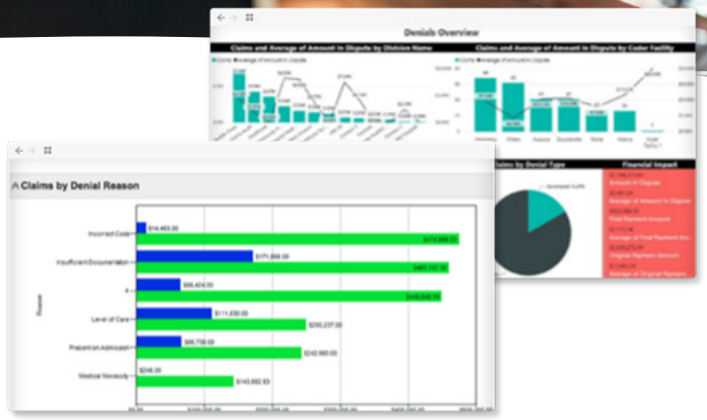


SAI360

Risk | Learning | EHS | Sustainability

WHITEPAPER

Evaluating in-house developed GRC Technology: Four major considerations

In-house developed solutions vs. GRC software

As recently as a few years ago, when executives and management teams discussed how to manage governance, risk management and compliance (GRC), some of the questions were:

- Excel spreadsheets seem to be working well for the organization, or aren't they?
- Should we use spreadsheets to "automate" compliance and risk management projects?
- Why spend precious budgets on software when much lower-cost solutions are available?
- Is it time to go through the trouble of selecting and implementing a GRC platform?

Today most discussions have moved well beyond "if" there is a need for a solution or the pros and cons of spreadsheets to now talking about how to solve GRC challenges with technology. Many executives and managers would like to get more out of their businesses, share verified information, compile one unified version of records, reduce repetitious work cycles across multiple functions, keep up with regulatory requirements better, avoid and manage risks, and document everything appropriately. It is a long list of improvements.

These business needs and new, more sophisticated technology mean that GRC support discussions now turn to focusing on whether to buy standard software or to build a solution in-house.

When organizations consider the needs of the business it may be tempting to think they will be best met when designed and built by the organization itself. However, consider the following aspects when building a GRC solution in-house rather than buying a commercially available GRC solution:

- **Design Complexity –** Easily underestimated, development costs will almost certainly be substantially higher than initially budgeted because of the level of detail, integration and expertise required for sophisticated enterprise capabilities. Examples of these are plentiful, some of which will be provided in this white paper.
- **Comprehensive Functionality –** Each business within the organization will have its own set of requirements for a software development project. Approaching a solution design without analyzing the overlaps and gaps between each may inadvertently leave capabilities out completely or fail to link those that should be integrated.
- **Certainty of Compliance –** In today's dynamic regulatory environment actual compliance can be difficult to prove, especially under the extra pressure of non-compliant situations and possible prosecution.
- **Maintenance and Development –** The continuous evolution of technology and regulatory issues will be difficult and costly to follow, even more so when it is not the organization's primary focus.
- **Ongoing Support –** Maintenance can be costly and the lack of team continuity, documentation, or technological expertise can often lead to issues with the ability to support the solution long term.

This whitepaper elaborates on the challenges of building GRC technology in-house and takes a critical view of why commercially available GRC solutions are the preferred choice. Here are three topics to explore first followed by a list of planning considerations for an in-house build.

1. DEFINE THE NEEDS OF EACH ROLE

As risk management and compliance needs surface in an organization, different roles and businesses address them from their own perspectives. The needs are defined in terms of that function in the organization. Each wants to build a solution to solve its own pains. The list of requirements becomes long with little or no organization or consideration for the desired and future states. Or, where there may be similar needs but in disparate places in the organization. However, these requirements need to be aligned to enable users to leverage the data from different processes. There is a strong need for a common data model, something mature GRC providers have already figured out. Consider the needs for risk and control framework localizations, approvals, integrated process mapping, audit trails, and point-in-time compliance reporting. There are many individual considerations, and all of them for the various roles, need to come together. Even design discussions to sort the business needs and the software requirements become lengthy. As there is no baseline, there is no easy way to guide and finalize requirements discussions.

The impact of this is significant. The bottom line is that merely planning for the project is time-consuming when it is an occasional exercise as opposed to leveraging GRC best practices.

2. PLAN FOR THE UPSIDE OF COMPLIANCE

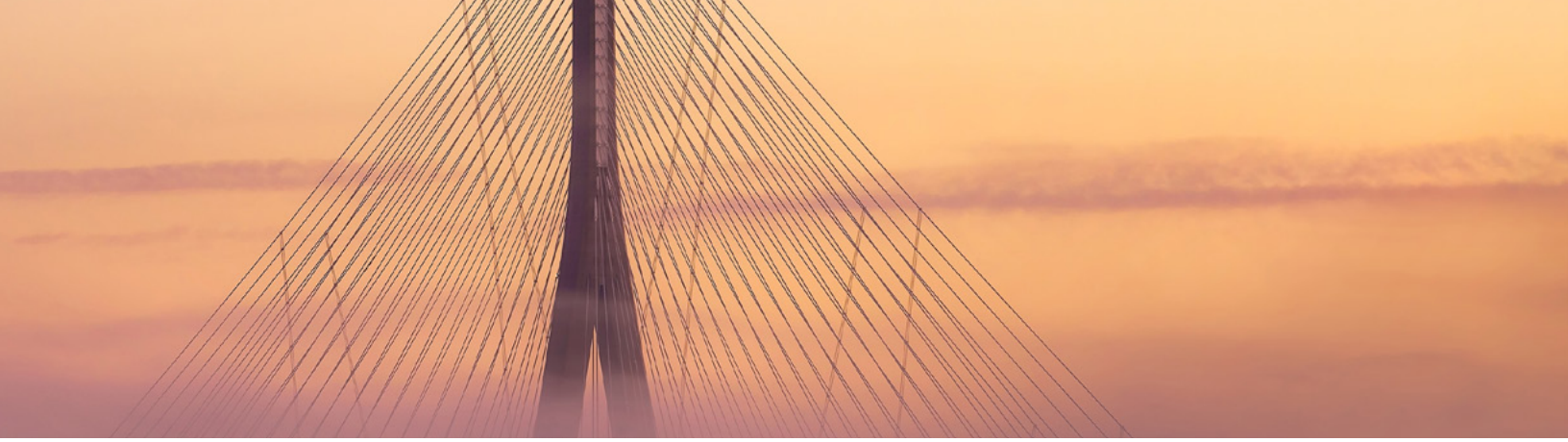
Organizations do need to prepare for what can go wrong. Anything from non-compliance to safeguarding the organization's reputation, to needing to mature business processes for greater efficiency are business realities of today. Having accurate, auditable records can significantly ease the burden that may occur when auditors and regulators need to become involved, or even more extremely, investigators, lawyers, or law enforcement. And it means the GRC solution needs to be implemented in a sensible, business-driven, and risk-based way. When implemented, a risk and compliance solution should be able to demonstrate all risks and controls, the effectiveness of those controls, and the associated evidence at any given moment depending on the regulation. Following a risk-based approach, an effective GRC solution can show for certain that controls are either not required, are effective, or that the risk is mitigated by another effective control.

The additional – incremental – benefits of a reliable enterprise wide integrated GRC solution include:

- Reliable information security, version management and data integrity
- Consistent data definitions for each control owner, using the same terminology per control
- Auditable data safely retained for long term reference
- Point-in-time compliance to demonstrate how responsibilities were defined, who was in charge and the effectiveness of the controls, all at a given moment in time These are aspects of a GRC system that mature GRC platforms have wired into their core architecture but that will have to be engineered into a system built in-house. The repercussions in regulatory fines due to a flawed audit trail, or the lack of historically correct reporting may cost much more than the investment in a GRC platform.

3. LEVERAGE THE BENEFITS OF CONVERGENCE

Convergence is the integration of various risk and compliance efforts into one approach, with one solution. There are limitless options for an integrated solution design. That is why the GRC system needs a set of agreed-upon rules and conventions, and an overarching view of the individual business unit needs.



Without them, the potential to have to organize manual reviews and corrective processes can be costly. Mature GRC platforms have based their architecture on hundreds and hundreds of implementations and practical experience with this. The pitfalls of failing to design this integration need to be calculated then factored into the business case for any house-build solution. In addition, the types of reporting capabilities that need to be written to support different roles and different views of the data are taxing. Technically, many things are possible but in a large-scale organization with little experience and expertise, it is expensive both today and into the future.

4. PREPARE FOR THE LONGER LIST OF BUILD CRITERIA

Even with the hurdles we've just discussed, an organization may still decide to build its own GRC solution. Experience shows that this approach is many times more expensive than buying a proven GRC solution. Commercially available solutions have been tried, tested, and optimized in many client situations. Hundreds of thousands of users are operating each commercially available platform daily. These providers have invested hundreds of thousands of development hours and continue to do so. In addition, the timeline of investing several months on software development to develop a system capable of meeting even basic regulatory compliance requirements is ambitious.

The other issues to address and capabilities to include in the solution is:

- **Content Management –** Integrate a content management system into the solution including version and authorization management.
- **Web-based and mobile-enabled –** Choose to make the solution web-based, it dramatically reduces IT maintenance. More and more solutions will be deployed on mobile devices with the distinction between mobile and non-mobile devices slowly disappearing.
- **Scalable –** Include the ability to hold thousands, even millions, of processes, risks, controls, issues, test results, etc. Many builds stumble on this and it can be very costly.
  - Simultaneously serve significant numbers of users. Although this might be achieved by adding a lot of hardware power if the solution is properly architected, it will also be costly. For example, serving 10 users simultaneously already exceeds some systems. Scalable architecture is expensive and, requires very experienced architects.
  - In international organizations, a multi-lingual application will increase user acceptance, yet the investments could be cost prohibitive to include in an in-house build.
- **Authorization Management –** With version management being one of the most important, authorization management could very well be the most important capability. The solution should be built so that authorizations may set entities, whole sets of processes, risks, and controls. This should be based on user and role configuration, preferably where these come from an LDAP / Active Directory database to avoid double user maintenance. Authorization should be easy to manage. It should not require every individual

entry in the database to be authorized which would cause application maintenance costs to explode. Note too that field level authorization may be important if the organization wants to keep certain confidential information from some users.

- **Convergence Management –** The solution should be capable of holding multiple risk and compliance frameworks and be able to help the organization to converge all the various frameworks. Preferably, the solution should have a process-based approach, allowing risks and controls to be integrated at the process level.
- **Standard Templates –** To quick start projects, having standard templates available will reduce costs, improve quality, and reduce ramp-up time.
- **Ease-of-Use –** This is probably one of the most difficult capabilities. If an organization wants to involve hundreds of people in a risk and compliance project, it is more than likely that some of them are not experts and are not too fond of IT in general. In these cases, automated email alerts with deep links that direct people to the proper page and easy questionnaires help to keep application support costs down.
- **Risk-based –** Implementing a risk-based approach is more than including a risk assessment. It enables GRC risk information to be leveraged into other processes. This is essential in GRC convergence and requires very advanced cross-referencing capabilities

CONSOLIDATED VIEWS ON RISK LEVELS AND COMPLIANCE FROM TOP-DOWN

- **Integrations –** Organizations are running SAP, Oracle, PeopleSoft, Vulnerability Scanning solutions, IT service management, Asset Management, Contract Management, or other similar systems. These all provide the relevant information that needs to be captured for risk, audit, and compliance purposes. The ability to use and analyze this information effectively will dramatically cut compliance costs, and further increase quality.
- **Continuous Developments –** The GRC market is constantly evolving. Heavy global competition and customer demands ensure GRC vendors in general and SAI360 are constantly investing in new technology and new standards. For example, ongoing innovation in response to the marketplace needs enables SAI360 software to effectively support the latest insights in risk management, continuous control and embedded testing, consolidated risk and compliance reporting, convergence of quality management and compliance, convergence of performance and risk management, etc. It will be impossible to keep up with the leading GRC vendors at this level; even coming close will be impressively costly. SAI360 spends millions of dollars annually on application development.

- **Application Maintenance –** When buying a GRC platform solution, you can rely on an internationally renowned vendor, whose sole business is to continuously satisfy customer demands. New versions of underlying databases, browser versions and operating systems are not a concern. Contrarily, an in-house build makes the organization vulnerable to employee departures, vacations, and any absence of key knowledgeable personnel. Alternatively, and equally expensive and less secure, is to outsource the application maintenance to a generic technology provider. But, even in the first year, the investments in teaching the capabilities and maintenance of a proper GRC solution easily surpass what is offered with a commercially available solution. So, as this white paper demonstrates, it is certainly possible to build a GRC solution in-house. However, there are four solid reasons organizations are moving away from this. Expensive lessons have been learned; budgets wasted. Let GRC software solutions do what they do best so you can focus on your core business. In the ideal case, cost estimates for home-built solutions are optimistic yet cannot take the full picture into account.

CLOSING REMARKS

The statements in this white paper are views from SAI360 based on years of experience in the industry. Similar views may be found with independent industry analysts like Gartner, Forrester, Chartis, GRC 20/20 and the Big 4 accounting firms. Asking the right questions at the beginning of the solution evaluation process will give you a transparent view on building your solution in-house vs. commercially available GRC platform solutions. This will enable you and your team to make the right choice to not only meet your requirements now, but for many years to come.

SAI360 helps organizations proactively manage risk to create trust and achieve business excellence, growth, and sustainability.

Our integrated risk management solutions are a combination of leading capabilities, services and advisory offerings that operate across the entire risk lifecycle allowing businesses to focus elsewhere. Together, these tools and knowledge enable clients to develop an integrated view of risk.

To see our tools in action, request a free demo. For more information visit **www.sai360.com/risk**.