Risk as a Process Challenge

Naresh Podila
Vice President, SDG GRC Solutions

SDG

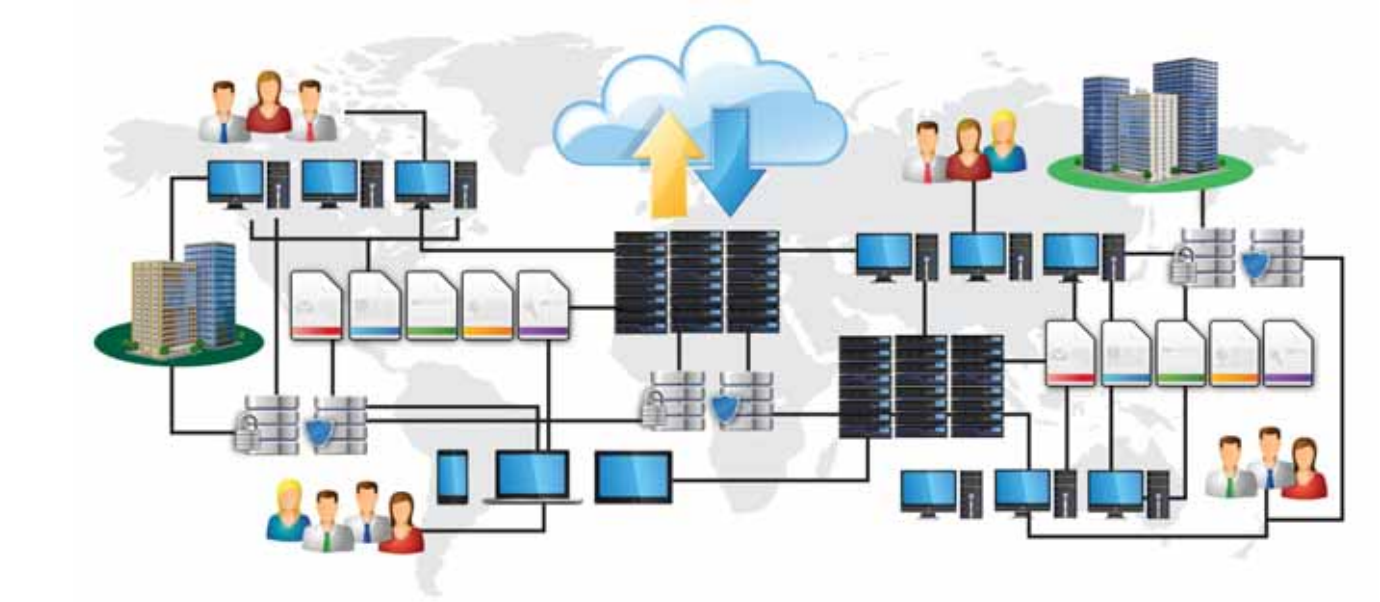
[technology + passion] - risk

Most organizations recognize that their competitiveness and sometimes their very survival depends on their IT applications and infrastructure working effectively and efficiently.

Managing IT risk is an urgent need for every organization and automation is generally required for true effectiveness. However, choose Governance, Risk, Compliance (GRC) automation that matches your organization's risk culture and process maturity. Overly complex GRC software might be making your task more difficult that it needs to be.

First, let's survey the IT landscape.

IT assets have proliferated. There are smartphones, tablets, laptops and desktops—and all are repositories of corporate data. Corporate applications span multiple assets. And they are often owned and managed by disparate teams. For example, the server infrastructure on which an application resides might be owned and managed by a different team than the database for the application. Compounding matters, the network over which the application works might yet be owned by a third team.

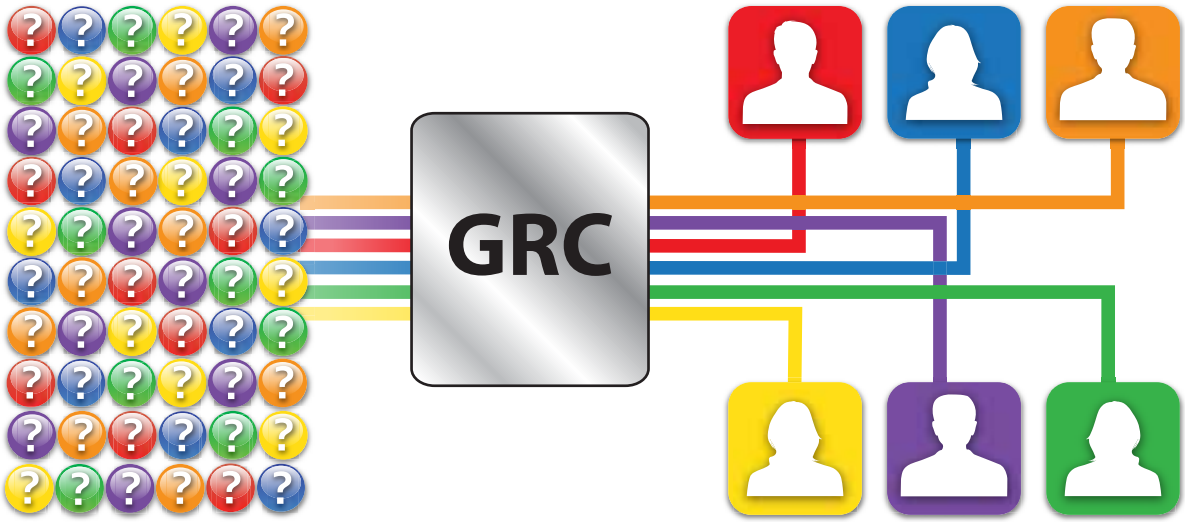


As a risk professional, you need to understand risk scenarios applicable to each of these unique aspects. This means you must ask of each owner different questions to unearth the risks. Numerous parties need to weigh in on any assessment. For example, if you are assessing the risk associated with the server on which the application is installed, you might want to know what kind of end-point protection mechanisms are in place. On the other hand, if you are assessing the risks associated with the underlying operating system, you will probably want to understand the patch management regime. As you question the owner of the data, it is important to know what kind of information is stored on the application—whether it is customer *Personally Identifiable Information (PII)* or corporate classified. The application owner might need to answer to assessment questions related to the processing of information to make sure there is no risk of S*tructured Query Language (SQL)* injection or Cross-Site Scripting (XSS).

Then there are questions that need to be asked of all Internet facing applications that are not relevant for internal applications. Depending on the nature of the application, risk assessment questions may arise that are completely custom to that application. If you expand this further and the application is in the cloud, there arises a whole new set of risks to be assessed. In addition, to develop a full-fledged risk profile, an assessment of the cloud provider also becomes necessary. If the application is also available on a mobile platform, that adds a whole new set of risks. There are countless possible scenarios to consider.

Simply stated, as hardware, software, hosting and delivery options for your corporate data, network and applications proliferate, so do the number of disparate parties you have to go out and query as part of your risk assessment. If you have one standard set of questions and you send out to all your constituents, the question set will be unnecessarily long and will have a lot of irrelevant questions for each individual constituent. So, the questions you ask must be customized to each aspect of the asset. Furthermore, questionnaires might need to be custom-built based on special considerations for each application.

It's important to note that because of today's enterprise complexity, constituents might not only be on different teams in different continents, they might also be part of outsourcing arrangements. In such a situation, your risk assessment might need to be delegated to a third-party organization.



Today's risk leader has to be able to manage a large bank of questions that can then be custom-served to each of the individuals or teams responsible for the different aspects of the application. It is important that they all see only those questions that are relevant to them and that they remain committed to the process. In addition, the responses might need to be routed through several rounds of reviews in the organization before final approval.

Questions of control.

The next step after getting back your risk assessment information is to ask appropriate control questions. As with risk assessment questions, control questions should be relevant to the situation and the appropriate controls framework (COBIT, COSO, ISO 27002, etc.). Not only must they relate to the aspect of the application that you are assessing, they must also tie directly to the answers provided to you on the risk assessment. For example, if an application handles PII data you might want to investigate further what kind of Data Loss Prevention (DLP) controls are in place to protect the data.

Do you have the right culture for risk management?

Organizations are still evolving to become fully risk-aware. Application and infrastructure owners are slowly getting sensitized to the subject. With the media reporting a slew of breaches and data loss events—seemingly every day—everyone is much more aware of risk. But at the same time, the demands of today's open culture are tugging us in the opposite direction to being less restrictive. Trends such as Bring Your Own Device (BYOD) and social media are developments in that direction. To deal with this yin and yang, risk managers face pressures to be more restrictive. Yet they must also respond to the cultural demands of our times. These facts require many important policy and posture decisions. The first of which is to evolve a common risk nomenclature and definitions around risk. What is the scale on which you want to measure the impact and likelihood of each risk? What is your organization's risk appetite? Who is the arbiter that determines when to accept a risk vs. when to invest further to mitigate that risk? Or do you stop doing an activity altogether because it carries too much risk for the organization?

...responding to the cultural demands of our times requires many important policy and posture decisions.

Calculating your options.

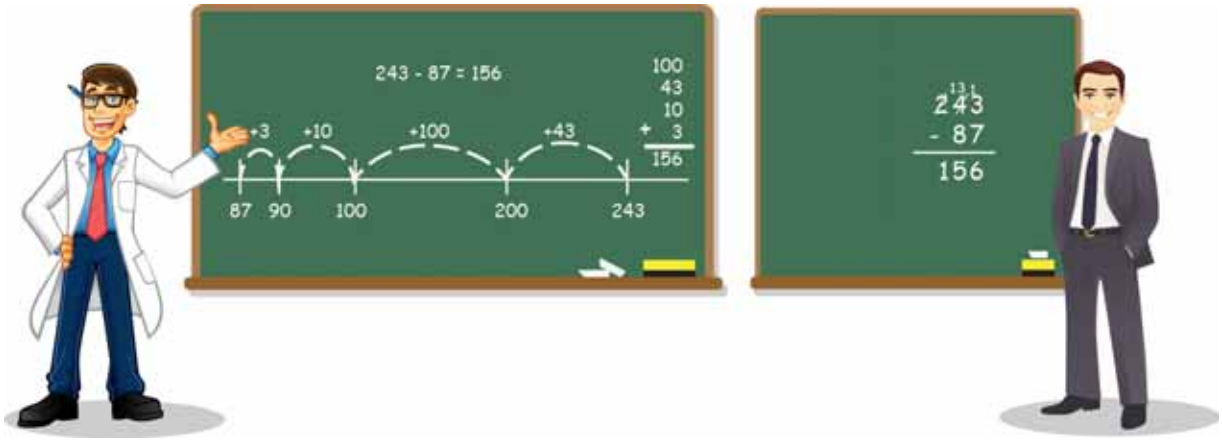
In addition to considering your organizational culture, there are calculations to be completed at every stage. The answers to the application questions must help you arrive at *Confidentiality, Integrity, Availability (CIA)* scores. Risk scenarios need to be evaluated. The answers to the risk questions must help you determine the impact, likelihood and a risk score for each scenario. Those numbers must go into your determination of which assets must be subjected to a controls evaluation and furthermore which applications need a formal risk treatment option. A comparison of the different risk treatment options might involve further computation to arrive at the option with the best ROI. If you are a large organization with a significant asset base, you have an incredible amount of data in question and perhaps thousands of applications. Thus, the process could take too long and drain too much manpower. That's because much of the calculation is done "behind the scenes" by the risk leader and his/her team and because there is no shared understanding of the risk environment. Lack of visibility to risk information means decision makers cannot make the best risk-aware decisions.

Making choices you can implement.

The need of the hour is not complicated risk assessment formulas, but simple, quick-to-implement risk management systems. These should help you solve for risk management as a process problem.

Most available solutions are too complex for where organizations are today...

Most risk management and GRC software solutions today have way too many "bells and whistles." Because of this, organizations either spend all their time trying to configure features that they will probably never use. Or they spend years waiting for the corporate risk culture to evolve so they can effectively utilize the software. It's no coincidence, for example, that Gartner© focuses on time to implement as part of their GRC Magic Quadrant© consideration. Most available solutions are far too complex for where organizations are today from a risk management culture and process perspective. So, in essence, their expensive risk management software becomes *shelfware*.



Your goal should be to evolve the risk culture in your organization and develop a simple and effective process to manage risk. It should not be in battling the *GRC* structure or risk management software to implement those features (or "bells and whistles") that you will never use.

Buying and implementing GRC software is an important part of having a successful risk management program. But let the software be an enabler in helping you manage and automate the process. It should also be an enabler in terms of doing the math for you. But the software will not put a process in place or propagate a risk-aware culture for you. You have to do that, which is hard work in itself. Don't let the "bells and whistles" distract you from this important work.

1. Survey the IT landscape
2. Identify key assets: applications, infrastructure, PII etc.
3. Implement your GRC tool & build your risk scenarios
4. Determine your controls (COBIT etc.)
5. Develop your risk questions
6. Let you risk culture evolve

Weigh your options carefully and choose wisely. Risk management software should be simple by design, quick to implement and be able to evolve with you. As your organization's risk processes and risk culture mature, it should mature with you.

About SDG

SDG is a leading provider of technology, consulting and risk management solutions to strengthen enterprise businesses while managing IT risk. We focus on six practices: Risk and Security; Identity and Access Governance; Digital Collaboration; Quality Assurance; Mobility and Cloud. In addition we offer a GRC solution, called TruOps, to manage enterprise IT risk and compliance.

"SDG helps enterprises realize their dreams by helping them develop, manage and deploy solutions with acceptable risk."

For over two decades, SDG has enabled enterprises to realize their dreams by helping them develop, manage and deploy solutions with acceptable risk. We combine technology, thought leadership and a relentless passion for customer success. SDG partners with enterprise brands, but we specifically focus on mitigating client IT risk. Our ultimate goal is to help enterprises realize the opportunity of technology, increase innovation, improve speed-to-market and maximize returns on investment.