visibility into access, and reporting on access risks was time consuming. There were significant inefficiencies, redundancies, as well as gaps. Some relied heavily on third party reporting software that would pull data from ERP systems like JD Edwards which was very time consuming as they had to manually key in all the specific things to look for and many things were being missed. Others were relying heavily on outsourcing this to expensive consulting firms to monitor and manage.

- **Why organizations choose Q Software.** Clients desire a full end-to-end enablement of access management and reporting across in their ERP environment(s). In evaluating solutions, they found that Q Software covered the spectrum of their requirements with an intuitive, easy to use, Cloud solution that has a lower cost of ownership. It was easier to implement, had the breadth of capabilities and reporting desired, and was competitive on price. One Q Software client stated they chose the solution because of:

  - ***Flexibility*** in the large number of rules in the Q Software solution.
  - ***Frequency*** they could run the analysis when they wanted without dependency on other third parties.
  - ***Scalability*** there is no limitation on how many rules they run the analysis on.

- **How organizations are using Q Software.** Q Software clients use the solution to manage access risks in ERP applications. Their common goal is to have a single information and technology architecture that enables access management to mitigate risk, meet compliance requirements, and drive efficiency and resilience. The ability to manage access risk and provide 360° contextual intelligence on access risks and roles is critical. Clients of Q Software are from a range of industries as well as organizations of various size, both public and privately held.

- **Where Q Software has excelled for organizations.** Organizations tell GRC 20/20 that the solution has excelled for them in automating access management and automation, while enabling reporting. Organizations are using it to provide an integrated view of access risks to manage and monitor the entire process. They find value in having a integrated solution with robust reporting through a harmonized process for access risk controls that provides a defensible system of record and single source of truth on access, SoD, and roles.

What Q Software Does

GRC 20/20 has evaluated the features and capabilities of the Q Software solution set and finds that it delivers an integrated and harmonized automated control management solution that works in multiple ERP environments. Q Software provides an automated access control risk solution that is intuitive and easy to use in a integrated Cloud and on-premise solution that centralizes all SoD and access control data in one place. This enables the organization to collaborate, manage, analyze, and report on critical access control and risk data.

Q Software enables the three lines of defense in access risk management as follows:

- **Business Operations.** The management of the organization across operations and processes comprise the roles that approve access to business systems. This represents the functions within departments and processes that ultimately own and manage risk and controls in the context of business activities. These roles need to be empowered to identify, assess, document, report, and respond to access risks, issues, and controls in the organization. This first layer operates within the policies, controls, and tolerances defined by the next layer of defense i.e. GRC professionals.

- **GRC Professionals.** The back office of GRC functions (e.g., internal control, risk management, compliance, security, and finance) are the roles that specify and define the boundaries of the organization that are established in controls and risk tolerances. These roles oversee, assess, monitor, and manage access risk, compliance, and control activities in the context of business operations, transactions, and activities.

- **Assurance Professionals.** The third layer of defense is assurance professionals (e.g., internal audit, external audit) that provide thorough, objective, and independent assurance on business operations, controls, and access risk. It is their primary responsibility to provide assurance to the Board of Directors and executives that the first and second lines of defense are operating within established boundaries and are providing complete and accurate information to management.

Q Software has developed an integrated, on-premise, and cloud-based solution for multiple Oracle ERP systems to enable users to manage access and user behavior from one location across platforms throughout the business. This enables an organization to see complex interactions and access control issues across systems to answer questions such as:

- Who can create a vendor and then pay that vendor with no oversight?
- Who has access to modify the chart of accounts, bank account data for vendors, or process journal entries?
- Who is turning approvals on and off or opening and closing periods?
- What data are your operating system administers and/or database administrators changing?

Q Software automates the audit and security lifecycle in business applications. This includes:

- **Audit Reporting.** Q Software allows the organizations to efficiently and effectively provide auditors with proof that Segregation of Duties (SoD) controls are in place, even for organizations who are not subject to regulations such as Sarbanes-Oxley.
- **Segregation of Duties.** Q Software enables Segregation of Duties (SoD) management to ensure that conflicts are not being allowed and that controls are in place to effectively prevent fraud and misconduct.
- **SOX Compliance.** Q Software streamlines internal control management, monitoring, and auditing in context of SOX requirements to ensure that a company's financial statements are accurate and give a complete and true reflection of its activities and performance.
- **Fraud Detection and Prevention.** Q Software monitors transactions and controls in ERP environments to find and detect fraud that could have gone undetected for years, and this would involve huge sums of money as well as damage to reputation and share price if it was not for Q Software.
- **Security Management.** Q Software effectively and efficiently manages security configurations and access in ERP environments that otherwise organizations find to be complex, time-consuming, and frustrating.
- **License Audit.** Q Software enables an organization to manage Oracle and JD Edwards licensing costs by keeping an accurate account of ERP use and what users are using what access. This enables compliance and controls of ERP system access; not only can the solution indicate when they are out of scope with their Oracle license, but it can also show who can access what application and enable them to plan potential license savings.

Benefits Organizations Have Received with Q Software

Most Q Software clients moved to the solution because they found their manual document-centric approaches for ERP access management consumed too many resources. Too often things were getting missed in the continuous barrage of ERP access complexity, as well as in regulatory and business change. Others moved to Q Software as they found their previous access risk solution was dated, cumbersome, too costly to own and maintain, and lacked the ease-of-use and intuitiveness that the business needed to understand access risk and related processes. Across these clients, there is consistent praise for the value of the ongoing cost of ownership of the Q Software platform, in the speed of deployment, return on investment, improved effectiveness, and agility to manage, monitor, and enforce access risk.

Specific benefits that GRC 20/20 finds that Q Software clients have achieved in their implementations are:

- *360° visibility into ERP access risk* where all information is in one place and gives complete situational and contextual awareness of user access risk and history of usage in relation to business role(s).
- *Elimination of hundreds of documents, spreadsheets, and emails,* and the time needed to monitor, gather, and report on them to manage access related activities and processes.
- *Significant efficiencies in time* through automation of workflow and tasks, as well as reporting. Specifically, the time it took to build reports from hundreds to thousands of documents and spreadsheets now is just a matter of seconds.
- *Fewer things slipping through cracks* as there are established tasks, monitoring, notifications, and escalation when access risk exposes itself in the ERP environment.
- *Efficiency in streamlining processes* through identification of controls, access rules, requirements, accountability, tracking, and getting things done.
- *Greater granularity and ability to report* on specific ERP access risk and control details that could not be done in documents or spreadsheets.
- *Increased awareness and accountability* of ERP access by business owners who are informed on the subject matter in context of their role and management of licenses in this context.
- *Collaboration and synergies across ERP* access management functions and business owners, instead of different roles doing similar things in different formats and processes.
- *Consistency and accuracy of information* as the organization conforms to consistent processes and information structures.

- *Accountability with full audit trails* of who did what and when in the ERP access environment.

- *Reduction in time needed to govern and manage ERP access requests* that are freed from manual processes - these resources can then focus on value-added activities.

- *Increased agility in context of change* that enables the organization to be proactive in keeping up with ERP access and roles when the business changes and not just reactive - leading to less access risk exposure and being caught off-guard.

- *Mitigation of fraud* in the ERP environments.

- *Full access review and monitoring* as clients are able to be less reliant on random sampling where critical access issues are often missed.

Considerations in Context of Q Software

Every solution has its strengths and weaknesses and may not be the ideal fit for all organizations in all situations. While GRC 20/20 has identified many positive attributes of Q Software to enable organizations to achieve consistent ERP access risk management processes, readers should not see this as a complete and unquestionable endorsement of Q Software.

Q Software's clients praise the company for its solution delivery, but also praise it for the depth of its understanding of their ERP environments and access risk. Q Software is there to work with the client and be a true partner and knowledge source, not just a software provider. Q Software enables organizations to efficiently manage ERP access risk across complex and distributed ERP environments. The applications facilitate real-time collaboration and access risk information sharing across the enterprise and provide comprehensive visibility into access risk management and compliance.

At the end of the day, Q Software saves organizations time over manual processes for ERP access risk that also delivers greater effectiveness and agility to the organization. This enables organizations to meet audit requirements, better understand segregation of duties, and document mitigating controls. Documentation and reports are ready to present to auditors and risk/board committees. Overall, it gives an organization a clear understanding of their ERP access risk that are throughout the business and does so in a context the business can understand without the overwhelming complexity IT often presents. Q Software delivers an integrated team of audit trained staff and IT security professionals that support the solution and advise their clients. The software is what client's use, but it is the experience of Q Software that makes it work for clients.

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.

GRC 20/20 Research, LLC
4948 Bayfield Drive
Waterford, WI 53185 USA
+1.888.365.4560
info@GRC2020.com
www.GRC2020.com