

GRC SUITE

General product presentation

2025



the
[LHoFT]
Grace Connect SARL
is a member of the
LHoFT ecosystem

KEY CHALLENGES OBSERVED

- **Non—Financial risks** are often managed in Excel spreadsheets, but when multiple objects are needed to produce management reports, this could lead to inconsistencies, errors in pivot tables, time consuming manual corrections.
- When data are stored into separate files or in separate systems, the **consolidation or aggregation** into management reporting **might be long and cumbersome**.
- Copy/paste of graphs including **inaccurate values might be subject to multiple quality reviews** or in the worst case **this could lead to wrong decision-making** by top management.
- **Static data in spreadsheets do not contain real time monitoring** and do not reflect progress or evolution made in the organization.
- **Risk analysts are spending 80% of** their precious and costly **time on spreadsheet administration instead of risk analysis**.
- **Risk management strategies are very often based on supplier-tooling rather than being based on clear functional requirements** including a holistic approach covering all control function requirements.

MAJOR IMPACTS ON BUSINESS PRACTICES:

- 1** Inability for management to take optimal risk/return decisions or unreliability of risk reporting due to poor data quality.
- 2** Inability to anticipate non-financial risks, and estimate accurately their related P&L impact or estimate their reputation exposure
- 3** Ad-hoc or incomplete internal control mechanisms.
- 4** Inefficiency in meeting changing regulatory requirements

MARKET GAP: RISK MANAGEMENT TOOL

1. Based on observations, the best practice is to automate analytics and production of reports (and avoid using manual Excel).
2. Existing tools do not integrate a data model that is sufficiently reliable to consolidate all information and produce dashboard or reporting in one single place.
3. Existing GRC tools are expensive, not sufficiently flexible to accommodate the current way of working of each organization, and do not provide reliable solutions covering all sub-domains of non-financial risk management i.e. operational risk management, privacy risk management, business continuity management, disaster recovery, cyber security management, data security management, compliance management or internal audit.

BUSINESS CONCEPT

- 1 A tool offering a comprehensive solution, based on modules with user interface enabling production of analytics and management reporting.
- 2 Software designed to substitute standalone Excel files.
- 3 Complete GRC Suite producing reporting directly in the tool itself.
- 4 Efforts and workload from 1st line of defense representatives will be reduced by having all modules within 1 single tool.
- 5 This will ensure a smooth embedding and deployment of risk culture.

GRACE CONNECT GRC SUITE

The Grace Connect GRC Suite has been designed to include all relevant modules supporting a smart and efficient deployment of a non-financial risk culture within your organization, while ensuring a smooth adherence to regulatory requirements, with particular focus on DORA.

KEY DIFFERENTIATING FACTORS

- User friendly interface easy to use allowing a quick understanding of all functionalities.
- Contains graphs, KPI's, and narratives that will allow to manage risks pro-actively instead of reactively.
- A calendar is included to log all important dates such as Risk Committees, testing, delivery to close an audit finding, high priority action delivery date, which in turn enable a smooth management of non-financial risks.
- Sophisticated Data Model supporting an effortless use of the GRC Suite.
- The Suite is fully customizable at reasonable cost, with deployment performed depending on your size, complexity, and maturity of existing risk framework.
- Time dimension is embedded in the GRC Suite as it is usually better to anticipate risks and delivery dates.
- Embedding of best market practices and advanced risk management evaluation tool (e.g. Cyber Security, GDPR,...).

GRACE CONNECT GRC SUITE: SHORT INTRODUCTION

The GRC Suite is based on intuitive and logical structure composed of separate modules. Through an innovative way, the GRC Suite makes the approach to manage non-financial risks smoother, smarter, and more efficient.

MODULES EMBEDDED

INDICATORS / KPI	RISK	IT GENERAL CONTROL	AUDIT & REPORTING	COMPLAINTS MANAGEMENT	COMPLIANCE QUARTERLY REPORTING
PROJECT	RISK MANAGEMENT Self-Assessment	CMMI Assessment & Capabilities	THIRD PARTY MANAGEMNT	GDPR Assessment	COMPLIANCE TRAINING
TASK	MITIGATION	THREAT RADAR	OUTSOURCING RISK Assessment	DATA PROTECTION IMPACT Assessment	CONFLICT OF INTEREST
EVENT TRACKER	OPERATIONAL RISK SCENARIO	RESILIENCE TESTING	DATA DICTIONARY	REGISTER OF PROCESSING ACTIVITIES	NEW PRODUCT
PROCESS & PROCESS BIA	INCIDENT	BUSINESS CONTINUITY MANAGEMENT	DATA QUALITY Self-Assessment	LEGITIMATE INTEREST Assessment	DORA ITS REGISTER OF INFORMATION
POLICY	SYSTEM, IT COMPONENT & CIA Classification	BCM Self-Assessment	DATA BREACH	PRIVACY RISK REGISTER	CONTRACT MANAGEMENT

New ▾

Home

Dashboard

Process

Task

Incident >

Complaint >

Risk >

Third party >

IT Register >

Policy >

Data Protection >

Audit >

Project

Compliance >

Event Tracker >

Documents

Home

News feed



Dutch begin COVID-19 vaccinations last EU nation t...

THE HAGUE Netherlands AP Nearly two weeks after most other European Union nations the Netherlands Q...

By: Admin User
06/01/2021 10:27 AM

[Read more](#)



UK goes into Tier 4 lockdown as new variant of COV...

Englands chief medical officer has informed the World Health Organization that the new coronavirus S...

By: Admin User
26/01/2021 12:28 PM

[Read more](#)

Risk category (Open)



Task priority

DORA

FOCAL POINT ON COMPLIANCE WITH DORA (1/2)

Based on our support of DORA project with market participants, we updated the Grace Connect GRC Suite to support your roadmap to compliance with DORA regulation. Modules presented in the table below are actively contributing to effective implementation of DORA requirements (incl. also ITS/RTS provisions).

ENTITY-LEVEL MODULES

DORA Ref.	Module
Art. 5 - Governance and organization RTS Risk Art. 2, 3	Policy framework
Art. 24.2 - General requirements for the performance of digital operational resilience testing	Event & trackers
Art. 6.7 - ICT risk management framework	Audit report & findings
Art. 11.6.a. - Response and recovery RTS Risk Art. 27	BCM Risk assessment
Art. 6.8.c - ICT risk management framework Art. 17.3.a - ICT- related incident management process	Indicators
Art. 13.6 - Learning and evolving	Training

PROCESS-LEVEL MODULES

DORA Ref.	Module
Art. 8.1, 8.5 - Identification Art. 28.3 - General principles	Process
Art. 11.2.b, 11.10 - Response and recovery Art. 17 - ICT-related incident management process Art. 18.1.(a-f) - Classification of ICT-related incidents and cyber threats Art. 19.1 - Reporting of major ICT-related incidents and voluntary notification of significant cyber threats Art. 28.7.a - General principles RTS Risk Art. 22 RTS Incident mgt Art 2 RTS Incident mgt Art 10	Incident
Art. 11.2 - Response and recovery Art. 13.2 - Learning and evolving RTS Art. 26	Crisis Reporting & Crisis Call Tree
Art. 8.3 - Identification	Risk management
Art. 5.1 - Governance and organisation Art. 6.3 - ICT risk management framework Art. 16.1.a - Simplified ICT risk management framework	Mitigation
Art. 8.2 - Identification	Scenario analysis
Art.11.5 - Response and recovery Art. 12.6 (RTO/RPO) - Backup policies and procedures, restoration and recovery procedures and methods RTS Risk Art. 24	Process BIA
RTS Risk Art. 5	CIA classification

Modules are mapped with specific DORA provisions and by having a comprehensive design of modules, Grace Connect GRC Suite demonstrate its capacity to cover maximum of DORA requirements in one single solution.

DORA

FOCAL POINT ON COMPLIANCE WITH DORA (2/2)

Grace Connect GRC Suite becomes the first GRC solution on the market offering a comprehensive support in DORA compliance efforts. The inter-connexion between all modules included in the Suite enable a smooth channeling of information in all ITS templates and eventually in the annual DORA report (RTS risk management Art. 27).

SYSTEM-LEVEL MODULES

DORA Ref.	Module
Art. 8.2 - Identification Art. 24.6 - General requirements for the performance of digital operational resilience testing RTS Risk Art. 24.1 RTS Risk Art. 25	Resilience testing report & findings
Art. 11.5 - Response and recovery Art. 12.6 - Backup policies and procedures, restoration and recovery procedures and methods RTS Risk Art. 24	System BIA
RTS Risk Art. 3.1 RTS Risk Art. 6	IT General controls
Art. 8.2 - Identification Art. 17.2 - ICT-related incident management process Art 18.2 - Classification of ICT-related incidents and cyber threats RTS Incident Mgmt Art. 16 RTS Risk Art. 3.1	Cyber threat analysis
Art. 12 - Backup policies and procedures, restoration and recovery procedures and methods RTS Risk Art. 11	Data dictionary
Art. 6 - ICT risk management framework RTS Risk Art. 4.2	System & IT component

ICT THIRD PARTY-LEVEL MODULES

DORA Ref.	Module
Art. 28.1.a, 28.3 - General principles RTS Third Party Art. 1 RTS Third Party Art. 3-6 (EU) 2024/2956_Roi (ITS Provisions)	Third Party
RTS Third Party Art. 5 RTS Third Party Art. 6	Third Party assessment
Art. 28.3.c - General principles RTS TP Art. 5.2 RTS Art. 6.1.a.	Outsourcing risk assessment
ITS all provisions	DORA ITS
Art. 28.4.e - General principles RTS Third Party Art. 8 RTS Third Party Art. 9 (EU) 2024/2956_Roi (ITS Provisions)	Contract & Service Assessment
Art. 28.4.e - General principles RTS Risk Art. 2.2.g. RTS Third Party Art. 7	Conflict of interest
RTS Risk Art. 5	Data classification
RTS Risk Art. 15	Project

ITS IMPLEMENTATION

GRACE CONNECT READINESS

Within Grace Connect GRC solution requirements for ITS reporting are fully embedded and can be further customized according with client's organizational structure

ITS Template	Template title	Relational keys	Modules in GC GRC Suite
B_01.01	Entity maintaining the register of information		DORA ITS Company information section
B_01.02	List of entities within the scope of the register of information		DORA ITS Consolidation perimeter
B_01.03	List of branches		DORA ITS List of branch(es)
B_02.01	Contractual Arrangements – General Information		CONTRACT MODULE
B_02.02	Contractual Arrangements – Specific Information	    	CONTRACT & SUPPLIER MODULES
B_02.03	List of intra-group contractual arrangements		CONTRACT MODULE
B_03.01	Entities signing the Contractual arrangements for receiving ICT service(s) or on behalf of the entities making use of the ICT service(s)		CONTRACT MODULE
B_03.02	ICT third-party service providers signing the Contractual arrangements for providing ICT service(s)	 	CONTRACT MODULE
B_03.03	Entities signing the Contractual arrangements for providing ICT service(s) to other entity within the scope of consolidation		CONTRACT MODULE
B_04.01	Entities making use of the ICT services	  	CONTRACT MODULE
B_05.01	ICT third-party service providers		SUPPLIER MODULE
B_05.02	ICT service supply chains	  	CONTRACT & SUPPLIER MODULES
B_06.01	Functions identification	 	PROCESS & BCM BIA Modules
B_07.01	Assessment of the ICT services	  	SERVICE ASSESSMENT
B_99.01	Definitions from Entities making use of the ICT Services		NA

ITS Structure

The Register of Information comprises 15 templates, interconnected through relation keys to link data (i.e. contract reference number, ICT third-party service provider identifier, function identifier, and ICT service identifier).

These keys are defined in 1 specific template and link the others. For instance, the contract reference number key, defined in RT.02.01, facilitates connections across templates such as RT.02.02, RT.02.03, RT.03.01, RT.03.02, RT.03.03, RT.04.01, RT.05.02, RT.07.01 creating relationships among their data.

Relational keys:

-  Contractual Arrangement Reference number
-  Function Identifier
-  LEI of entity making use of the ICT Services
-  Type of ICT Services (annex III)
-  Identification code of the ICT Service Provider
-  Identification code of the branch

INTUITIVE TOOL WITH A USER-FRIENDLY LOOK AND FEEL

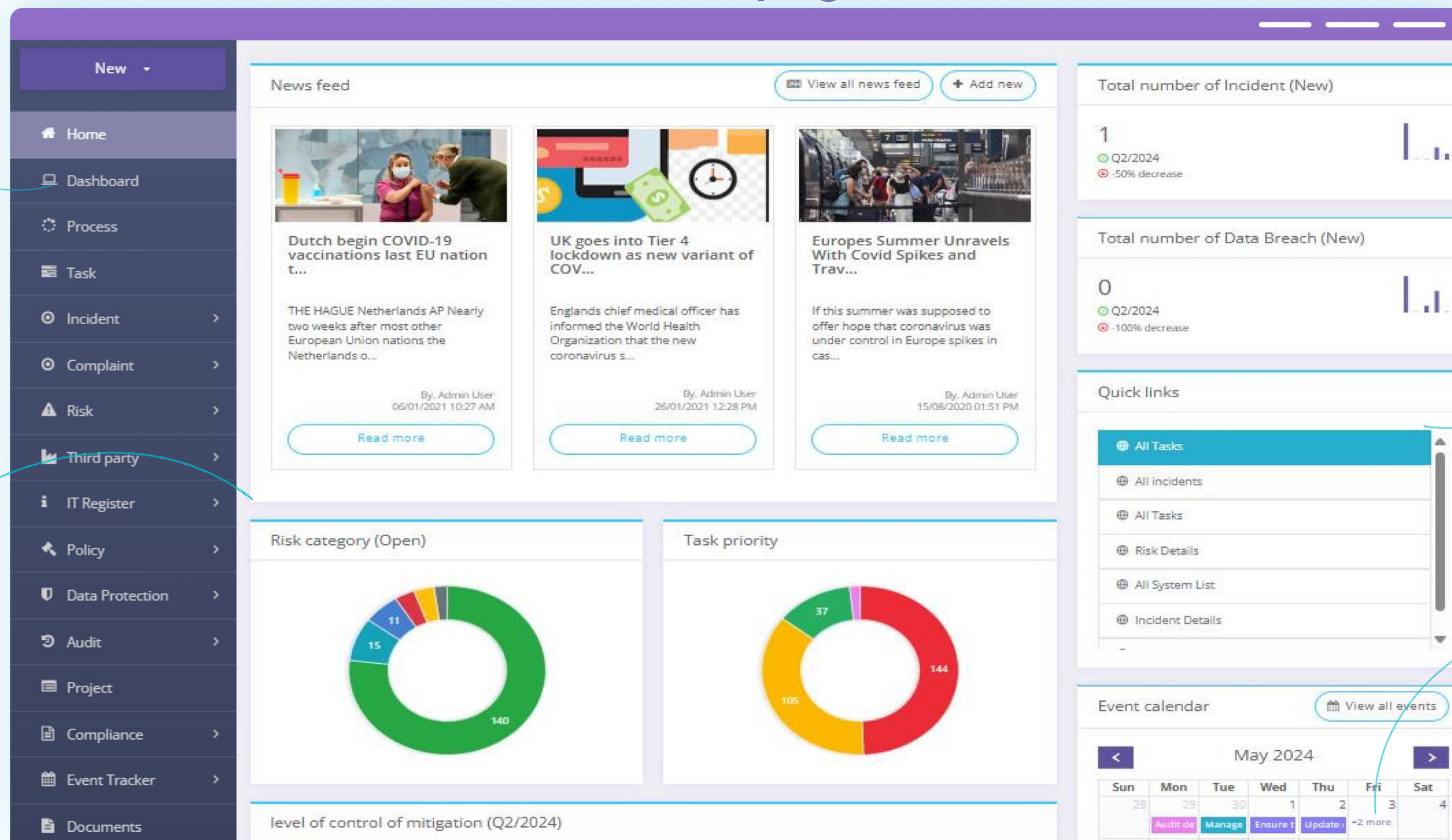
home page

List of subscribed modules for comprehensive and clear overview

The interface is designed to minimize user clicks and find information in the shortest time possible

Shortcuts to user-preferred modules

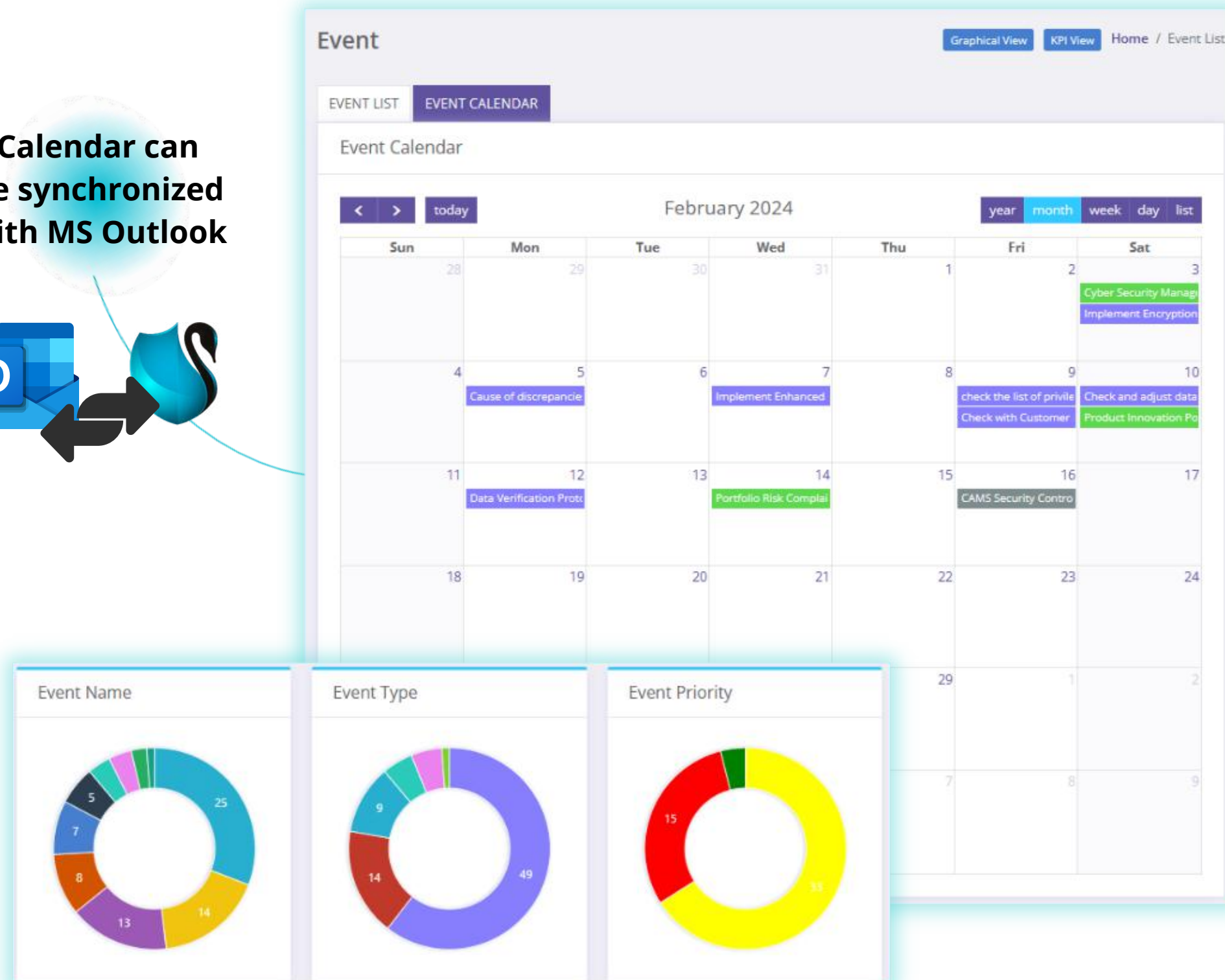
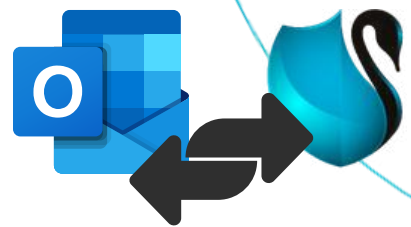
Calendar – the time dimension in the GRC tool is a key differentiating factor from other GRC tool



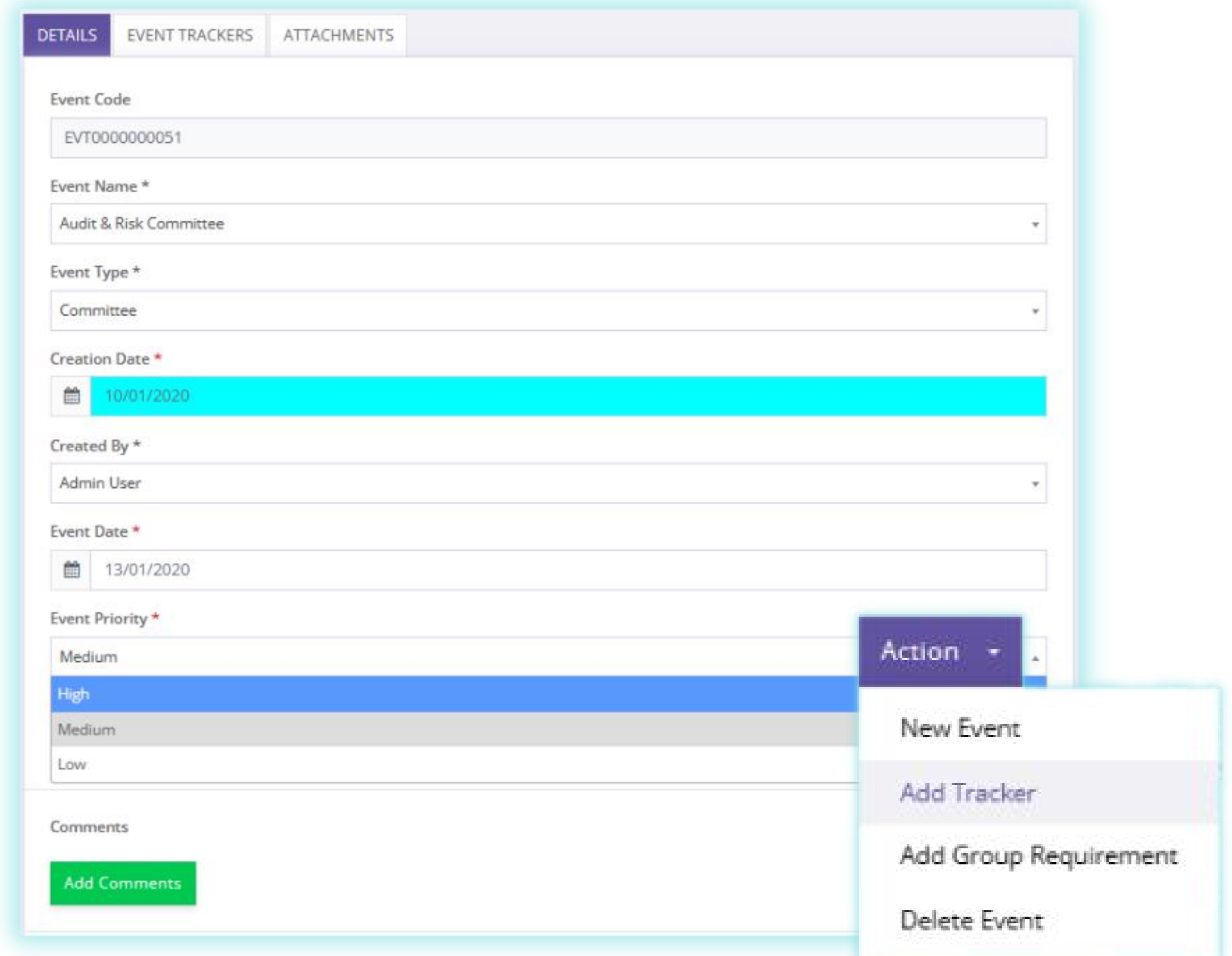
EVENT MANAGEMENT

To facilitate monitoring of significant dates the **Event Management** module allows users to log and track date related to **Regulatory due date, Resilience testing, Audits due date, Tasks, Trainings, key meetings**. Dates can be logged through the dedicated module Event Management or through linked modules (e.g. Audit, Regulatory Watch, Resilience Testing, Tasks)

Calendar can be synchronized with MS Outlook



Events calendar and graphical view



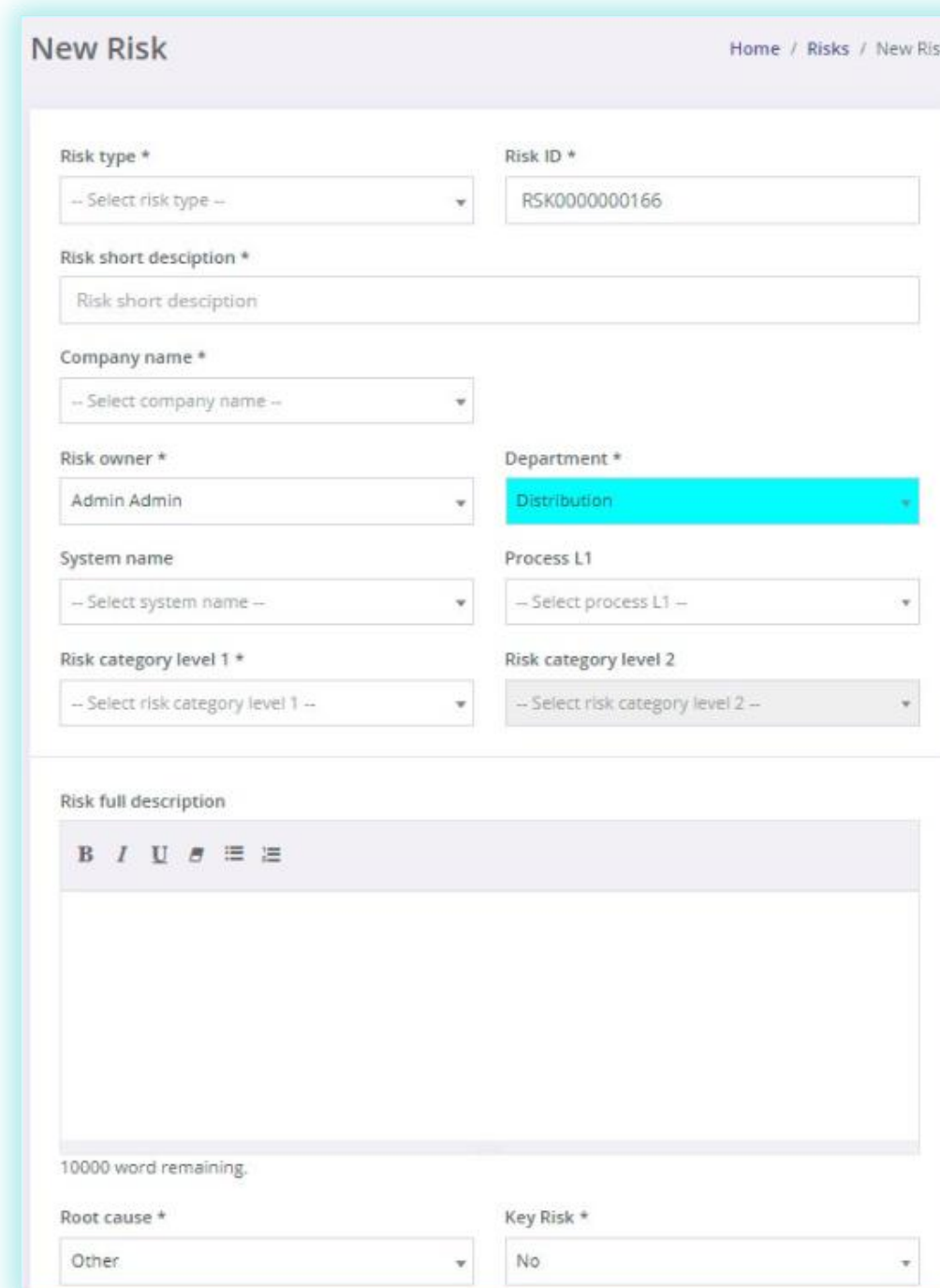
The screenshot displays the 'Event' module interface in the 'DETAILS' tab. It shows a form for creating or editing an event. The form includes fields for Event Code, Event Name, Event Type, Creation Date, Created By, Event Date, and Event Priority. An 'Action' dropdown menu is open, showing options: New Event, Add Tracker, Add Group Requirement, and Delete Event.

Field	Value
Event Code	EVT0000000051
Event Name *	Audit & Risk Committee
Event Type *	Committee
Creation Date *	10/01/2020
Created By *	Admin User
Event Date *	13/01/2020
Event Priority *	Medium

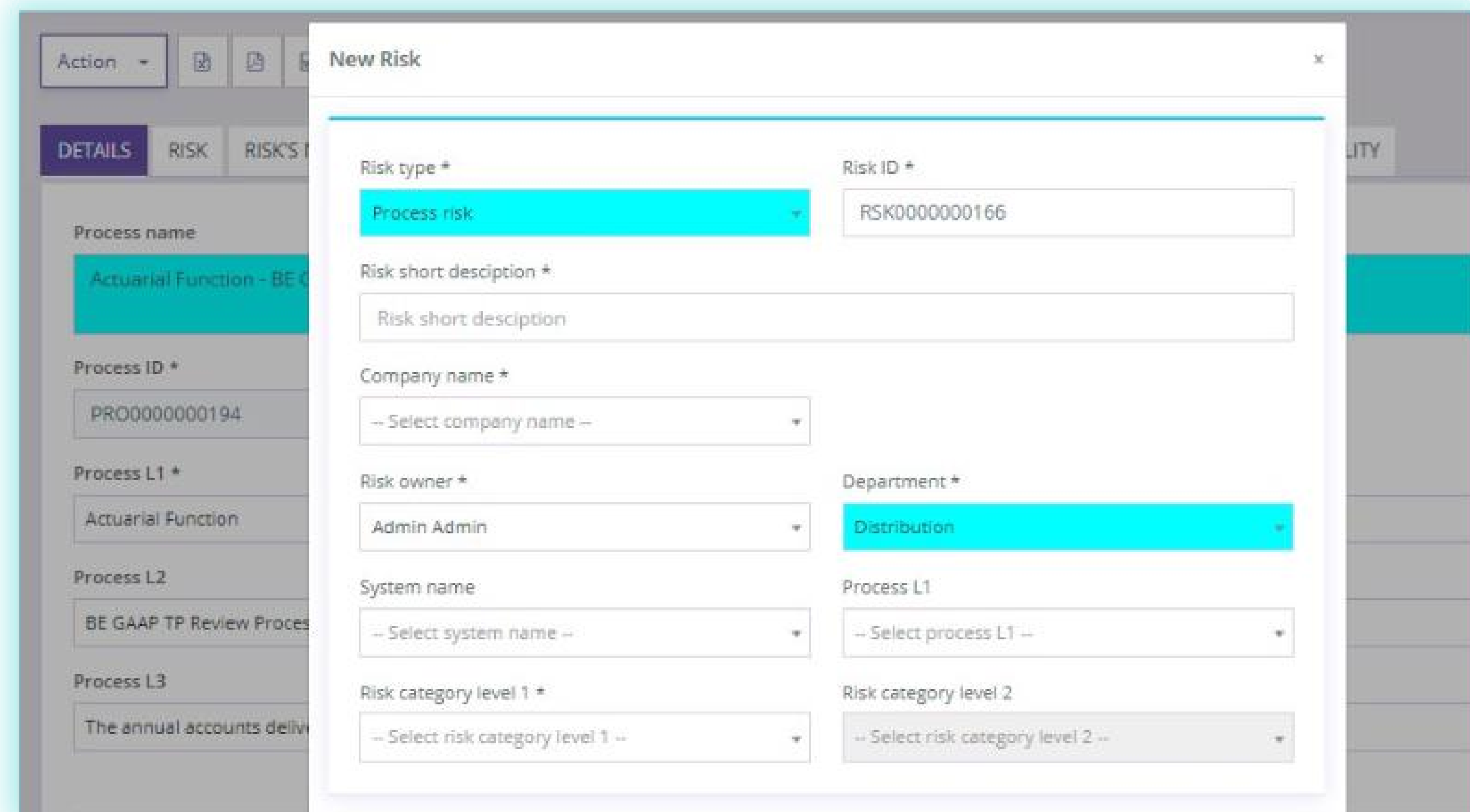
Event detailed view

INTUITIVE USER INPUT WITH EASY TO USE FORMS

User input forms are intuitive and include all required information to be reported / included in KPI's and graphs.



User input form (New risk)



Drop down window for input of information in related objects (New Process risk). This enhances controls and reduces manual errors (input failures).

All data fields are selected and designed to meet client requirements, comply with industry best practices and regulatory expectations. Similar approach for input form is **used in all modules of the GRC Suite**.

HOMOGENEOUS LIST VIEW THROUGHOUT ALL MODULES

Once information is introduced by users in the GRC Suite, a **list view** is available with all columns and metadata. From this list view, users can:

DIRECTLY ACCESS GRAPHS OR KPI'S VIEWS

DOWNLOAD IN PDF OR XLS FORMAT

DIRECTLY PRINT OUT THE LIST VIEW

Complaints List

+ New Complaints

Show 500 entries

Search

SR. NO.	COMPLAINTS NAME	COMPLAINT TYPE L1	CONTRACT ID	PRODUCT CLASS	COMPLAINT ORIGINATOR	COMPLAINT FINAL ORIGINATOR	COMPLAINT MANAGED INTERNALLY?	COMPLAINT RECEIVED FROM	COMPLAINT RECEIVER ACTIVE	HANDLER	HANDLER ID	HANDLER DEPARTMENT
1	malfunctioning of an ATM	Other	7894	Other	Other	No	No	Phone	No	Compliance_Director Banking	BKCOMP	Compliance
2	payment software not operational	Other	5678	Other	Other	Yes	No	Email	No	Compliance_Director Banking	BKCOMP	Compliance
3	sell order not placed	Brokers	1452	Other	Third Party	No	No	Email	No	Credit_BO_agent Banking	BKCB0	Credit Back Office
4	ordered credit card never received	Other	978	Other	Other	No	No	Other	No	Credit_BO_agent Banking	BKCB0	Credit Back Office
5	Unsatisfactory settlement offer	Sales	000001234567324	Patrimoine	Other	No	No	Email	No	Complaint_agent Insurance	INSCOMPLAINT	Complaint Management
6	App for Life Insurance contract management failure	Claims	00000012453687	Other	Other	No	No	Email	Yes	Complaint_agent Insurance	INSCOMPLAINT	Complaint Management
7	Incoming complaint from Mrs. Giuditta Ambrosoli	Claims	00000013456738	Patrimoine	Other	No	No	Other	Yes	Complaint_agent Insurance	INSCOMPLAINT	Complaint Management



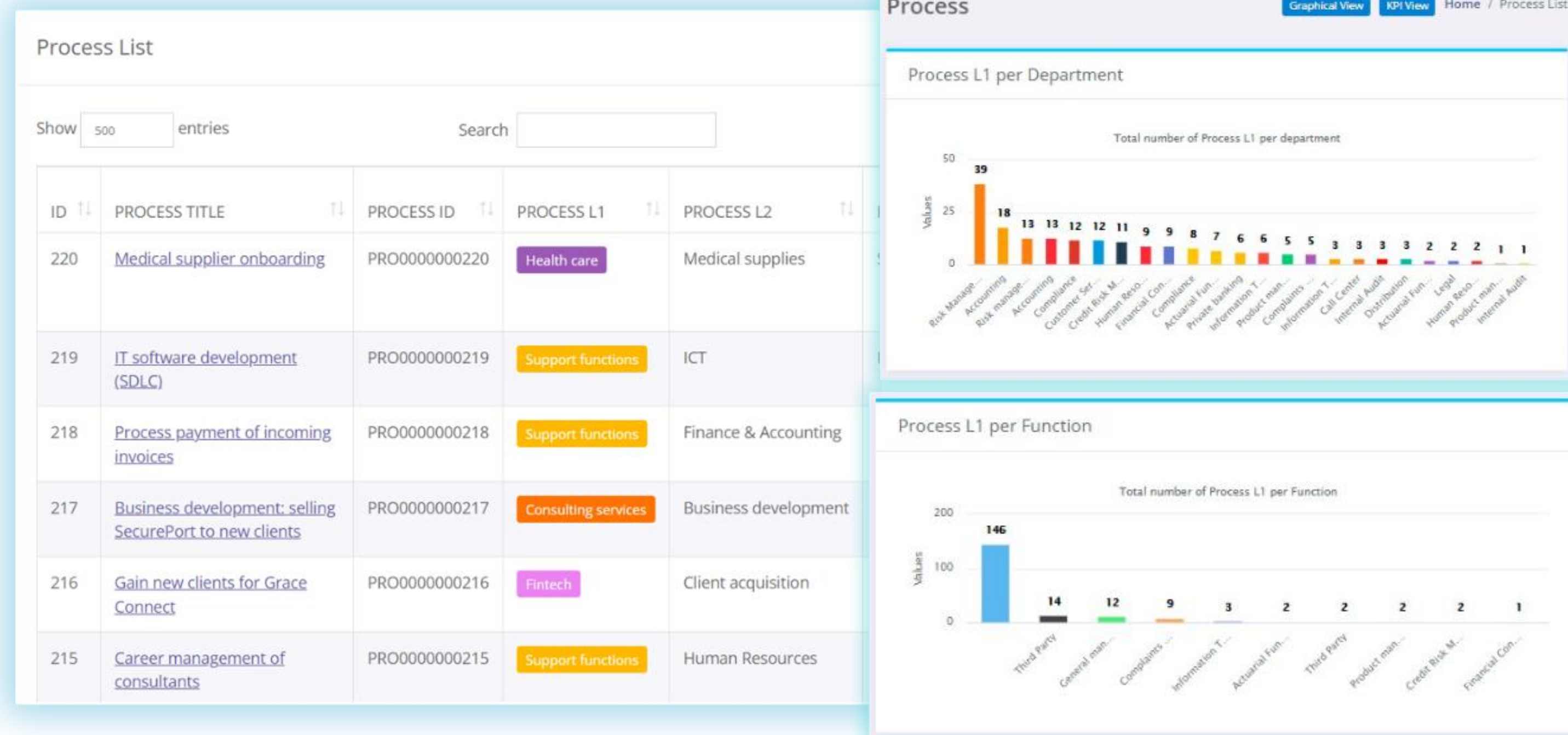
- The user interface is the same for all modules included in the GRC Suite: users get familiar with the interface quickly and are comfortable using new modules.
- The view can be modified by adding, hiding, sorting, filtering columns depending on user's preferences and needs.

PROCESS-BASED ORGANIZATION AS A BACKBONE

There are various ways to look at an organization, especially depending on its size, complexity of products, and operating processes.

The GRC Suite is designed to integrate a Process view enabling users to map out:

Risks, Controls, Incidents | BCM business impact analysis | Data Quality issues | Audit Findings linked to business processes
(likewise majority of the modules in the GRC Suite)



Process module can be
linked with existing
documentation tools
through API

The **Process module serves as the backbone of the GRC Suite**, enabling the centralized documentation of organizational processes and activities.

This will allow users to have a consolidated view on all related items cutting through a process. For smaller organization, a view per department is designed by default.

WORKFLOW-BASED INCIDENT MANAGEMENT MODULE

Incident modules enables users to log, track, and manage incidents originating from various sources, including operational risks, cyber security threats, and compliance issues.

data quality issues

cyber security incidents

data breaches (GDPR requirement)

Incidents List

Show entries Search

ID	INCIDENT TITLE	INCIDENT TYPE	INCIDENT CATEGORY
166	server damage to a fire in IT room	Operational Risk	Damage to physical assets
165	Wrong credit interest rate applied	Client complaint	Complaint received from client
164	ransomware	Information Security	Information Security failure
163	Data leakage	Cyber Security	Cyber security incident
162	DDOS attack	Cyber Security	Cyber security incident
161	phishing attack by email	Cyber Security	Cyber security threat monitoring
159	Failure of an infusion pump	Operational Risk	Business disruption & system failure
158	Misplaced documents interchanged between	Client complaint	Complaint received from client

Simple list view (all incidents)

New 79	Analyze 12	Remediate 6	Notify 38
Data breach - Payment made to wrong bank Operational Risk Difference: 3 Years 3 Months 28 Days Risk rating: Very low LORE-78 IT_Director Banking	Connection issue switch box located in server room Operational Risk Difference: 3 Years 4 Months 7 Days Risk rating: Very low ORED-Test-01	Unavailability of data center Operational Risk Difference: 3 Years 5 Months 7 Days Risk rating: Very low ORED-Test-03 IT_Director Banking	Unavailability of network Operational Risk Difference: 3 Years 5 Months 3 Days Risk rating: Very low ORED-Test-02 IT_Director Banking
Fraud case In LifeCo Operational Risk Difference: 3 Years 3 Months 14 Days Risk rating: Very low EVENT-01 IT_Director Banking	Data breach - 2183 documents sent to wrong customers by post Operational Risk Difference: 3 Years 2 Months 18 Days Risk rating: Very low LORE-68 IT_Director Banking	Data breach - 3 documents shared with wrong client Operational Risk Difference: 3 Years 2 Months 18 Days Risk rating: Very low LORE-S6 IT_Director Banking	Correction 86 contract_complain Operational Risk Difference: 3 Years 4 Months Risk rating: Very low LORE-81 IT_Director Banking
Data breach - 2183 documents sent to wrong customers by post Operational Risk Difference: 3 Years 2 Months 15 Days Risk rating: Very low LORE-682 CISO Insurance	Accounting system failure Operational Risk Difference: 2 Years 12 Months 3 Days Risk rating: Very low INC0000000056	Incident test RBS Operational Risk Difference: 1 Years 11 Months 2 Days Risk rating: Low INC0000000119 PROJECT_Mgr Insurance	Postal fraud - Falsified surrender document G.R. Operational Risk Difference: 3 Years 4 Months Risk rating: Very low LORE-05 IT_Director Banking

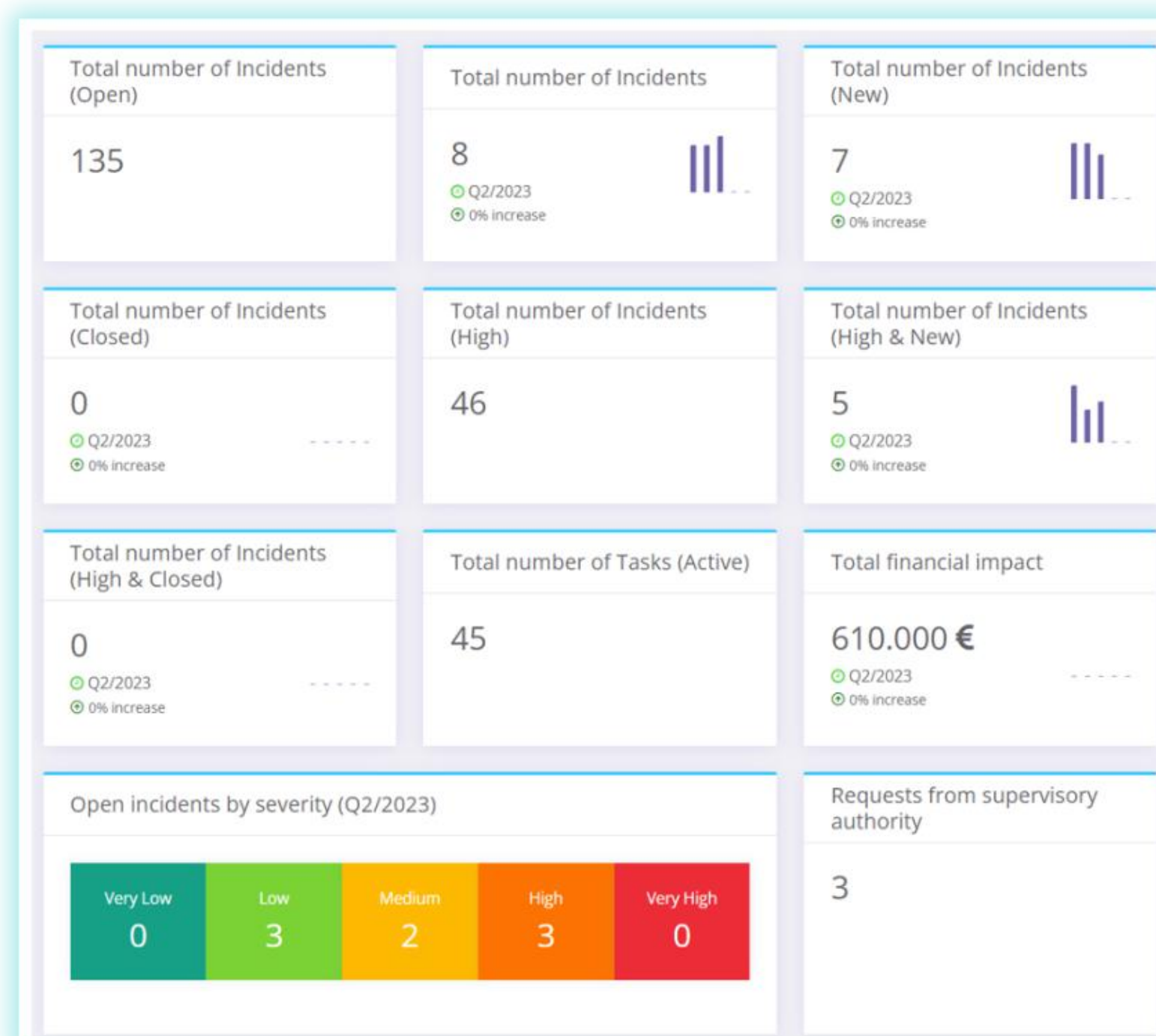
Incident tracking view (all incidents)

Possible connection
with JIRA
(through API)

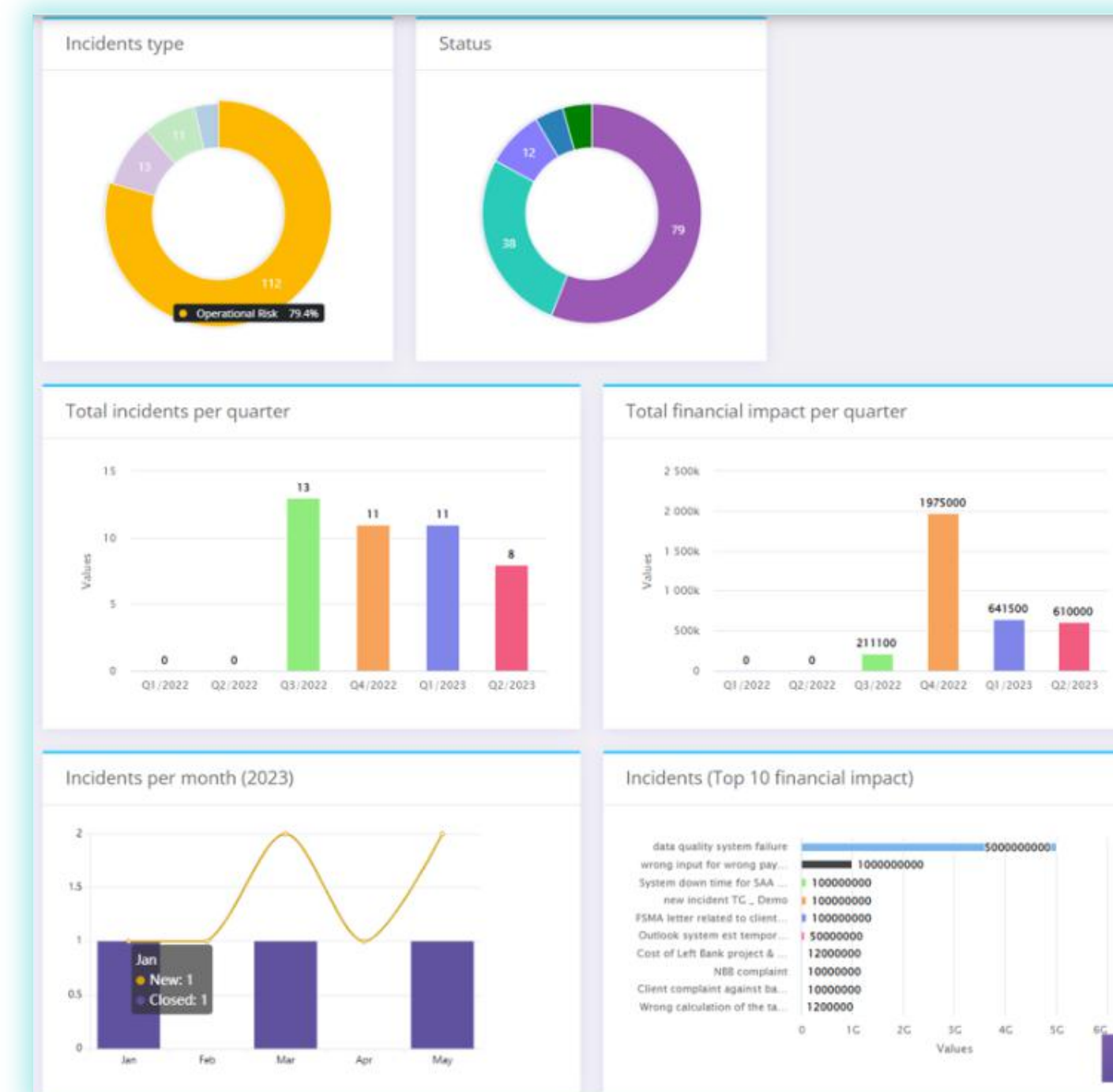
Incidents are listed and illustrated with predefined graphs and are an input to Key Performance indicators (KPIs). This allows users to real-time monitor, ensuring timely resolution and **in compliance with DORA requirements**.

WORKFLOW-BASED INCIDENT MANAGEMENT MODULE

A **set of KPI's and graphs** has been pre-defined in each module of the GRC Suite to provide users and management with a clear insight on critical issues that require immediate attention.



KPI's view (all incidents)



Graph view (all incidents)

KPI's and graphs uploaded in the GRC Suite provide a comprehensive view on **incidents**. In addition to graphs and KPI's embedded in each module, a separate module offers the possibility to add custom-built KPI's. For advanced users, additional KPI's and graphs can be added upon request.

POLICY FRAMEWORK IN A CENTRALIZED REPOSITORY

The **Policy framework module** provides GRC Suite users with a single repository of all internal (or group) policies. Specific details of policies such as name, version, approval dates, next review date, policy owner, regulatory references, etc are stored and updated.

Policy List

+ New Policy

Show 50 entries Search

POLICY ID	POLICY NAME	DEPARTMENT	POLICY VERSION	POLICY CONFIDENTIALITY LEVEL	POLICY TYPE	POLICY CATEGORY	POLICY DOMAIN	SUBJECT TO COMPLIANCE REVIEW
POL0000000049	Code of Conduct	Data Governance	0.3	Internal	Group Policy	General governance requirement	Governance Policy	No
POL0000000047	Payment Innovation Policy	Payment & Cash Management	1	Public	Local Policy	General governance requirement	Governance Policy	No
POL0000000046	Product Innovation Policy	Innovation & New Technology	0.1	Internal	Local Policy	Local Policy	Governance Policy	No
POL0000000045	Data Privacy Policy	Legal	0.2	Internal	Group Policy	Cloud Computing	Privacy Policy	No
POL0000000044	Sustainability Policy	Innovation & New Technology	0.3	Internal	Group Policy	General governance requirement	Compliance Policy	No
POL0000000043	Investment Policy	Back Office - Life	11	Internal		Risk management - Article 44 S	Risk Control Policy	No
Pol_42	Emergency concept for reducing counterparty risks in banks and similar service providers	Risk Management	4.2	Internal		Other	Business Control Policy	No
Pol_41	Appointing authorized	Risk Management	0	Internal		Other	Business Control Policy	No

- ✓ Easy downloading of the **list of Policies** with the XLS-based or PDF-based functionalities.
- ✓ A **set of graphs and KPI's** is also available for users and management.
- ✓ **Policy documents** are accessible directly within the GRC Suite (see also Document Management).

RISK MANAGEMENT ENABLED GRC SUITE

The **Risk module** provides GRC Suite users with most advance analytical tools in a single repository. Specific details of risks are stored and updated, such as:

description

root cause

categories

owners

impacted process

likelihood, impact

risk score

and more ...

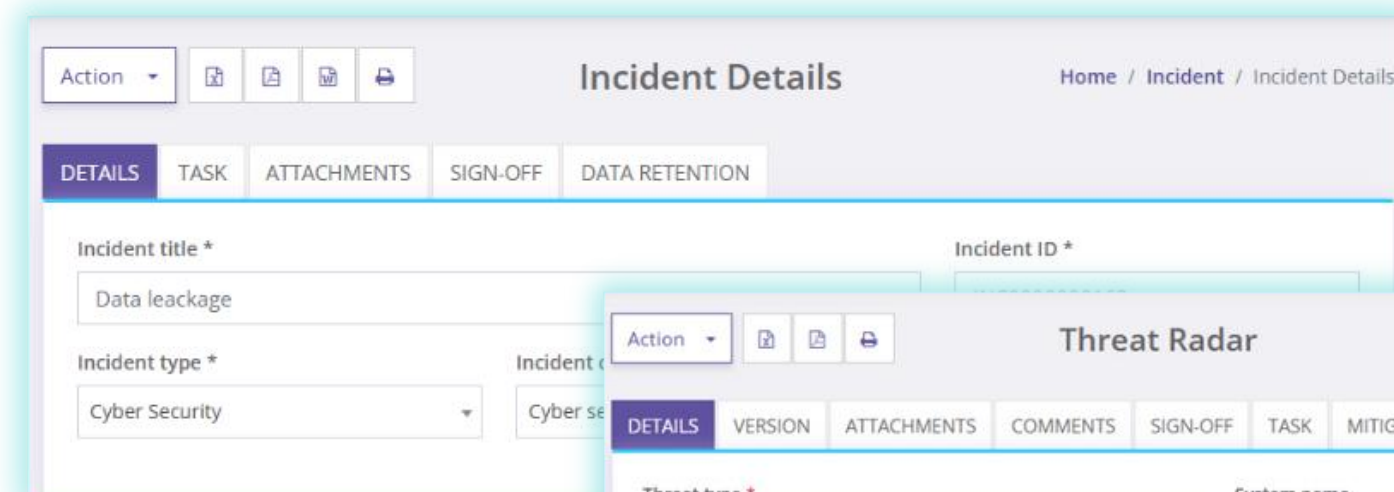
+ New Risk									
Show 50 entries Search									
SR. NO.	RISK TYPE	RISK SHORT DESCRIPTION	RISK OWNER	PROCESS L1	RISK CATEGORY LEVEL 1	ROOT CAUSE	KEY RISK	START DATE	RISK STATUS
1	Process risk	Risk that the medical supplier is not delivering as expected	Head-of_Medical Devices Hospital	Health care	Operational risk	Other	No	26/04/2023	New
2	Risk Dashboard	Risk that BO application is out of support from external provider	PCM_Director Banking	Banking	Operational risk	System	No	06/03/2023	Existing
3	Risk Dashboard	Cybersecurity lapses	IT_Director Banking	Banking	Operational risk	People	Yes	15/02/2023	New
4	Risk Dashboard	Inadequate Employees training	RISK_Director Banking	Banking	Operational risk	People	No	02/01/2023	New
5	Financial risk	Counterparty risk	RISK_Director Banking	Banking	Operational risk	External Event	No	02/01/2023	Existing
6	Project risk	have 2 authorized access persons off at the same time	CISO Insurance	Insurance	Operational risk	Other	No	31/01/2023	Existing

A set of graphs and KPI's is available for users and management. It has been designed including "narrative" so that users can easily transfer identified by the tool main observations directly and automatically to their management report.

CYBER SECURITY MODULE IN GRC SUITE

Grace Connect GRC Suite includes a set of modules dedicated to the **management of Cyber Security risks**.
A maturity assessment enables to focus on areas to reinforce in the short term and design a roadmap to increase the maturity for Cyber security in the long term.

Cyber security incidents are logged in a dedicated module and **Cyber threats** are monitored on a frequent basis to ensure that the organization is aware of possible threats arising from the cyberspace.

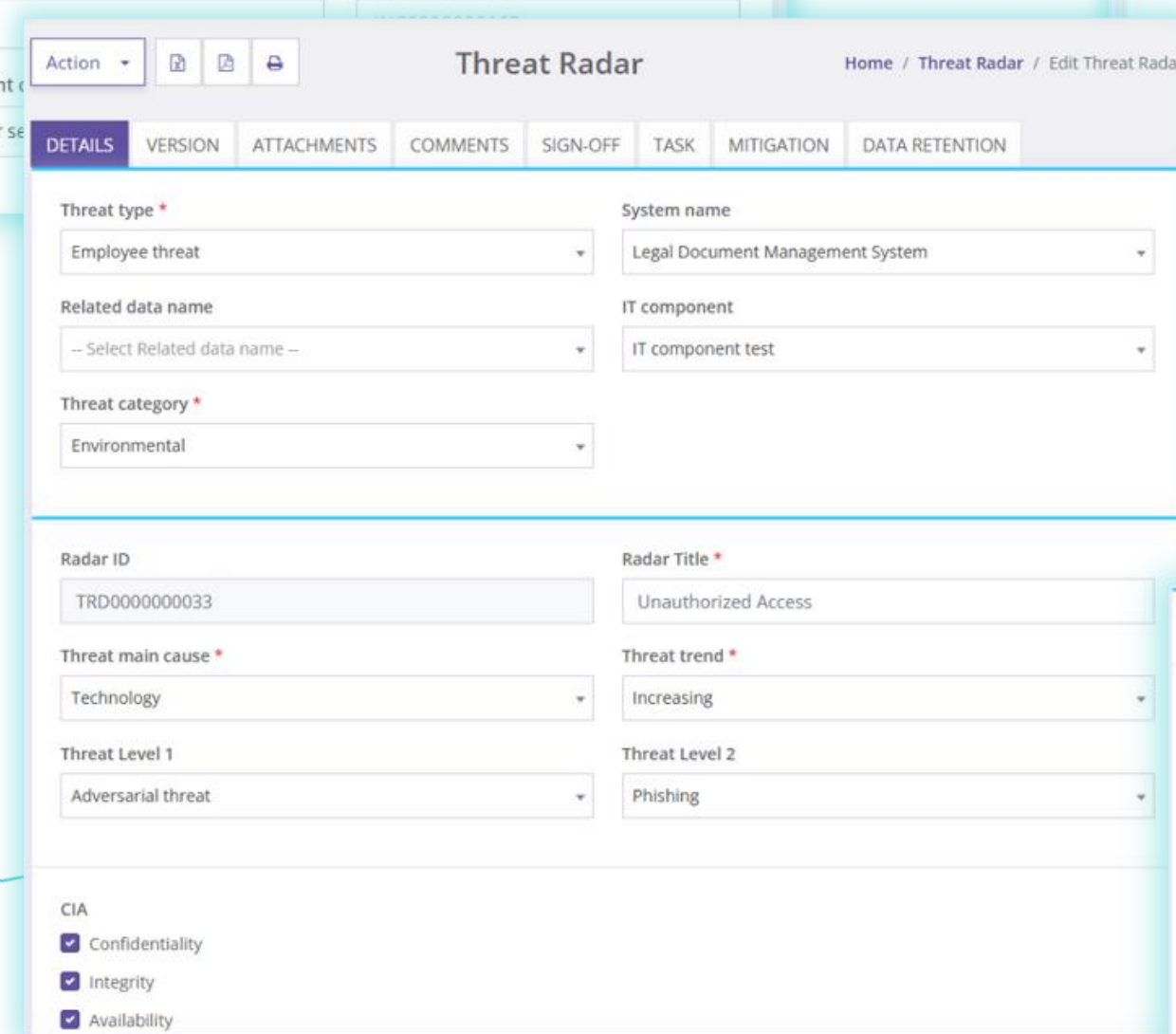


Incident Details

Incident title *
Data leakage

Incident ID *

Incident type *
Cyber Security



Threat Radar

Threat type *
Employee threat

System name
Legal Document Management System

Related data name
-- Select Related data name --

IT component
IT component test

Threat category *
Environmental

Radar ID
TRD0000000033

Radar Title *
Unauthorized Access

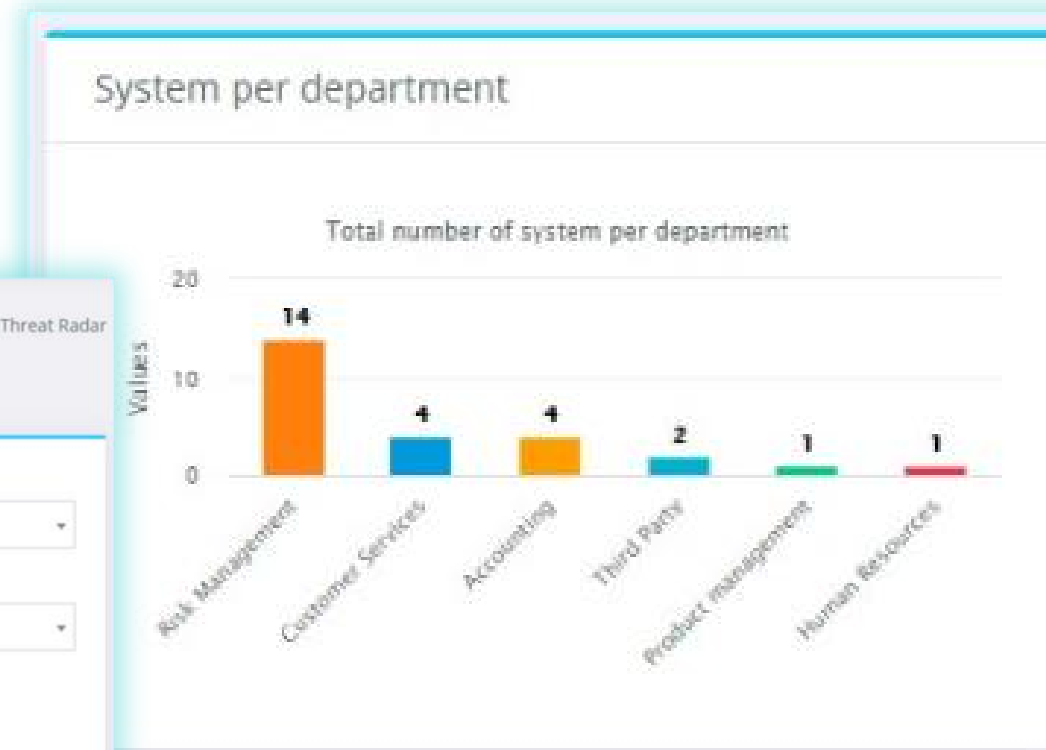
Threat main cause *
Technology

Threat trend *
Increasing

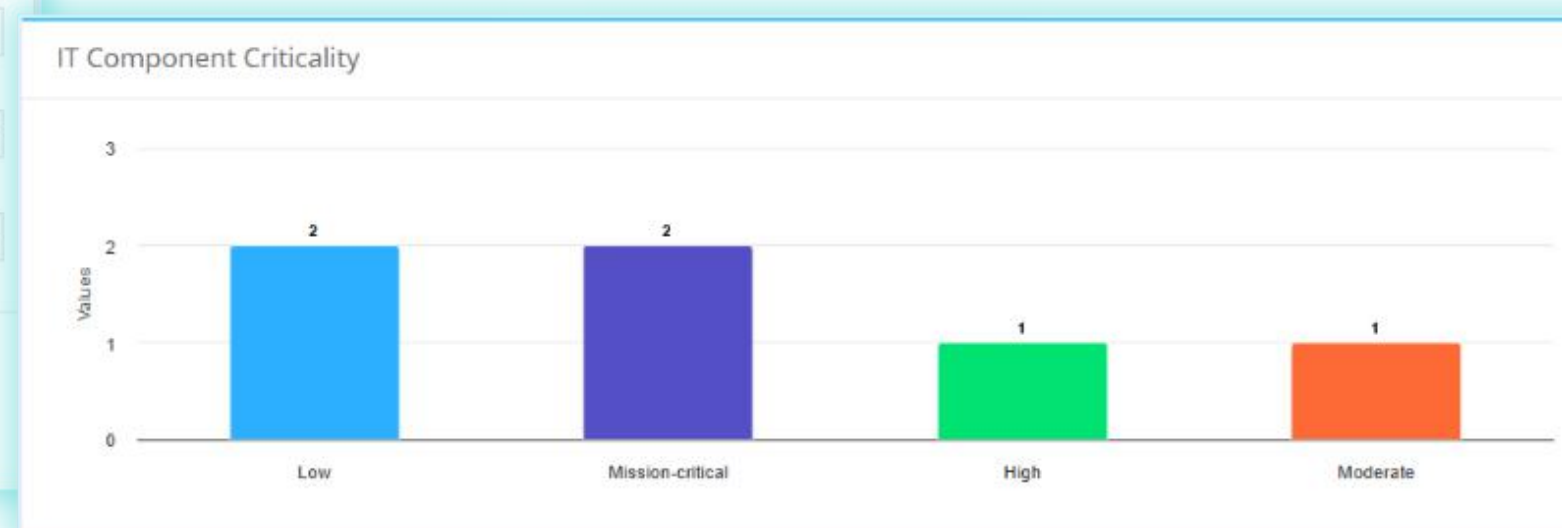
Threat Level 1
Adversarial threat

Threat Level 2
Phishing

CIA
☒ Confidentiality
☒ Integrity
☒ Availability



View on Systems stored in the GRC Suite



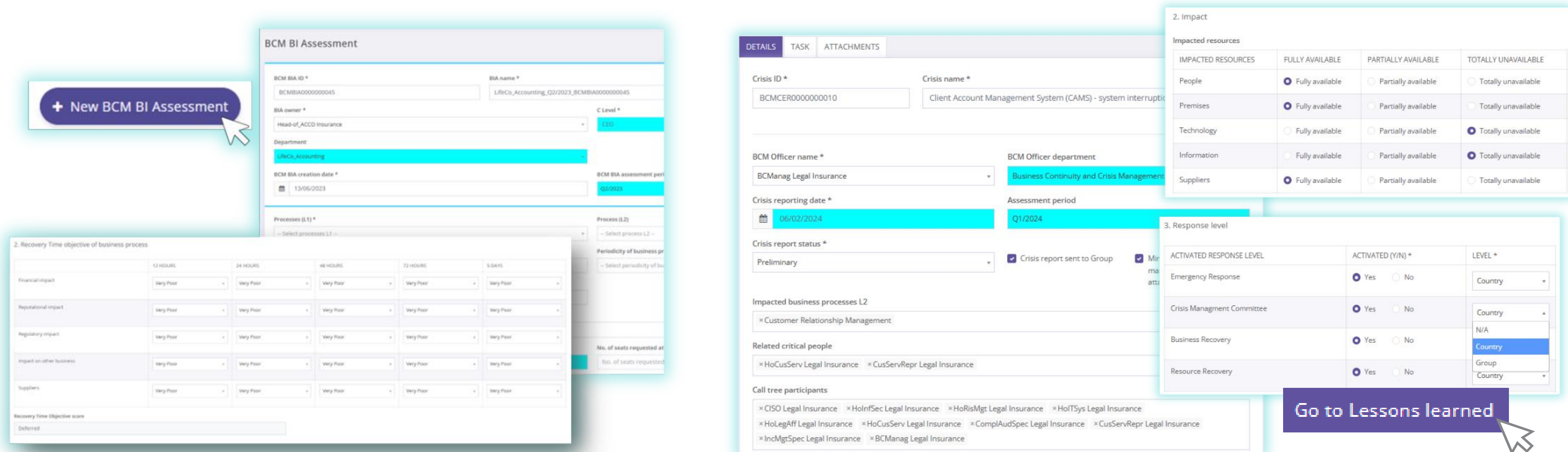
View on IT Components stored in the GRC Suite

- The Cyber security module is fully aligned with **Information Security CIA classification** and is applicable to all systems and IT components stored in the GRC Suite.
- Possibility to have a Cyber Security maturity assessment stored and mapped out with Grace Connect Task tracking module.

Cyber security
related modules
can be linked with
CTI feeds (through
API)

BUSINESS CONTINUITY & CRISIS MANAGEMENT MODULE IN GRC SUITE

The purpose of the list view of the **Business Continuity Management BI Assessment** module is to show to users (Process Owners) all information included in their Business Impact Assessments, including their attributes. This includes details on potential threats and their scoring that could lead to remediation actions (Tasks).



+ New BCM BI Assessment

BCM BI Assessment

BCM BIA ID *
BCMBIA0000000045

BIA name *
LifeCo_Accounting_Q2/2023_BCMBIA0000000045

BIA owner *
Head-of_ACCO Insurance

C Level *
C20

Department
LifeCo_Accounting

BCM BIA creation date *
13/06/2023

BCM BIA assessment period
Q3/2023

Processes (L1) *
-- Select processes L1 --

Process (L2)
-- Select process L2 --

Periodicity of business process
-- Select periodicity of business process --

No. of seats requested at
No. of seats requested

2. Recovery Time objective of business process

	12 HOURS	24 HOURS	48 HOURS	72 HOURS	5 DAYS
Financial impact	Very Poor	Very Poor	Very Poor	Very Poor	Very Poor
Reputational impact	Very Poor	Very Poor	Very Poor	Very Poor	Very Poor
Regulatory impact	Very Poor	Very Poor	Very Poor	Very Poor	Very Poor
Impact on other business	Very Poor	Very Poor	Very Poor	Very Poor	Very Poor
Suppliers	Very Poor	Very Poor	Very Poor	Very Poor	Very Poor

Recovery Time Objective score
Deferred

DETAILS TASK ATTACHMENTS

Crisis ID *
BCMCER0000000010

Crisis name *
Client Account Management System (CAMS) - system interruption

BCM Officer name *
BCManag Legal Insurance

BCM Officer department
Business Continuity and Crisis Management

Crisis reporting date *
06/02/2024

Assessment period
Q1/2024

Crisis report status *
Preliminary

☒ Crisis report sent to Group

☒ Mirror main attachment

Impacted business processes L2
* Customer Relationship Management

Related critical people
* HoCusServ Legal Insurance * CusServRepr Legal Insurance

Call tree participants
* CISO Legal Insurance * HoInfSec Legal Insurance * HoRisMgt Legal Insurance * HoITSys Legal Insurance
* HoLegAff Legal Insurance * HoCusServ Legal Insurance * ComplAudSpec Legal Insurance * CusServRepr Legal Insurance
* IncMgtSpec Legal Insurance * BCManag Legal Insurance

2. Impact

IMPACTED RESOURCES	FULLY AVAILABLE	PARTIALLY AVAILABLE	TOTALLY UNAVAILABLE
People	☒ Fully available	☐ Partially available	☐ Totally unavailable
Premises	☒ Fully available	☐ Partially available	☐ Totally unavailable
Technology	☐ Fully available	☐ Partially available	☒ Totally unavailable
Information	☐ Fully available	☐ Partially available	☒ Totally unavailable
Suppliers	☒ Fully available	☐ Partially available	☐ Totally unavailable

3. Response level

ACTIVATED RESPONSE LEVEL	ACTIVATED (Y/N) *	LEVEL *
Emergency Response	☒ Yes ☐ No	Country
Crisis Management Committee	☒ Yes ☐ No	Country
Business Recovery	☒ Yes ☐ No	N/A
Resource Recovery	☒ Yes ☐ No	Country

Go to Lessons learned

The detailed form is used to create new **BCM BIA** entry with all relevant information to be introduced by users. The **Crisis Management module** enables effective communication and response coordination in emergencies. It serves as a central repository for incident descriptions, impact assessments, response logs, and records of key decisions made during crisis management.

AUDIT REPORTS AS A CORNERSTONE OF THE GRC SUITE

As the third line of defense, **Internal Audit** assesses the operational effectiveness of control activities integrated within business operations. These evaluations are documented in audit reports stored in the GRC Suite, and they are connected to specific processes.

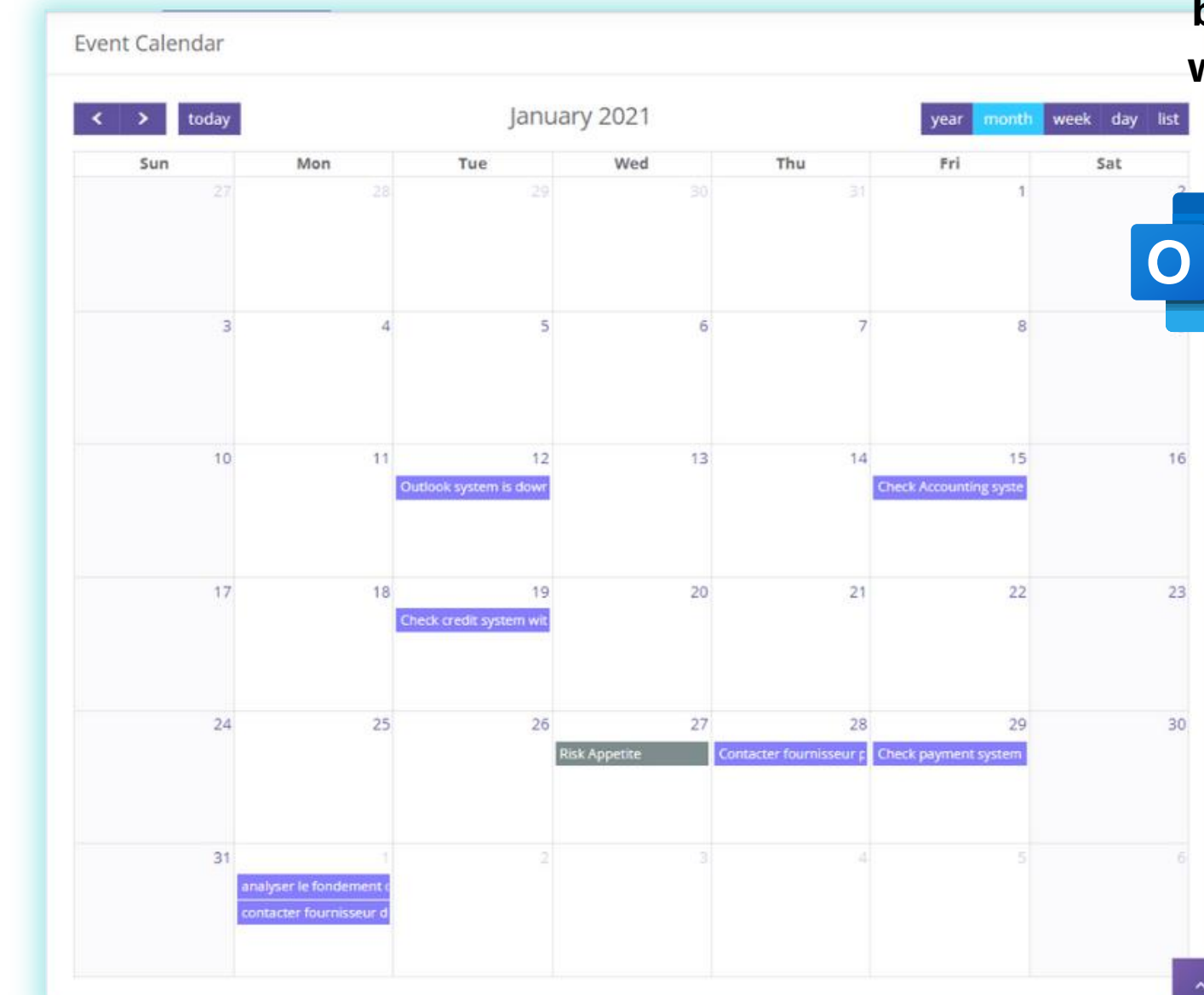
AUDIT REPORT LIST					
AUDIT TRANSVERSAL VIEW					
Audit Report List					
+ New Audit Report					
Show 10 entries Search					
SR. NO.	ID	AUDIT REPORT NAME	AUDIT REPORT ID	COMPANY NAME	AUDIT REPORT OWNER
1	20	Bank's IT systems security	ARP0000000020	Universal Bank	AUDIT_Director
2	19	Efficiency of the loan origination process	ARP0000000019	Universal Bank	AUDIT_Director
3	18	Client account opening	ARP0000000018	Universal Bank	PCM_Director B
4	17	Regulatory reporting activities	ARP0000000017	Universal Bank	Accounting_Dire
5	16	Insurance practices	ARP0000000016	Grace Connect SARL	GC_admin Kevin
6	15	new test by gajanan - 02/03/2021	ARP0000000015	Life Insurance Co	Admin User
7	14	2020 Annual Audit	ARP0000000014	Telecom	
8	13	5G reporting	ARP0000000013	Telecom	

List view of all Audit reports stored in the GRC Suite



Audit **reports stored in the GRC Suite are available to users and management** (with restricted access rights), so that they could consult audit observations, findings, and track the progress on closing audit recommendations at any time during the life-cycle of the audit and during the implementation of remediation measures.

A dedicated set of KPI's and graphs is available to users and management to ensure a comprehensive view on all findings.



Calendar view of Audit findings (High)

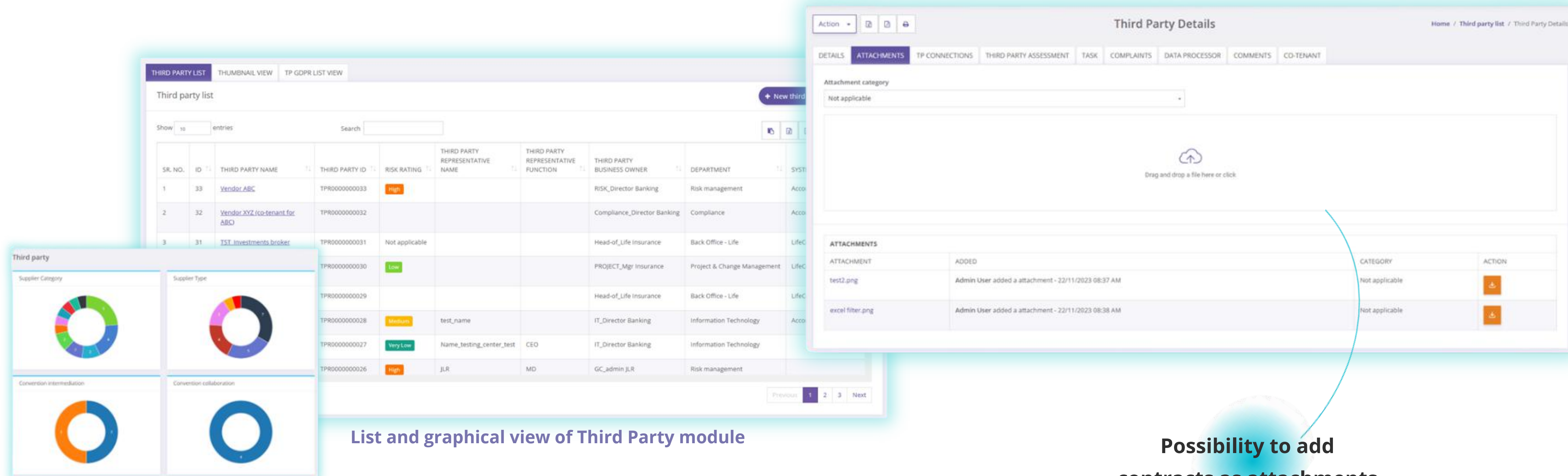
Calendar can be synchronized with MS Outlook



When clicking on KPI's or graphs, GRC Suite users will automatically filter the list of all related objects, thus enabling faster research and analysis. Because remediation of audit findings with high importance is critical for an organization, the GRC Suite will post an entry in the Events Calendar module, enabling user notifications to be issued ahead of the agreed due dates.

THIRD PARTY MODULE IN GRC SUITE

Third Party Risk Management (TPRM) module helps to fortify your organization against unforeseen risks while fostering secure and productive partnerships with your external service providers. The module is designed to store supplier related information and perform supplier risk assessment (incl. storing checks and controls on suppliers).



The screenshot displays the Third Party module interface. On the left, a 'Third party' sidebar shows four donut charts for 'Supplier Category', 'Supplier Type', 'Conversion intermediation', and 'Conversion collaboration'. The main area is divided into two sections: 'Third party list' and 'Third Party Details'.

Third party list

SRL NO.	ID	THIRD PARTY NAME	THIRD PARTY ID	RISK RATING	THIRD PARTY REPRESENTATIVE NAME	THIRD PARTY REPRESENTATIVE FUNCTION	THIRD PARTY BUSINESS OWNER	DEPARTMENT	SYSTEM
1	33	Vendor ABC	TPR0000000033	High			RISK_Director Banking	Risk management	Acco
2	32	Vendor XYZ (co-tenant for ABC)	TPR0000000032				Compliance_Director Banking	Compliance	Acco
3	31	TST_Investments broker	TPR0000000031	Not applicable			Head-of_Life Insurance	Back Office - Life	LifeC
			TPR0000000030	Low			PROJECT_Mgr Insurance	Project & Change Management	LifeC
			TPR0000000029				Head-of_Life Insurance	Back Office - Life	LifeC
			TPR0000000028	Medium	test_name		IT_Director Banking	Information Technology	Acco
			TPR0000000027	Very Low	Name_testing_center_test	CEO	IT_Director Banking	Information Technology	Acco
			TPR0000000026	High	JLR	MD	GC_admin JLR	Risk management	Acco

Third Party Details

Attachment category: Not applicable

Attachments:

ATTACHMENT	ADDED	CATEGORY	ACTION
test2.png	Admin User added a attachment - 22/11/2023 08:37 AM	Not applicable	
excel filter.png	Admin User added a attachment - 22/11/2023 08:38 AM	Not applicable	

List and graphical view of Third Party module

Possibility to add contracts as attachments

Key Features and Benefits:

Enhanced risk visibility, **improved compliance for ICT providers and outsourcing services**, cost reduction, reputation protection and strategic decision-making

SUPPLIER RISK ASSESSMENT

The **Supplier Risk Assessment** module allows end-users to evaluate suppliers by analyzing risk parameters such as reputation, history, financial capacity, organization, compliance, competence, and data protection. The evaluation provides a final score to support informed decision-making and risk management.

Supplier Risk Assessment

Supplier Risk Assessment ID *

TPRA0000000005

Company name *

Legal Insurance Company XYZ

Supplier name

Grace Connect

Supplier ID

SPR0000000003

Reputation

History

Financial capacity

Organization and compliance

Partners and sub-contractor(s)

Competence

Data protection

Which is the probability of payment failure (Graydon sourced) ?

Add new

Did the supplier face an "arrêt-saisie"?

Yes

No

Date

DD/MM/YYYY

Attachment

Choose file

Browse

Supplier rating *

Medium

Fit for purpose rating *

Medium

Creation date *

16/09/2024

Assessment period *

Q3/2024

All documentation can be stored in the attachment section to ensure evaluations are well-supported, organized, and easily accessible, enabling effective oversight, supporting audits, and reducing the risk of regulatory breaches or service disruptions.

Possibility to add attachments

OUTSOURCING RISK ASSESSMENT MODULE IN GRC SUITE

The **Outsourcing Risk Assessment (ORA)** module is designed to evaluate and manage risks associated with outsourcing arrangements, particularly critical outsourcing files. It ensures **compliance with EBA Guidelines on Outsourcing and the DORA Regulation**, while supporting organizations in mitigating potential vulnerabilities effectively.

TECHNOLOGY

TASK

ATTACHMENTS

Which data will be involved in the proposed solution ?

Customer Data:

Personal Identification Information (PII): Names, addresses, contact details, and any other personal details necessary to identify and communicate with the customer.

Account Information: Customer account numbers, service history, transaction history, and account status.

Interaction Records: Details of all customer interactions, including call logs, email correspondence, chat transcripts, and social media interactions.

Operational Data:

Service Level Metrics: Data related to the performance against SLA targets, such as response times, resolution rates, and customer satisfaction scores.

Workforce Management Data: Information on staff scheduling, workload distribution, and agent performance metrics.

Issue Resolution Data: Details on customer issues, resolution steps taken, and outcomes.

ORA LIST

LOCATION

Outsourcing Risk Assessment List

+ New Outsourcing Risk Assessment

SR NO.

ID

OUTSOURCING ID

OUTSOURCING NAME

REQUESTER NAME

REQUESTER DEPARTMENT

CREATION DATE

ASSESSMENT PERIOD

OWNER

OUTSOURCING TYPE

OUTSOURCING CATEGORY

1	10	ORA0000000010	Outsourcing of CRM system	Head-of-IT Insurance	Information Technology	16/11/2022	Q4/2022	Head-of-IT Insurance	NEW	Critical
2	9	ORA0000000009	Outsourcing of inbound / Outbound mailing	IT_Director Banking	Information Technology	26/10/2022	Q4/2022	IT_Director Banking	NEW	Critical
3	8	ORA0000000008	Outsourcing of accounting services	Accounting_Director Banking	Bank_Accounting	26/10/2022	Q4/2022	Accounting_Director Banking	NEW	Critical
4	7	ORA0000000007	Outsourcing of legal archives	IT_Director Banking	Information Technology	26/10/2022	Q4/2022	IT_Director Banking	NEW	Critical
5	6	ORA0000000006	credit card manufacturing	IT_Director Banking	Customer Services	26/10/2022	Q4/2022	IT_Director Banking	CHANGE	Critical
6	5	ORA0000000005	Outsourcing of mobile data	IT_Director Banking	Information Technology	26/10/2022	Q4/2022	IT_Director Banking	NEW	Critical
7	4	ORA0000000004	Private Bank client data migration	IT_Director Banking	Information Technology	26/10/2022	Q4/2022	IT_Director Banking	NEW	Critical
8	3	ORA0000000003	Migration of Data Center	Head-of-IT Insurance	Information Technology	16/11/2022	Q4/2022	Head-of-IT Insurance	NEW	Critical

ORA Details

DEFINITION OF REQUEST

TASK

ATTACHMENTS

+ New Outsourcing Risk Assessment

Outsourcing name *

outsourcing of CRM system

Requester name *

Head-of-IT Insurance

Requester department

Information Technology

Creation date *

16/11/2022

Assessment period

Q4/2022

Owner *

Head-of-IT Insurance

Outsourcing type *

NEW

Outsourcing category *

Critical

Reporting to Supervisory Authorities

☐ Yes
☒ No

Outsourcing file sending date

DD/MM/YYYY

Choose file

Attachments

ATTACHMENT

ADDED

ACTION

Possibility to add
attachements

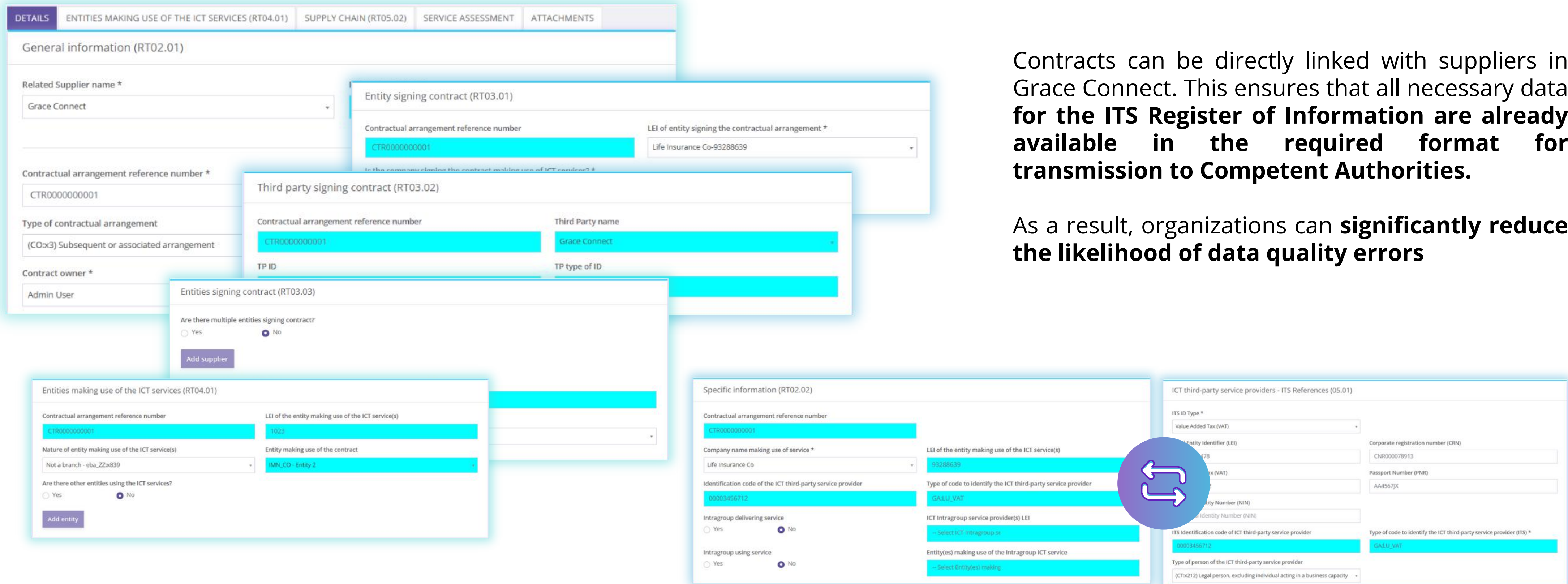
Detailed view of Outsourcing Risk
Assessment

CONTRACT MANAGEMENT

The **Contract Management module** facilitate the record of comprehensive data for each contract, including specific terms, applicable laws, connections with other suppliers and conditions for termination. It ensures consistency and accuracy, **leveraging templates from DORA's ITS Register of Information**.

Contracts can be directly linked with suppliers in Grace Connect. This ensures that all necessary data **for the ITS Register of Information are already available in the required format for transmission to Competent Authorities**.

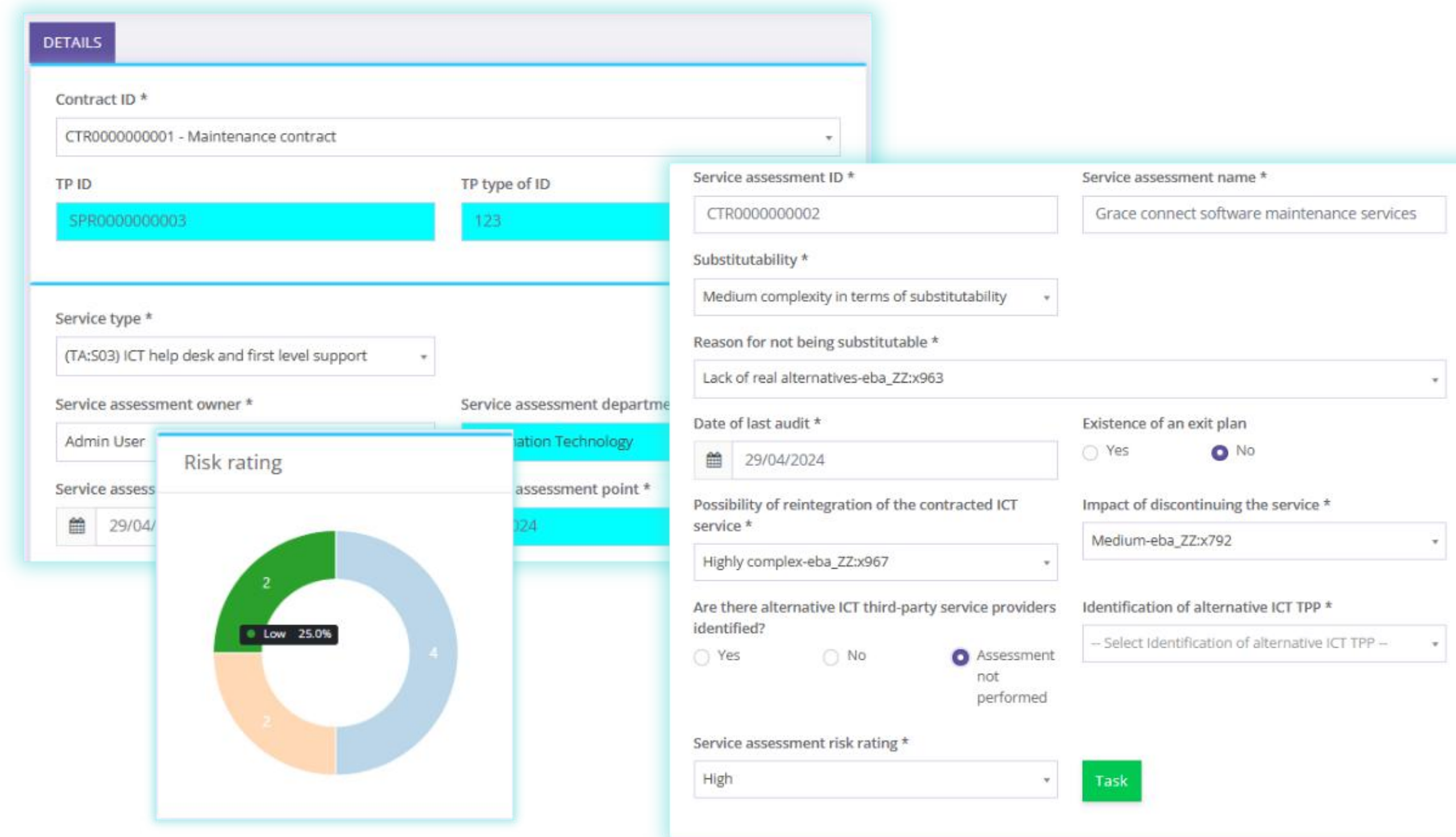
As a result, organizations can **significantly reduce the likelihood of data quality errors**



The screenshot displays the Grace Connect Contract Management module interface, which includes several overlapping forms for data entry. The main form is titled "General information (RT02.01)" and contains fields for "Related Supplier name *" (Grace Connect), "Contractual arrangement reference number *" (CTR000000001), "Type of contractual arrangement" ((COx3) Subsequent or associated arrangement), and "Contract owner *" (Admin User). Overlaid on this are three smaller forms: "Entity signing contract (RT03.01)" with fields for "Contractual arrangement reference number" (CTR000000001) and "LEI of entity signing the contractual arrangement *" (Life Insurance Co-93288639); "Third party signing contract (RT03.02)" with fields for "Contractual arrangement reference number" (CTR000000001), "Third Party name" (Grace Connect), "TP ID", and "TP type of ID"; and "Entities signing contract (RT03.03)" with a radio button for "Are there multiple entities signing contract?" (No) and an "Add supplier" button. At the bottom, there are two more forms: "Entities making use of the ICT services (RT04.01)" with fields for "Contractual arrangement reference number" (CTR000000001), "LEI of the entity making use of the ICT service(s)" (1023), "Nature of entity making use of the ICT service(s)" (Not a branch - eba_ZZx839), "Entity making use of the contract" (IMN_CO - Entity 2), and a radio button for "Are there other entities using the ICT services?" (No); and "Specific information (RT02.02)" with fields for "Contractual arrangement reference number" (CTR000000001), "Company name making use of service *" (Life Insurance Co), "Identification code of the ICT third-party service provider" (00003456712), "Type of code to identify the ICT third-party service provider" (GALU_VAT), "Intragroup delivering service" (No), "Intragroup using service" (No), "LEI of the entity making use of the ICT service(s)" (93288639), "Type of code to identify the ICT third-party service provider" (GALU_VAT), "ICT Intragroup service provider(s) LEI" (Select ICT Intragroup s), "Entity(es) making use of the Intragroup ICT service" (Select Entity(es) making), and "ICT third-party service providers - ITS References (05.01)" with fields for "ITS ID Type *" (Value Added Tax (VAT)), "Entity Identifier (LEI)" (93288639), "Corporate registration number (CRN)" (CNR000078913), "Passport Number (PNR)" (AA4567X), "Entity Number (NIN)", "ITS Identification code of ICT third-party service provider" (00003456712), "Type of code to identify the ICT third-party service provider (ITS) *" (GALU_VAT), and "Type of person of the ICT third-party service provider" ((CTx212) Legal person, excluding individual acting in a business capacity). A circular arrow icon is overlaid on the bottom right of the forms.

SERVICE ASSESSMENT

The **Service Assessment** module allows users to perform an in-depth analysis of the inherent risks linked to specific services, with a focus on the criticality of the service and related possibilities for suppliers replacement.



The screenshot displays the 'DETAILS' section of the Service Assessment module. It includes a form with the following fields and values:

- Contract ID ***: CTR000000001 - Maintenance contract
- TP ID**: SPR000000003
- TP type of ID**: 123
- Service type ***: (TA:S03) ICT help desk and first level support
- Service assessment owner ***: Admin User
- Service assessment department**: Information Technology
- Service assessment point ***: 24
- Service assessment ID ***: CTR000000002
- Service assessment name ***: Grace connect software maintenance services
- Substitutability ***: Medium complexity in terms of substitutability
- Reason for not being substitutable ***: Lack of real alternatives-eba_ZZ:x963
- Date of last audit ***: 29/04/2024
- Existence of an exit plan**: ☐ Yes ☒ No
- Possibility of reintegration of the contracted ICT service ***: Highly complex-eba_ZZ:x967
- Impact of discontinuing the service ***: Medium-eba_ZZ:x792
- Are there alternative ICT third-party service providers identified?**: ☐ Yes ☐ No ☒ Assessment not performed
- Identification of alternative ICT TPP ***: -- Select Identification of alternative ICT TPP --
- Service assessment risk rating ***: High
- Task**: [Task button]

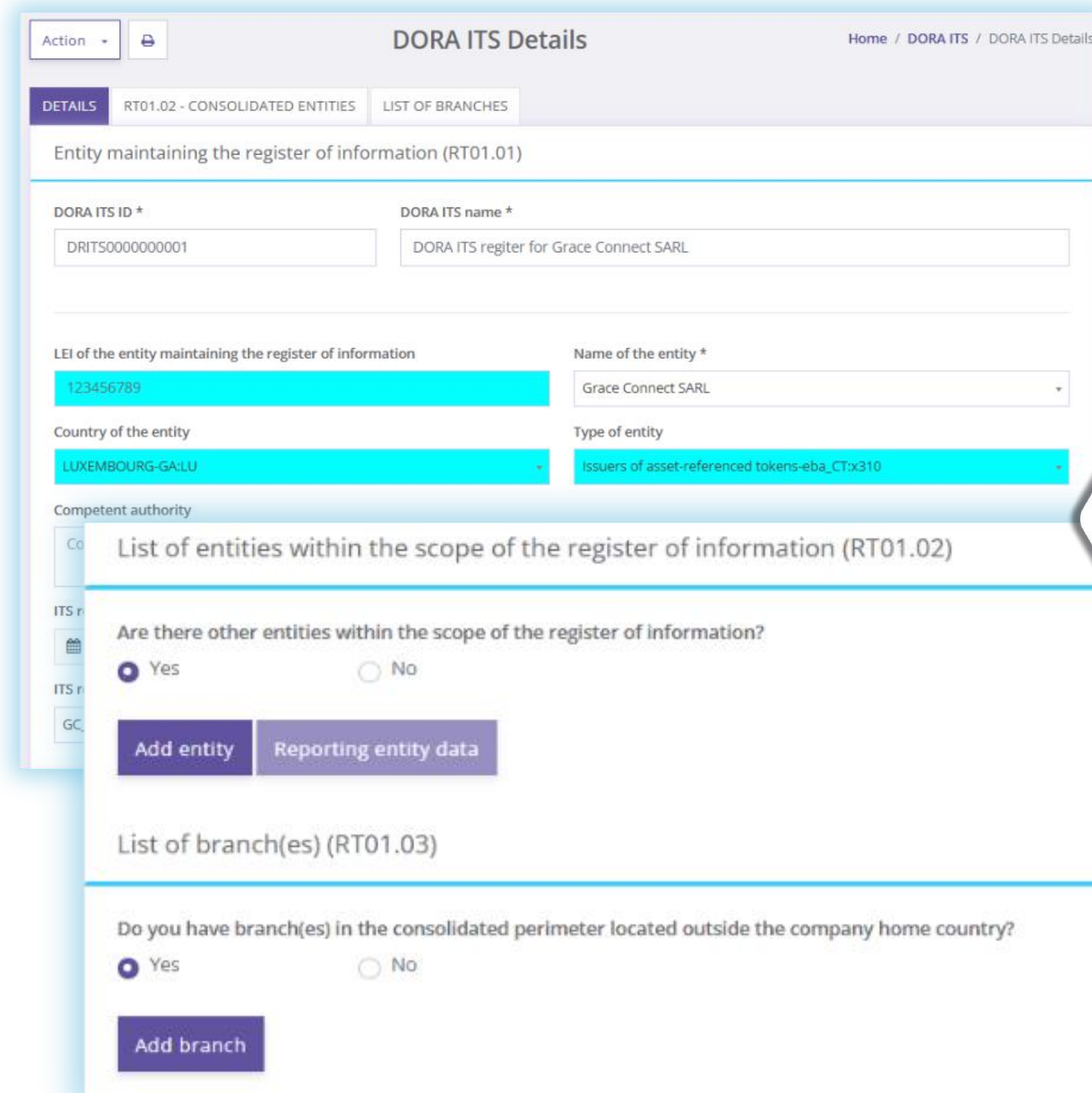
A **Risk rating** donut chart is also shown, indicating a **Low 25.0%** risk rating. The chart is divided into four segments: 2 (green), 4 (blue), 2 (orange), and 2 (yellow).

The module guarantees that **all necessary information for the Register of Information is incorporated**, enabling organizations to fully adhere to ITS RoI requirements.

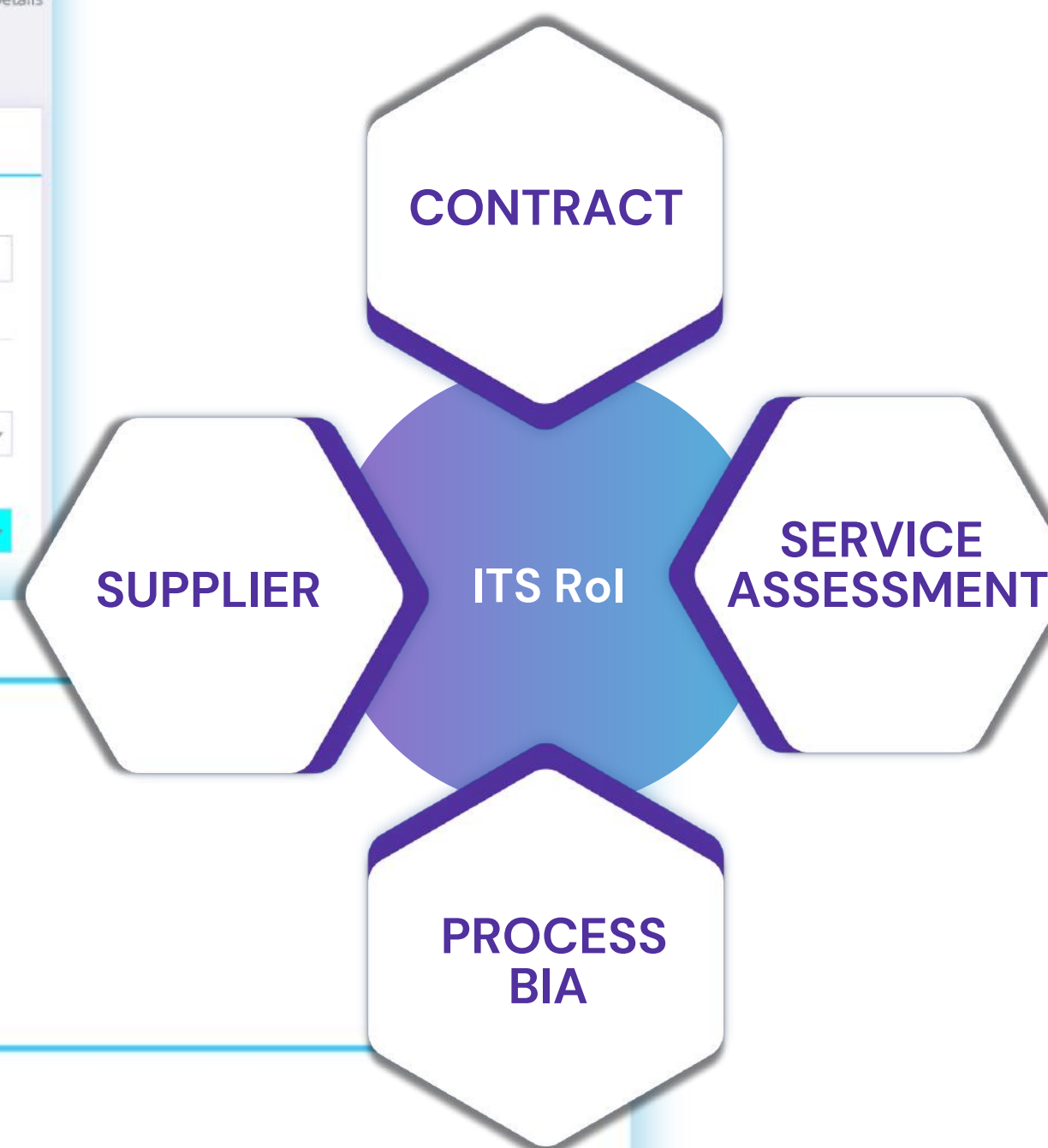
By integrating data seamlessly, the module improves the accuracy of service evaluations and supports more informed decision-making. The internal connections within the GRC Suite provide real-time updates and maintain consistency across different modules.

DORA ITS REGISTER

The **DORA ITS** module in the GRC Suite automatically generates reports using existing data from the **Supplier, Contract, Process BIA, and Service Assessment modules**. It is designed to meet DORA's reporting requirements, and it ensures accurate integration of relevant information without extra data entry or manipulation.



The screenshot shows the 'DORA ITS Details' form. It includes fields for 'DORA ITS ID *' (DRTS0000000001), 'DORA ITS name *' (DORA ITS register for Grace Connect SARL), 'LEI of the entity maintaining the register of information' (123456789), 'Name of the entity *' (Grace Connect SARL), 'Country of the entity' (LUXEMBOURG-GA:LU), and 'Type of entity' (Issuers of asset-referenced tokens-eba_CT:x310). Below these fields are sections for 'List of entities within the scope of the register of information (RT01.02)' and 'List of branch(es) (RT01.03)'. The 'List of entities' section has a question 'Are there other entities within the scope of the register of information?' with 'Yes' selected. The 'List of branches' section has a question 'Do you have branch(es) in the consolidated perimeter located outside the company home country?' with 'Yes' selected. Buttons for 'Add entity', 'Reporting entity data', and 'Add branch' are visible.



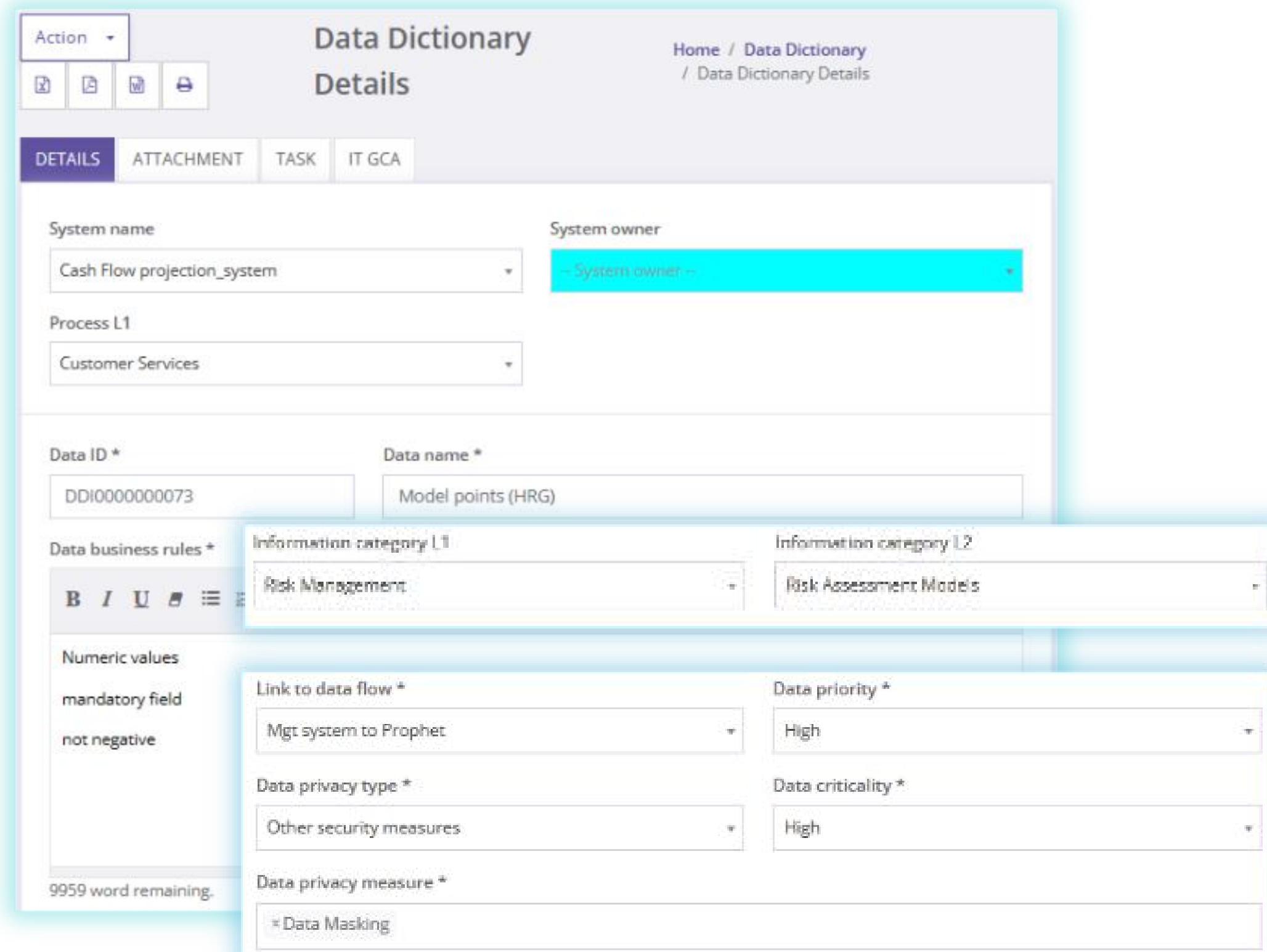
Key benefits:

- **Efficiency and Time-Saving:** significantly reduces manual effort typically required in data compilation and report generation.
- **Accuracy and Reliability:** automates reporting using pre-existing validated data to minimize human error and increases the reliability of the reports generated.
- **Regulatory Compliance:** built-in templates regularly updated to reflect the latest ITS requirements. The module ensures that all reports are current and fully compliant with DORA regulations, simplifying compliance for organizations.

DATA RELATED MODULES IN GRC SUITE

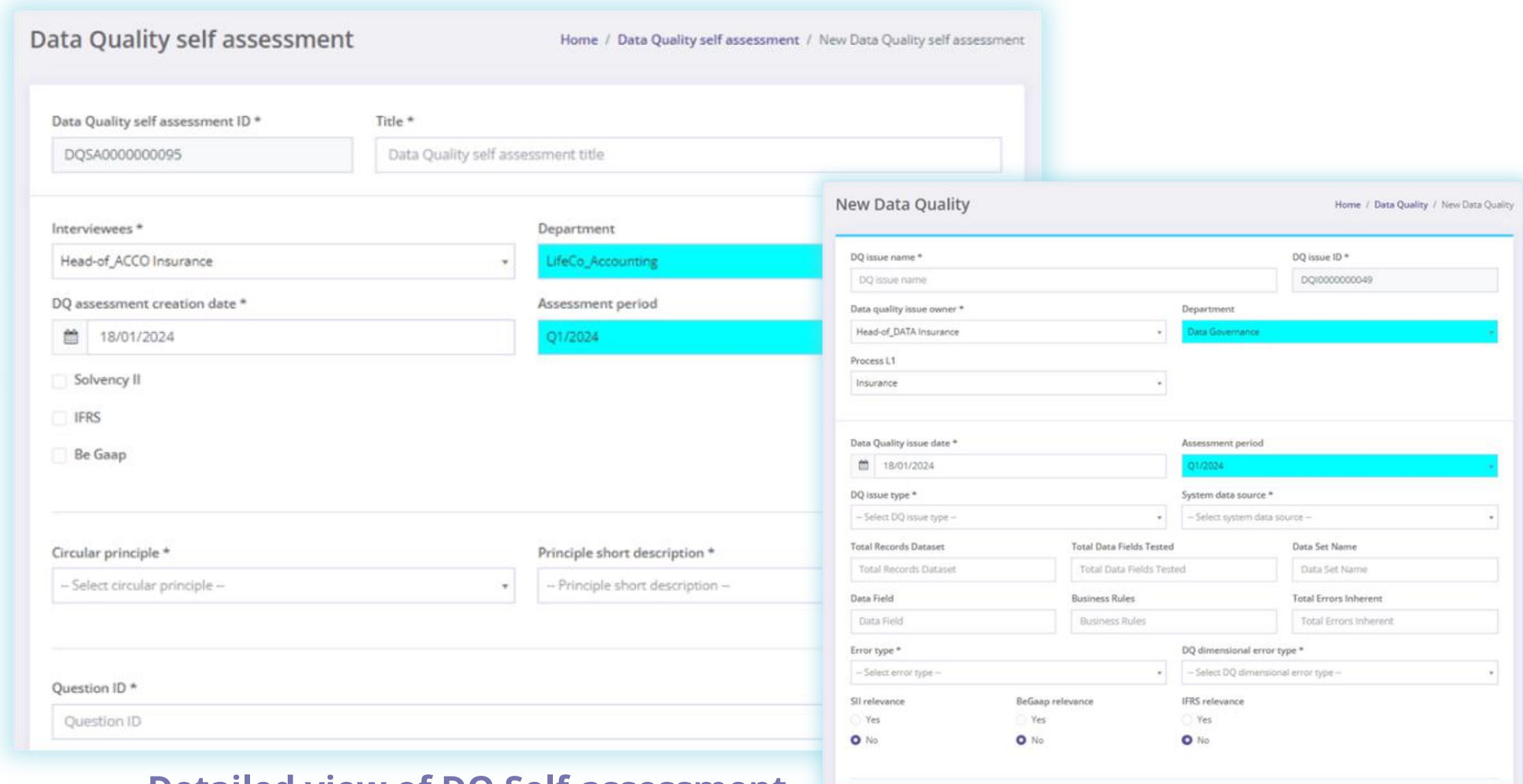
The **backbone of GRC Suite is the documentation of processes, systems (incl. IT components), and data.** This enables end-users to link each risk and control evaluation performed in the suite at appropriate level of the organization and eventually decide on high priority investments to close gaps, vulnerabilities, or decrease risk exposures.

The **Data dictionary** module enables to list all data handled in the organization, and links them to the related **systems** and **Data Security Controls**. **Data Quality Self assessment** module enable to track maturity for data quality.



The screenshot shows the 'Data Dictionary Details' interface. It includes fields for 'System name' (Cash Flow projection_system), 'System owner' (System owner), 'Process L1' (Customer Services), 'Data ID' (DDI0000000073), 'Data name' (Model points (HRG)), 'Data business rules' (Risk Management), 'Information category L1' (Risk Assessment Models), 'Information category L2' (Risk Assessment Models), 'Link to data flow' (Mgt system to Prophet), 'Data priority' (High), 'Data privacy type' (Other security measures), 'Data criticality' (High), and 'Data privacy measure' (Data Masking). A 'Numeric values' section shows 'mandatory field' and 'not negative'.

Detailed view of data dictionary



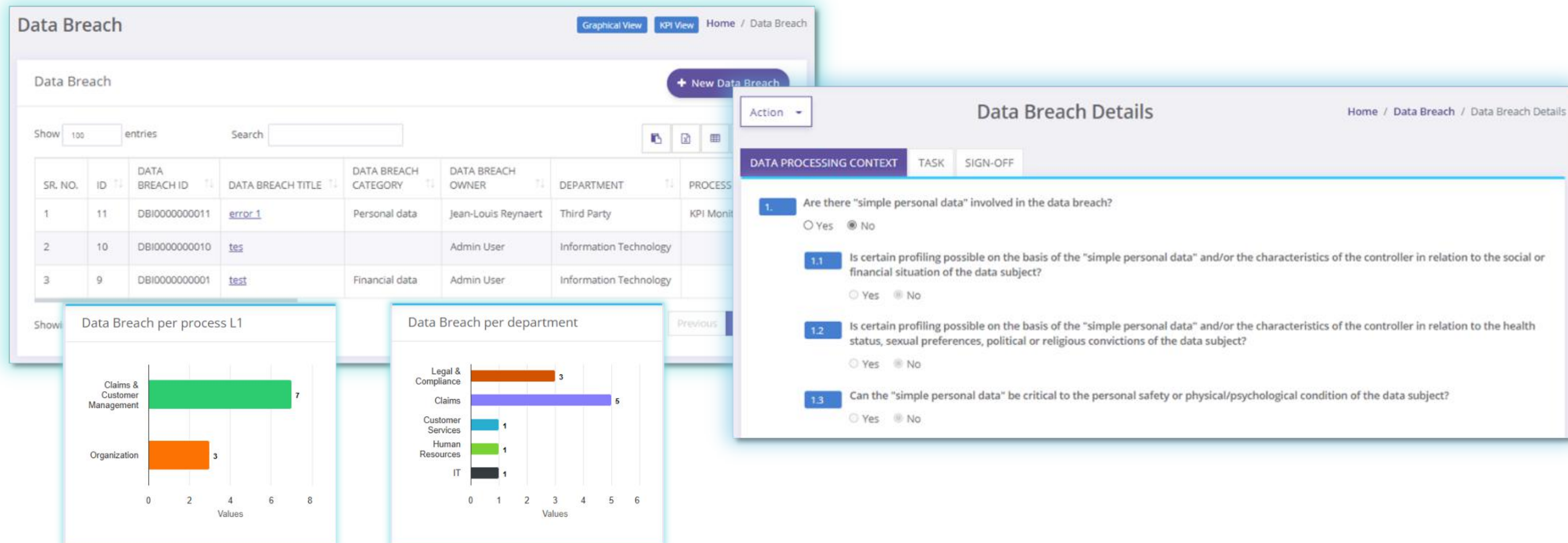
The screenshot shows two overlapping forms. The top form is 'Data Quality self assessment' with fields for 'Data Quality self assessment ID' (DQSA0000000095), 'Title' (Data Quality self assessment title), 'Interviewees' (Head-of-ACCO Insurance), 'Department' (LifeCo_Accounting), 'DQ assessment creation date' (18/01/2024), 'Assessment period' (Q1/2024), 'Solvency II', 'IFRS', 'Be Gaap', 'Circular principle' (Select circular principle), 'Principle short description' (Principle short description), 'Question ID' (Question ID), and 'Question ID' (Question ID). The bottom form is 'New Data Quality' with fields for 'DQ issue name' (DQ issue name), 'Data quality issue owner' (Head-of-ACCO Insurance), 'Department' (Data Governance), 'Process L1' (Insurance), 'Data Quality issue date' (18/01/2024), 'Assessment period' (Q1/2024), 'DQ issue type' (Select DQ issue type), 'System data source' (Select system data source), 'Total Records Datasets' (Total Records Datasets), 'Total Data Fields Tested' (Total Data Fields Tested), 'Data Set Name' (Data Set Name), 'Data Field' (Data Field), 'Business Rules' (Business Rules), 'Total Errors Inherent' (Total Errors Inherent), 'Error type' (Select error type), 'DQ dimensional error type' (Select DQ dimensional error type), 'SI relevance' (Yes/No), 'BeGaap relevance' (Yes/No), and 'IFRS relevance' (Yes/No).

Detailed view of DQ Self-assessment

Detailed view of DQ issue

DATA BREACH MODULE IN GRC SUITE

The list view of the **Data Breach module** provides users with all entries recorded. This enables to update graphs and KPI's. The list includes all relevant data fields included in the data breach detailed form.



The screenshot displays the Data Breach module interface. The main list view shows a table of data breaches with columns: SR. NO., ID, DATA BREACH ID, DATA BREACH TITLE, DATA BREACH CATEGORY, DATA BREACH OWNER, DEPARTMENT, and PROCESS. Below the table are two charts: 'Data Breach per process L1' and 'Data Breach per department'.

SR. NO.	ID	DATA BREACH ID	DATA BREACH TITLE	DATA BREACH CATEGORY	DATA BREACH OWNER	DEPARTMENT	PROCESS
1	11	DBI0000000011	error 1	Personal data	Jean-Louis Reynaert	Third Party	KPI Moni
2	10	DBI0000000010	tes		Admin User	Information Technology	
3	9	DBI0000000001	test	Financial data	Admin User	Information Technology	

The 'Data Breach per process L1' chart shows the following data:

Process	Value
Claims & Customer Management	7
Organization	3

The 'Data Breach per department' chart shows the following data:

Department	Value
Legal & Compliance	3
Claims	5
Customer Services	1
Human Resources	1
IT	1

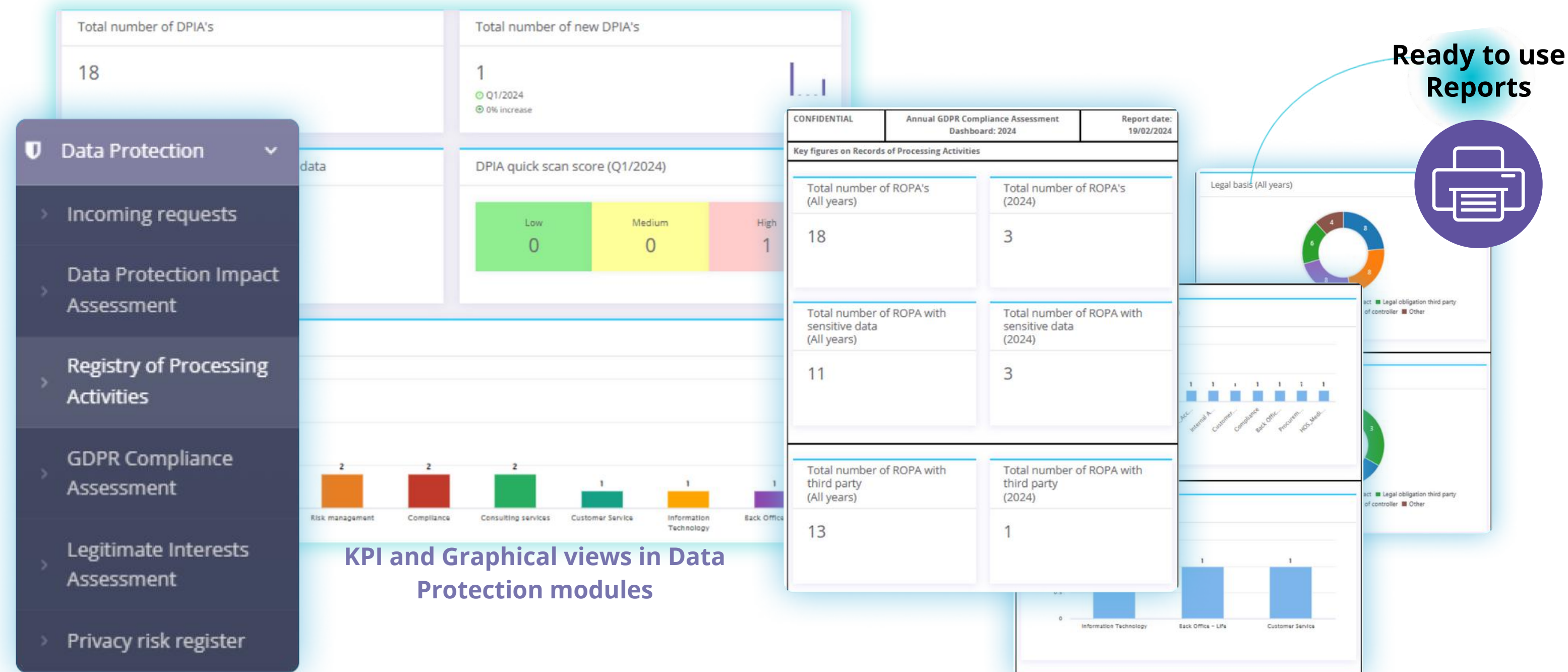
The 'Data Breach Details' view shows a form for assessing the severity of the data breach based on the ENISA methodology. The form includes questions such as:

- 1. Are there "simple personal data" involved in the data breach? (Yes/No)
- 1.1 Is certain profiling possible on the basis of the "simple personal data" and/or the characteristics of the controller in relation to the social or financial situation of the data subject? (Yes/No)
- 1.2 Is certain profiling possible on the basis of the "simple personal data" and/or the characteristics of the controller in relation to the health status, sexual preferences, political or religious convictions of the data subject? (Yes/No)
- 1.3 Can the "simple personal data" be critical to the personal safety or physical/psychological condition of the data subject? (Yes/No)

The assessment of the severity of the data breach is based on questions included in the **ENISA methodology**. An algorithm underlying questions is in place to calculate the exposure of the data breach.

DATA PROTECTION MODULES IN GRC SUITE

Grace Connect GRC Suite encompasses a suite of modules specifically crafted to fortify **Data Privacy Risk Management** endeavors. Data Protection modules include: **Data Protection Impact Assessment (DPIA)**, **Registry of Processing Activities (ROPA)**, **GDPR Compliance Assessment**, **Legitimate Interest Assessment (LIA)** and **Privacy Risk Register**.



Data Protection modules:

- Empower organizations to conduct comprehensive assessments, enabling them to pinpoint areas for immediate reinforcement.
- Offer flexibility in task management by allowing organizations to seamlessly store and map Data Protection maturity assessments.

DATA PROTECTION MODULES

GDPR ASSESSMENT

GDPR Compliance Assessment offers a step-by-step guidance to navigate complexities of GDPR compliance with precision. This modules helps to safeguard your organization against potential penalties and reputational risks.

DATA PROTECTION PRINCIPLES
TASK
ATTACHMENTS
SIGN-OFF

1.1. Fairness, lawfulness and transparency

What is the legal ground you rely on to process personal data?

☐ Yes, performance of a contract
☒ Yes, authorized by law
☐ Yes, based on the data subject's explicit consent
☐ No

Do you process judicial data or sensitive personal data?

☒ Yes
☐ No

What is the legal ground you rely on to process personal data?

☒ Under the control of an official authority
☐ Authorised by Union or Member State law

+ New GDPR Compliance Assessment

Action
GDPR CA Details
Home / GDPR CA / GDPR Compliance Assessment Details

GENERAL INFORMATION
TASK
ATTACHMENTS
SIGN-OFF

SR. NO.	ID	TYPE	OBJECT SOURCE	OBJECT SOURCE TITLE	TASK TITLE
1	316		GDPR Compliance Assessment	GDPR_annual_report_2022	Define roadmap for data minimization for 2023

Key Features & Benefits:

- Comprehensive GDPR checklist and compliance scoring.
- Facilitate strategic planning and continuous improvement.
- Possibility to customize reports.

Example of questions raised in the GDPR CA module

DATA PROTECTION MODULES

DPIA

Data Protection Impact Assessment (DPIA) helps to evaluate and mitigate risks in data processing activities. DPIA module enables your organization to preemptively identify and mitigate data processing risks. This module serves as the cornerstone of your proactive data privacy framework, enabling a robust defense against potential compliance breaches.

Key Features & Benefits:

- Automated evaluation algorithms.
- Strengthen defenses against potential compliance violations.
- Seamless integration with your existing data privacy framework.
- Findings from DPIAs can update the ROPA with details on risk assessments and mitigations for high-risk processing activities.

DPIA quick scan

- Do you process sensitive personal data, 'judicial data' or 'data of a highly personal nature'?
☒ Yes ☐ No
- Are the individuals part of vulnerable groups (e.g. minors, employees, people with physical health issues, whistleblowers, elderly people) or minorities?
☒ Yes ☐ No
- Will the personal data be combined with other data used in another context than the current processing activity, e.g. to perform profiling of an individual?
☒ Yes ☐ No
- Will you transfer data outside EEA to external third parties?
☐ Yes ☒ No
- Do you use automated processing producing significant effects for individuals?
☐ Yes ☒ No

3. Provisional balancing test

3.1. Assessing the controller's legitimate interests: Identify and document the relevant legitimate interest(s) of the controller

3.1.1. Is the controller acting in the public interest and/or interest of the wider community when doing the processing? E.g. Fraud prevention. (Input from ROPA)

☐ Yes ☒ No

Non sensitive personal data

Identification data	Personal characteristics	Life habits	Household composition
Yes	Yes	No	No
Training and education	Employment	Record of sounds	
No	No	No	
Sensitive data			
Health data	Racial or ethnic data	Sex life data	Political opinion data
No	No	No	No

DPIA quick scan score

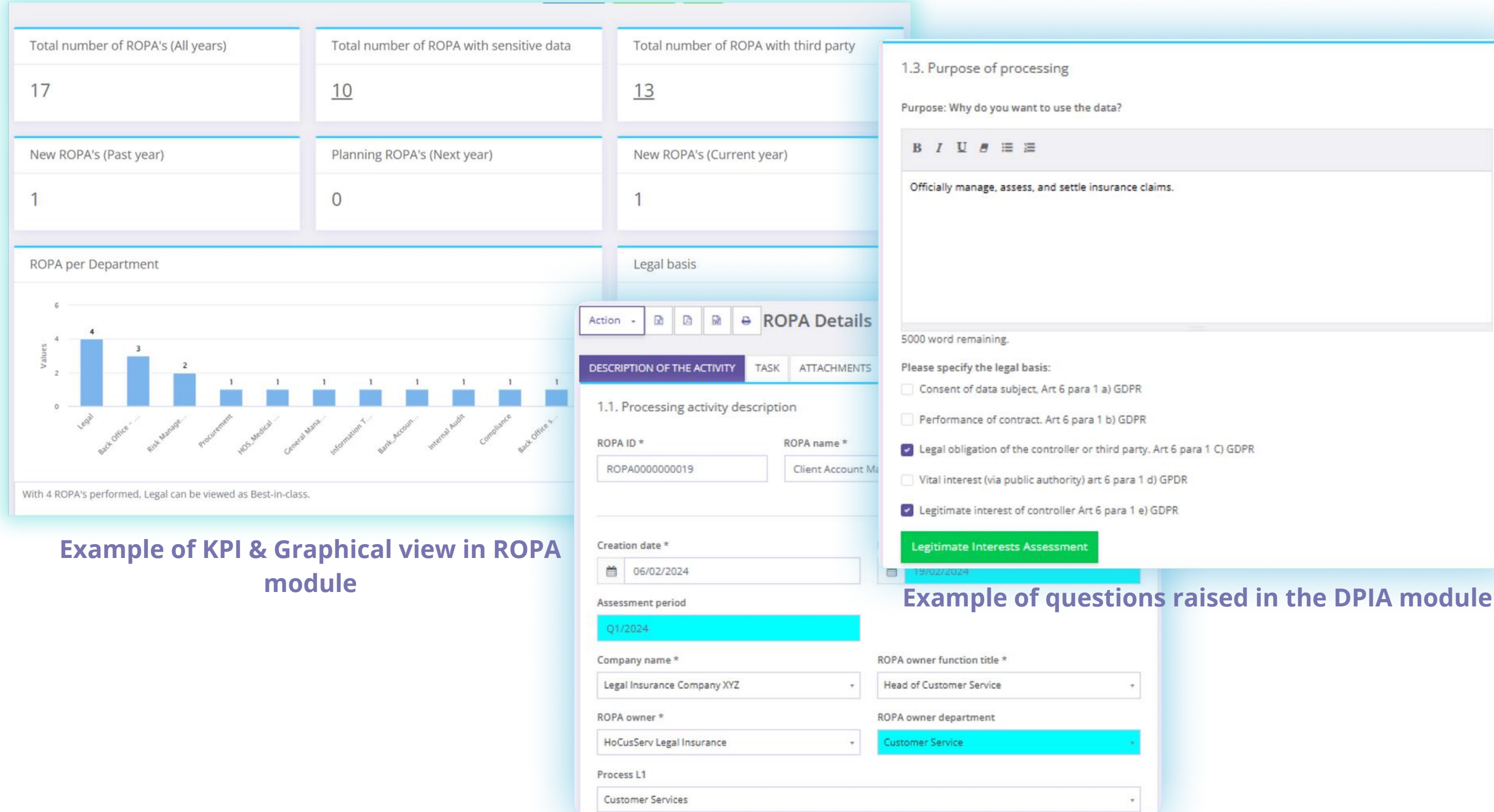
High

Example of questions raised in the DPIA module

DATA PROTECTION MODULES

ROPA

Registry of Processing Activities (ROPA) serves as a centralized database to manage and document processing activities. This module offers a panoramic view of your data processing landscape, enabling your organization to maintain compliance with ease while ensuring every interaction with data meets data protection standards.



Example of KPI & Graphical view in ROPA module

Example of questions raised in the DPIA module

Key Features & Benefits:

- Centralized repository to store all data processing activities in one organized location.
- Clarity and operational efficiency of your data governance framework.
- Easy-to-navigate interface for swift data retrieval.
- Based on ROPA final score a DPIA can be initiated directly from ROPA module.

DATA PROTECTION MODULES

LIA

The **Legitimate Interests Assessment (LIA)** module supports risk assessment to ensure that data processing is lawful and aligns with the General Data Protection Regulation (GDPR) requirements

LIA quick scan

1.

Special personal data categories: Processing of sensitive personal data (including health and/or judicial data) or 'data of a highly personal nature'?

☒ Yes
 ☐ No

2.

Vulnerable groups are specifically targeted?(vulnerable groups e.g. minors, employees, people with physical or mental health issues, whistleblowers, elderly people) or minorities

☐ Yes
 ☒ No

3.

Matched or combined datasets: The personal data will be combined with other data used in another context than the current processing activity, in a way which goes beyond reasonable expectations of the individuals behind e.g. to perform profiling of an individual

☒ Yes
 ☐ No

4.

Personal data is transfer outside EEA to (external) third parties

☒ Yes
 ☐ No

5.

Automated decision making with legal effect: Automated processing is done producing significant effects for individuals

☐ Yes
 ☒ No

6.

Profiling & Predicting : Personal aspects of individuals are scored or categorised, including profiling and predicting (e.g. performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements)

☒ Yes
 ☐ No

LIA Details

GENERAL INFORMATION

TASK

ATTACHMENTS

SIGN-OFF

ID *

LIA name *

AD000000008

Security & Fraud Prevention

ated ROPA name *

aim Processing Workflow

owner *

LIA department

ead-of_RISK Insurance

Risk Management

process L1

LIA main system

Select LIA process L1 --

LifeCo_Finance_system

creation date *

LIA Assessment period

03/01/2024

Q1/2024

name *

ead-of_DATA Insurance

Comments

Add Comments

Example of questions raised in the LIA module

Example of LIA detailed form

DATA PROTECTION MODULES

PRIVACY RISK REGISTER

Privacy Risk Register (or Privacy Impact Assessment) is inspired by market standards proposed by Regulatory Authorities. It allows end-users to perform in-depth analysis of privacy risk exposure including security measures effectively in place.

Key Features & Benefits:

- It could be initiated from a project when a deep-dive should be performed on privacy risks.
- Input in the module is performed by Project Managers, 1st line responsible, and reviewed by DPO.
- A 12 questions preliminary analysis provides a first assessment score before entering into the full PIA.

PIA (preliminary analysis)

- The collection, use or disclosure of personal information?
☒ Yes ☐ No
- The collection, use or disclosure of additional personal information held by an existing system or source of information?
☒ Yes ☐ No
- A new use for personal information that is already held?
☒ Yes ☐ No
- Sharing of personal information within or between external Third Parties?
☒ Yes ☐ No
- The linking, matching or cross-referencing of personal information that is already held?
☐ Yes ☒ No
- The creation of a new, or the adoption of an existing, identifier for individuals or biometric?
☐ Yes ☒ No

PIA preliminary assessment score

High

Action

Privacy Impact Assessment

Home / PIA / PIA

PIA CONTEXT

THIRD PARTY

POLICY

END-USER

DATA DICTIONARY

SYSTEM

ATTACHMENTS

SIGN

General overview

Data

Data life-cycle (Data processing) and supports

Back

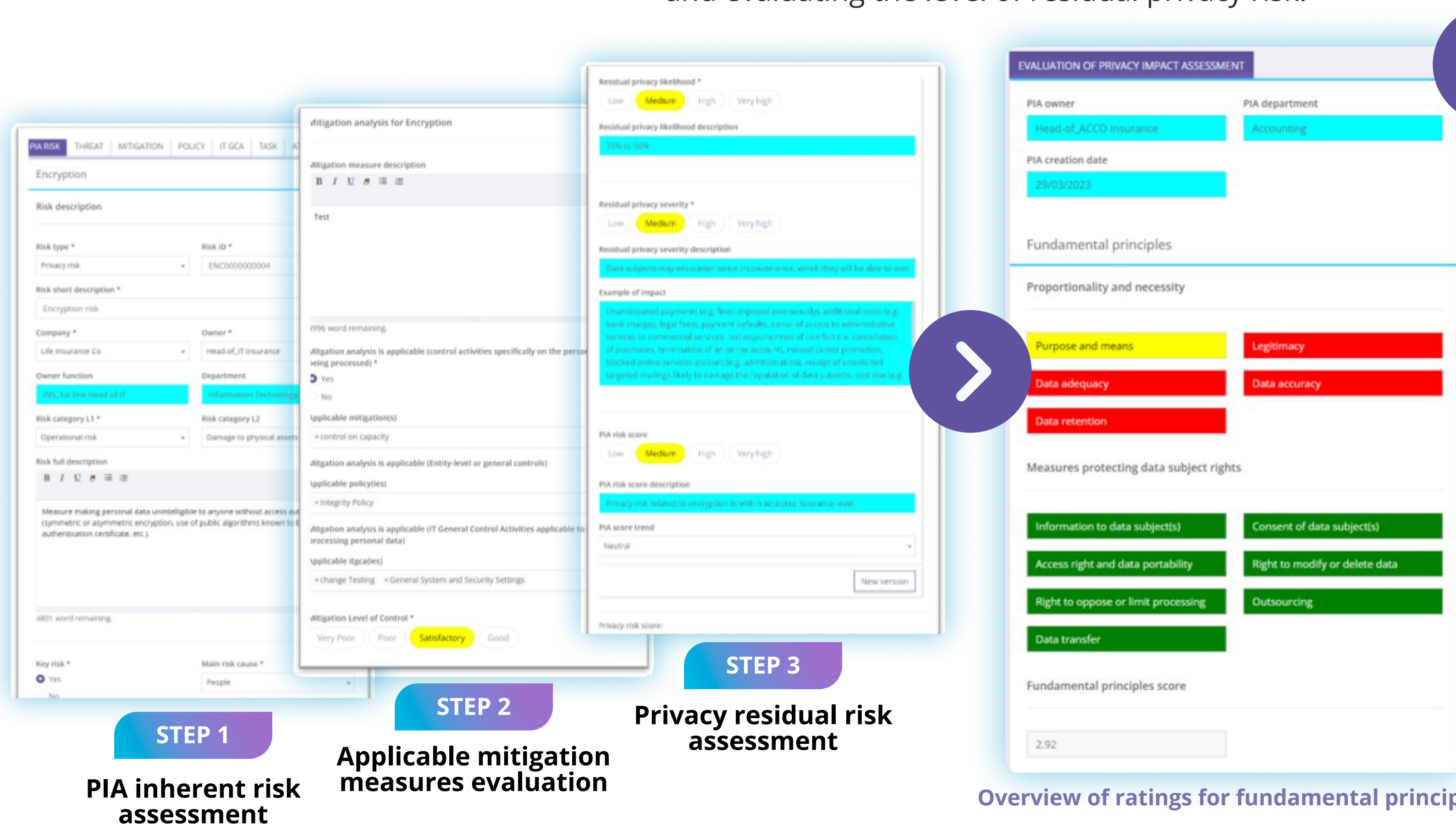
Go to Fundamental principles - PNP

Save

Example of questions raised in the Privacy Risk Register module

DATA PROTECTION MODULES PRIVACY RISK REGISTER

The Privacy Risk Assessment relies on a **3-steps approach** to identify relevant inherent threats. This includes identifying relevant control activities and evaluating the level of residual privacy risk.



CONFLICT OF INTEREST REGISTER AND DECLARATION IN GRC SUITE

The **Conflict-of-interest (COI)** modules in Grace Connect GRC Suite are designed to have an exhaustive register of all conflicts of interest that may arise in the organization. This register is populated by declaration forms filled-in by individual users. This enables to protect the interests of the organization by avoiding that personal interests are interfering with duties and responsibilities. Declarations are sent out internally as part of preventive campaign to disclose potential conflicts or investigating conflicts.

COI Register Home / COI Register / New COI Register

General information

COI source *
Other

COI register ID *
COIR0000000004

COI register short name *
COI register short name

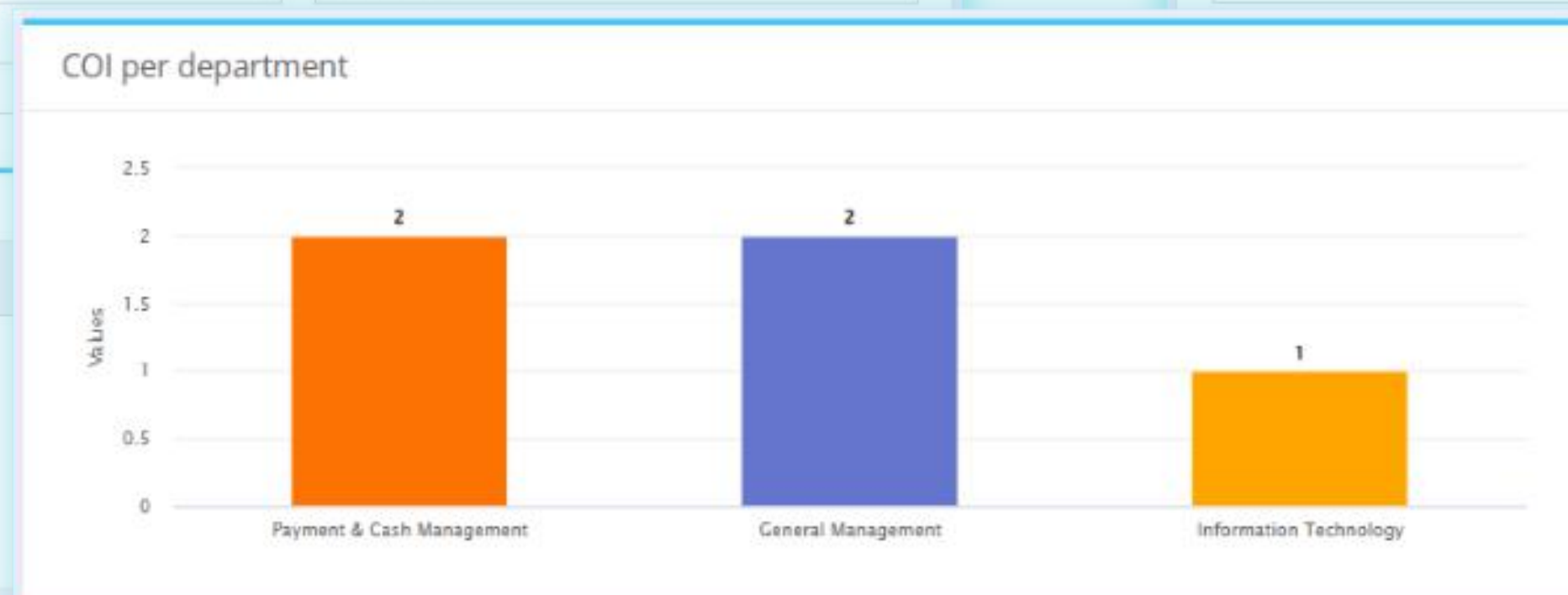
COI register category
Potential

COI register nature
Permanent

COI register type
Personal

COI description

5000 word remaining.



Detailed and graphical view of COI Register

COI Declaration Details Home / COI Declaration / COI Declaration Details

DETAILS TASK ATTACHMENTS MANDATES RELATIONSHIPS TR

General information

COI register ID *
COI register ID

COI declaration ID *
COID0000000005

COI declaration name *
Family link with CFO

COI category
Realised

COI Assessment period
Q2/2022

Employee declaration

I have completed the Conflict-of-Interest eLearning module. I understand the obligations on me to declare all potential or actual conflicts. I understand that failure to do so may result in disciplinary actions being taken against me. My declaration covers all, present or past (covering 5 years in the past), of my direct and indirect interests in:

- Proposed & current transactions
- Contracts and relationships between ARAG Belgium and any other group entity or external companies
- Personal or professional relationships with individuals
- Situations of political influence or political relationships

I confirm I have provided details of all the interests of which I'm aware as of 29/04/2022 in the attached appendices.

4283 word remaining.

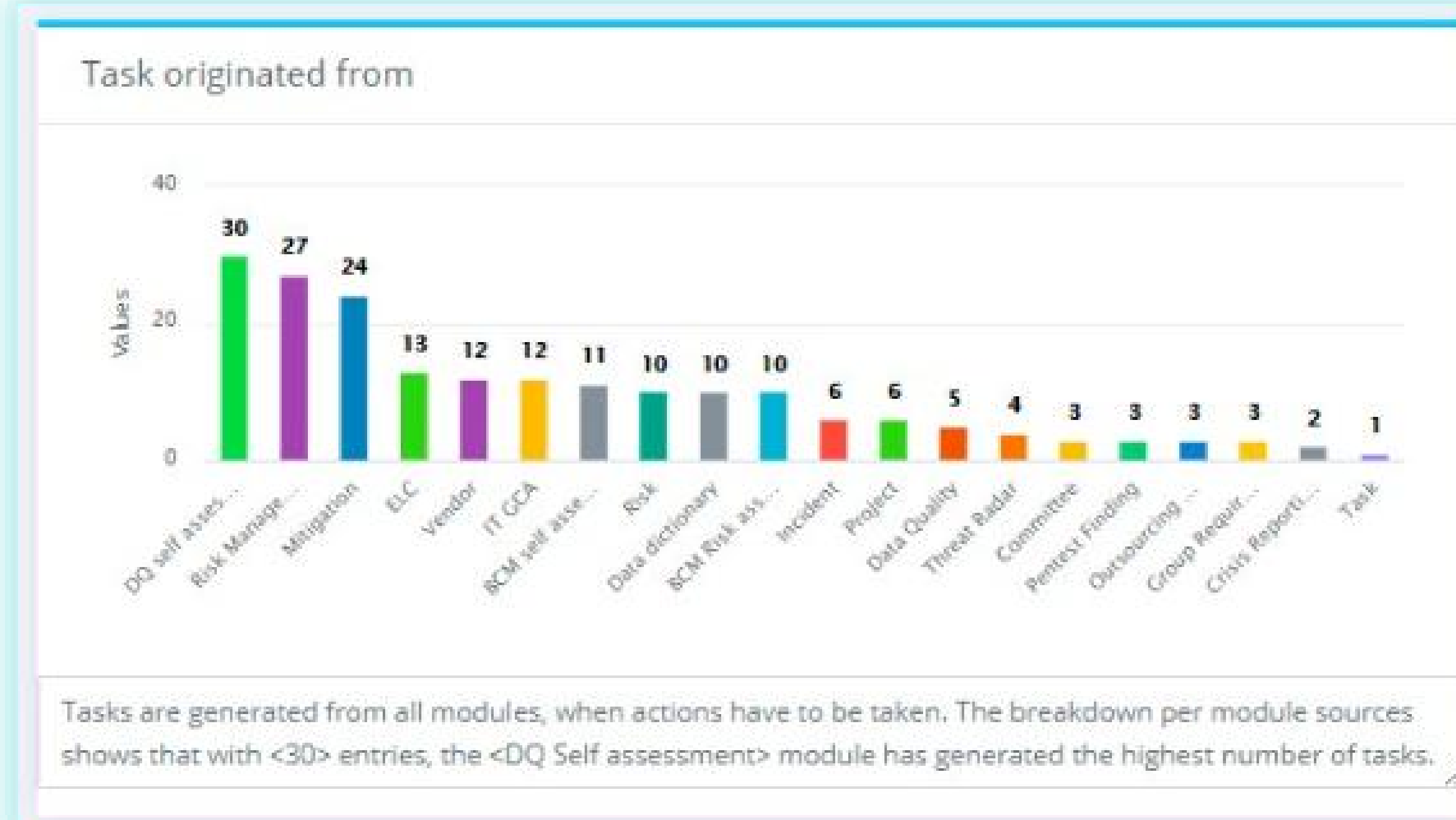
Detailed view of COI Declaration

In the context of the DORA regulation, provisions related to management of conflict of interest towards ICT third party service providers are covered by Grace Connect GRC Suite COI modules.

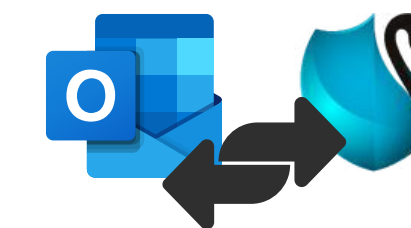
EFFECTIVE DECISION MAKING RELYING ON TASKS MODULE

The graph below illustrates the full capacity of the GRC Suite - actions (“**Tasks**”) initiated in any modules are stored and tracked centrally and are accessible through a single point of control within the tool.

This holistic view on **Tasks** provides users and management a clear insight on effort, workload, and remediations.



Task module
synchronized with
MS-Outlook tasks



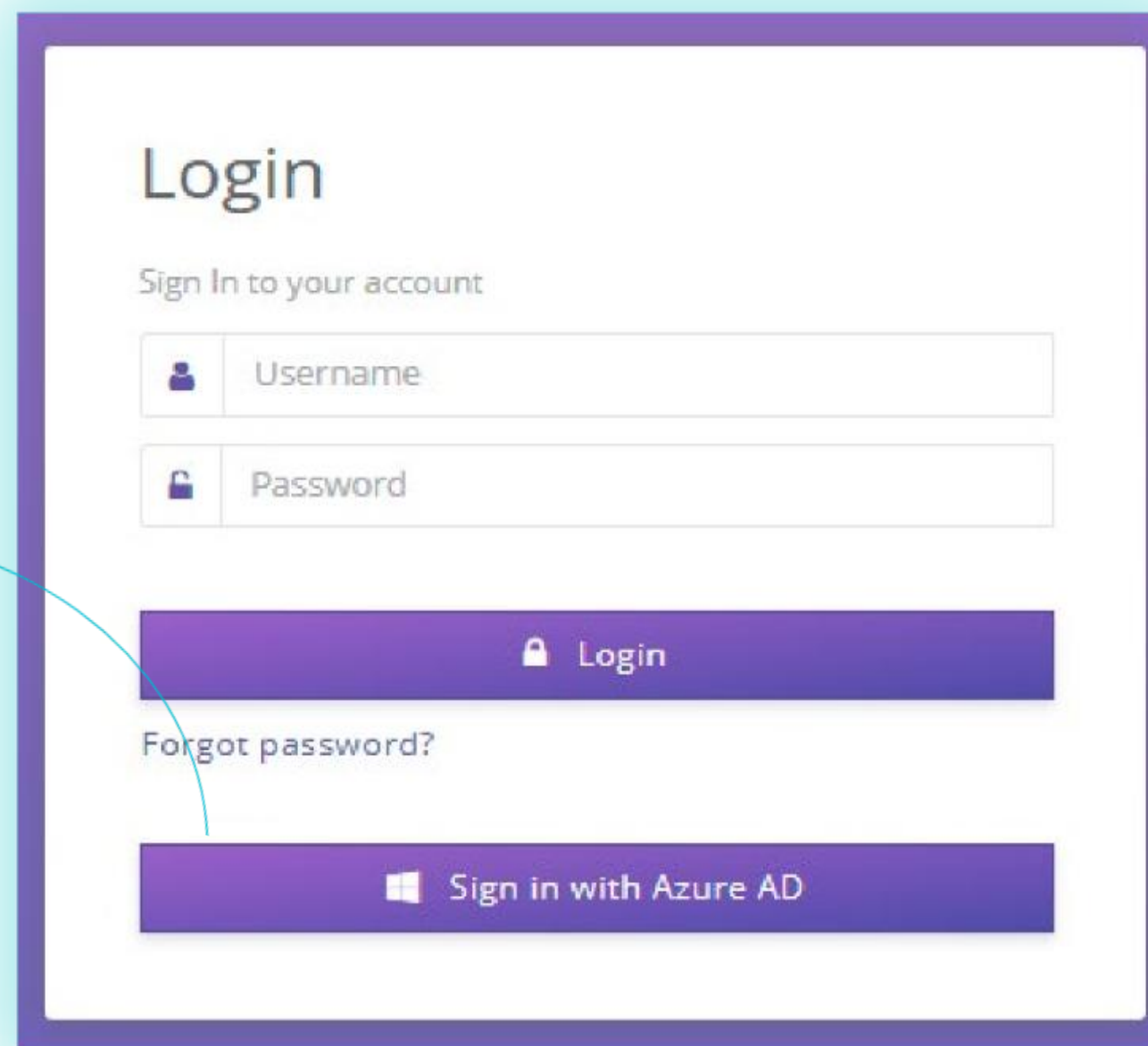
Graph view with number of Actions in the GRC Suite originated by all modules

Silo-oriented organizations often rely on stand-alone monitoring of their actions, as they are originated for a specific purpose. The GRC Suite is designed to use all information to enable a comprehensive but effortless tracking of actions and timely resolution.

SECURITY EMBEDDED IN GRACE CONNECT GRC SUITE

Information stored in the GRC tool can be classified as highly confidential, therefore the GRC Suite is designed based on latest security technologies enabling a controlled use of the tool.

Single sign-on with Active Directory (MS) for Login authentication with domain restriction.

Login

Sign In to your account

Username

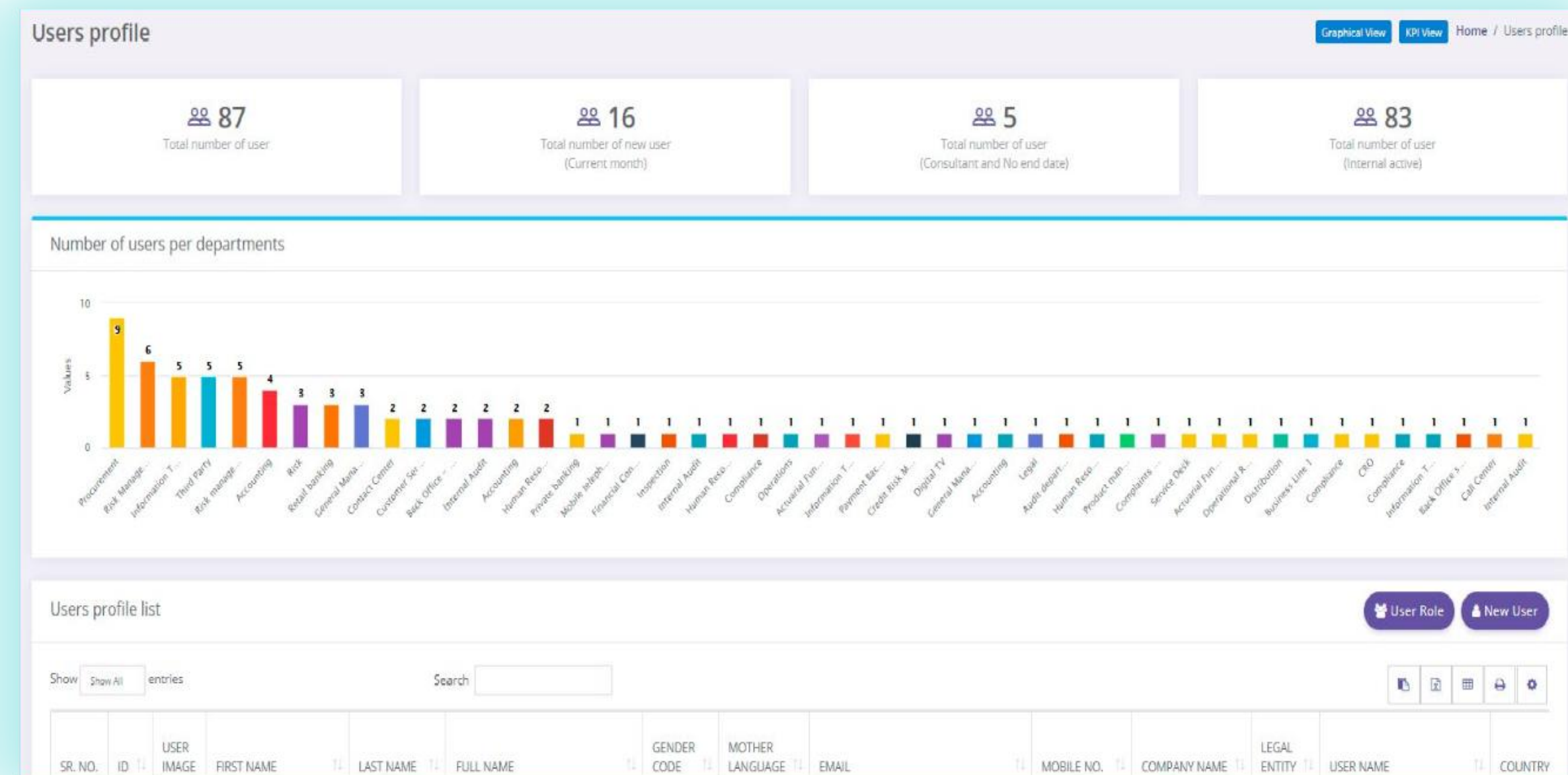
Password

Login

Forgot password?

Sign in with Azure AD

Entry screen with individual user recognition



Dedicated interface for user administration

User rights management is based on **Identity and Access Management (IAM)** principles, which are core in the Information Security domain. This approach ensures that the GRC Suite provides the right information to the right person. The GRC Suite is designed to be plugged in the client's Active Directory ensuring a secured synchronization.



Veronika ZUKOVA

Contact details

☎ +352 691 615 216 | @ veronika.zukova@gracegrc.com | 🌐 www.gracegrc.com

📍 Grace Connect SARL 28 rue Jean Marx, 8250 Mamer - Luxembourg

Additional notes:

- A free-demo of the software (in its current version and as included in this presentation) is directly available for clients, upon demand. For further information or enquiries, please contact your local distributor or representative of Grace Connect SARL directly.
- The content of this presentation belongs to Grace Connect SARL, any reproduction in full or in part is subject to prior explicit consent of Grace Connect SARL.

