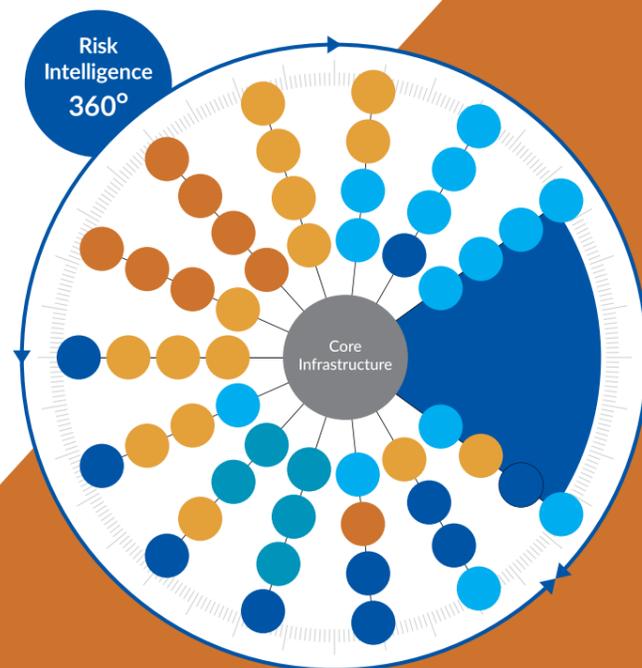


Compliance Module



Compliance Module



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.

- Governance
- Risk
- Audit
- Compliance
- Intelligence
- Core Infrastructure

In today's world, particularly within the financial services industry, more and more regulations, rules, laws and legislation are being introduced, in a global effort to enforce appropriate ethical conduct by firms and individuals alike. Both the sheer volume of such regulatory requirements, as well as the speed of change in existing regulations, create the ever-present and increasing risk of non-compliance by the firm and its staff. At the same time, in order to function efficiently and in an appropriate business manner, most organisations establish formal policies, guidelines and frameworks to govern the manner in which various business activities are performed, supported by detailed procedures which describe exactly how specific tasks aimed at supporting the policy are carried out. Ensuring that the business both has the necessary policy, procedures and instructions and that staff adhere to them has become part of the responsibilities of the compliance function, both at group or holding-company level and within each business entity.

The Graci - Compliance module provides everything that is needed for the independent compliance function within small, medium, large and global conglomerate firms to ensure compliance with regulatory and legislative obligations and internal policies and procedures. It also facilitates appropriate oversight on and challenge to the business where conduct or business activities deviate from the direction provided through such regulation, legislation and/or policy.

Graci - Compliance consists of nine core functional areas, each of which draw upon and use the firm's legal, geographic and operating entity structures. These nine functional areas are supplemented by the set of common functions contained within the Graci - Core Infrastructure module and available in an integrated manner across all Graci modules. These include remedial actions, authorisation and review structures and requirements, notifications and calendars, attestations and meeting functionality, audit trails and the integrated intelligent report writer.

Graci - Compliance shares classification taxonomies, organisational infrastructure and business-related data such as processes, risk, controls, business applications or systems, vendors, business partners, policies, regulations, corporate and business objectives with other control functions, along with data produced specifically within those functions, including incidents and loss events, customer complaints, audit findings and new initiatives, thereby facilitating a 360° perspective of the firm for the compliance function.



Regulations Library



Graci – Compliance includes the Regulations Library, which contains numerous published regulations, rules, notices and consultation papers published by various regulators and supervisors around the world. Each regulation is a reflection of the structure published by the applicable regulator or supervisor, with chapters, sections and sub-sections as relevant. As changes are identified, or when new regulations appear and rescind or replace older regulations, these get added into the Regulations Library.

The compliance function can browse and explore the public Regulations Library, can select applicable regulations and flag them for further use by the firm, or can add their own versions of regulations not already contained within the Regulations Library. The firm may also elect to make use of the Graci – Intelligence Crawl capability, where machine-learning enabled intelligent data collection applications can be deployed against targeted external data sources to collect data sets such as regulations, then present them to authorised users for consideration, rejection, or acceptance into the firm's private Regulation Library area. Note that a workflow enabled notification and change-management process is available for use in conjunction with the Regulations Crawlies.

In looking at applicable regulations, the firm has many choices, ranging from undertaking its own internal legal and regulatory assessment of each section and documenting its conclusions; through deriving a common set of compliance requirements across multiple regulations and conceptually replacing individual sections with the defined compliance requirement; to linking specific regulatory sections to the applicable corresponding sections of internal policies and procedures. The firm may also define a set of regulatory topics or themes and apply these to regulations and regulatory sections, then use the themes for both filtering/ searching and as the basis for ensuring compliance.

Regulations can also be linked to those legal and operating entities to which they apply by jurisdiction, as well as to products and business activities. A matrix-reflecting regulation applicability by these factors is available as a standard enquiry. The Regulations Library can also be searched or filtered using the firm's regulatory topics or themes or using metadata tags applied at the section level. Links to the firm's taxonomy structures for risk types, risk categories, control types, process types, product types and business lines, can also be applied.

Policy Management

Graci – Compliance also hosts the firm's repository of policies and procedures, with options around document type and document security classification, for example, to differentiate between groupwide policies, entity-specific policies or geographically bounded policies. The full policy lifecycle can be managed from draft through approvals and implementation, with detail at the section and sub-section level. Periodic and ad hoc reviews can also be established and undertaken, using the Graci – Core Infrastructure Reviews component.

Policies and procedures can be linked to the firm's taxonomy structures for risk types, risk categories, control types, process types, product types and business lines and to individual process, risk, control and causal registers at applicable business entities. If the firm elects to use pre-defined compliance requirements, these can be attached to applicable sections, then used in compliance tests, assessments and profiles, while regulatory topics or themes and metadata tags can also be included per section. Specific sections of policies and procedures can also be linked to the relevant sections of applicable regulations.



Reporting Obligations

Graci – Compliance allows for the establishment of both internal and external reporting obligations of varying types, with assignment to applicable entities and individual report preparers, reviewers and submitters. This facilitates the definition, for example, of external regulatory reporting, external statutory reporting, external taxation reporting, internal management reporting and internal financial reporting structures.

For each reporting obligation, the intended audience can be established, with internal reporting going to committees, working groups or individual senior managers and external reporting going to nominated regulators, tax authorities, government agencies, financial exchanges, etc. The frequency of reporting, specific data such as security classification, source, data storage requirements and report delivery options can be defined, along with the entity for which the report will be submitted, the entity responsible for submission, the entity or control function with oversight on submission and the individual employees who will prepare, review and submit the report. Links to applicable regulations and policies can be established.

Once the reporting obligation has been put into place, details of the next report are added to the relevant employees' calendars and reminders will be generated. Once prepared, a report can be sent for review and once reviewed, the submitter can record details of the submission and upload a copy of the submitted report, thereby creating evidence of submission.



Compliance Assessments

A core aspect of Graci – Compliance is assisting the compliance function in ensuring compliance with relevant regulations, policies and procedures. This is facilitated through the Compliance Assessments functionality, which allows for five different forms of compliance assessment to be applied across the firm.



COMPLIANCE PROFILES

A compliance profile for a specific legal entity or operating entity reflects the set of business activities which the firm undertakes, described through the entity's processes, grouped using process types defined within the firm's classification taxonomy. The applicable process types are used as one axis of a two-dimensional grid, with applicable regulations and sections, or applicable policies and sections used as the other grid. Sub-profiles by specific regulation or policy, or by jurisdiction, regulator or product type, can also be created, with the option to later aggregate these to the entity level, if required. With each compliance point or intersection of process type and section, the assessor should assess (i) if the section is applicable or not, then if applicable (ii) either the potential for non-compliance and/or the deemed consequences of non-compliance. Options exist for controls to be taken into account, as well as to use a likelihood and impact/consequence matrix if desired. The option to raise compliance findings or to establish remedial action plans is available at the compliance-point level.

REQUIREMENTS PROFILES

A requirements profile is essentially the same as a compliance profile with the same functionality, except that they map the firm's defined compliance requirements against the entity's process types. As an alternative to compliance requirements, the set of regulatory topics of themes can also be used as the basis for the compliance assessment.

COMPLIANCE RISK ASSESSMENTS

The risk of non-compliance may materialise in many different ways and the prudent firm will take steps to mitigate such risks. Graci – Compliance assists such mitigation in two specific ways: firstly, through facilitating the management of emerging risks and secondly, through risk identification, assessment and remediation activities.

Emerging risks may be unearthed in various ways, some within Graci and others external to Graci. Where an emerging risk is identified and documented, it can be assigned to those entities deemed exposed to such a risk, with notifications sent to applicable employees. This then provides the option to consider the emerging risk and either reject it, providing a rationale as to why it is not applicable; or to accept it and to include it in the entity's compliance risk register.

Dependent on the firm's approach to compliance risk assessments, Graci – Compliance supports both point-in-time assessments, where specific risks are selected from the compliance risk register then assessed at a point in time; and continuous risk assessment, where the focus is more on the risk register than an assessment and from where the entity can update its assessment of its exposure to specific risks whenever such exposure is considered to be changing. The option to raise compliance findings or to establish remedial action plans is available at both the assessment or the risk-register level.

COMPLIANCE TESTS

Graci – Compliance supports the establishment of specific test objectives, the scheduling of tests for selected entities, the initiation of a test and the documentation of the test results, with the option to raise compliance findings or to establish remedial action plans. Compliance tests may be supplemented using control tests supported from the Graci – Governance Processes and Controls functionality.

MINIMUM CONTROL STANDARDS

There is the option against either (or both) regulations or policies to define applicable controls per section. The Graci – Governance Processes and Controls functionality allows for the definition of minimum control standards, mapping process types against relevant control types applicable within each process type, defining if such a control type is mandatory, recommended, optional or not applicable for that process type. These minimum control standards can then be filtered within Graci – Compliance to only include those control types related to selected regulations and/or policies, then to undertake an assessment of the level of compliance with the minimum control standards. Compliance is usually measured as fully compliant, partially compliant or not compliant, with the specific controls linked to the control standard as evidence or compliance findings or remedial action plans where only partially compliant or not compliant.

Management Control Testing

In today's world, it is important for the compliance function to be able to evidence to management, the (Risk and) Compliance Committee, the Board of Directors and to regulators, that the firm is applying appropriate management of its risks and exposures. The Graci – Compliance Management Control Testing functionality facilitates the collection of such evidence.

The first step in management control testing is usually an assessment of regulated legal entities and critical operating entities, where management control is crucial in mitigating compliance risks. As a component of the 360° concept, information for a defined time period from the Graci – Governance, Risk, Audit and Intelligence modules for each assessment entity can be aggregated and presented for assessment by compliance staff, supplemented by compliance-specific questionnaires and risk assessments, to derive an overall management control risk rating for the entity. Typical data from the other Graci modules included in such management control risk assessments would include incidents and loss events, risk registers and current risk exposure assessments, control registers and associated control effectiveness assessments and test results, regulatory matters and compliance findings, audit findings, open remedial actions, customer complaints, selected key risk/control/performance indicator values, litigation cases and comparable industry data.

Once the priority of management control testing has been determined, testing sessions can be scheduled, with notifications sent to relevant staff and calendar entries created. At the appropriate time, compliance staff can initiate management control testing, using various tools provided within the Graci – Compliance Management Control Testing functionality. These tools include: minimum control standard evaluations, control testing (with the option to include predefined test cases and accompanying expected test results), policy compliance profiles, regulations compliance profiles, compliance requirements profiles or assessments, regulatory topic or theme assessments, reporting obligation compliance profiles or assessments and free-form questionnaire-based assessments. Each form of assessment supports the establishment of compliance findings and remedial action plans, where appropriate. An overall management control test rating can then be determined and applied to the entity, with the option to generate a management control testing report for management acceptance. Management control testing can be supplemented by periodic management attestation of being "in control", if required.



Regulatory Matters

A critical aspect of compliance activity involves interaction with regulators and supervisors with jurisdiction over the firm. Such interaction may relate to regulatory examinations and reviews, regulatory enquiries, self-identified issues raised with the regulator, employee-related issues, or sanctions and fines. As these various forms of regulatory matters arise, Graci – Compliance facilitates tracking of all interaction with the regulators; documenting each request and response, meetings (both internal and with regulators) and the resolution of each regulatory matter.



Case Management



Most firms have point-of-transaction suspicious transaction detection systems in place, as well as fraud identification systems, KYC systems, sanction-breach prevention systems and countering financial crime systems. These solutions tend to be standalone applications integrated into the firm's core transactional systems. Graci – Compliance adds the case management capability to take flagged transactions, allow a compliance analyst to review and determine whether the flagged transaction is a false positive or an actual suspicious transaction, then to manage the regulatory notification, all ensuing requests and responses, meetings and the final determination by the applicable regulator, providing the evidence of how the firm managed the specific situation.

Litigation Management

The Graci – Compliance Litigation Management functionality allows for the definition of the relevant judicial system(s) which the firm has to manage, with different levels of court (municipal, tribunal, high, appeal, etc.) being user definable, as well as the individual courts themselves. The legal function can also define the various forms of law which may give rise to cases, such as civil, criminal, constitutional, etc., as well as the various stages of proceedings and status which cases will be subjected to.

Facility is available for the firm to be plaintiff, defendant or respondent, as well as to manage co-defendant and co-respondent roles. The specific legal entity involved as well as any specific business entity and/or individual can also be recorded. Facility is available to identify clients on either a named or anonymous basis.

Where a litigation process starts with the firm being served with a subpoena, the full ability to record the subpoena details is provided, along with the ability to define key dates and events, with calendar entries being generated and a user-by-user or case-by-case calendar also being available to monitor. The entire process can then be documented, step-by-step as the case proceeds through the judicial process, with the option to attach and manage all forms of case-related documentation and tasks or actions which arise from the case, with comprehensive and unlimited notes and comments capability.

Cases may be assigned to authorised external lawyers to litigate on behalf of the firm, with the ability to record resultant charges and fees and to manage the billing authorisation process, or simply to use the Graci – Audit Time Management functionality to track internal legal staff time per case. A complete diary function by lawyer, internal and external, by case, by court or by date, for a user defined number of days forward, is provided. Where applicable, accounting provisions can be raised against a case, as well as legal settlements when the case is resolved. Adverse settlements can be transferred into the Graci – Risk Internal Loss Events functionality for further management.



REPORTING

No compliance solution is complete without the ability to generate management reports and (Risk and) Compliance 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.





For more information on
Graci by RiskBusiness, please visit

www.riskbusiness.com

or email us at info@riskbusiness.com