WHITEPAPER

Measuring the ROI of GRC Software

Executive summary

There are always questions of how an investment in Governance, Risk, and Compliance (GRC) benefits an organization. The answer for how to measure ROI isn't always easy. Far too many organizations see it as purely preventing potential future losses. Of course, that is true, but there are still a lot of tangible benefits that organizations can realize – if they take the time and effort to do so. But, if the organization does, they will find that the rewards far outweigh the costs.

As mentioned by KPMG "Listing tangible benefits is easy; quantifying these benefits is the hard part."* It may be difficult to quantify the value of GRC through traditional Return on Investment (ROI) calculations as they fail to take into account alternative investments. While there are compulsory pieces an organization must adhere to, it's left to the business to evaluate how best to use the capital it has. Here at SAI360 we've taken our experience with hundreds of customers to actually quantify the benefits and provide you with a representative example. In our example the customer was a global enterprise operating in 3 continents and implementing Enterprise & Operational Risk, Third-party & Vendor Risk, IT & Cybersecurity Risk, and Business Continuity.

In this white paper, we illustrate how an organization might articulate the business and financial benefits of investing in GRC and GRC software. Organizations should expect to receive measurable benefits in the years following the initial investment thanks to efficiencies gained through improved risk management processes, control optimization, better capital and resource allocation, and operational improvements.

*https://advisory.kpmg.us/articles/2019/optimizing-roi-grc-implementation.html

SAI360
RISK FROM EVERY ANGLE

The case for investing in GRC software

All organizations face a variety of risks from the strategic to the operational. An investment in a GRC tool has a variety of benefits that will vary by organization. However, there are two areas nearly every organization will see positive ROI.

IT Comparison

With GRC solutions, the ROI benefits pay dividends in the first year, and they can be implemented in a matter of around 2 to 4 months. In contrast, IT investments that do the same thing have a payback period in the three-year time frame while also taking 9-12 months to implement. GRC solutions are simple to implement and require little IT involvement.

Key Value Drivers

There are several key value drivers that GRC solutions offer to any organization, including:

- Time savings in the execution of risk management processes
- Data feed automation
- Control monitoring
- Compliance (e.g., Dodd-Frank, HIPAA, EPA, FDA, etc.)
- Reporting

Organizations often have lean resources dedicated to risk management processes. Assessments, for example, are often performed by separate functions that do not collaborate or coordinate with each other. If an organization is using a GRC solution, it integrates information so that similar types of data can be obtained from multiple parts of the organization. This saves time in control testing, optimization, reporting and issue remediation.

Why GRC and why now

The avalanche of changes brought by the pandemic has cemented GRC as a key tool in building organizational stability and business resilience. Sudden changes like the shift to working from home are meeting pre-pandemic obstacles such as increased regulation. Fundamentally, managing it all comes down to robust, adaptable risk management. Companies looking to get ahead of this curve are looking at issues including the following:

Intensifying regulatory requirements

As global regulatory bodies ramp up requirements, manual risk management processes bring increased scrutiny and the risk of significant fines. There are also significant costs related to remediating the system's flaws, and reputational damage that can hurt the organization's bottom line. Implementing a GRC solution pre-emptively and effectively removes this significant threat.

Growing dominance of analytics

Analytics have become a core focus in GRC, as good data allows organizations to pinpoint where, why and how control failures are happening. Analytics help uncover systemic issues within the organization so appropriate changes can be made.

Increased C-Suite involvement

Intensifying regulatory requirements are driving the C-Suite to get more involved in GRC. An efficient solution provides a way to track risk events and find out which parts of the operation are experiencing more events and how quickly employees are reporting those events. The C-Suite can then identify and remedy underlying issues causing lost profits or reputational damage.

Holistic coverage and tech integration

In large organizations, there are often multiple risk management systems in use across the business. For example, technology events such as outages or cybersecurity issues are often recorded in separate systems and must be manually reported to the risk management system. A GRC solution can reduce the time and effort spent doing this by automatically reporting based on multiple factors, such as the severity of the threat or duration of the issue.

ROI Illustration

To understand the relative effects of a GRC investment, an organization must break down the specifics of capital and resources (time) to implement and sustain its risk management processes, evaluate how the investment in a GRC tool may influence those activities and determine how these may translate into benefits. Below is an example of how our illustrative organization found the ROI from a GRC investment.

GRC Investment costs

After a review of the organization's requirements, a GRC proposal was submitted quoting implementation fees of $150,000 up front and $50,000 in year one. Ongoing annual costs in the form of subscription fees were $250,000 per annum. Costs were inclusive of discounts and quoted for a five-year period.

Assessment process

The organization started by aligning risk and control data to strategic objectives. The risk outcomes from each objective were mapped to relevant areas of the business, allowing the organization to identify groups to obtain information from. Groups included:

- Front office
- Risk management
- IT
- Legal
- Compliance
- Select vendors

Individuals from these groups collaborated to create a risk assessment that met each group's information needs.

The assessment used a common taxonomy and framework to evaluate each risk, and process maps were created across the value chain where risk and controls information could be mapped. The information was input into the GRC software, which sent out the assessment electronically to identified individuals. Follow-up was performed by relevant subject matter knowledge individuals as necessary.

By utilizing the GRC software, the group estimated that it could save approximately $72,250 each time the assessment process was performed.

Completion of the assessment process

- Original process included: preparation, interview, analysis, summary, which amounted to, on average 250 hours/group or a total of 5 x 250 = 1,250 hours.
- Amended process: preparation, collaboration, analysis, interview (as needed), which amounted to 80 hours/group for a total of 5 x 80 = 400 hours.
- Although the company's costs (wages and salaries as benefit costs were roughly equivalent) per employee varied, by group, the average cost after counsel with human resources, was determined to be $85/hour.
- The resulting savings equates to $72,250 for each time the assessment process is conducted.

Another benefit was a better use of resources. Individuals could focus on the risks with the highest potential exposures given the organization's goals. Risk managers could work with the business and respective functional areas to better understand how risk was manifesting itself, educating these individuals on the broader exposure, and allowing them to create practical courses of action to shore up the control and management environment. It also enabled the business to improve throughput of products, with a reduction of unnecessary controls increasing volume by 10%. This resulted in an increase in profitability of $750,000.

Management and control activities

The benefits extended beyond pure operational processes. Control weaknesses could be documented and reviewed by each group. The centralization of data within the GRC tool allowed for communications to be sent out automatically to individuals needing to take action to remedy the control environment. This had the benefit of not inundating nor duplicating information to the same individuals.

The information from the GRC software enumerated the controls that needed to be tested. Collaborating with audit, functional groups like legal, compliance, and IT identified common controls and the necessary steps needed to evaluate the efficacy of each one. Instead of each group working with different parts of the business, the appropriate groups were engaged. This allocation of resources maximized the time with business's employees to assure that controls were working as intended.

Additionally, controls that could be automatically tested were documented. The GRC software could take the data feeds from the control testing automation process and include it in the relevant Key Performance, Key Risk, and Key Control Indicators (KPIs, KRIs, KCIs) to evaluate changes in risk tolerance levels.

Control and management activity optimization

- **Original process:** each risk oversight group identified critical risks, evaluated the control environment, and tested controls. Total average time invested per risk assessment over a twelve-month period: 3,500 hours. Hourly rate remained constant at $85/hour.
- **Revised process:** critical risks identified, common controls documented, common controls parsed to respective functions, controls tested and some automated. Average time invested per risk assessment over a twelve-month period: 1,500. Coding to automate control testing: $25,000.
- **Estimated approximate annual savings:**
  Year 0: 145,00 = (3,500 – 1500) x 85 – 25,000
  Years 1 – n: 170,000

Reporting

The organization spent a great deal of time on report- ing to understand and depict the risk and control environment across all parts of the organization. Improved collaboration across all risk management areas and a centralized, organized repository of risk allowed the organization to develop an "apples-to-apples" view of risk that removed senior executive confusion of how risk was being evaluated.

Additionally, other stakeholders had their own reporting needs, whether it be by function (e.g., legal, IT, HR, audit, insurance) or by parts of the organization itself (e.g., business operations and value chain processes, IT, and vendor management). This included regulatory and local reporting across the organization's global locations. The GRC software could be configured such that dashboards and reports could provide supporting risk and control data in a sustainable, consistent manner, in real time.

Reporting

- **Original process:** done by separate functions. Total individuals doing ad-hoc or periodic reporting across the company: equivalent of 8 Full Time Employees (FTE).
- **Amended process enabled through GRC software:** largely centralized and staffed by 2 FTE (offshore staff) and equivalent time in functional areas by the equivalent of 2 FTEs.
- **Estimated cost savings:** Reduction of 3 FTEs at an average hourly rate of $25.00 for an annual savings of $200,000.

Compliance

The number of laws and regulations applicable to organizations can be staggering. Understanding which laws and regulations apply and how to operationalize each one requires coordination between compliance, legal and other applicable functions (e.g., IT). GRC technology helps make conformance a persistent reality.

Identifying relevance

One feature of a GRC solution is its ability to automatically pull relevant laws and regulations into the governance structure. Policy relevancy and rationalization is a frequent issue. Understanding which policies are relevant to which part of the organization was challenging. This organization had over 2,000 policies that had been created over time. This left employees, support functions, and the business confused about how relevant regulations and laws translated into day-to-day activities.

Calculating compliance savings

The organization, as part of a larger policy project, evaluated the costs for identifying relevant laws and regulations with outside counsel as the primary information source. Average annual cost globally was $500,000. After an evaluation of the necessary data and vendors that could provide it, the GRC software was programmed to get data feeds automatically. Internal counsel, with the help of compliance, would "translate" those into policy and communicate to the applicable parts of the company.

The regulatory feed manager within the GRC software removed the need to engage with external counsel on an ongoing basis. After subscription fees, coding, and the ad-hoc use of counsel, the result was an annual savings of $200,000

Closing gaps

The GRC software could identify the key processes and where the controls were sufficient or insufficient based on different variables. Gaps were closed through training, augmentation of systems, workflow redesigns, and policy and documentation changes.

In this example, the data within the GRC system could accomplish two things:

First, it identified control gaps of legacy systems that were not updated with proper coding from regulatory changes. Training was performed with the business on how to identify gaps where documentation needed to be sent to customers.

Second, after a review and testing by audit, it was discovered that there were products that were not being updated with appropriate marketing literature.

A review of these practices by the organization's regulator resulted in a product mis-selling fine of $500,000. Control improvements were made in systems and in processing totaling $75,000. These improvements resolved this issue and satisfied ongoing regulatory concerns. These capital expenditures were believed to be a sunk cost of investing in the business operations and the organization did not account for future fines.

Other specific risk topics

Fraud

The organization faced fraud issues that amounted to roughly $5 million over a five-year period, in addition to fines totalling $500,000 by multiple states' attorneys general.

The organization utilized the GRC system and data feeds from both external vendors and acquired systems to assure a complete review of the customer information required to obtain a certain product. The information was obtained through XML feeds and matched to transactions and processes deemed to be more fraudulent. Through this process, the number of fraudulent transactions dropped nearly 75% after the first year with associated implicated costs of $1,000,000. Fraud was expected to decrease in both frequency and amount per fraud, on average, by 20% in subsequent years.

Cybersecurity

Cybersecurity was a significant inherent risk to the company and maintaining the integrity of customer data was of the utmost importance. Regulatory compliance became increasingly difficult after discovering how many places customer data existed due to the acquisitions the organization made over the last decade.

The expectations from global regulators forced the organization to evaluate a broad set of actions to understand how cyber-attacks could occur and precipitate across the organization. Led by IT, and coupled with data from external vendors, vulnerabilities were identified and mapped to the various parts of the business.

Many of the acquired companies had manual processes that were not as sophisticated or secure as the systems of the acquiring organization, and there were many duplicative controls across software used by multipleareas. Although the organization had an explicit strategic objective of active cross-selling of its products, there was no cohesive way of pulling customer information together across the value chain — leaving the organization exposed at multiple access points.

The IT team could use the risk and control information centralized in the GRC software to identify capital expenditures and thwart cyber threats more efficiently. The result was investment in:

- An upgrade to vulnerability scanners
- Software used to protect data from mobile attacks
- Hardware applied to multiple data entry points
- Expanded firewalls
- Strong encryption

The number of attacks on the organization did not decrease, but successful breaches were reduced by 98% and the number of customer records at risk per breach decreased from an average of 33,000 to 1,000.

The organization used information from IBM's research, adjusted given the company's reputation, to estimate the average cost of a lost or stolen record at $150.

The use of the GRC software helped to operationalize the program, report on its effectiveness, and lay the foundation for how it was being sustained.

Illustrative business benefits

GRC software was also used in conjunction with other IT investments to pinpoint weaknesses in product quality and customer service. With the help of machine learning, the organization took information from customers to populate dossiers of key products. Volume increased and errors were reduced by 20% while customer satisfaction rose 20%. It was also believed to increase new customer acquisition by 5%, resulting in profitability of $150,000.

Calculations

The organization used a valuation technique to evaluate the efficacy of investing in the GRC software. The original estimate is shown in the below table. These figures were adjusted in subsequent years based on actual data and results. Moreover, the organization performed scenarios based on changes in the organization, product and process improvements, customer demographics, and strategy alternatives (like product expansion and introduction). For example, certain risk factors like fraud and compliance violations could be stressed if the organization was interested in acquiring another company.

	Year 0	Year 1	Year 2	Year 3	Year 4
Investment Costs					
Implementation Costs	($150,000)	($50,000)			
Annual Costs	($250,000)	($250,000)	($250,000)	($250,000)	($250,000)
Savings and Expected Savings					
Assessment Process		$72,250	$72,250	$72,250	$72,250
Increase in Volume/Profibility		$750,000	$750,000	$750,000	$750,000
Control and Management Optimization	$145,000	$170,000	$170,000	$170,000	$170,000
Coding	($25,000)				
Reporting		$200,000	$200,000	$200,000	$200,000
Compliance Activities					
Law and Regulation Updates		$200,000	$200,000	$200,000	$200,000
Control Improvements (address mis-selling fine)	($75,000)				
Fraud Reduction		$1000,000	$800,000	$640,000	$512,000
Cyber Control and Management		$150,000	$150,000	$150,000	$150,000
Business Volumn Profitability Increases		$150,000	$150,000	$150,000	$150,000
Total	($355,000)	$2,392,250	$2,242,250	$2,082,250	$1,954,250

Outcomes

The information and subsequent calculations were presented to the organization's executive committee and ultimately presented to the board for approval. The risk function needed to explain how the capital use in GRC would add value to the business versus alternative uses.

Additionally, the executives and board asked for updates on the progress of the program and whether the assumptions were correct (e.g., was fraud really dropping by 20% in subsequent periods?). Using fraud as the example, this request required risk management to articulate how current management activities reduced the current scope of fraud as well as how the fraud risk profile changed (i.e., increasing given a recent acquisition). The GRC software could easily segment this data. Holistic reporting gave the executive team (and the board) the confidence that risk management was a fluid part of the organization's ongoing strategic plans.

Other areas benefited from using the GRC software as part of risk management. For example, investigations of control breakdowns and risk exposures were more effective. Some of the areas included were:

- Marketing
- Sales
- Promotional practices
- Management remuneration
- Research and development
- Customer complaints

The GRC software helped prioritize risk areas where there were control breakdowns so that dedicated resources were better allocated and focused on the most vulnerable parts of the business.

Current and future challenges GRC solutions can address

As demonstrated above, adopting a GRC solution does more than provide a tangible return on value, it also offers a means of future-proofing an organization against myriad unforeseen challenges. The following are just a few of the current developments organizations must consider.

Growing emphasis on ESG

Environmental, Social and Governance (ESG) is becoming more of a focal point. There are many control issues surrounding ESG, especially for businesses selling products with ESG credentials. Organizations need GRC solutions to centralize data feeds that make up ESG product credentials, and keep up with quickly shifting standards.

Climate change and reputation

The advance of climate change brings two significant risks. One is a growing slate of climate change regulations, which will necessitate swift action in implementing new policies. Another is public perception and reputation related to how "green" a company is. Companies that lag behind in sustainability efforts due to slow adaptation to regulations will not be viewed favorably.

Operational resilience

The pandemic has highlighted the need for robust operational resilience in the face of rapid changes to supply chains, the switch to work-from-home and more. Organizations with adaptable GRC solutions will always be able to pivot more quickly and remain more resilient than those without.

Expect the unexpected

The ability for a GRC software solution to integrate risk and control data, yet providing the underlying detail, assures that any efficiencies and improvements justify capital, business, and delivering quality products and services. The world never stays static, and new challenges will always appear whether expected or not. An investment in a GRC solution is an investment in an organization's stability, and its ability to grow, flex and ultimately thrive in the unpredictable business landscape.Additionally, other stakeholders had their own reporting needs, whether it be by function (e.g., legal, IT, HR, audit, insurance) or by parts of the organization itself (e.g., business operations and value chain processes, IT, and vendor management). This included regulatory and local reporting across the organization's global locations. The GRC software could be configured such that dashboards and reports could provide supporting risk and control data in a sustainable, consistent manner, in real time.

Reporting

- **Original process:** done by separate functions. Total individuals doing ad-hoc or periodic reporting across the company: equivalent of 8 Full Time Employees (FTE).
- **Amended process enabled through GRC software:** largely centralized and staffed by 2 FTE (offshore staff) and equivalent time in functional areas by the equivalent of 2 FTEs.
- **Estimated cost savings:** Reduction of 3 FTEs at an average hourly rate of $25.00 for an annual savings of $200,000.

Compliance

The number of laws and regulations applicable to organizations can be staggering. Understanding which laws and regulations apply and how to operationalize each one requires coordination between compliance, legal and other applicable functions (e.g., IT). GRC technology helps make conformance a persistent reality.

Identifying relevance

One feature of a GRC solution is its ability to automatically pull relevant laws and regulations into the governance structure. Policy relevancy and rationalization is a frequent issue. Understanding which policies are relevant to which part of the organization was challenging. This organization had over 2,000 policies that had been created over time. This left employees, support functions, and the business confused about how relevant regulations and laws translated into day-to-day activities.

Interested in learning more about the ROI of SAI360's GRC software?

[Request a demo.]

Our unified approach to risk sets us apart

Today's complex risk landscape demands more. SAI360 leads the way with an integrated GRC platform and Learning solution that spans the entire risk spectrum.

Risk Management Solutions

- Enterprise & Operational Risk Management
- Regulatory Change Management
- Policy Management
- Third-Party Risk Management
- Internal Control
- Internal Audit
- Incident Management
- Conflicts of Interest (COI) Disclosure Management
- IT & Cybersecurity
- Business Continuity Management

Ethics & Compliance Learning Solutions

- Anti-Bribery & Anti-Corruption
- Competition & Anti-Trust
- Conflicts of Interest
- Data Protection & Privacy
- Information Security
- Exports, Imports & Trade Compliance
- Harassment & Discrimination

SAI360 RISK FROM EVERY ANGLE

SAI360 is giving companies a new perspective on risk management. By integrating Governance, Risk, Compliance (GRC) software and Ethics & Compliance Learning resources, SAI360 can broaden your risk horizon and increase your ability to identify, manage, and mitigate risk. See risk from every angle.
Visit www.sai360.com.

150971 0424