Key Considerations When Selecting GRC Software

Understanding key controls & how to select risk management software.

By Norman Marks

Table of Contents

About Norman Marks

I have been a practitioner and thought leader in internal audit, risk management, and governance for a long time. I have led large and small internal audit departments, been the Chief Risk Officer and Chief Compliance Officer, and managed IT Security and governance functions.

I have two blogs, www.theiia.org/blogs/marks and normanmarks.wordpress.com, I try to post on both once a week.

I retired in early 2013. However, I still blog, write, train, and speak – and mentor individuals and organizations when I can. You can reach me at nmarks2@yahoo.com.

My latest adventure is a collaboration with Richard Anderson, former chairman of the Institute of Risk Management. Risk ReImagined includes webinars and one-day in-person events around the world where we can have a conversation about the effective management of risk.

I am fortunate to have been recognized and made a Fellow by OCEG for my commentary on GRC, and an Honorary Fellow of the Institute of Risk Management for my contribution to the risk management field. I am also pleased to contribute to the profession through my activities in support of the IIA and ISACA, articles in various publications, and membership of periodical review boards (including the *Internal Auditor*, *ISACA Journal*, and *EDPACS*).

-Norman Marks

User Access Risk and SOX Compliance

When you take a top-down, risk-based approach to the assessment of internal control over financial reporting (for Sarbanes-Oxley, "SOX", compliance purposes), it is quite possible to make a significant reduction in the number of key controls included in scope.

The only controls that need to be included in the scope for SOX are those that are relied upon to either prevent or detect a material misstatement of the financial statements. We call those "key controls".

In my best-selling book, *Management's Guide to Sarbanes-Oxley Section 404: Maximizing Value Within Your Organization*, I suggest this definition:

> *A key control is a control that, if it fails, means there is at least a reasonable likelihood that a material error in the financial statements would not be prevented or detected on a timely basis.*
>
> *In other words, a key control is one that is required to provide reasonable assurance that material errors will be prevented or timely detected.*

The top-down, risk-based approach (which US regulators require external auditors to follow and encourage management to adopt) focuses the attention on key controls.

Organizations have a great many controls designed to address their various business risks. The top-down, risk-based approach enables management to exclude from the SOX scope controls that may be necessary for other business reasons (e.g., to protect valuable intellectual property) but are not key controls for SOX.

It is also possible to limit the number of controls, or "rules", relied upon for user access risk for SOX.

By “user access”, I am talking about access to computer systems not only by business users (such as those in accounts payable, manufacturing operations, or cash management) but by people in IT charged with maintaining the systems in question.

I have led training classes for SOX program managers for quite a few years. A recurring theme is that the organizations they represent may have hundreds of access controls (“rules”) in their SOX scope.

They don’t need them all, not for SOX. They are not all SOX key controls.

Some history may be required to explain what I mean.

Many if not most organizations designed the IT portion of their SOX scope, including access controls, separately from the business process and risk side. They did not take a top-down, risk-based approach to identify what might go wrong in IT processes and activities that would lead to a material error or omission in the financial statements filed with the SEC. Instead, they relied on some combination of:

- Checklists from consultants and others that listed access that should be limited, especially combinations of access that might represent a segregation of duties problem
- Their experience of what constituted best practice in limiting user access
- “Rules” included by vendors in their access control software – typically these can number about 140

But very often these rules may be necessary to run the business but highly unlikely to result in a material error or omission in the financial statements.

Examples of rules I have seen that are not critical for SOX, not key controls that need to be included in scope, are:

- Rules about who can authorize a purchase requisition or order. Even if an unauthorized individual orders millions of dollars of materials or services, the financial statements may be correct: they will accurately record the expense and the level of cash

- Rules about the ability of HR personnel to access payroll records. While it is possible that fictitious employees are set up and paid, it is highly unlikely that would ever be material to the financials – and the expense, though improper, has been incurred

The question to ask for all access rules is "if this happened, if this access was granted, is there at least a reasonable possibility (given all other key controls) that an undetected material error would be introduced into the financial statements?"

But there is a need for some level of access control rules. Examples include rules where:

- A key control limits who can perform an activity, such as the approval of a journal entry
- Access needs to be limited to certain powerful system commands, such as "root" access, that would enable an individual to bypass controls

At my last companies, we applied a top-down, risk-based approach and were able to reduce the number of access control rules in scope for SOX from more than 100 to less than 20.

But, managing user access can be a challenge.

When I ran the internal audit function at Maxtor, a $4bn manufacturer of disk drives, I also led the SOX compliance work on behalf of management.

When it came to access controls, our top-down and risk-based approach allowed us to reduce the number of rules in scope very significantly.

But we still had a problem!

We used software to identify violations of the SOX user access rules.

- The first time we ran the software, we had more exceptions than employees! Management agreed to take prompt action and we came back after a few weeks.

- We reran the software and the number of exceptions was down from the thousands to a couple of hundred. Some were repeat exceptions that management had missed, but an equal number were new ones! Management again agreed to act quickly and we returned in about two months.
- Again we ran the software. This time, there were no repeat exceptions. But there were over a hundred new ones. We told management that time was running out to correct the situation before year-end.
- We ran the software with hope and trepidation. Fortunately, there were less than ten exceptions and we were able to identify some mitigating controls, to the extent that we did not have a material weakness for SOX.
- Around year-end, our external auditors ran their software to test these key controls. I went to my knees in prayer. Thankfully, their scans came out clean.

The right software can help you manage access risk. In fact, I am not sure that the typical organization can manage it acceptably without software. That will be the subject of a second blog post on this topic of user access.

For more on this issue, please refer to *Management's Guide to Sarbanes-Oxley Section 404: Maximizing Value Within Your Organization.*

Selecting Software to Help Manage User Access Risk

I believe software is essential in managing user access risk, not only for SOX but also for other business risks.

In fact, the potential harm from inappropriate access is typically greater for other business risk (such as the possibility of disruption of activities such as revenue generation or manufacturing, reputation risk, and the protection of valuable intellectual property) than it is for SOX.

The first step to selecting software, for this or any other purpose, is to define your needs. What do you need, which are the priorities, and how valuable is satisfying each need?

Is this just for SOX or, as I prefer, to manage all access business risk?

For most organizations, these needs will probably include:

- A report that will identify violations of each access rule
- A report of changes to access rules
- The (provisioning) ability to scan requests for access, before such access is granted, to identify potential rule violations so they can be denied
- The ability in the access provisioning system to ensure that the owners of each system, the manager of each employee, and others as needed, approve all requests for access
- Reports for each owner of a system that will enable a review of who has access to each system he or she is responsible for
- Reports for each manager so he or she can review what access their employees have
- The ability to manage access within and across multiple systems, i.e., not just the financial systems or ERP, but every system where access needs to be managed
- ...and more

In many cases, a single software package will be needed. But where access to multiple systems is needed, it may be necessary to obtain a combination of software products.

For example, different software may be needed to run reports of access to the financial systems; a manufacturing system; a wire transfer system; and a system that manages physical access to buildings.

Given that, here are some criteria I would consider in selecting a software package:

- Does it meet my needs, in particular those of the highest priority? Will it meet my needs for the foreseeable future?
- How will I have to change my business processes? Will it support the way I want to do business?
- What do current users of the software have to say about the vendor?
  - Do they say that the software meets their needs?
  - Are their needs similar to mine?
  - How easy is the software to implement?
  - How easy is it to maintain?
  - Is the vendor's customer service excellent?
  - What other solutions did they consider?
  - Do they recommend this software?

- What is the vendor's reputation? Are there complaints or lawsuits against the vendor and do they relate to this piece of software?
- Is the vendor financially sound? Is it committed to this software (if it has a small market share, it may limit future investment) or is this a small part of a larger offering? Is the vendor a target for acquisition?
- How does the vendor manage upgrades or new releases? If there is a problem with functionality, how does it decide whether and when to issue upgrades?
- Does the vendor have not only sales but also support staff who understand the business? Do they understand access management and how it needs to be managed?'

Is the support and development staff substantial and able to maintain and upgrade the software when needed?

- If, as is likely, consulting services will be needed to assist in the implementation of

the software, are reliable consultants available, at a reasonable cost, who have the necessary expertise and experience? How good are their references?
- What is the cost of the software, considering not only the initial acquisition cost but the cost of services that will be required to implement and then maintain it, and the ongoing software license cost?
- Will the IT staff be able to provide necessary internal support? Will it be compatible with the network strategy?

A couple of thoughts from experts at consulting firms build on my points:

- "When choosing your software, you want to make sure the vendor has the expertise to keep the methodology up to date. Otherwise, you may be constantly training your vendor," Said Matt Bonser, Risk Assurance Director at PwC. "Choose a vendor that is making investments in their tools instead of making changes by only reacting to customer issues."
- "We recommend to our clients that they prepare a technology-agnostic solution design as the first step in selecting a GRC tool or any other enterprise-level application", said Ronan O'Shea, Protiviti's Global ERP Solutions practice leader. "Analyze the business processes, business rules, data, event triggers, reports, etc. from an optimization and automation perspective and let the solution design, supported by critical use cases, drive the choice of technology, not vice versa."

A vital consideration is the question of who will own the software within the company. I have seen situations where nobody takes ownership of the responsibility for managing user access risk.

I highly recommend resolving that question *before* acquiring software. Whoever will be responsible for managing the business risk from inappropriate access should lead the acquisition process.

Over the years, I have been involved in acquiring access software for several companies. Sometimes, it was straightforward but the more complex the business and the variety of access rules that need to be managed, the more critical it is to get this right.

If I was to leave you with one message it is this: make sure you have a robust provisioning capability. If you are able to *prevent* excessive access being granted, you will save the cost of the software quickly – IT and management won't have to spend many hours chasing and correcting exceptions only to see new ones every month.

Most important, you will be able to maintain user access risk at acceptable levels.

In the previous blog post, I shared my story at Maxtor. The reason that new access violations kept appearing was that while reports were available to identify violations, the process for granting access was very weak. Our risk was high until we fixed the provisioning process.

I hope this paper will strengthen your selection process.