GRC FAQ

Frequently Asked Questions about Governance, Risk, and Compliance (GRC) Systems

Last reviewed by the EDUCAUSE IT GRC Advisory Committee and the HEISC GRC Working Group: June 2016

What is a Governance, Risk, and Compliance (GRC) system?

Governance, Risk, and Compliance (GRC) systems are integrated applications that typically offer "modules" that help automate these basic business processes. Some of the kinds of processes they can help organize are:

- managing the policy development, dissemination and attestation process;
- tracking requirements of law, regulations, standards, and frameworks such as ISO and NIST;
- monitoring and ensuring compliance obligations are met, such as those required by PCI DSS, GLBA, and HIPAA;
- issuing surveys to business units to check themselves against those requirements to find gaps;
- doing risk assessment exercises and treating risk factors, especially against the gaps found;
- tracking mitigation activities taken to reduce those risks;
- automating incident or issue tracking to ensure each is logged, tracked, routed to the right person, completed, etc.;
- and often much, much more!

Why would I want to invest in a GRC system?

Basically, a GRC system allows you to pull together policy, compliance, risk, remediation, data archiving, and reporting information all into one tool.

A GRC system can help in inventorying and classifying data, and in documenting and monitoring the required security controls. Such a tool can help aid in a more efficient and effective approach to privacy and information security, organization-wide; and ultimately can help lessen the burden of the end-user and/or information technology staff.

Numerous compliance obligations, as required by law, regulation and contractual agreements, require institutions to monitor activity through questionnaires and surveys pertaining to information security and privacy, as well as other risk-related areas. Web-based questionnaires based around compliance requirements can be built and distributed using a GRC tool, rather than having a variety of manual processes in place – no more spreadsheets emailed back and forth!

Most GRC solutions offer cross-referenced security controls related to compliance and other standards and frameworks, allowing the end-user to answer one question which will trigger or skip another based on the answer. Rather than filling out numerous disconnected spreadsheets asking similar questions, the end-user or IT staff can be prompted to verify previously entered and saved information at predetermined intervals, in order to satisfy overlapping compliance requirements. The tracking of information assets can be managed and data on endpoints can be maintained in a more efficient and effective process.

The use of one portal for all governance, risk and compliance needs supports a collaborative approach between internal offices such as audit, information privacy, security and compliance, to name a few. Data entered and used for one aspect of the governance, risk, and compliance processes can be accessed and re-used for another aspect without requiring end-users or IT staff to re-enter their responses. This is particularly effective when used for the full life-cycle of GRC processes: managing inventories of assets, compiling inventories of compliance obligations, recording answers to self-assessments of assets against compliance obligations, automatically monitoring compliance (for some types of controls such as firewall settings and workstation settings), identifying gaps in compliance, applying risk assessment variables to those gaps, choosing the highest risk gaps to address, and tracking remediation plans to reduce those risks, archiving data, and providing reporting. Considering that these processes should be taking place at regular intervals such as annually or bi-annually, automating them through an integrated, enterprise-wide GRC can make this daunting task feasible, efficient, and effective.

Many GRC systems offer designated and dynamic dashboards to allow units to self-manage their own compliance and risk, with oversight from respective internal authorities. Through reporting features, senior leadership also has the option to quickly assess the overall compliance posture of the institution, identify gaps, measure risk, do trend analysis, and use this information when strategic planning and allocating resources.

Is a GRC system only used by Information Technology?

Although many GRC systems on the market today only encompass what is called IT-GRC, or started out only offering an IT-GRC solution, these systems are being designed for and used by many other areas of the business today, including enterprise policy management, enterprise risk management, compliance tracking for areas such as Environmental Health & Safety, and even for management of Internal Audit processes. As you can imagine, if you find a way to automate some basic processes that IT needs to manage, you could then USE those processes in any number of business areas.

This is one reason why the GRC market can be so confusing! Some organizations will purchase and use a GRC tool for only one or a few purposes /business needs (such as IT, or risk assessment), and others will use it for a number of different business needs. Some will use it only within one administrative structure or unit, while others will use it enterprise-wide.

So, do I want an IT-GRC or an Enterprise GRC product?

It depends! Here are some hints:

- In general, a product being advertised as an IT-GRC solution will be more functional – have more "bells and whistles" – applicable to managing IT, than will an enterprise GRC solution. But an enterprise GRC will offer more types of functionality in order to serve a number of different business functions.
- IT-GRC systems are more likely to offer the ability to automatically test IT controls; that is, for the system to automatically connect to devices and check if a control (such as a firewall setting) is still in place or not, and report back. However, you may find that, even if you are only going to use it for IT-GRC, a particular enterprise GRC solution offers all that you want.
- It seems as though enterprise tools require more configuration and tweaking, but we don't have a good way to verify this. It may just be that there is a lot more that CAN be configured in such tools, to make them seem this way.

- In many cases the knowledge bases for IT controls weren't as comprehensive in an enterprise product. However, even with comprehensive libraries of IT information, you still have to do a lot tweaking of that information to fit your environment. An enterprise product will also have other libraries of GRC information that you may find useful.
- If your organization has an Enterprise Risk Management office, or a Risk Management office, be sure to check with them before deciding one way or the other.

Keep in mind that the marketplace is constantly evolving, so do not be too quick to discount solutions that others or even the vendor have labeled as one type or the other. Focus on the functionality you need and which vendors provide it.

What modules do I need?

There is no standardization for naming of the "modules" provided by GRC vendors, so it can be challenging to figure out what module or modules offered by each vendor will meet your specific business needs. Also, the name of the vendor's module might be very specific to a business purpose, but actually the module could be used by any other business purposes that have the same underlying basic process needs.

So for example your compliance staff might use a tool's "Compliance" module to manage compliance with OSHA, while your IT folks might use the same module, or one called "IT-GRC," to implement an ISO 27001 or 2 framework. Your business continuity folks might use a "Policy Management" module to develop and track BC plans, using the routing to have someone review the plans submitted, while Human Resources might use it to draft, review and issue the institution's HR policies. And your Risk Management folks might use a "Risk Management" module to assess risk in any number of areas, including IT. Or maybe just your IT folks use the Risk Management module to assess IT risk.

How do I differentiate between all the various GRC vendors and products?

There are a number of ways to differentiate between the products:

- Each vendor's product will be stronger in some areas, and weaker in some areas. They seem to all be trying to be all things to all people, but if you pay attention you can figure out which products are particularly robust in what functions. Thus, it depends on your goals for the use of the tool by your institution, as to what you will be looking for in a GRC system, and thus what you will end up with as the best product for the purposes you identified.
- If you decide to go with a true enterprise solution to use beyond IT, then the pool of vendors will be different than if you look for an IT-GRC. Some vendors fit both categories, but others can only provide functionality in one or the other.
- Some vendors only provide a hosted solution, while others allow you to load the software locally and run it yourself. Some provide both options. Consider who will manage the infrastructure in your implementation – the server, the web app, the database, the application, etc. – and in test, development, and production environments. Involve them in the process of choosing a product.
- Consider your staffing and your plans for local enhancements. If you do not plan to support the development of local solutions and enhancements using the tool, look for a product that offers more of what you need "out of the box." On the other hand, if you do plan to customize or create local enhancements, ensure you choose a vendor that supports your local enhancement needs.

What should I do first if I am interested in procuring a GRC system?

First, identify what business functions will use the system. Clearly define and consider what processes you want to improve, and what kind of improvements you are seeking. This is KEY to being able to narrow down the large pool of available GRC systems!

Although some corporations purchase all modules for use in nearly all business areas in a true enterprise GRC implementation, it is hard to imagine a college or university so centralized that it would decide EVERYONE will use it for ALL governance, risk, and compliance activity. More realistically, there will be a champion (maybe this is you) who will be leading the initiative to obtain a GRC system for his or her own business function. Depending on the culture at your institution, consider inquiring as to whether other potential GRC stakeholders would be interested in joining with you on the initiative. This will help you determine the scope of your project and what modules you are most interested in procuring.

Possible GRC Stakeholders may include:

- Central Compliance Office
- Central Information Technology/CIO
- Privacy
- Risk Management/Enterprise Risk Management
- Information Security, including Incident Response
- Business Continuity
- Environmental Health & Safety
- Research Compliance, Human Subjects, Clinical Trials
- HIPAA Compliance/Health Sciences
- HEOA/Clery Campus Safety Compliance
- Human Resources
- Financial, including PCI DSS
- Internal Audit

This process of determining what enterprise business functions will use the system, and for what processes, can take a lot of time up front, but it is well worth it to ensure that you choose a product that will fit you and your institution. Otherwise, you may eliminate GRC products that fit your realistic needs well, because you are specifying far more functionality (which always comes with more complexity) than what you will ever need.

Perhaps in ten years, we will have seen other college and university business units besides IT buying in and working together to implement a truly enterprise governance, risk, and compliance solution, but we aren't seeing that yet. Thus, today you will see the higher education institutions profiled here focusing on various different aspects of a GRC implementation.

What are some of the challenges others have experienced in their implementations, that I should be sure to consider? What have others done to address these challenges?

- Realize that GRC products are complex, even ones that are characterized as usable "out-of-the-box." Be prepared, and plan for many hours of consulting and configuration before deployment - probably months. For example, the University of Florida purchased Modulo for IT risk management in August 2011, began Webex-based consulting in September, and probably won't deploy until spring 2012.
- Consider other related organization-wide projects and whether the various products need to have the ability to communicate. If so, make sure while choosing a product that the back-end technologies have the ability to integrate with one another.
- Consider authentication needs if your organization has an existing common technology to access applications, such as Co-sign or Shibboleth. What are your campus authentication/directory/IDM implementation requirements? Ensure the vendor can support your requirements – many cannot.
- Ask vendors if you may test/pilot their product before making a decision to purchase. Arrange for an internal team to test all aspects of the product, especially any integration or authentication needs, to make sure it is a good fit for your institution. Penn State used this method and learned that not all systems can integrate as well as the vendor thinks they do.
- What roles do you need the product to understand? How will you populate your organization's structure and assets into the new tool? Who has authority to access various modules of the application? These are some of the largest challenges you will face as you begin an implementation project.

Higher Education Institutions Currently Investing in GRC Systems

- California State University System
- Indiana University System
- Penn State
- University of Florida
- University of Maryland University College

Web Resources and Articles

Higher Education Resources

- EDUCAUSE IT GRC Initiative
- ECAR Report on IT GRC in Higher Education
- The Economics of an IT Governance, Risk, and Compliance Solution - A presentation delivered by Chrisan Herrod (AVP/Chief Information Security Officer, University of Maryland) at the EDUCAUSE Mid-Atlantic Regional Conference 2012.
- Governance, Risk, and Compliance Systems in Higher Education - A presentation delivered by Merri Beth Lavagnino, Sarah Morrow, Jennifer Stewart, and Cheryl Washington at the Security Professionals Conference 2012.

Additional Resources

- MetricStream IT GRC Software Solutions - scroll down to see a list of benefits
- Brinqa - provides a visual overview of their solutions
- Modulo - shows the solutions and differentiators
- SC Magazine Policy and Risk Management Group Test

Questions or comments? Contact us.

Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0).