Risk Module

Graci

by RiskBusiness

Risk Module

Emerging Risks

Incident Management

KRI Monitoring

Risk Appetite

Operational Resiliency

Risk and Control Assessments

Internal Loss Events

Scenario Library

Models Register

Insurance Management

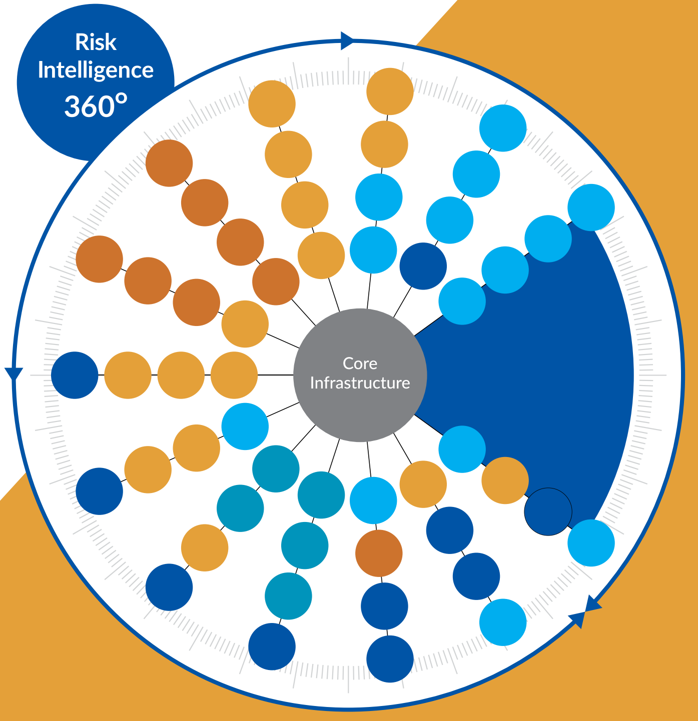
Risk Profiling

KRI Library

Scenario Assessment

Supply Chain Management

Data Privacy and Security



● Governance ○ Risk ● Audit ● Compliance ● Intelligence ● Core Infrastructure

Risks manifest themselves on the organisation from every direction and modern, integrated management requires a 360 degree perspective encompassing all second and third line of defence functions for proactive risk and business decision making.

Most firms seek to co-ordinate risk management on an enterprise-wide basis, covering the various permutations of operational risk, such as information security risk, operational/business resiliency risk, legal and litigation risk, conduct risk, operations risk, financial crime risk and even compliance risk in a common, structured manner. In many cases, integrated or enterprise risk management includes the co-ordination of risk management approaches for credit risk, market risk and liquidity risk along with operational risk, while some firms also include strategic risk, business risk and environmental risk management under the integrated or enterprise risk management umbrella.

The Graci – Risk module provides support for fully integrated enterprise risk management. However, while facilitating the identification, assessment, monitoring and mitigation of "pure" credit risk, market risk and liquidity risk, it does not include explicit credit risk management, market risk management or liquidity risk management tools. Core to the facilitation of fully integrated enterprise risk management is the definition of the risk taxonomy which the firm will use. The risk types contained within the firm's taxonomy, defined and maintained within Graci – Governance, limit the breadth of risk definitions and the accompanying risk-related activity within Graci – Risk.

Emerging Risks

Every firm has difficulty identifying new and emerging risks. Once identified, they must then manage the process by which potentially affected business entities are advised of the new risk, can contemplate whether that risk applies to them and maintain evidence of how that decision was reached. New and emerging risks may be identified from a wide variety of sources, such as public media, industry associations or consortia, new or proposed regulation, or from actual incidents and events which affect certain areas of the firm.

The Graci – Risk Emerging Risks functionality can sit on top of many other areas of Graci functionality, and allow the authorised user to indicate that the item constitutes a new or emerging risk, classify the risk using the firm's risk taxonomy, then assign that risk to those operating entities where it is thought possible the risk could manifest. It is also possible to create an emerging risk directly within Graci without linking it to any other data item. The most common starting point for emerging risks is from the Graci – Intelligence Newsflash functionality.

Once an emerging risk has been identified and assigned, selected employees within the target operating entities receive notification, can review the emerging risk and, where appropriate, the underlying data item, then either accept the risk into the entity's risk register or reject the risk, providing rationale as to why. There is automated action tracking on risk acceptance and rejection, with reminders and emerging risk reporting.

Risk and Control Assessments

A core functionality provided by Graci – Risk is the ability to maintain a risk register per operating entity, capable of aggregation across operating entities to divisional level or up to the total firm level, as well as supporting aggregation from the operating structure to the corresponding geographical or legal perspectives of the firm. Risks can be added to the risk register from the Graci – Risk Emerging Risk functionality, created directly from some form of incident or event, raised as the consequence of some audit or compliance activity or added directly into the risk register by the business itself. Note that an operating entity's risk register contains all of its risks, but can be filtered by control function to only see those risks applicable to that specific control function or risk area.

The risk and control functionality within Graci – Risk can be configured for various forms of assessment, including business environment factor assessments, control effectiveness assessments, risk and control self-assessments or "real-time" continuous risk register-based assessments. Ratings scales to be used can be defined, while the specific fields to be assessed and the basis on which they are to be assessed (inherent versus residual, typical case versus worst case, likelihood x impact, etc) is all configurable, with 9 different risk assessment use cases supported.

Where risks are assessed, the option to include control effectiveness assessments and to view corresponding control test results and control design strength criteria, is available, as is the option to view corresponding audit findings, compliance findings, loss events, incidents and key risk and control indicators. Assessed risks can be compared to risk thresholds and remedial action plans established to enhance risk mitigation.

Risk Profiling

A risk profile is typically a graphical depiction or heat map of areas of risk concern for a specific operating entity, capable of aggregation upwards to divisional and parent organisational level, as well as to applicable legal entity level. The risk profiling functionality within Graci – Risk provides for two forms of profile completion – either start from a blank profile and "colour it in" by assessing each risk point or intersection of process type and risk category (you can also start from an existing risk profile and simply reassess those risk points you deem necessary). Or, work from a risk assessment or the risk register and allow Graci to reverse engineer the risk profile from the most recent individual risk assessment values.

Risk profiles can also be used to compare against industry risk profiles, loss profiles, risk appetite utilisation profiles and to compare profiles between operating entities. Risk profiles can also be used to view losses, scenarios, key risk/control/performance indicators, newsflashes, consortium loss data, audit findings, compliance findings, regulatory matters and other data associated with each risk point.

Incident Management

Graci – Risk allows for the creation of an unlimited number of incident forms, each of which will have its own data requirements, lifecycle and workflow processes. An incident can be initiated anywhere within the firm, with the incident being routed to specific employees based on its lifecycle status and processing activity, with additional data added to the incident as it progresses through the firm. Specific functionality is available to support time-critical incidents, for example privacy breach reports, where alternative communication methods can automatically be employed by Graci in an after-business-hours situation and anonymous incident reporting is also supported. Incidents may also be converted into loss events where necessary.

Internal Loss Events

Loss events reflect where a risk has manifested itself on the firm and usually resulted in either some form of financial loss, adverse efficiency impact or an unexpected gain, although some firms may also elect to record data on so-called near misses or "almost losses". In contrast to an incident, a loss event is usually analysed and classified in greater detail, with a more thorough analysis of the financial, efficiency, reputational and other consequences. It is common for incidents to become loss events once the complete impact of the incident becomes known, as well as for loss events to arise from litigation settlements and from regulatory fines and sanctions.

The Graci – Risk Internal Loss Events functionality supports direct reporting according to European Union regulatory reporting standards (COREP) and facilitates the direct transfer of losses into any loss data consortia running on the Graci – Intelligence Loss Data Consortium service. Standard export files to other loss data consortia are also provided.

KRI Library

Graci – Risk includes detailed risk content provided from the KRI Library, a repository of over 2,500 detailed specifications of risk, control and performance indicators for the banking sector and a further 1,200 detailed specifications of risk, control and performance indicators for the insurance sector. The KRI Library is also known as KRIeX.org. The firm can use these public indicators as specified, can select and modify indicators and create private variants of the indicators, or can use the KRI Library to document their own indicators.

KRI Monitoring

Once the firm has defined the various risk, control and performance indicators it wishes to use, the first step in configuring the KRI Monitoring functionality is to assign those indicators to the various operating entities which need to report against the indicator, then to select the specific employees who will be the data provider for each one. Once the sourcing of the KRI data has been attended to, the target consumers who will receive the KRI data can be identified, along with defining the frequency and submission calendars for each indicator. Facility is available to set thresholds and escalation levels on each indicator and to define different types of alerts when thresholds are triggered.

Graci – Risk supports a number of ways by which KRI data can be collected, including self-harvesting data from all the Graci modules where available (for example, open remedial actions, open audit findings, number of customer complaints, number of models not reviewed, etc), automatically calculating derived KRIs (such as percentages, ratios, moving averages, etc.) as soon as the source KRI data is available, manual entry by nominated data providers and pre-formatted spreadsheet import or direct interface from source business applications using the KRI API provided.

Scenario Library

Graci – Risk includes detailed risk content provided from the Scenario Library, a repository of over 600 detailed specifications of scenarios, cross-referenced to public loss events as illustration of how the scenario could manifest itself on the firm. The firm can use these public scenarios as specified, can select and modify scenarios and create private variants of the scenario, or can use the Scenario Library to document their own scenarios.

Scenario Assessment

The Graci – Risk Scenario Assessment functionality supports various methods of scenario assessment, including facilitated workshops, one-on-one interviews and online submission. Assessments can be scheduled and specific scenarios assigned to each participant or per workshop for assessment purposes. The firm can choose what data it wishes to collect and can collect different types of data for different forms of scenario assessment (for example, the data collected for risk-centric scenario assessment is more likely to focus on direct impact, whereas the data collected for business resiliency-centric scenario assessment is more likely to focus on frequency and indirect impacts such as operational efficiency and reputational damage).

Risk Appetite

The concept of risk appetite is to define how much risk the firm is prepared to accept, both overall and at detailed levels of exposure. Risk appetite is commonly defined in both qualitative (i.e. descriptive words) terms and in quantitative (i.e. as specific values) terms. Once risk appetite has been defined, the prudent firm will implement mechanisms to calculate its exposure to the risks on which risk appetite has been set and then to calculate the degree to which that exposure is utilising or consuming the risk appetite, with specific thresholds set for where management is required to intervene to reduce exposure.

The Graci – Risk Risk Appetite functionality provides for both qualitative and quantitative risk and loss appetite statements, as well as various key risk, control and performance indicators to be used as a measure of risk exposure, with thresholds and alert notifications where thresholds are broken. Risk (or loss) appetite statements can be defined at any level of the firm's legal structure or operating structure, as well as at product type, business line and risk category levels.

In addition to qualitative and quantitative risk appetite statements, Graci – Risk supports the concept of "real-time" risk appetite exposure profiles. An exposure profile maps applicable process types against risk categories and for each intersection or exposure point, you can define what data sources should be monitored, with applicable weightings for the exposure at that exposure point. Then, as loss events occur, audit findings are raised, remedial actions become overdue, KRI submissions break thresholds or new regulatory matters arise, Graci automatically calculates the impact on all relevant exposure points and where pre-defined thresholds are breached, triggers warning notifications to nominated management. Trend lines and history over time is maintained.

Models Register

Today, most regulatory jurisdictions require firms to maintain an inventory of mathematical, statistical and actuarial models used within the business and to have some form of model-risk management practices in place to ensure models are both used appropriately and are accurate in their calculations.

Graci – Risk provides a range of models-related functionality, including a models register, a spreadsheet register and a tools register, each of which can be maintained firmwide, by division or by operating entity. Decision trees can be used to assist model owners in determining if a candidate model is actually a model, or else perhaps a spreadsheet or tool, or simply a software application unrelated to models.

Within the individual registers, options are available to record and maintain information on each model, as well as on review cycles, changes to models, model validation activity, regulatory reviews and approvals, and to store model documentation. Calendar alerts and notifications are generated to model owners and nominated reviewers or validators whenever a review or revalidation is required. Model governance can be incorporated using Graci – Governance to set up a model governance committee and to manage committee meetings.

Supply Chain Management

The Graci – Risk Supply Chain Management functionality covers vendor management, contract management, outsourcing arrangement management and the definition of third, fourth and subservient levels in the firm's supply chain. Functionality is grouped around three conceptual registers: a register of vendors, suppliers and service providers, a register of agreements and contracts per supplier and a register of goods, services or outsourced activity per contract. Due diligence is supported at both the supplier and agreement level, with the option for documentation to be sent directly from Graci to the supplier, with online completion/submission and the use of notifications and alerts available, as needed. Service level breach reporting is provided, along with managing the resolution of all SLA breaches. Periodic reviews at the supplier, agreement and service level are supported.

The Supply Chain Management functionality also includes the ability to define requests for proposal, requests for information and tender invitations, then to manage the procurement lifecycle through evaluation to selection and contract closure.

The Graci – Risk Supply Chain Management functionality can be augmented with a data collection application from the Graci – Intelligence Crawlies library. This can then be configured to monitor suppliers at selected levels (direct, third party, fourth party, fifth party, etc.), collecting information from public sources on such parties, as well as building relationship maps between them and other external parties to provide a 360° perspective on the supply chain. Crawlies employ machine learning capability so as to reduce false positives and to ignore data on external parties which is not required.

Operational Resiliency

It is imperative for a firm to remain operational despite facing various forms of business interruption, whether due to natural causes, pandemics, social unrest, war or terrorism, system failures, cyber-attacks or industrial relations disputes. Graci – Risk facilitates this with its Operational Resiliency functionality, which covers business continuity, disaster recovery, emergency evacuations, other crisis planning and overall crisis management. The business continuity functionality allows for the identification of business continuity critical processes and activities, the performance of business impact assessments on such processes under an array of scenarios, and the documentation and maintenance of business continuity plans.

The disaster recovery functionality allows for risk assessments per business application, data centre or location, the definition of secondary and subsequent alternate operating centres and recording the details of recovery point and recovery-time objectives, as well as the necessary business assets needed to ensure continuity. From an emergency evacuation perspective, functionality is available by location to define escape routes, assembly areas, define wardens and marshals and to specify the location of emergency exits, medical equipment and assembly points.

Facility is then provided to maintain records of plan reviews, different forms of plan testing and staff training requirements and to establish crisis-call trees. Review cycles, training cycles and testing cycles can be established, with relevant dates inserted into the applicable employee calendars and with notifications generated at defined lead-times. Where an actual operational resiliency event occurs, facility is available to initiate transition to a crisis status, to convene a crisis committee and to record all details of decisions made and actions taken throughout the crisis. Post crisis, assessments and review forms can be circulated to determine what lessons need to be learned and what remedial actions should be implemented.

REPORTING

No risk solution is complete without the ability to generate management reports and Risk Committee and Board of Directors reporting. The Graci – Core Infrastructure Report Writer facilitates the design of various forms of reports, which can then be selected, populated with the appropriate data and either generated as required or per a pre-defined schedule, then distributed to applicable recipients in electronic format. All reports, when viewed online, support drill-down into appropriate underlying data. A number of pre-defined report templates are provided for use.

Insurance Management

Firms use insurance both as a risk mitigant and as a risk transfer mechanism. The Graci – Risk Insurance Management functionality allows for the establishment of an insurance register, detailing the types of insurance and any exclusions or conditions attached to them, tracking renewal dates and information on relevant insurance brokers and carriers. Reminders are generated to nominated functions ahead of renewals, to allow time for renewals to be adequately negotiated.

Where the firm has to file a claim, the option to record details of the claim and its status are supported, along with tracking details of any claim settlement. Insurance claims can be linked to internal loss events or to litigation cases where appropriate. The firm's taxonomy can be mapped to standard insurance terms and policies, so that loss events can be assessed as to coverage under current insurance policies.

Data Privacy and Security

The Graci – Risk Data Privacy and Security functionality can be divided into four broad categories: developing and maintaining a register of all confidential data across the firm; managing data subject access requests and records of data processing relating to confidential information; recording and managing data privacy breach incidents; and undertaking data privacy and information security risk assessments.

Having defined what confidential data means in different jurisdictions and for different purposes across the firm, facility is available to select those processes which use or generate confidential data and to record what confidential data is involved and what happens to it. A comprehensive data model can be established and reused across both such processes as well as the business applications used by the processes, or from which or into which confidential data is stored. Facility is also available to maintain physical data stores.

As individuals file data subject access requests, a workflow process supports routing requests to the relevant area, tracking compliance and fulfilment of the request, the subsequent response to the requestor and any information-commissioner reporting required as a result of the request. Similarly, records of data processing can be created, updated and made available whenever required.

Where an actual or suspected privacy breach occurs, facility is available for a workflow driven approach to recording, notifying, managing and reporting such breaches, along with the necessary remedial actions to prevent reoccurrence. Records of data privacy breach reports to the applicable information commissioner can be maintained, along with periodic returns to relevant information commissioners.

Various forms of information security risk assessment can be established, scheduled and then executed, with ad hoc or periodic risk rating and the incorporation of information security and cyber risks into the relevant operating entity's risk register. Included amongst the assessments is a data privacy-focussed Equivalency Checker, which allows for privacy rule equivalency to be checked for specific jurisdictions, maintaining an audit trail of previous checks and results.

RiskBusiness

For more information on
Graci by RiskBusiness, please visit

www.riskbusiness.com

or email us at info@riskbusiness.com