SAI360
Risk | Learning | EHS | Sustainability

WHITEPAPER

Operational Risk Management

Operational risk and its supporting software play a critical role in an organization; but how can its activities add value along the way?

Operational risk and operational risk management continue to be a topic of interest across industries. Uncertainties abound. Cyber risks are pervasive as ever. Talent management has become more challenging with the “Great Attrition.” Awareness of environmental, social and governance (ESG) risks is increasing in importance for stakeholders. Many organizations are facing disruption, whether it is technology, unconventional new entrants, or new ways of doing things, forcing a closer look at systems, processes, and skills. The list of threats goes on.

On the flip side, there are also a lot of positive changes that are influencing operational risk management activities. Structuring data, data analytics, digitization, and topics like machine learning are creating new opportunities within operational risk that requires a dynamic process to support them. Automation of activities, like continuous monitoring, can assure that controls are functioning as they were intended. Data feeds can assure that the company is kept abreast of emerging risks.

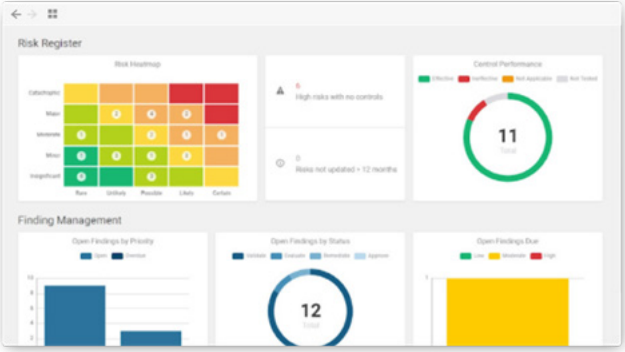
One constant that helps enable the operational risk process and addresses both the positive and negative events facing an organization is an integrated risk management or GRC (Governance, Risk, and Compliance) software platform.

Although operational risk management is still in its relative infancy compared to market and credit risk, there is typically consistency in the underlying activities. There are two important aspects here. One: operational risk activities should be iterative and typically take their start from an organization's annual risk assessment process.

However, risk management today isn't just about a "one-and-done" process. It must be fluid. Risk threats, like those that emanate from technology (cyber, social media, etc.), occur with such a high frequency that activities within the operational risk cycle need to come to the forefront at any point in time. This means that the lines of defense can jump from say, assessing the risk, managing the event, establishing metrics to monitor trends, and reporting the risk's status to interested parties on a near real time basis.

GRC SOFTWARE'S ROLE

Pulling together the tactical aspects of operational risk management is cumbersome for risk management and the business without GRC software. As figure 1 depicts, GRC software needs to be at the heart of the operational risk management process and provide the enabling levers to facilitate the efficient and value-added risk management activities across the lines of defense. A closer look at each part of the operational risk management processes can uncover software's role and the value therein.



RISK IDENTIFICATION

An integrated GRC software platform can pull information from external sources (via RSS feeds, ORX, etc.) as well as provide an audit trail and database of past events to make risk identification a holistic process across the lines-of-defense. The automation of importing data as well as the ability to mine data from a central source brings efficiencies and economies of scope in the risk identification process.

The identification of relevant risks can be neatly grouped into four buckets: (1) events that have occurred in the past; (2) current events; (3) potential events; or (4) emerging risks. Regardless of where the events occur, a methodology that allows for the aggregation and disaggregation of risk is important. For example, at the highest level, a risk may be categorized as information technology. The next level may be systems. The level after that may be the specific type of system (e.g., SAS, Oracle) and so on. Basel (bis.org) offers a similar categorization. In this case, the categorization may be "business disruption and system failures" as level one, "systems" as level 2, and "software" as the third level. Categorizing risk events in this fashion can act as support for incorporating applicable risks to the organization as well as offering a taxonomy that assures consistency.

Unless the organization has completely stopped offering a particular service (e.g., outsourcing) or discontinued a product, past events are still applicable. The degree of applicability will be determined within the risk assessment as unwanted risks have been mitigated to some extent. However, this doesn't mean that they should be ignored. Change can shed light on past events offering the possibility that once low rated exposures may now be rated higher.

External events require a bit more diligence to determine how well suited they are to the organization. At the highest level of definition, there is likely little debate to an events relevancy. For example, external fraud at one organization is still relevant to another, even if they are in different industries. The challenge is extrapolating how applicable the severity of external events are, given varying business models, geographic and regulatory environments, and customer segments.

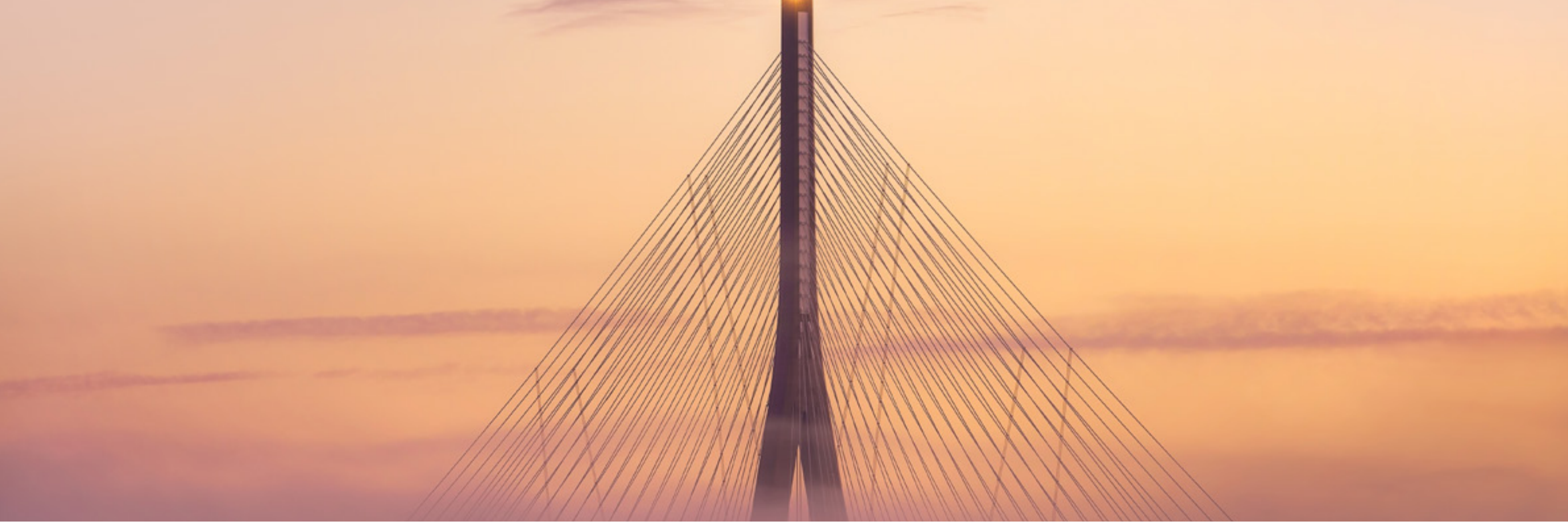
Finally, potential events are most often associated with scenarios, or the estimation of how events that have not occurred at the company could materialize. GRC software can automatically bring in data from external data sources, such as from ORX, to the software for relevancy to the organization and analysis. This data can also be used in modeling to calculate variances in product valuation or determining a Value-at-Risk (VaR). Additionally, stress and back testing are another excellent use for extrapolating the impact of potential events and is frequently used to satisfy regulator interest (e.g., CCAR and DFAST in the US).

RISK ASSESSMENT

A familiar way of assessing risk is on an inherent (absent of controls and management actions) and residual (accounting for mitigating measures) basis. GRC software provides efficient methods for collecting risk and control data through various top-down and bottom-up mechanisms, whether it is through facilitating a workshop, surveying parts of the organization, or conducting interviews.

Moreover, a robust GRC software can support the assessment process vis-à-vis an algorithm, where residual risk is a calculation based upon the inherent risk and control assessment, or allow for qualitative judgment to amend the assessment based on input from expert opinion (e.g., outside counsel).

GRC software enables the lines-of-defense to assess risk with the flexibility needed to align to various stakeholder needs.This most commonly includes defining criticality through the evaluation of a risk's likelihood of occurrence and severity and comparing it to appetite and tolerance levels. GRC software can enable a function like compliance to set its own thresholds, usually a zero tolerance for non-conformance, yet allow the business to set higher tolerance levels to account for risk taking activities. Pulling the information together to provide an overall picture of a risk's exposure across the value chain assures that there is a comprehensive set of details that can inform decision making.



Determining the criticality of a risk requires an evaluation of the existing organization's control and management environment. Codifying this through, for example, process maps, creates a clear demarcation of where risks and controls exist and assists in establishing accountability.

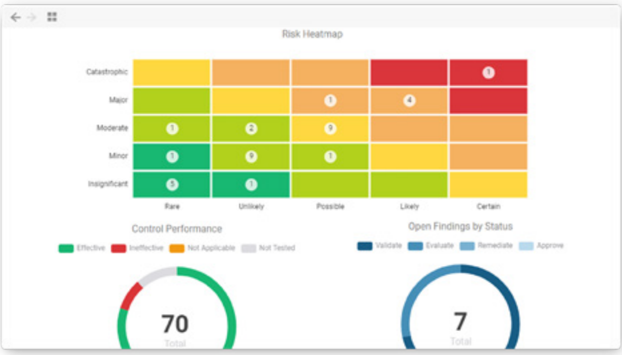
RISK CONSOLIDATION AND EVALUATION

Consolidating risk information is efficient with data in GRC software and can usually be easily accessed through dashboards that can depict the risk profile in real time.

Heatmaps, which depict a risk's severity through a spectrum of green to red, show the distribution of risk severity. Moreover, GRC software makes seeing the details of each risk (e.g., control assessments, processes, events, action plans, etc.) as easy as a simple click.

A critical aspect in the risk evaluation process that many organizations fail to do is to gauge how a risk's severity has changed over time. The purpose? To show how well an organization's limited resources (employee time, capital) are performing.

One organization used the assessment update process to articulate how capital expenditure in the control environment actually produced a tangible reduction in the risk's severity. This evidence was supported through a reduction in both frequency and magnitude of internal loss events and gave the business, Executives, the Board, Audit Committee and regulators evidence that the risk profile was improving.



Another example in complementing changes in the risk profile is codifying and quantifying the cost of controls and comparing it to the risk assessment. Simplistically speaking there is a simple rule of thumb: Cost where S = severity = impact x likelihood. The total cost of the controls should be less than the expected change in severity. For example, if the estimated assessment of a particular risk is $100. It destroys value ($10) if the organization spends $30 to control the risk and at a future point in time the expected severity has an assessment of $80. If $30 is spent to control the risk the expected reduction in the risk's severity needs to be less than $70. Only then is risk management doing what stakeholders expect it to do.

An important feature of a powerful GRC software is in its audit trail abilities. This history of risk and control data offers risk managers the ability to go back and see the affects of controls, management activities, and capital expenditures. Even though these activities may not always meet the business' intentions to relax the control environment, it still offers insight to substantiate the need for further action.

RISK MITIGATION, ACTION PLANNING (AND CONTINUOUS MONITORING)

Articulating the controls supporting a risk is one of the fundamental expectations of a risk manager. The same question always seem to pop up, "what is being done to control the risk?" Mining the GRC software makes this an easy answer and can include the action owner, accountable executive, timing to closure, control deficiencies, etc. The software can generate reminders and updates to trigger the business to provide updates to the second line of defense. This can also signal audit for its independent review of the control environment to assure that mitigating activities are meeting expectations.

The ability for the organization to stay aware of changes in the risk environment is tantamount to the value it can bring to the organization. Continuous monitoring is one way of doing that and is facilitated through GRC software. For example, one organization uses an outside vendor, and an RSS feed, to monitor relevant regulatory changes to the organization. This is done automatically and fed into the GRC system for users to monitor. Links to relevant policies and standards is done through the system's policy management capabilities.

Another organization is using continuous monitoring to analyze changes in the control environment. Key Risk Indicators (KRIs) highlight changes in interest rates and spikes in mortgage applications. Key associated controls are then reviewed and stressed to assure their efficacy in reducing errors in the underwriting process.

An area where risk management could stand to improve its transparency to managing risk is through the insurance program. Mitigating harmful exposures naturally means improving the control environment. The risk and control data detailed within the GRC software can evidence the risk management's strength. Moreover, a reduction in internal losses through controls or management activities may be an opportunity to self-insure, or to retain certain risk exposures.

A good example of this may be through a cyber policy. Taking steps to understand how the risk management profile relates to the insurance program could mean savings of insurance premiums, resulting in real dollars being saved.

Insurance plays a complementary role. Insurance can make the income statement whole, but does not reflect the potential reputational damage done by an event that captures the customer's or the public's eye. Do not minimize managing the event because there is an insurance policy in place.

EVENT MANAGEMENT

A robust GRC software can provide the capabilities to manage events. It can provide insight into the risk and control environment by defining details about the loss. It also can provide the data for input into quantitative analysis for things like VaR calculations and potential support for holding economic or regulatory capital (see risk quantification and analytics below).

GRC software can also make tracking an event to closure simpler. For example, a particular event can produce an immediate loss, but it may be difficult to extrapolate the full amount because of insurance recoveries or potential lawsuits. Managing events can bring clarity to functions like legal where experience and judgment can assist in determining reserves.

Understanding risk events can also act as a feedback mechanism to the business. Losses concentrated in certain geographies, products/services, or in operational processes can provide support for enhancing, or reducing for that matter, the control environment.

Tying events to performance measures is also gaining some traction, especially within the executive ranks. This assures that there is alignment between risk taking and risk avoidance. For example, one organization uses loss amounts as one of the variables for an executive's bonus – higher losses equate to a lower bonus.

KEY RISK INDICATOR (KRI) AND METRIC MANAGEMENT

The adage “you can’t manage what you can’t measure” is one truism that organizations’ risk management programs should do their best efforts to follow. Granted, there will always be some qualitative judgment, but using numbers to understand the risk environment brings fact based support to decision making, links to profitability, and justification for courses of action.

An integrated GRC software tool can make the metric management process dynamic and fluid. Metrics, whether they are risk, control, or performance related, offer insight into how the business and risk management environment is changing. It offers insight into trends, limits, and changes in the underlying risk profile. A good mix of both lagging and leading indicators helps to predict future performance and prevent problems before they escalate.

> “Too often organizations are inundated with a plethora of risks and controls where there is little understanding of the possibility of duplicative controls or the lack of recognizing diversification effects across risk classes.

Creating relevant metrics is key to prioritizing risk management activities. Too often organizations are inundated with a plethora of risks and controls where there is little understanding of the possibility of duplicative controls or the lack of recognizing diversification effects across risk classes. KRIs should have a definition that align to the residual risk exposure. They also should be based upon breakpoint analyses of the processes underlying the value chain. As these KRIs trend to uncomfortable levels, testing of the underlying control environment should be done.

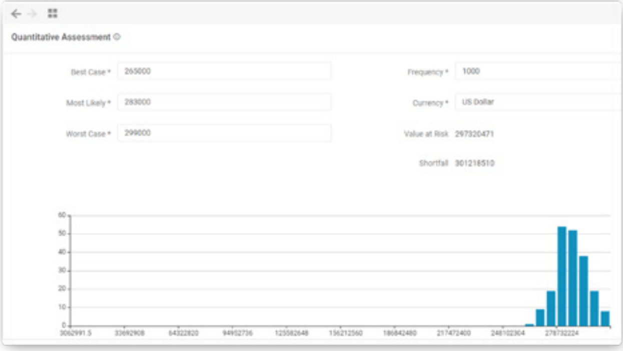
One organization is using its GRC software as a means of integrating information across the lines-of-defense. KRIs were developed by operational risk management, IT, compliance and the business to monitor instances of external fraud associated with its mortgage business. Data from the first and second lines-of-defense were used to evaluate business trends such as applications, changes in interest rates, etc. There was also collaboration with audit to assure that weaknesses were codified and offered the business a clear plan of action to mitigate. The GRC software made these processes efficient and gave the business the confidence it needed to ensure it was meeting its risk management and control objectives.

RISK QUANTIFICATION AND ANALYTICS

Quantifying risk and data analytics continue to capture attention. For example, the financial services sector has seen Basel rear its head when it plans to remove the Advanced Measurement Approach (AMA) in favor of the Standardized Measurement Approach (SMA) to facilitate comparability across companies. This is putting increasing pressure to assure there is quality internal loss data. Modeling losses is now primarily a part of scenario analyses and stress testing.

Big data, blockchain, digitization, and machine learning are creating improvement opportunities in risk management as well as specific agenda items for organizations. These include establishing explicit data strategies to find, structure, and mine quality data. There is also an ancillary need to protect this important asset and to assure conformance with protecting these assets.

Moreover, the importance of a GRC software to pull disparate data sources together is becoming progressively essential to substantiate a robust risk management framework. Data comes from legacy systems, acquired technologies from inorganic growth, and each business and support functions. Collecting this data in a systematic way is a crucial foundation for substantiating the statistical accuracy of the conclusions of using advanced quantitative methods. Although the regulatory impetus for a robust capital calculation engine may have subsided, there is still interest in extrapolating how the risk profile may affect the organization given changes in the competitive, macro and microeconomic, and business environment. Utilizing integrated GRC software can bring confidence that reporting reflects a current view of risk and control information for the entire organization and confidence in risk management efforts to address unwanted exposures (e.g., through action plan creation, management, and issue tracking).



Quantitative Assessment

Best Case * 265000

Most Likely * 283000

Worst Case * 299000

Frequency * 1000

Currency * US Dollar

Value at Risk 297320471

Shortfall 301218510

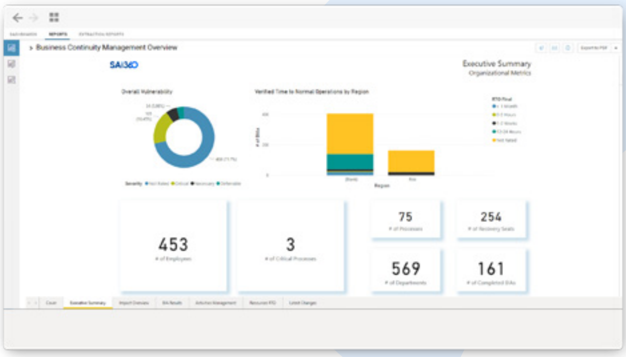
REPORTING AND DASHBOARDS

Arguably, producing meaningful data summaries is perhaps the most essential element to risk management. Reporting provides a picture of the risk and control environment, its details, and offers tangible substantiation to how the risk program is being embedded into the organization. Similarly, dashboards are the day-to-day diagnostic of the risk profile. Dashboards can offer current information into new threats, courses of action, or unfavorable metric trends.

A goal for the risk management function is for it to do its best to appraise the organization of risk and avoid surprises (figure 5). This can only be achieved by having a fluid and dynamic risk management culture supported by tools that create transparency into the organization's risk and control environment.

Many organizations still have a formal cadence of an annual risk assessment with quarterly updates. Unfortunately, it provides little confidence to executives, the Board, and regulators that risks that occur with a higher frequency may be missed because they occur right after the assessment. For example, cyber threats, distributed denials of service (DDoS), and other technology based threats occur, potentially, multiple times a day. What escalation mechanisms exist and how are these types of threats being monitored and thwarted?

Integrated GRC software can take data from an array of sources to quickly visualize changes in the risk profile through both bespoke and standard dashboards and reports, whether it is by role, function, or the organization as a whole. The software also offers the possibility to drill down into the risk and control detail. The real time awareness that is created through these mediums provides insight, for example, into weaknesses in the control environment thereby stimulating the need for action. It also provides the mechanism of the completeness of the risk management program and its sustainability. This gives confidence to executives, audit, The Board, and regulators that there is breadth and depth to the risk management program.



> “Additionally, opportunities exist for operational risk management activities to evolve to add value, delivering more value and a higher quality of oversight while at the same time increasing efficiency.

CONCLUSION

Operational risk and operational risk management is unmistakably garnering more attention as organizations face an onslaught of new threats, new responses to disruptive technologies, new competitors, and continual pressure to grow. Although process standardization is emerging, integrating disparate risk management activities and data is becoming increasingly important. Additionally, opportunities exist for operational risk management activities to evolve to add value, delivering more value and a higher quality of oversight while at the same time increasing efficiency. Organizations that use an integrated GRC software solution will make this shift to realize competitive advantage, support a better service delivery model, reduce structural costs, and bring transparency into the risk profile.

SAI360 GRC PLATFORM

SAI360 offers multiple role-based software modules for Risk Management, Internal Control, Internal Audit, Regulatory Change & Policy Management, IT Risk, Business Continuity, Third-Party & Vendor Risk, and Environment, Health, Safety & Sustainability (EHS&S).

About SAI360

SAI360 is a leading provider of Risk, Learning, EHS, and Sustainability software. Our cloud-first SAI360 platform contains flexible, scalable, and configurable modules for a better vantage point on risk management. Our unified approach to risk management is what sets us apart, helping organizations across the globe manage risk, create trust, and achieve business resilience for over 25 years.

SAI360 is headquartered in Chicago, U.S., and operates across Europe, the Middle East, Africa, the Americas, Asia, and the Pacific. Discover more at **sai360.com** or follow us on **LinkedIn**. To see our platform in action, **request a demo**.