GRC SUITE

General product presentation

2025

GRACE CONNECT

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

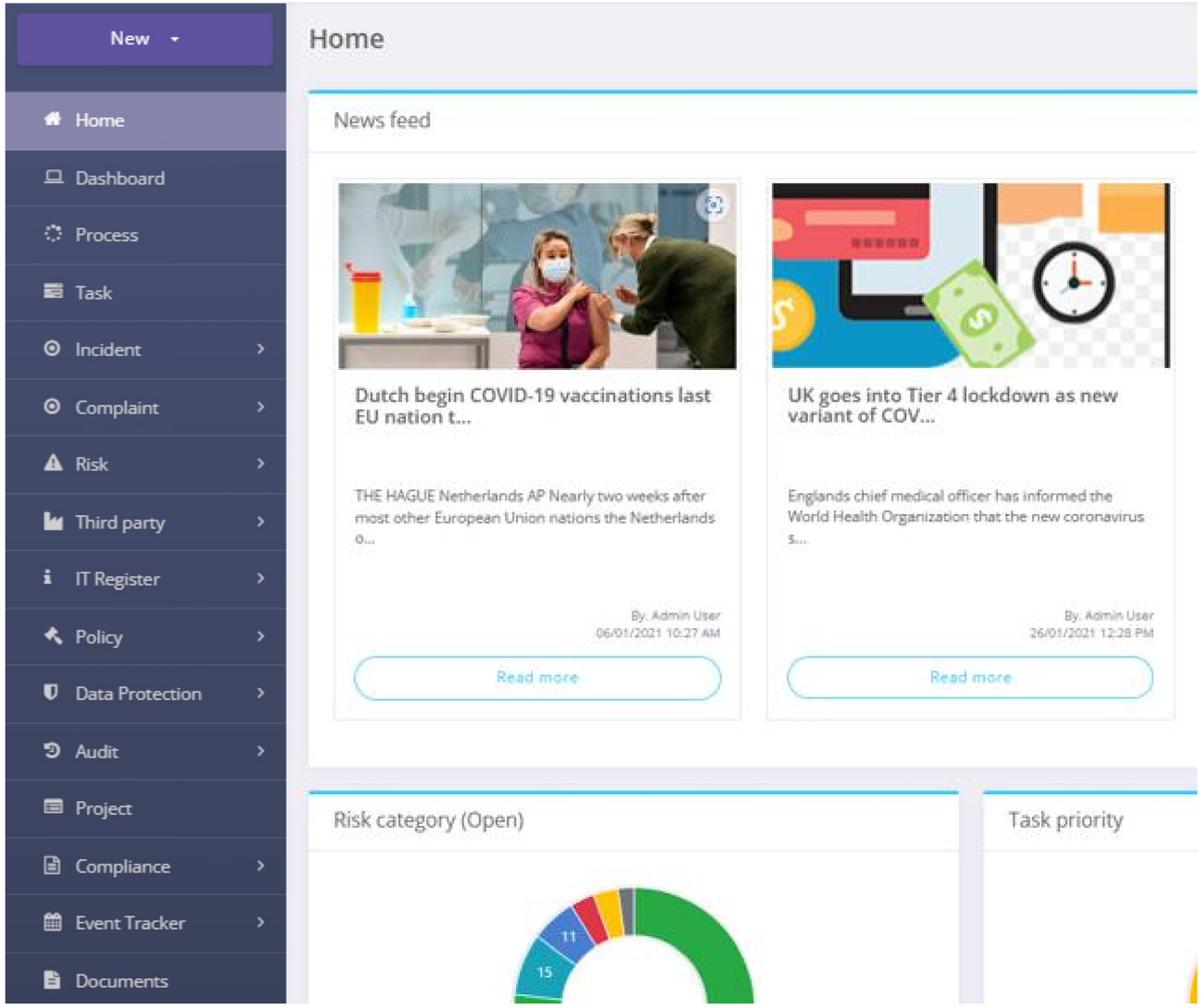
- **User friendly interface easy to use allowing a quick understanding of all functionalities.**
- **Contains graphs, KPI's, and narratives that will allow to manage risks pro-actively instead of reactively.**
- **A calendar is included to log all important dates such as Risk Committees, testing, delivery 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 CONTINUTY MANAGEMENT	DATA QUALITY Self-Assessment	LEGITIMATE INSTEREST Assessment	DORA ITS REGISTER OF INFORMATION
POLICY	SYSTEM, IT COMPONENT & CIA Classification	BCM Self-Assessment	DATA BREACH	PRIVACY RISK REGISTER	CONTRACT MANAGEMENT



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.

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 eventualy 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	Identification code of the branch	DORA ITS List of branch(es)
B_02.01	Contractual Arrangements – General Information	Contractual Arrangement Reference number	CONTRACT MODULE
B_02.02	Contractual Arrangements – Specific Information	Function Identifier; Type of ICT Services (annex III); Contractual Arrangement Reference number; Identification code of the ICT Service Provider; LEI of entity making use of the ICT Services	CONTRACT & SUPPLIER MODULES
B_02.03	List of intra-group contractual arrangements	Contractual Arrangement Reference number	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)	Contractual Arrangement Reference number	CONTRACT MODULE
B_03.02	ICT third-party service providers signing the Contractual arrangements for providing ICT service(s)	Identification code of the ICT Service Provider; Contractual Arrangement Reference number	CONTRACT MODULE
B_03.03	Entities signing the Contractual arrangements for providing ICT service(s) to other entity within the scope of consolidation	Contractual Arrangement Reference number	CONTRACT MODULE
B_04.01	Entities making use of the ICT services	LEI of entity making use of the ICT Services; Contractual Arrangement Reference number; Identification code of the branch	CONTRACT MODULE
B_05.01	ICT third-party service providers	Identification code of the ICT Service Provider	SUPPLIER MODULE
B_05.02	ICT service supply chains	Type of ICT Services (annex III); Contractual Arrangement Reference number; Identification code of the ICT Service Provider	CONTRACT & SUPPLIER MODULES
B_06.01	Functions identification	LEI of entity making use of the ICT Services; Function Identifier	PROCESS & BCM BIA Modules
B_07.01	Assessment of the ICT services	Type of ICT Services (annex III); Contractual Arrangement Reference number; Identification code of the ICT Service Provider	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 trough 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

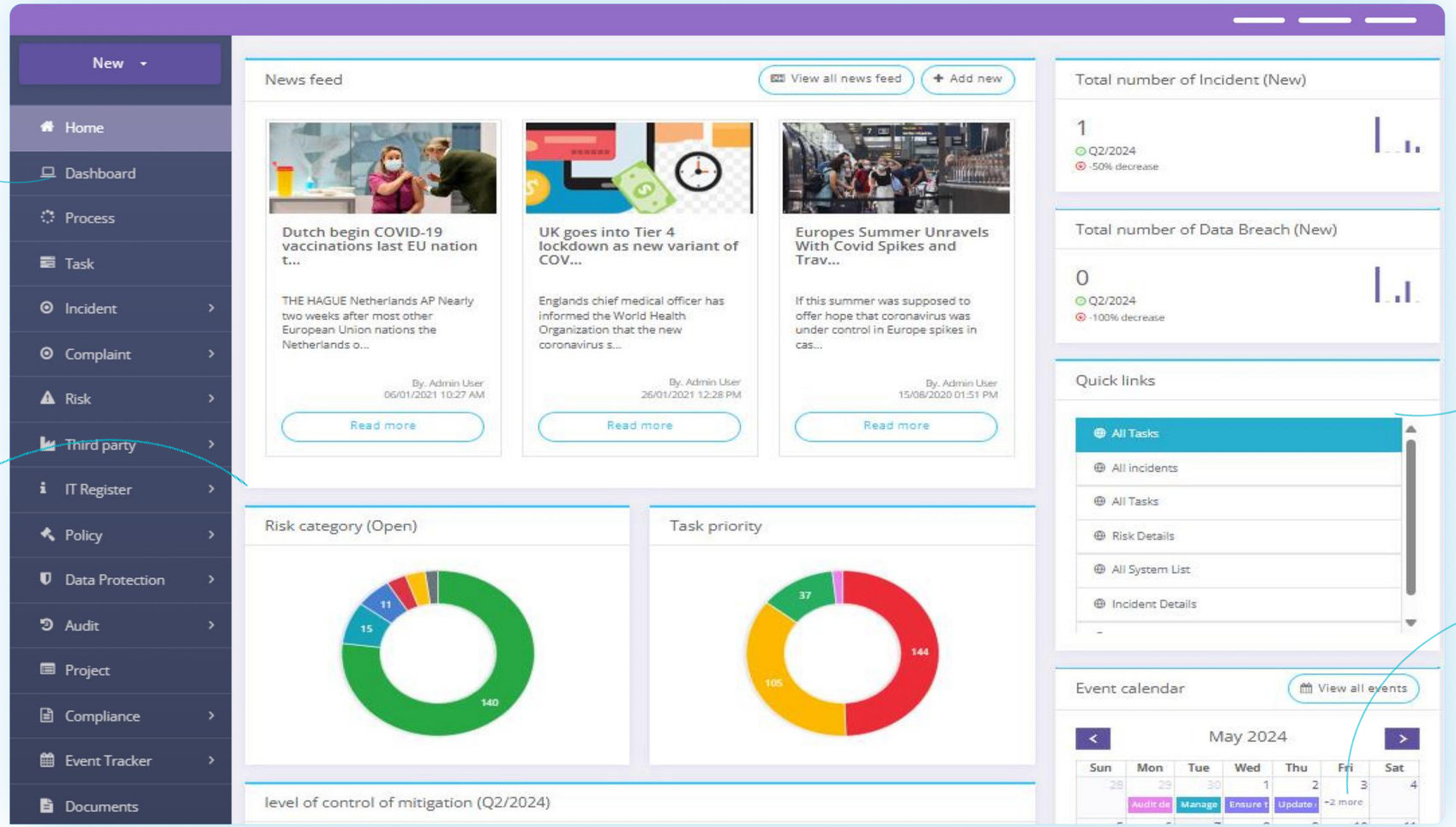
home page

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

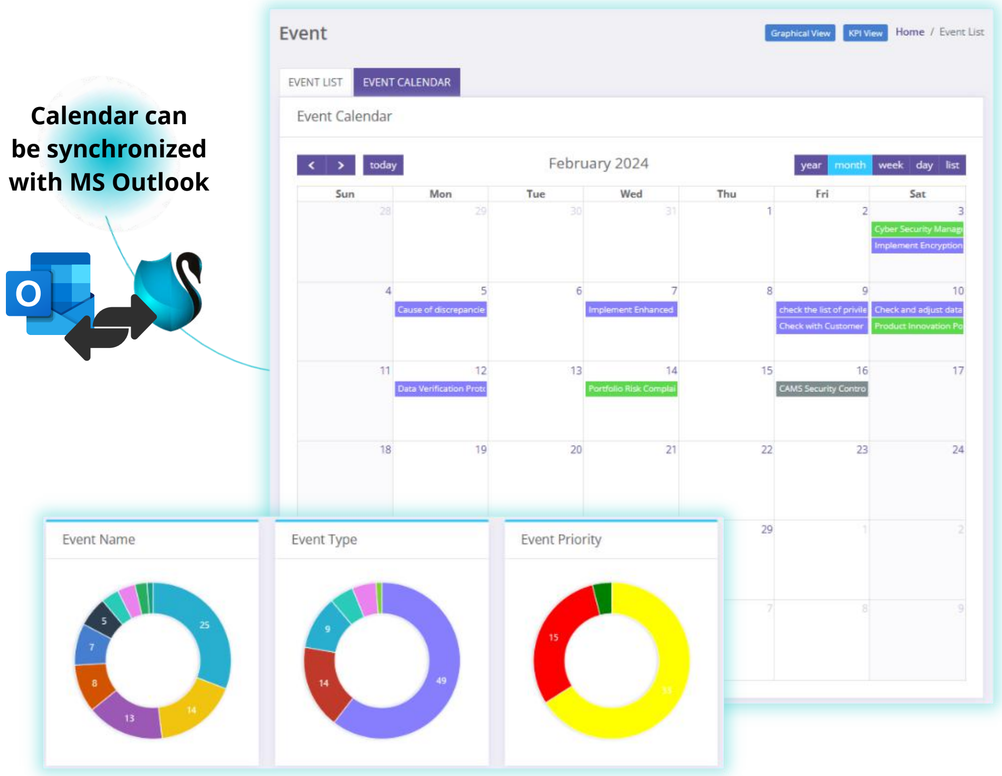
Calendar – the time dimension in the GRC tool is a key differentiating factor from other GRC tool



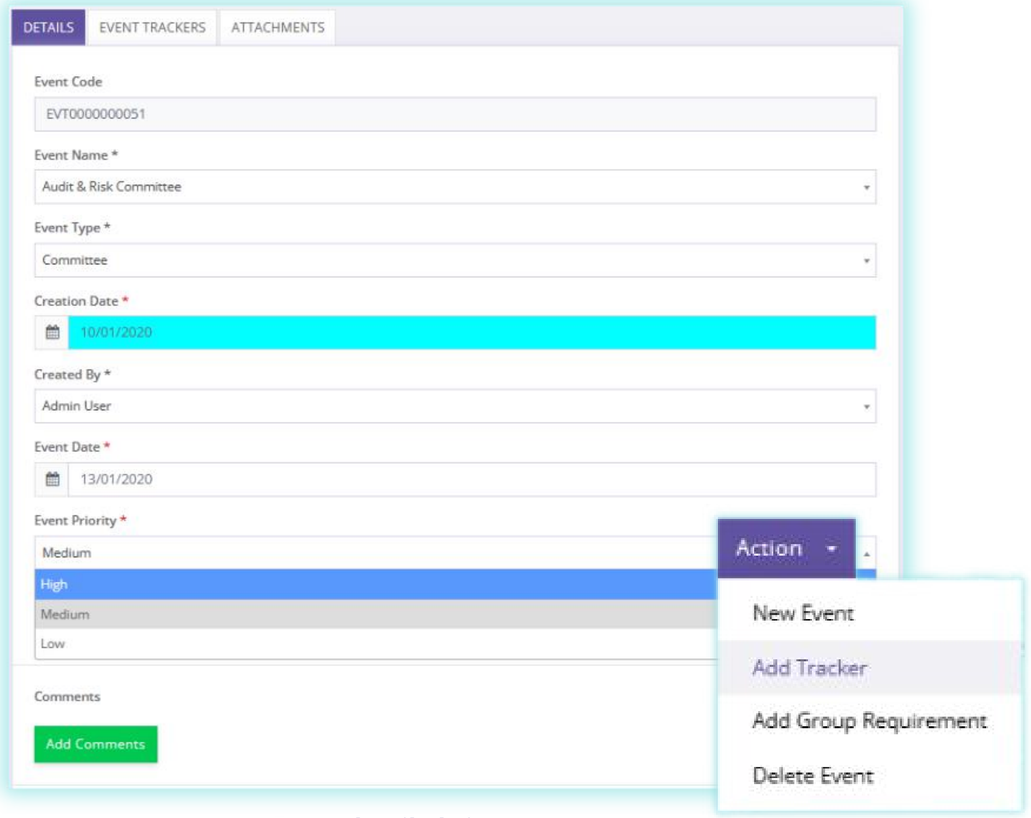
EVENT MANAGEMENT

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 trough the dedicated module Event Management or through linked modules (e.g. Audit, Regulatory Watch, Resilience Testing, Tasks)

Calendar can be synchronized with MS Outlook



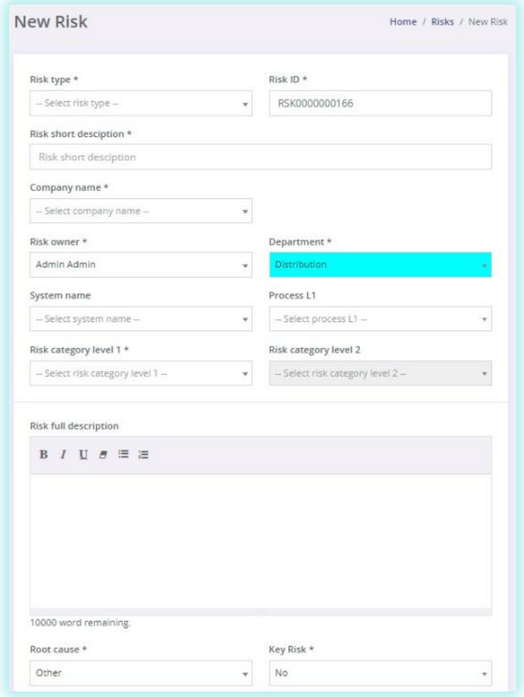
Events calendar and graphical view



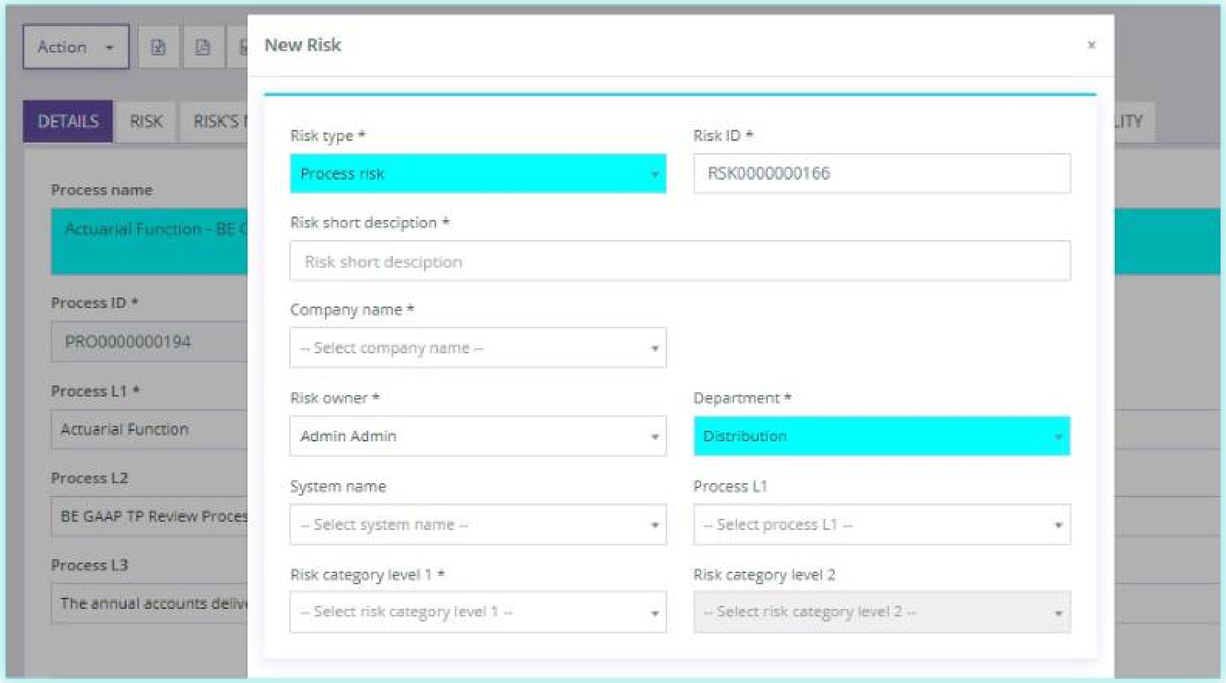
Event detailed view

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

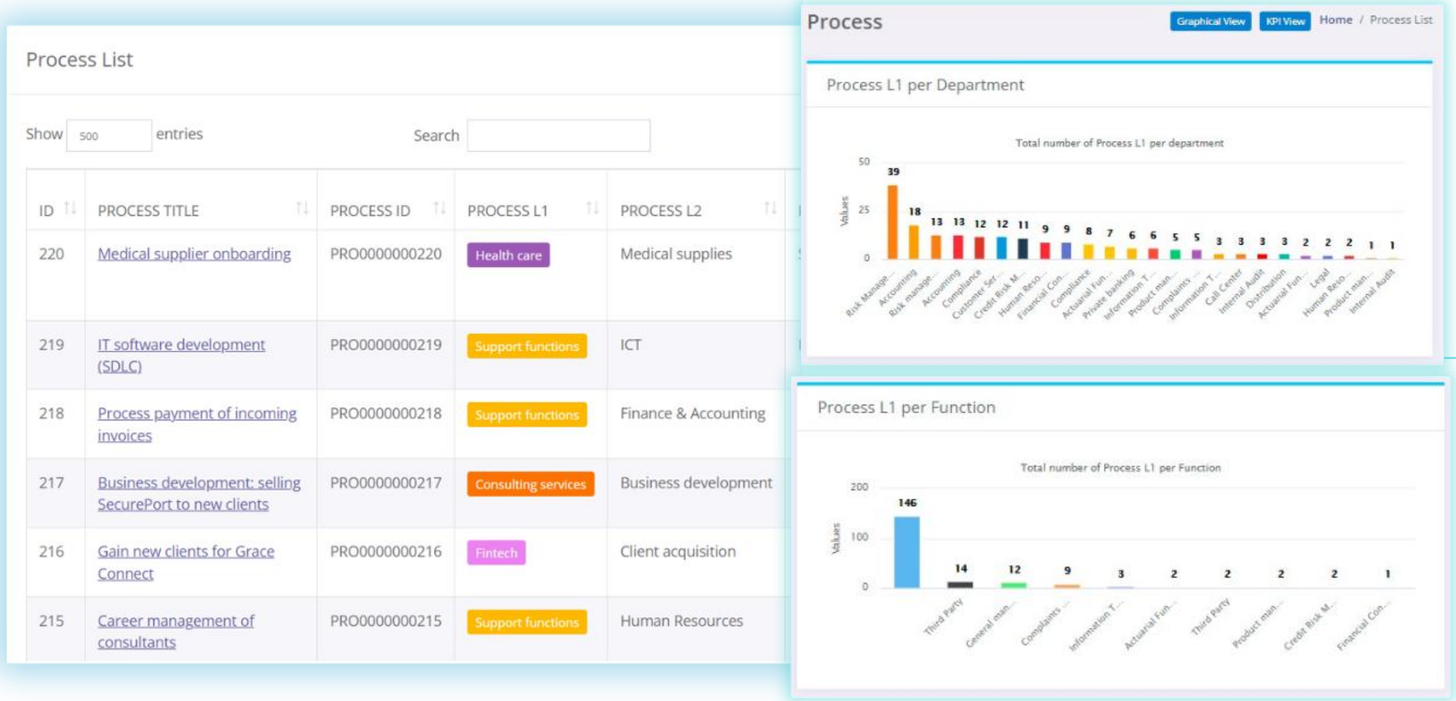
SR. NO.	COMPLAINTS NAME	COMPLAINT TYPE L1	CONTRACT ID	PRODUCT CLASS	COMPLAINT ORIGINATOR	COMPLAINT FINAL ORIGINATOR	COMPLAINT MANAGED INTERNALLY?	COMPLAINT RECEIVED FROM	COMPLAINT RECEIVER ACTIVE	HANDLER	HANDLER ID	HANDLER DEPARTMENT
1	malfunctioning of an ATM	Other	7894	Other	Other	No	No	Phone	No	Compliance_Director 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	BKCBO	Credit Back Office
4	ordered credit card never received	Other	978	Other	Other	No	No	Other	No	Credit_BO_agent Banking	BKCBO	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.

Covering DORA Art. 8.1, 8.5, 28.3

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.

Covering DORA Art.11.2.b, 11.10, 17, 18.1(a-f), 19.1, 28.7.a RTS Risk Art. 22, RTS Incident Mgmt Art.2, 10

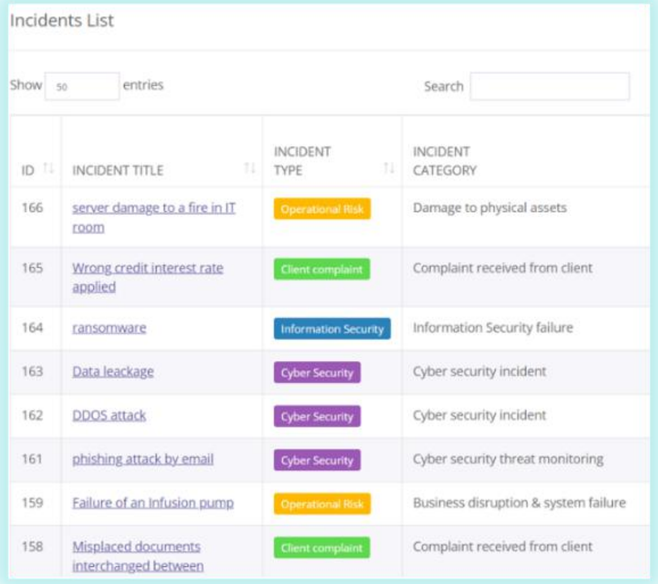
WORKFLOW-BASED INCIDENT MANAGEMENT MODULE

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

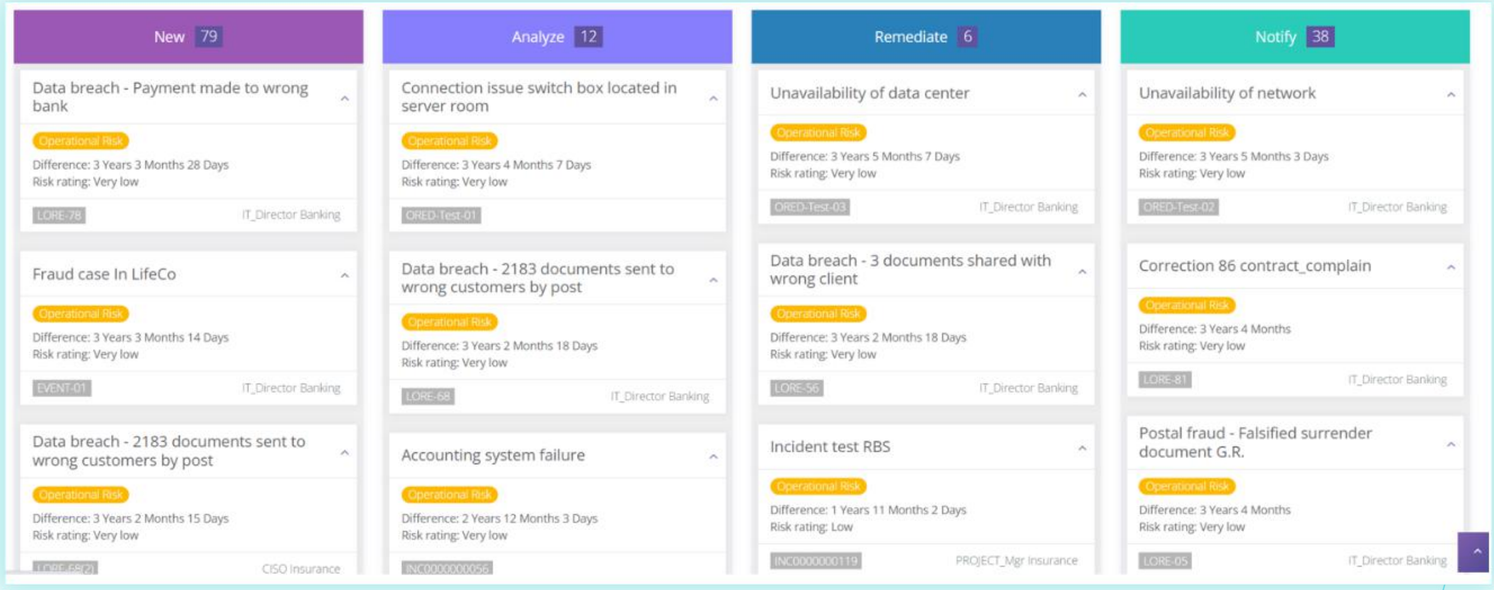
data quality issues

cyber security incidents

data breaches (GDPR requirement)



Simple list view (all incidents)



Incident tracking view (all incidents)

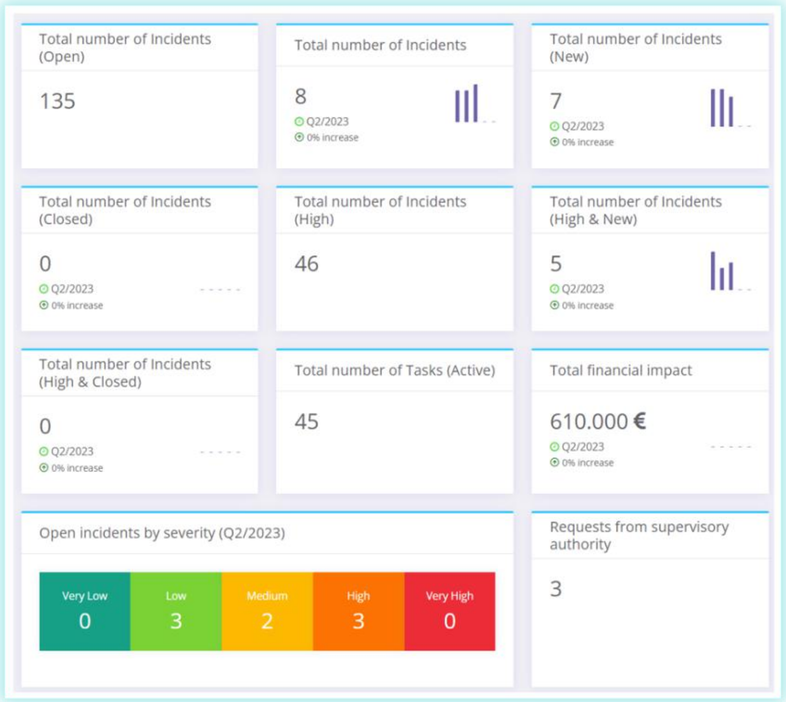
Possible connection with JIRA (through API)

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.**

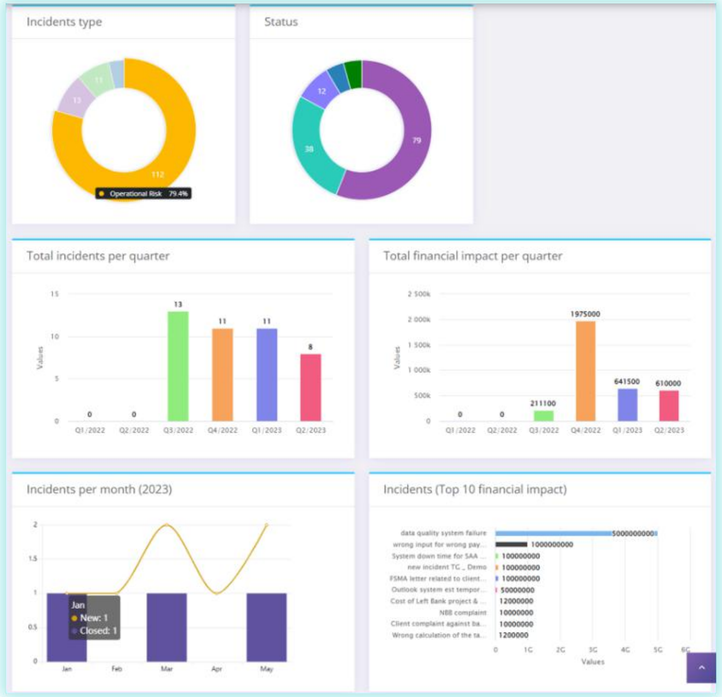
Covering DORA Art.11.2.b, 11.10, 17, 18.1(a-f), 19.1, 28.7.a RTS Risk Art. 22, RTS Incident Mgmt Art.2, 10

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)



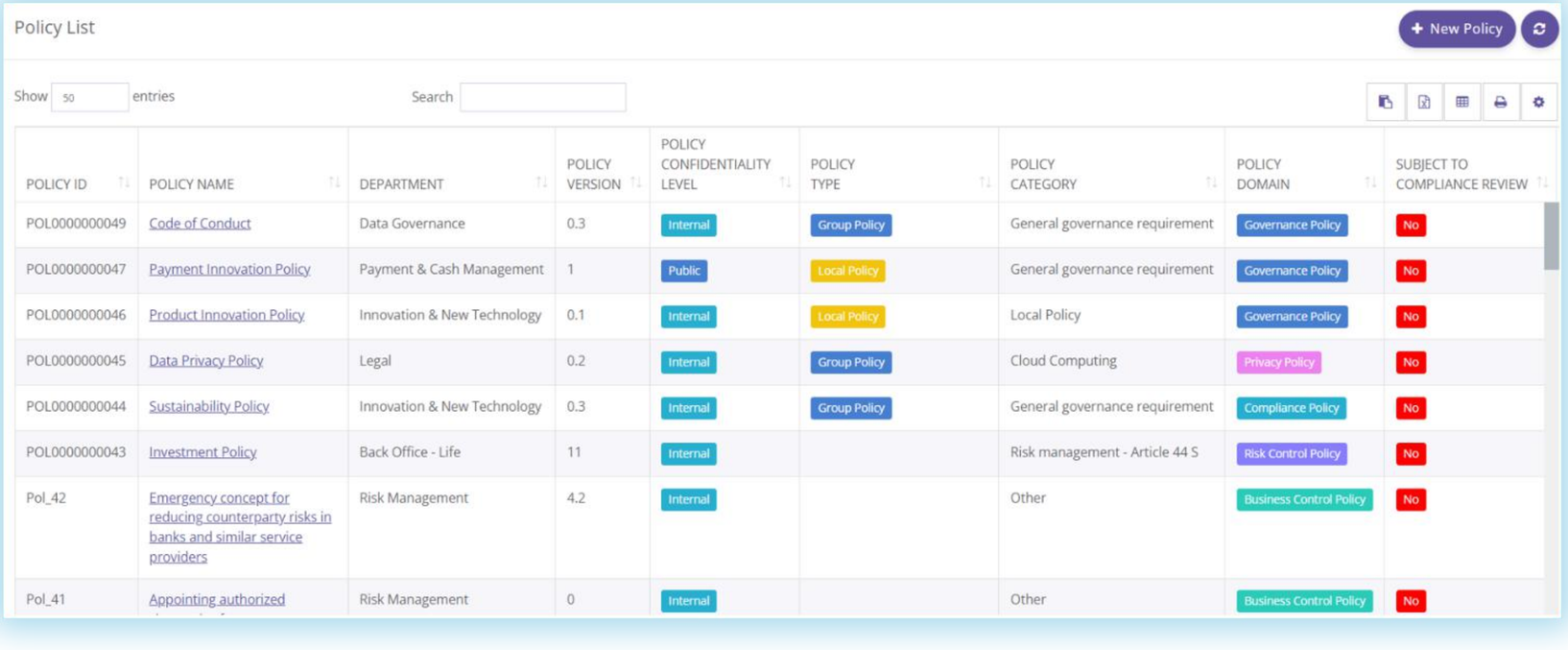
Graph view (all incidents)

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.

Covering
DORA Art. 5
RTS Risk Art. 2, 3

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).

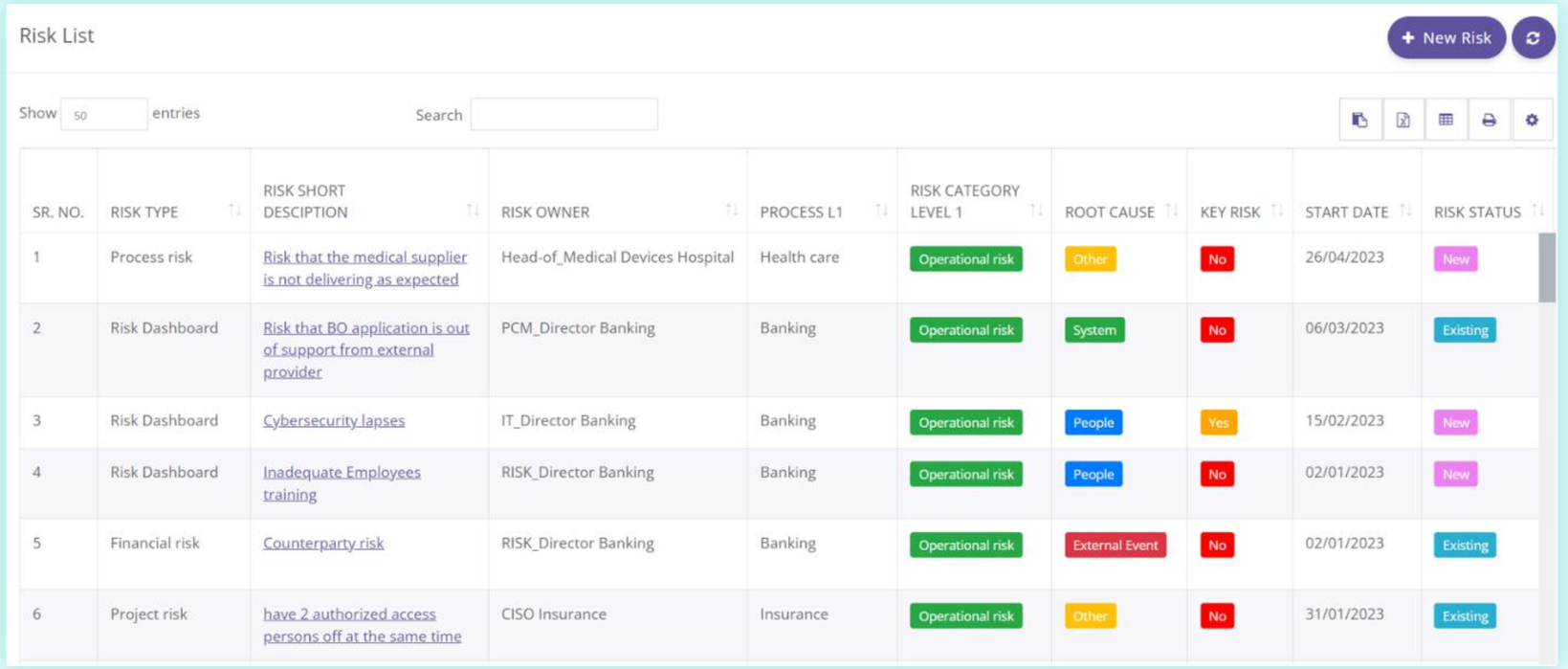
Covering DORA Art. 8.3

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 ...



Risk List

+ New Risk

Show 50 entries Search

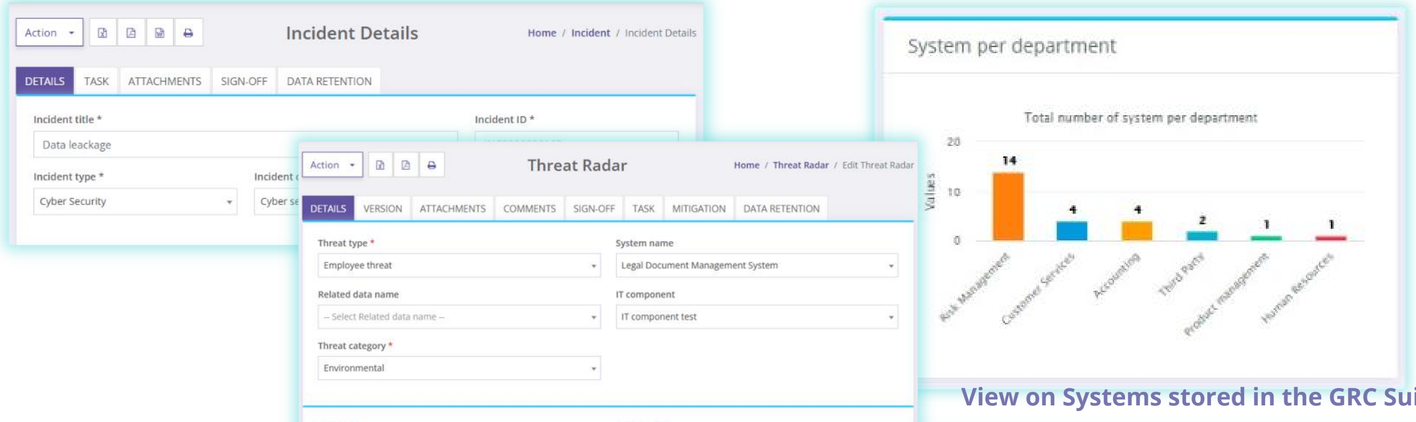
SR. NO.	RISK TYPE	RISK SHORT DESCIPTION	RISK OWNER	PROCESS L1	RISK CATEGORY LEVEL 1	ROOT CAUSE	KEY RISK	START DATE	RISK STATUS
1	Process risk	Risk that the medical supplier is not delivering as expected	Head-of_Medical Devices Hospital	Health care	Operational risk	Other	No	26/04/2023	New
2	Risk Dashboard	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.

Covering DORA Art. 8.2, 17.2, 18.2 RTS Incident Mgmt Art. 16 RTS Risk Art. 3.1

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.



View on Systems stored in the GRC Suite

View on IT Components stored in the GRC Suite

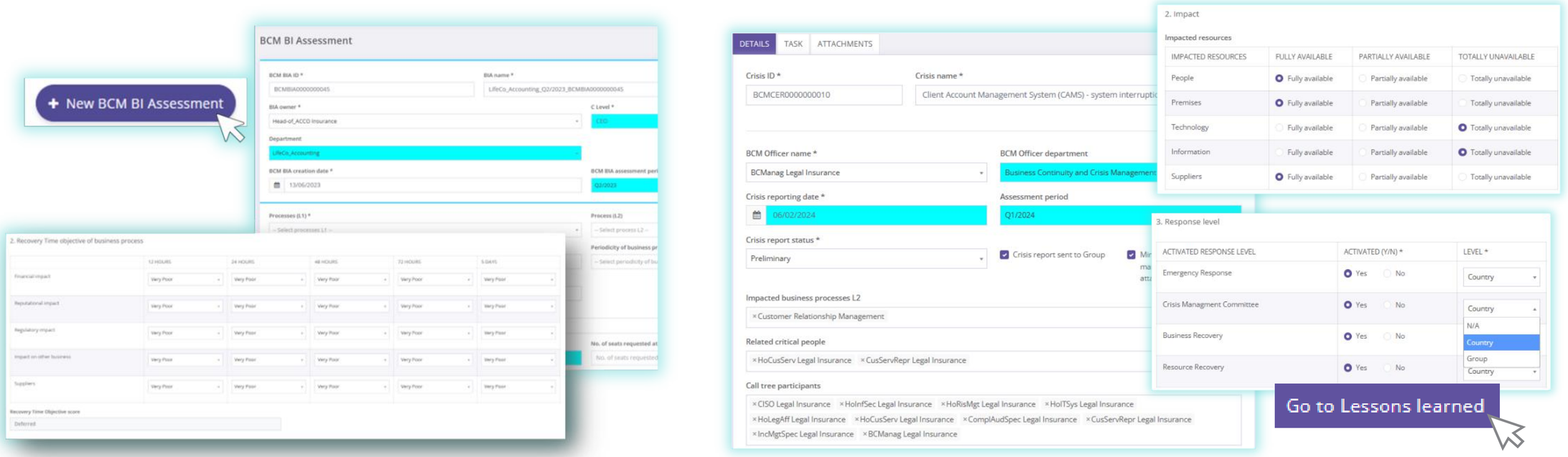
- The Cyber security module is fully aligned with **Information Security CIA classification** and is applicable to all systems and IT components stored in the GRC Suite.
- Possibility to have a Cyber Security maturity assessment stored and mapped out with Grace Connect Task tracking module.

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

Covering
DORA Art. 11.2, 11.5, 11.6.a, 12.6, 13.2
RTS Art. 26
RTS Risk Art. 24, 27

BUSINESS CONTINUTY & 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).

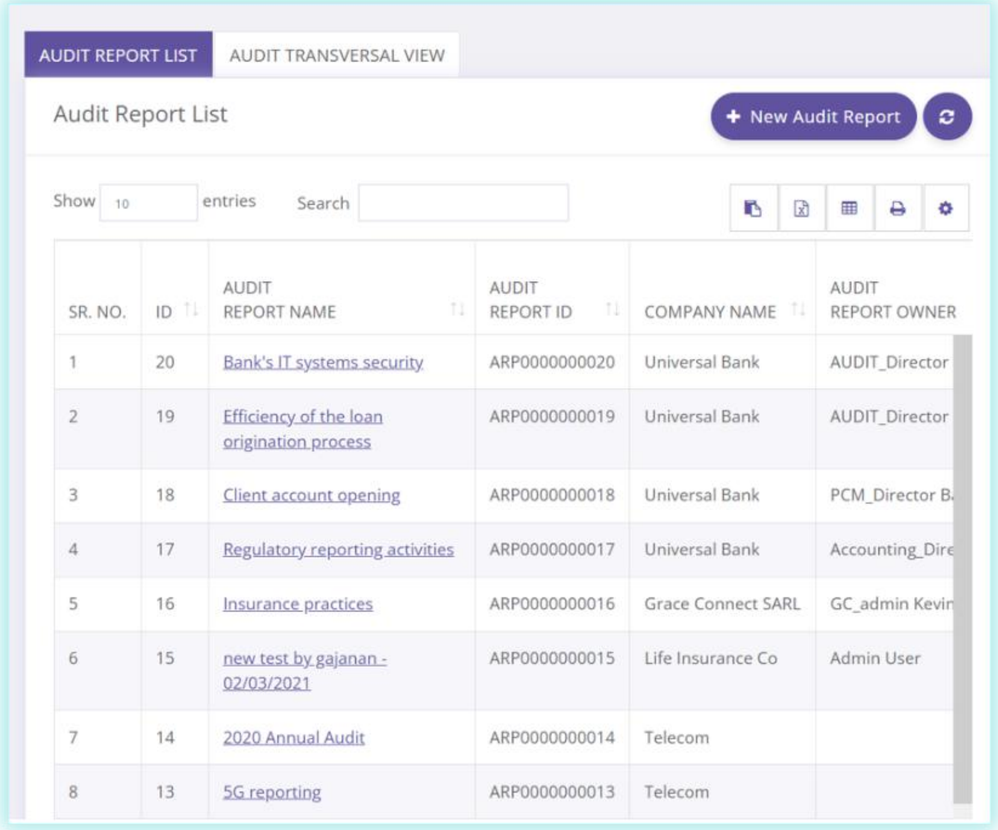


The detailed form is used to create new **BCM BIA** entry with all relevant information to be introduced by users.
The **Crisis Management module** enables effective communication and response coordination in emergencies. It serves as a central repository for incident descriptions, impact assessments,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

Covering DORA Art. 6.7

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.



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

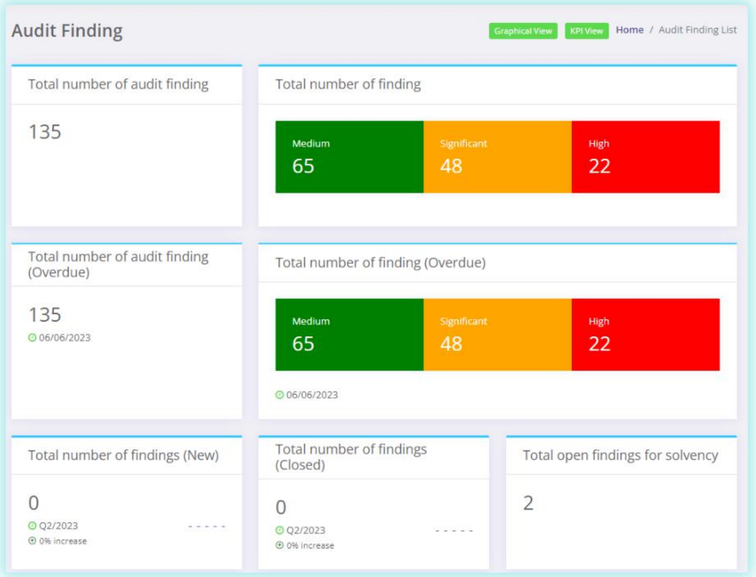
Graphs and KPI's for Audit reports

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.

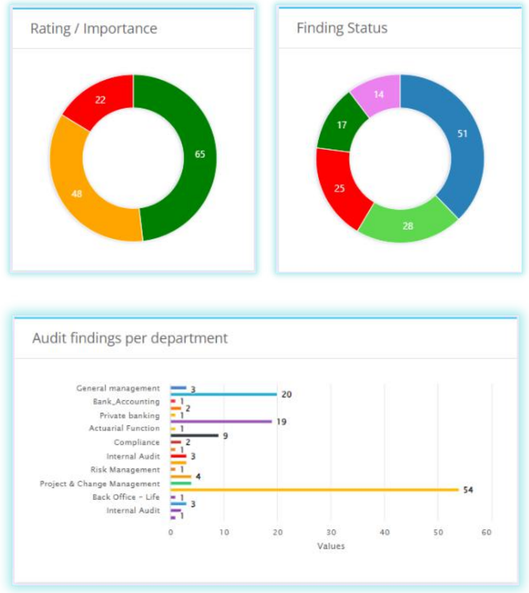
Covering DORA Art. 6.7

AUDIT RECOMMENDATIONS MONITORING IN GRC SUITE

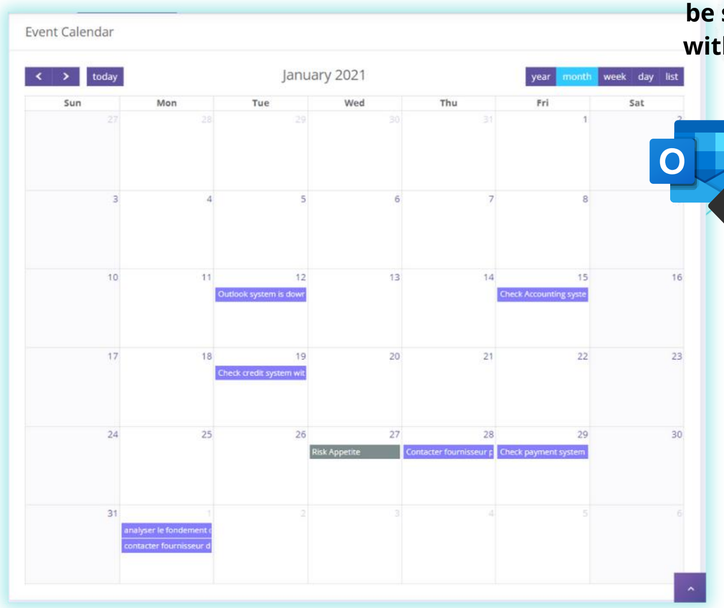
Monitoring of audit recommendations is available in the GRC Suite.
A dedicated set of KPI's and graphs is available to users and management to ensure a comprehensive view on all findings.



KPI's on Audit findings



Graphs on Audit findings



Calendar view of Audit findings (High)

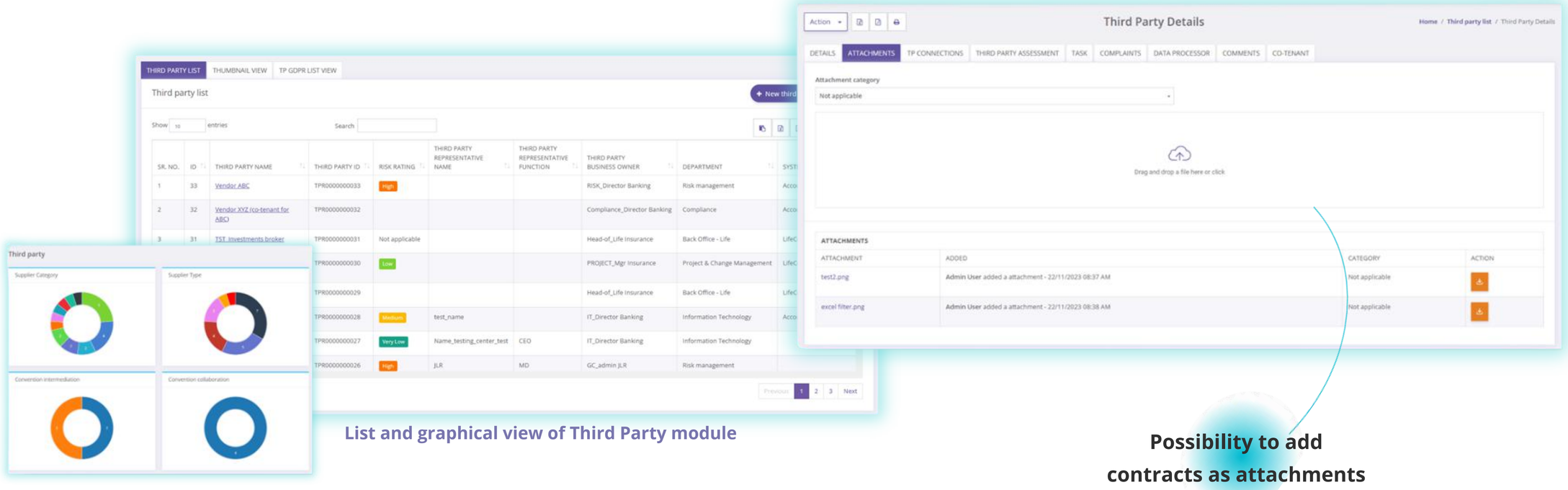
Calendar can be synchronized with MS Outlook

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.

Covering
DORA Art. 28.1.a, 28.3
RTS TP Art. 1, 3, 4, 5, 6
ITS RoI provisions

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).



List and graphical view of Third Party module

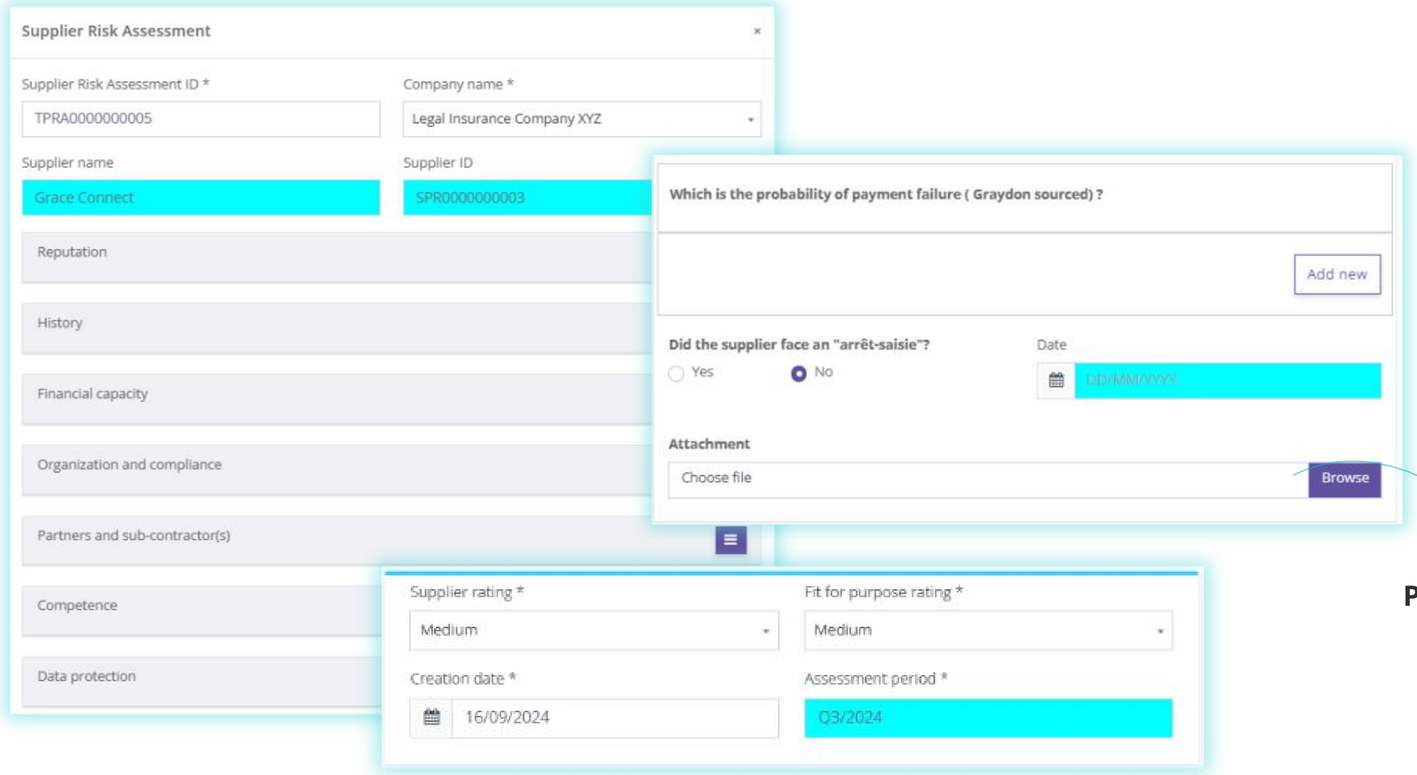
Possibility to add contracts as attachments

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

Covering
DORA Art. 28.1.a, 28.3
RTS TP Art. 1, 3, 4, 5, 6
ITS RoI provisions

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.



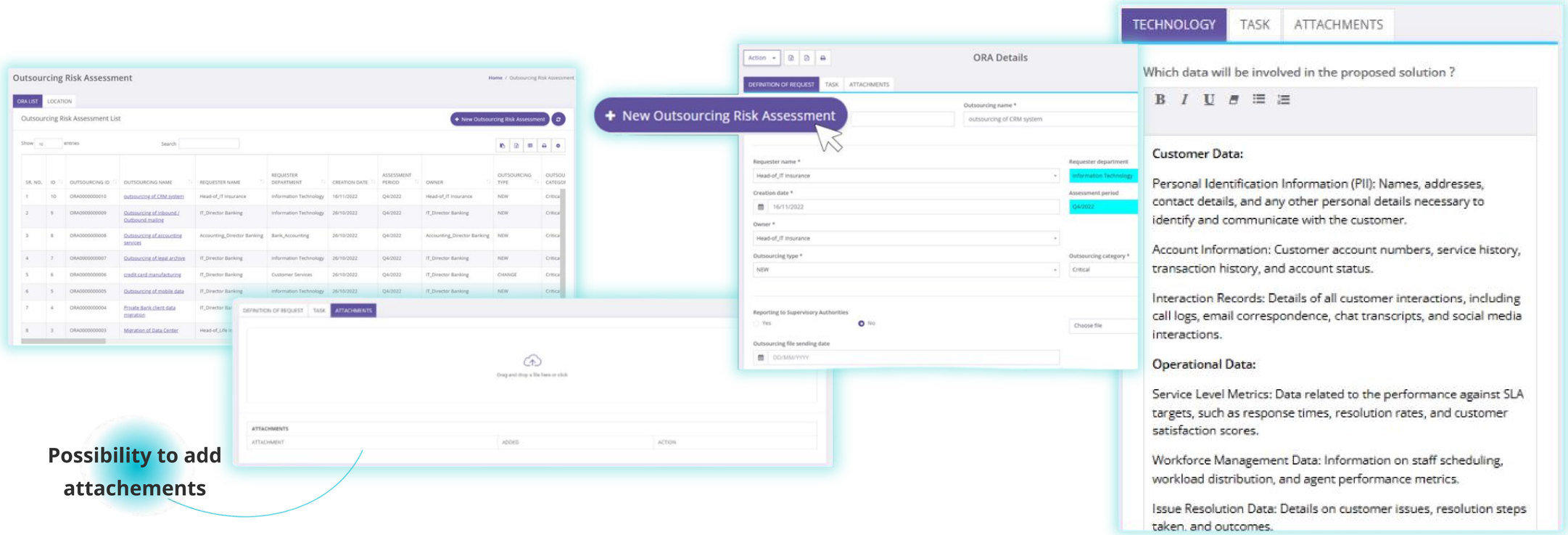
All documentation can be stored in the attachment section to ensure evaluations are well-supported, organized, and easily accessible, enabling effective oversight, supporting audits, and reducing the risk of regulatory breaches or service disruptions.

Possibility to add attachments

Covering
DORA Art. 28.3.c
RTS TP Art. 5.2
RTS Art. 6.1.a

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.



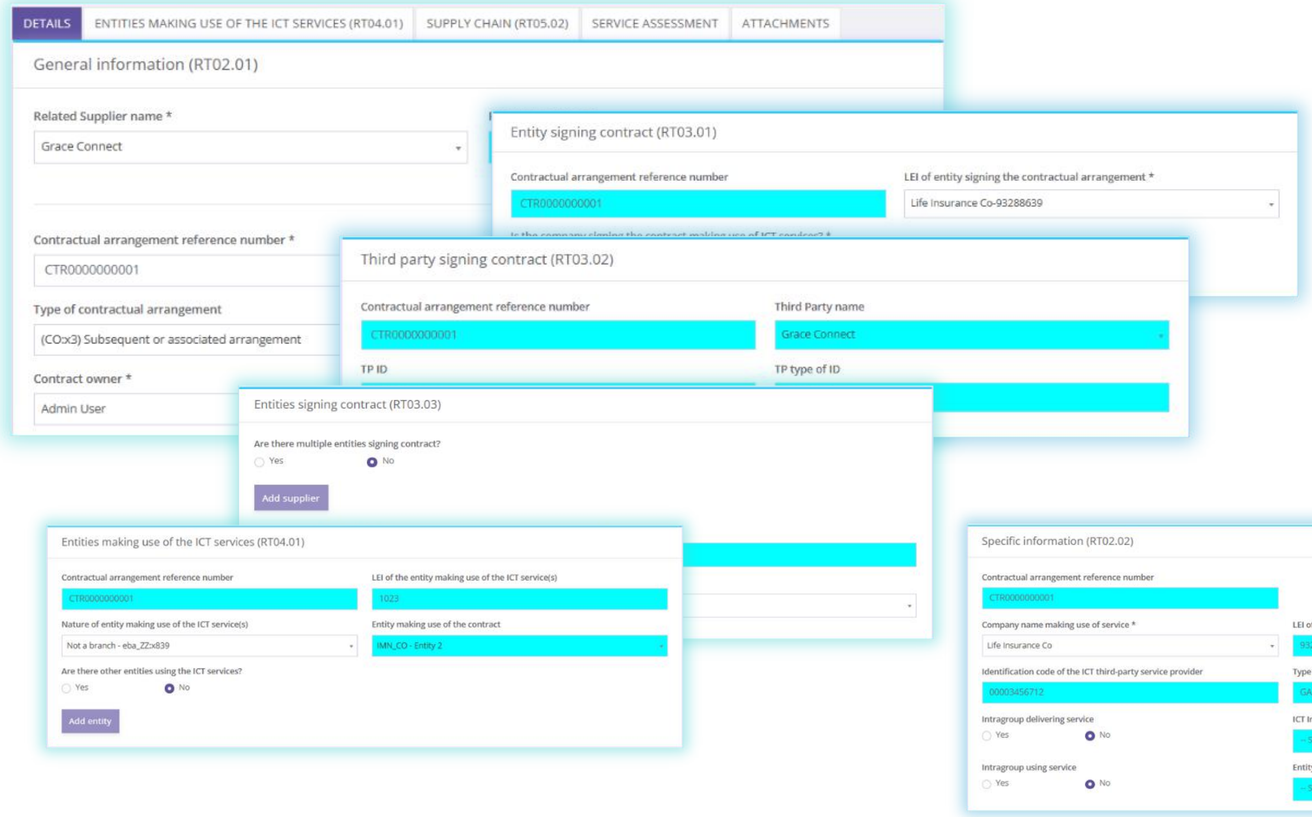
Possibility to add attachements

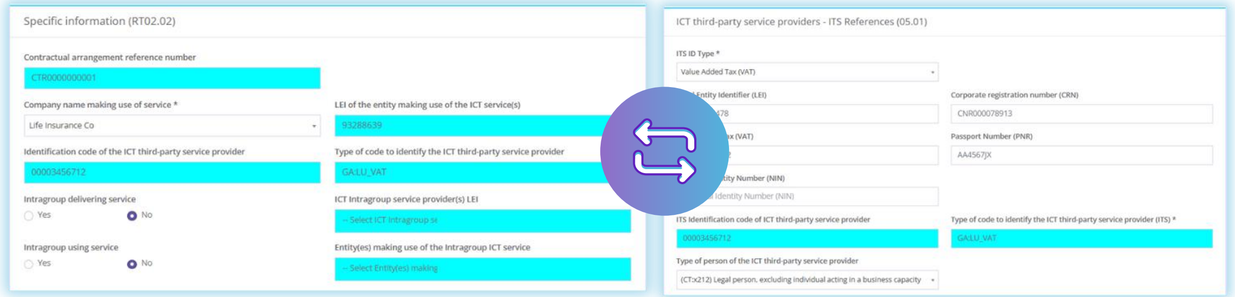
Detailed view of Outsourcing Risk Assessment

Covering
Art. 28.4.e
RTS TP Art. 8, 9
ITS all RoI
provisions

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.**





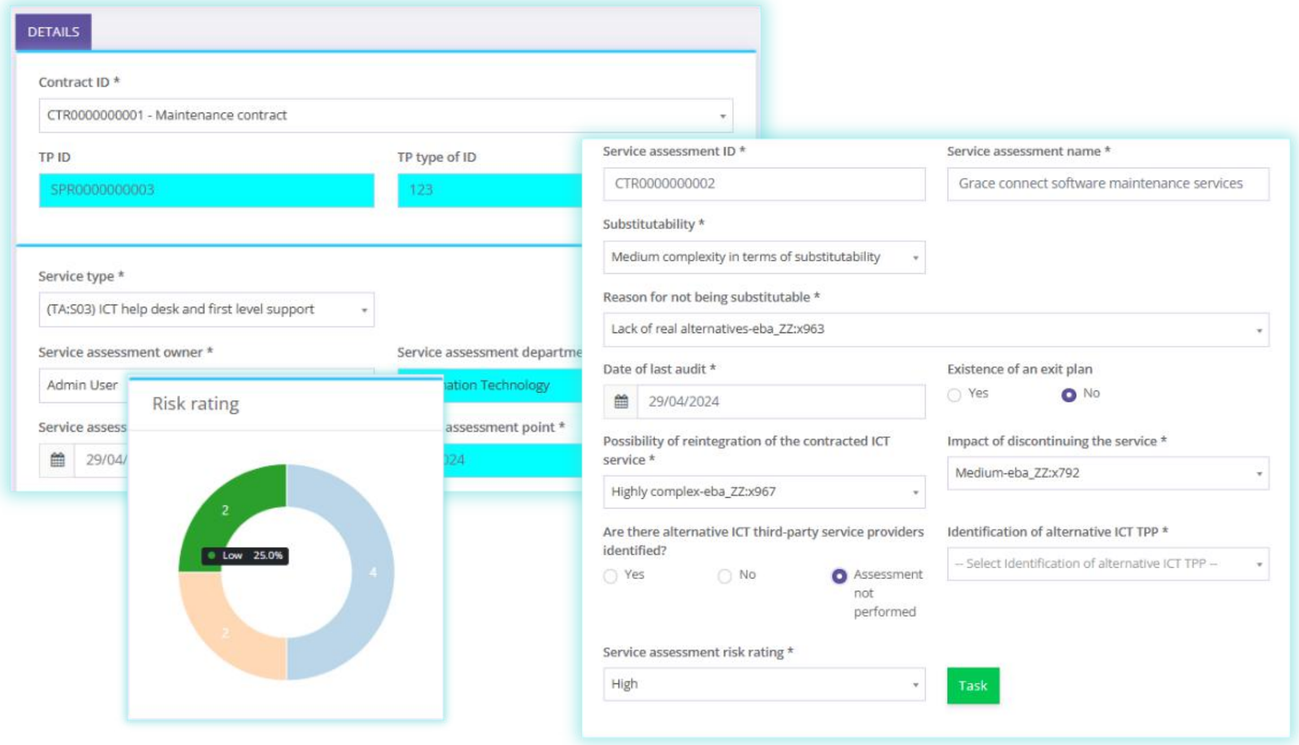
Contracts can be directly linked with suppliers in Grace Connect. This ensures that all necessary data **for the ITS Register of Information are already available in the required format for transmission to Competent Authorities.**

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

Covering All ITS RoI provisions

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.



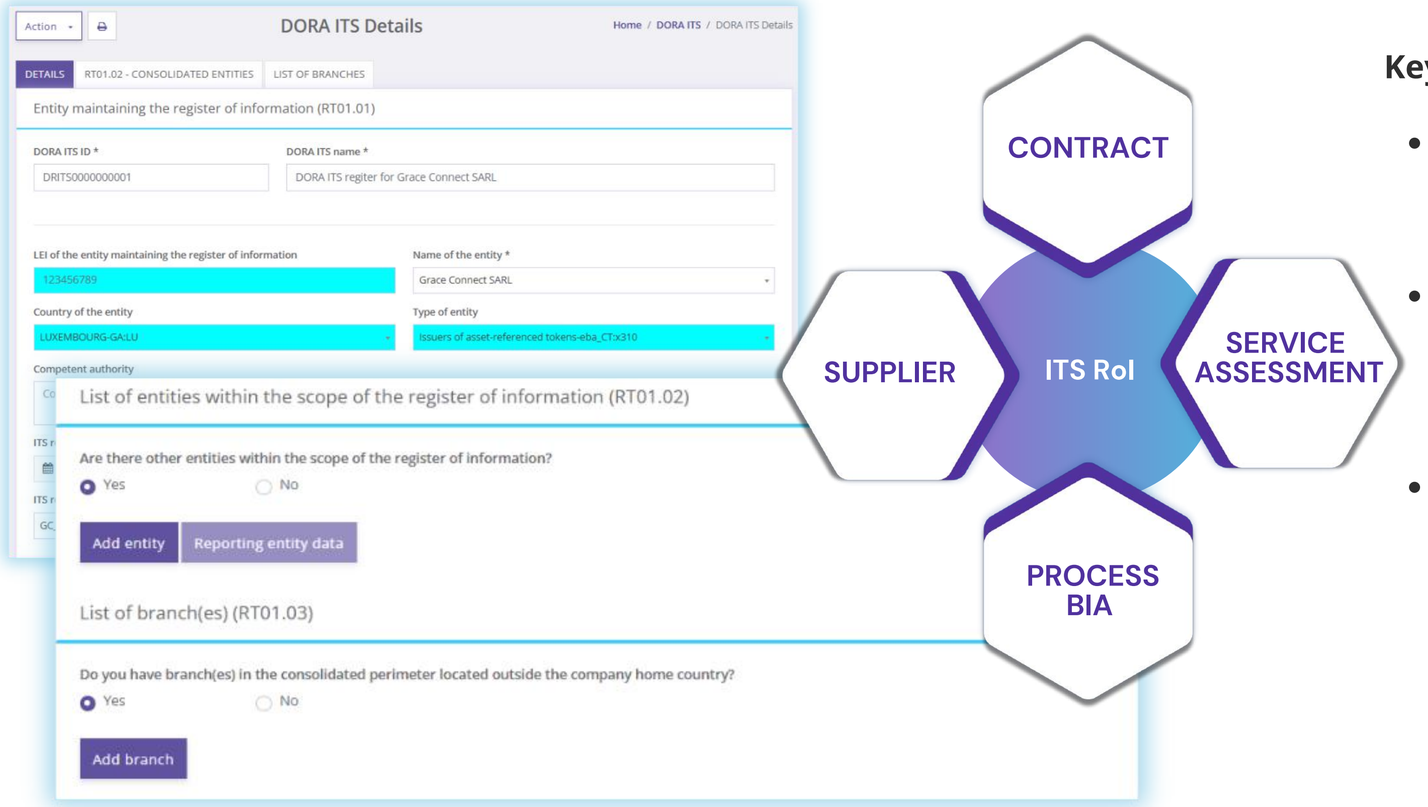
The module guarantees that **all necessary information for the Register of Information is incorporated**, enabling organizations to fully adhere to ITS RoI requirements.

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.

Covering All ITS RoI provisions

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.



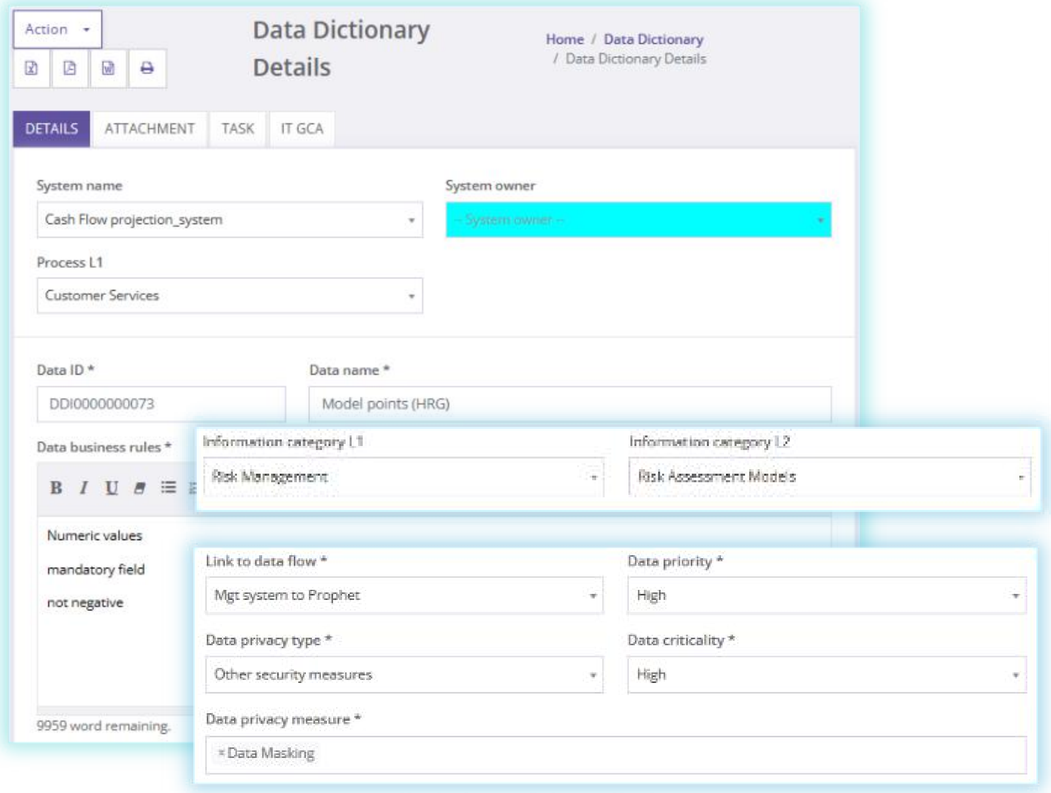
Key benefits:

- **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.

Covering
DORA Art. 12
RTS Risk Art. 5, 11

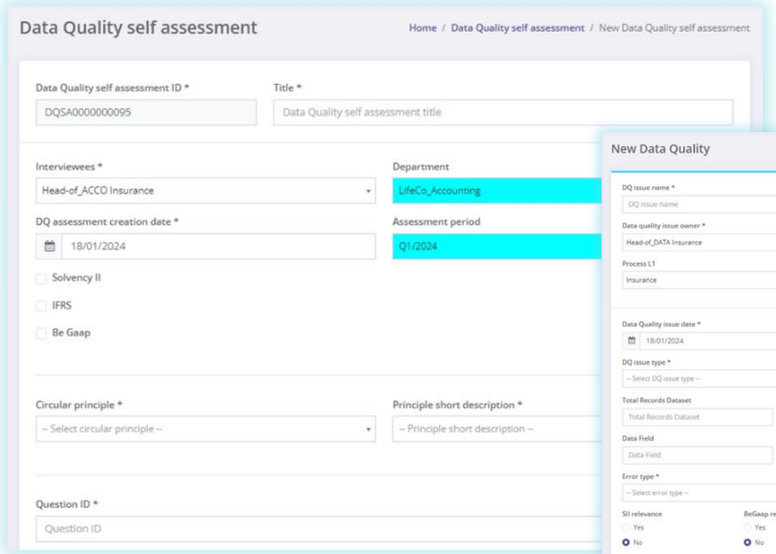
DATA RELATED MODULES IN GRC SUITE

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.

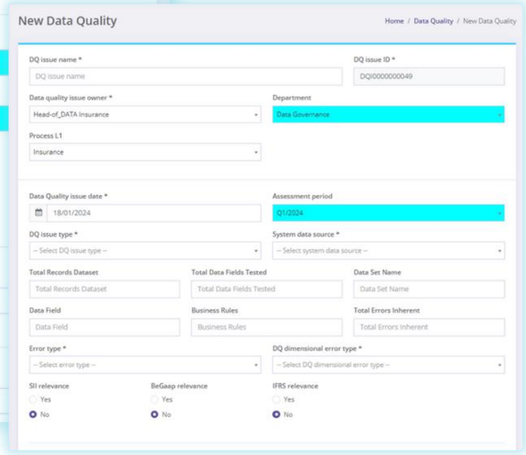


Detailed view of data dictionary

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.



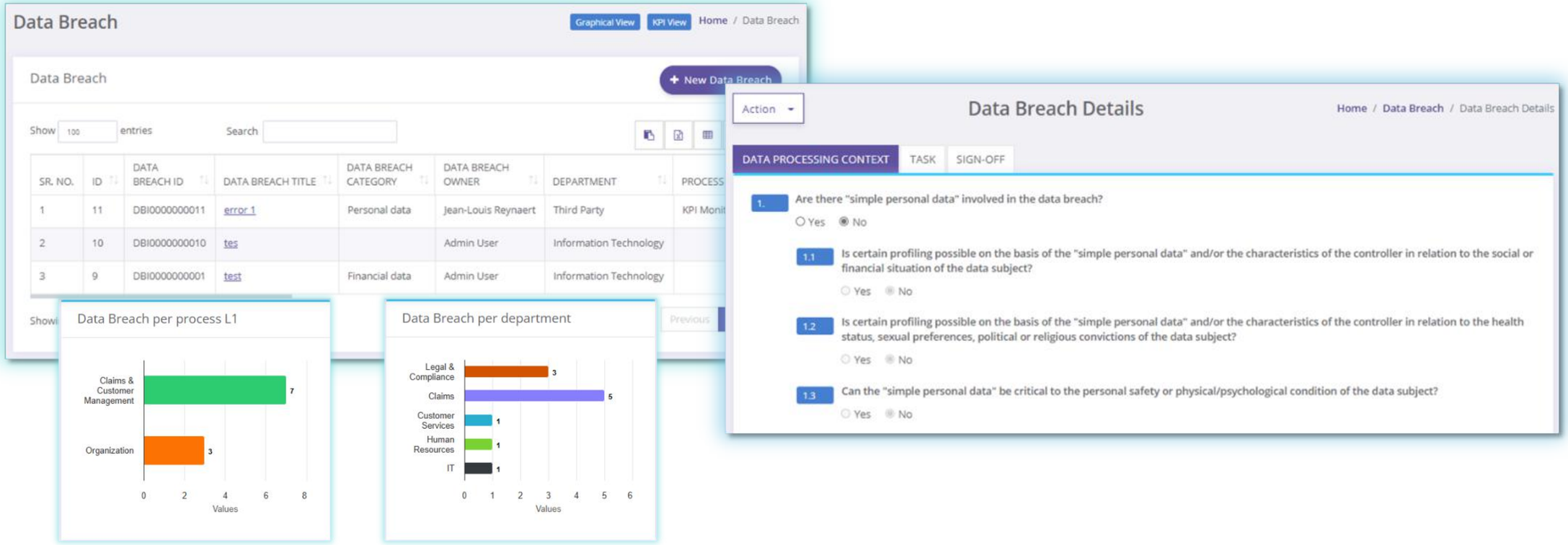
Detailed view of DQ Self-assessment



Detailed view of DQ issue

DATA BREACH MODULE IN GRC SUITE

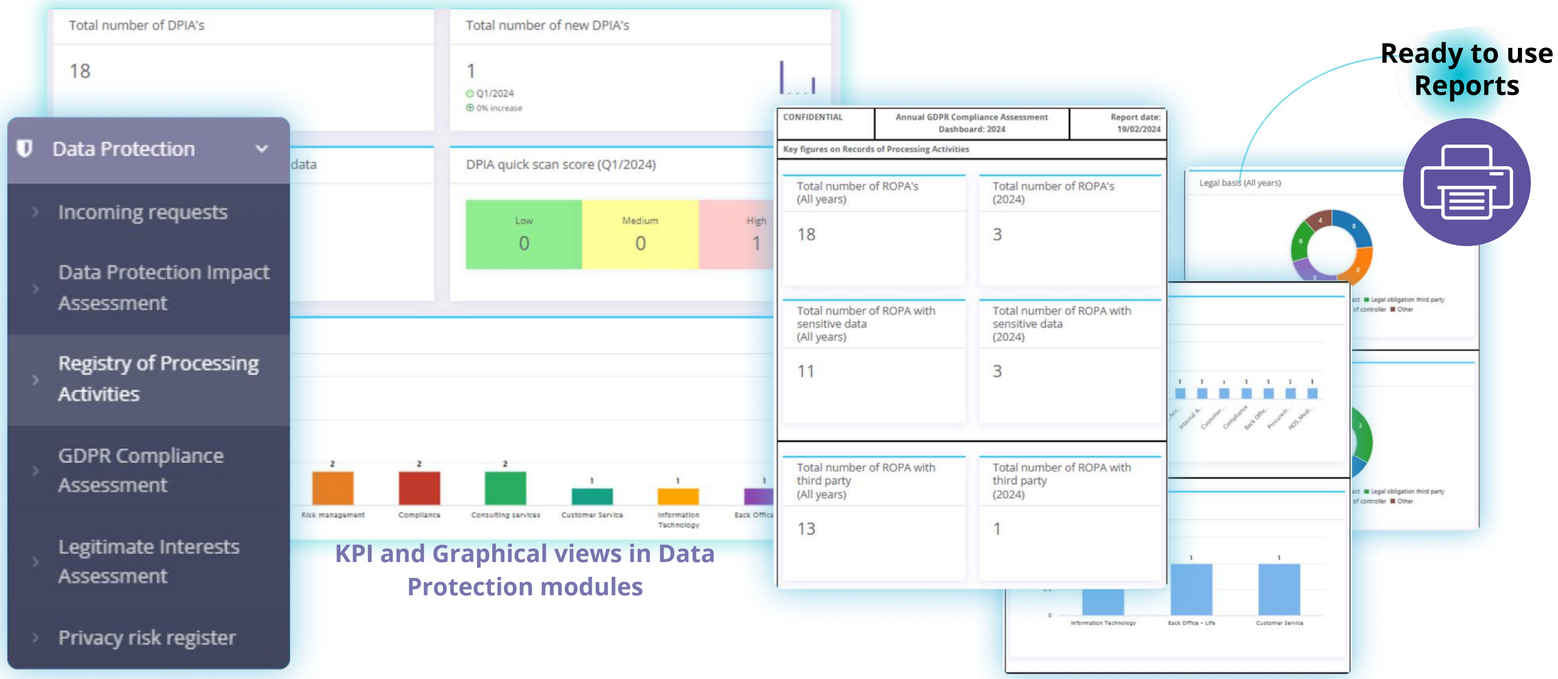
The list view of the **Data Breach module** provides users with all entries recorded. This enables to update graphs and KPI's.
The list includes all relevant data fields included in the data breach detailed form.



The 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.**



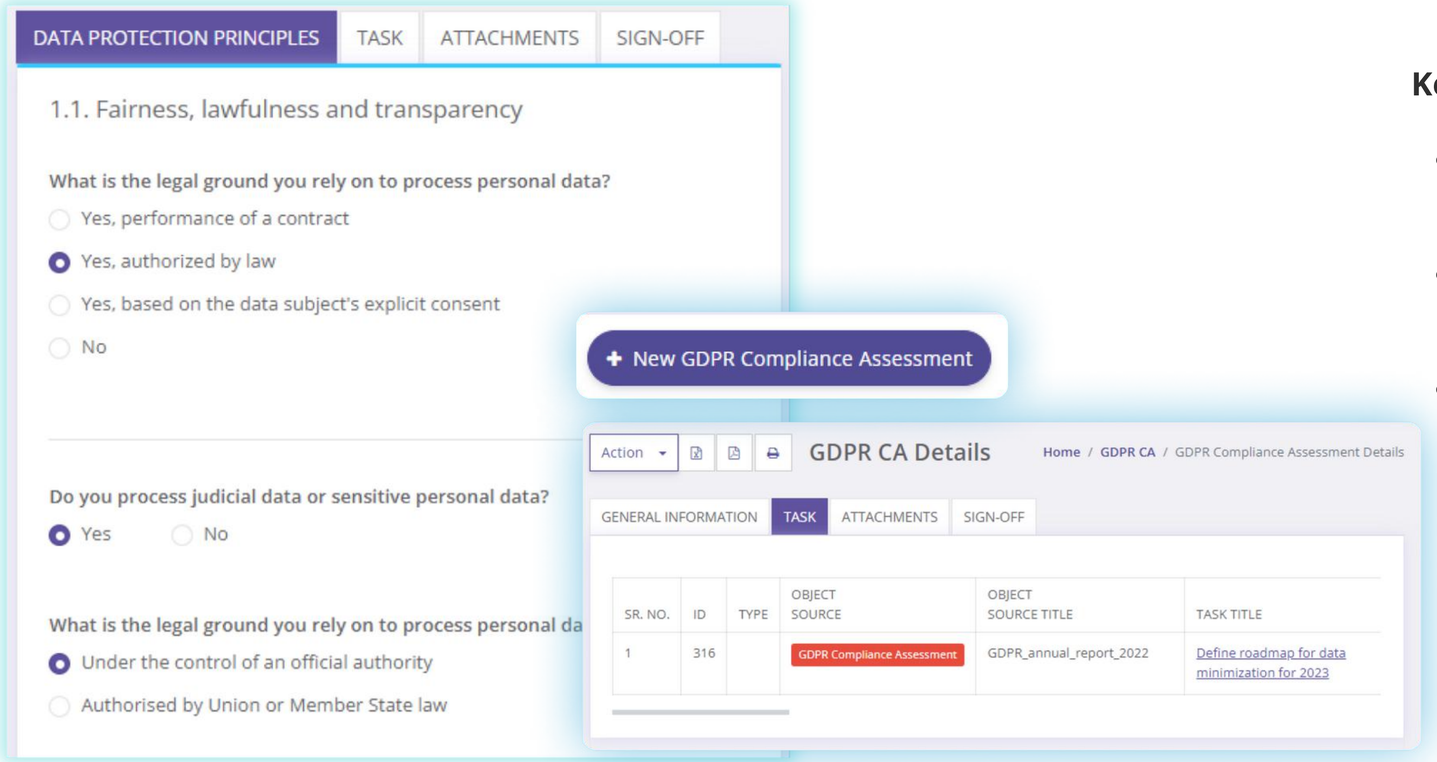
KPI and Graphical views in Data Protection modules

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.



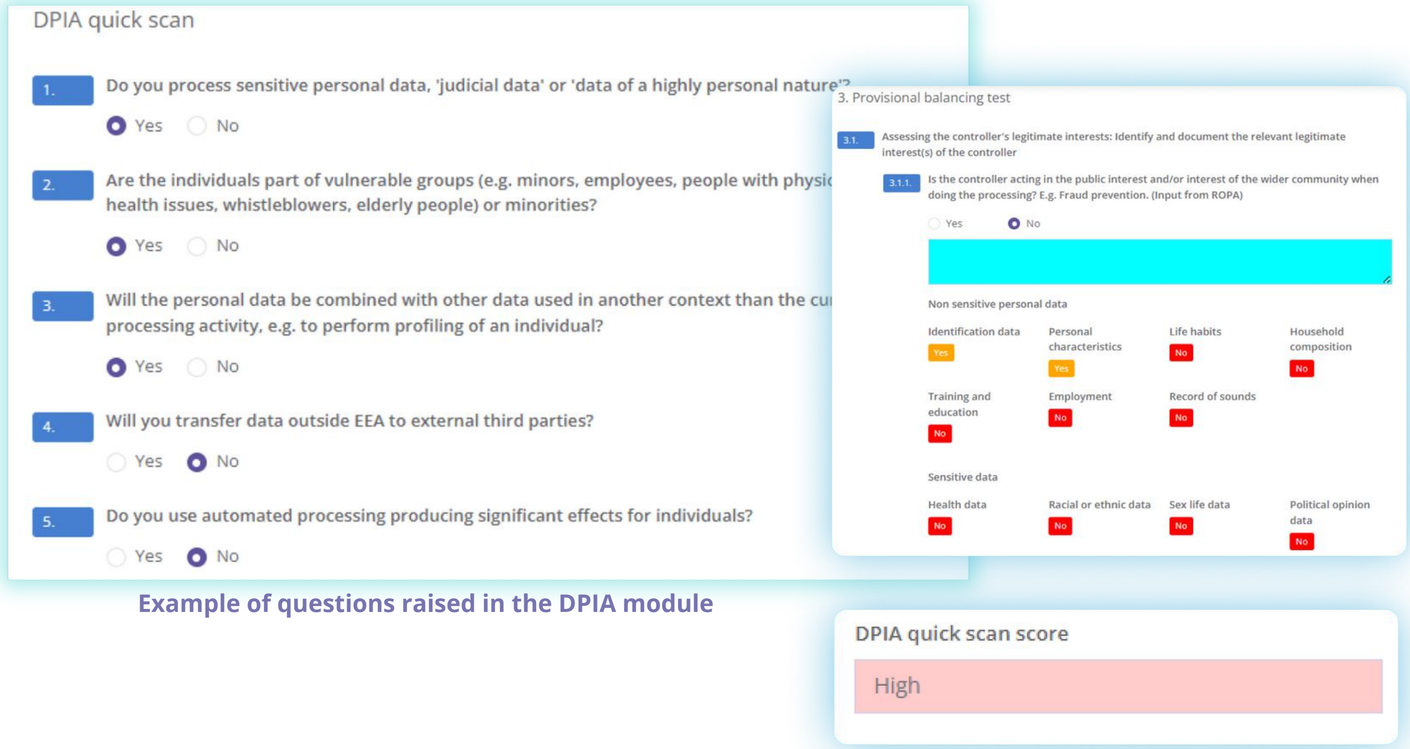
Example of questions raised in the GDPR CA module

Key Features & Benefits:

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

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.



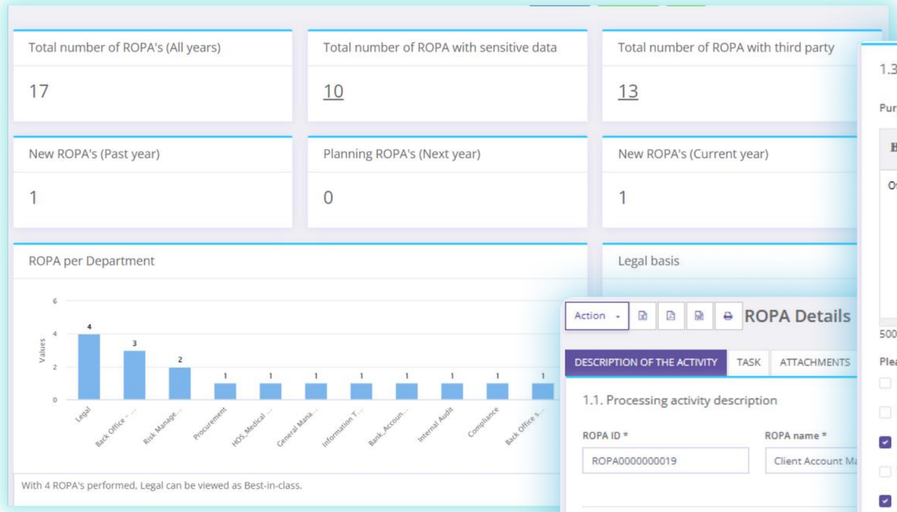
Example of questions raised in the DPIA module

Key Features & Benefits:

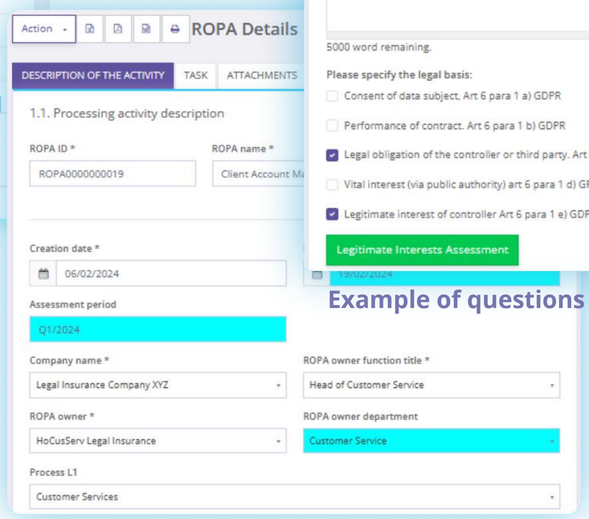
- Automated evaluation algorithms.
- Strengthen defenses against potential compliance violations.
- Seamless integration with your existing data privacy framework.
- Findings from DPIAs can update the ROPA with details on risk assessments and mitigations for high-risk processing activities.

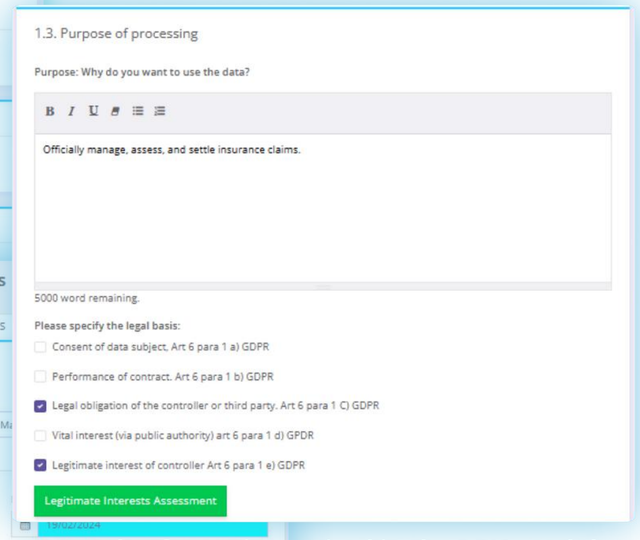
DATA PROTECTION MODULES
ROPA

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





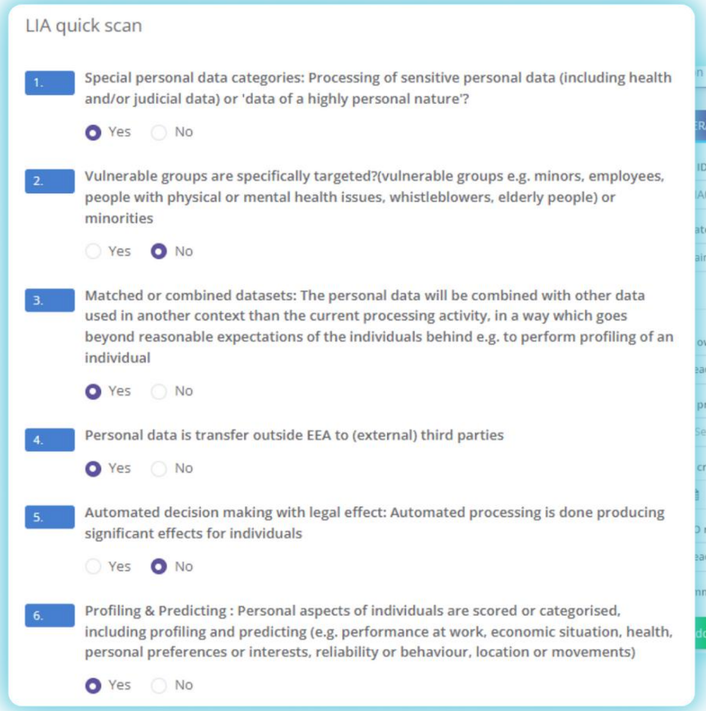
Example of questions raised in the DPIA module

Key Features & Benefits:

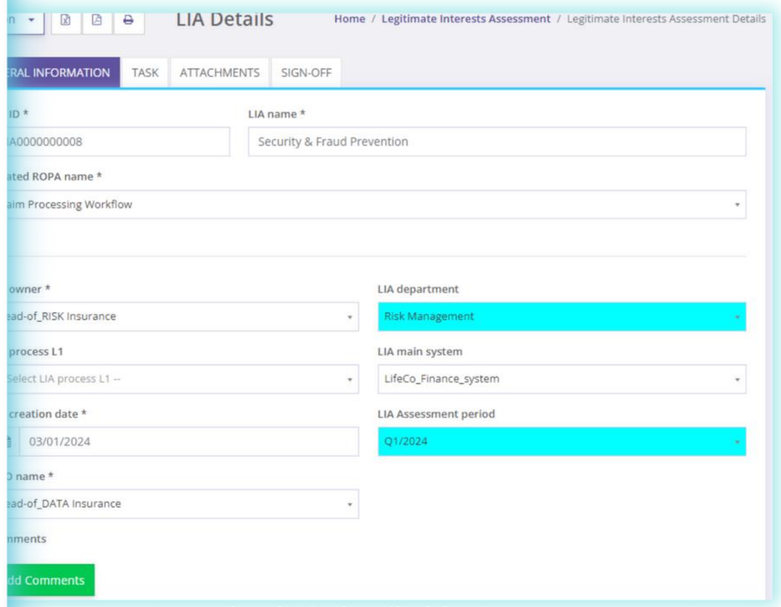
- Centralized repository to store all data processing activities in one organized location.
- Clarity and operational efficiency of your data governance framework.
- Easy-to-navigate interface for swift data retrieval.
- Based on ROPA final score a DPIA can be initiated directly from ROPA module.

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



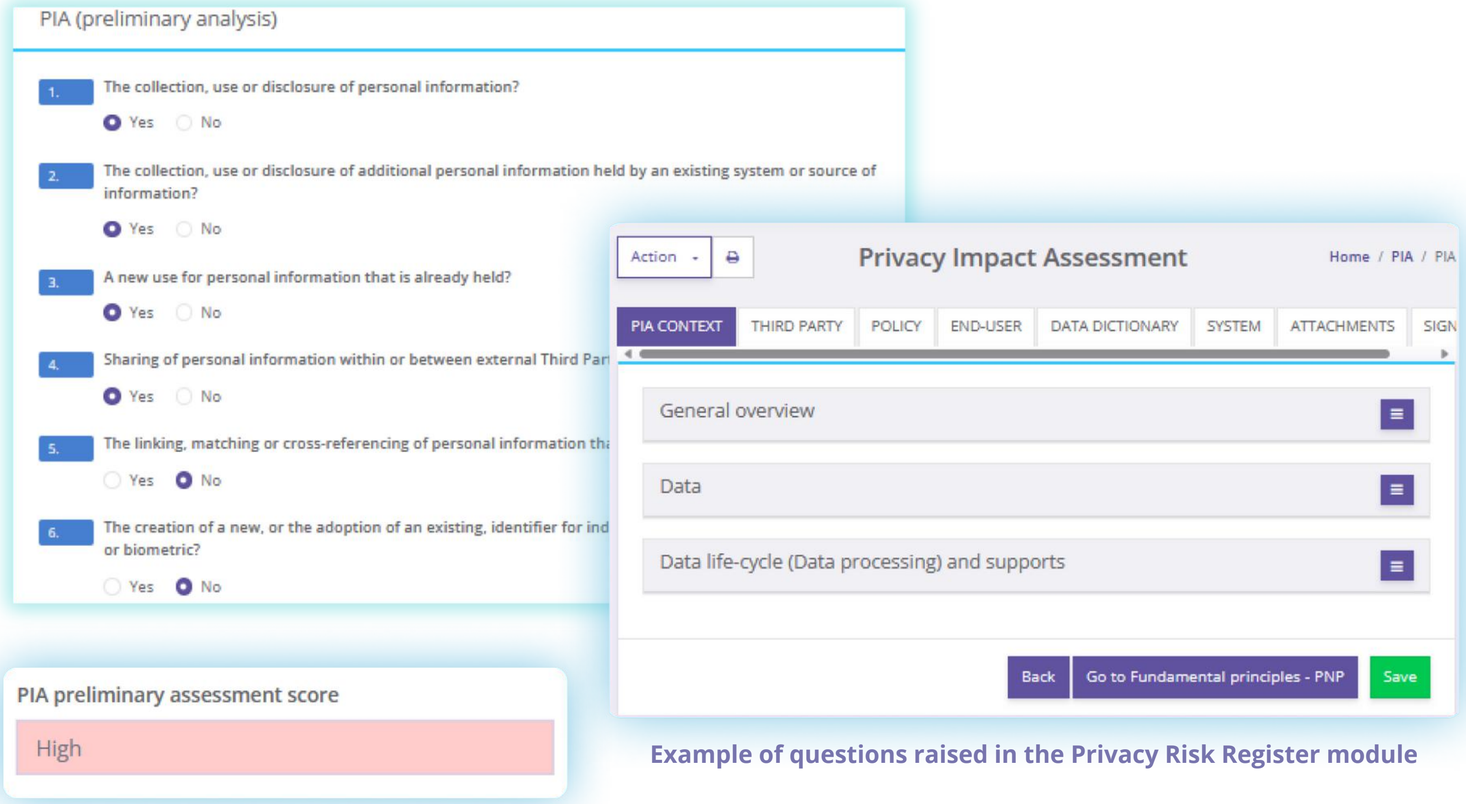
Example of questions raised in the LIA module



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.



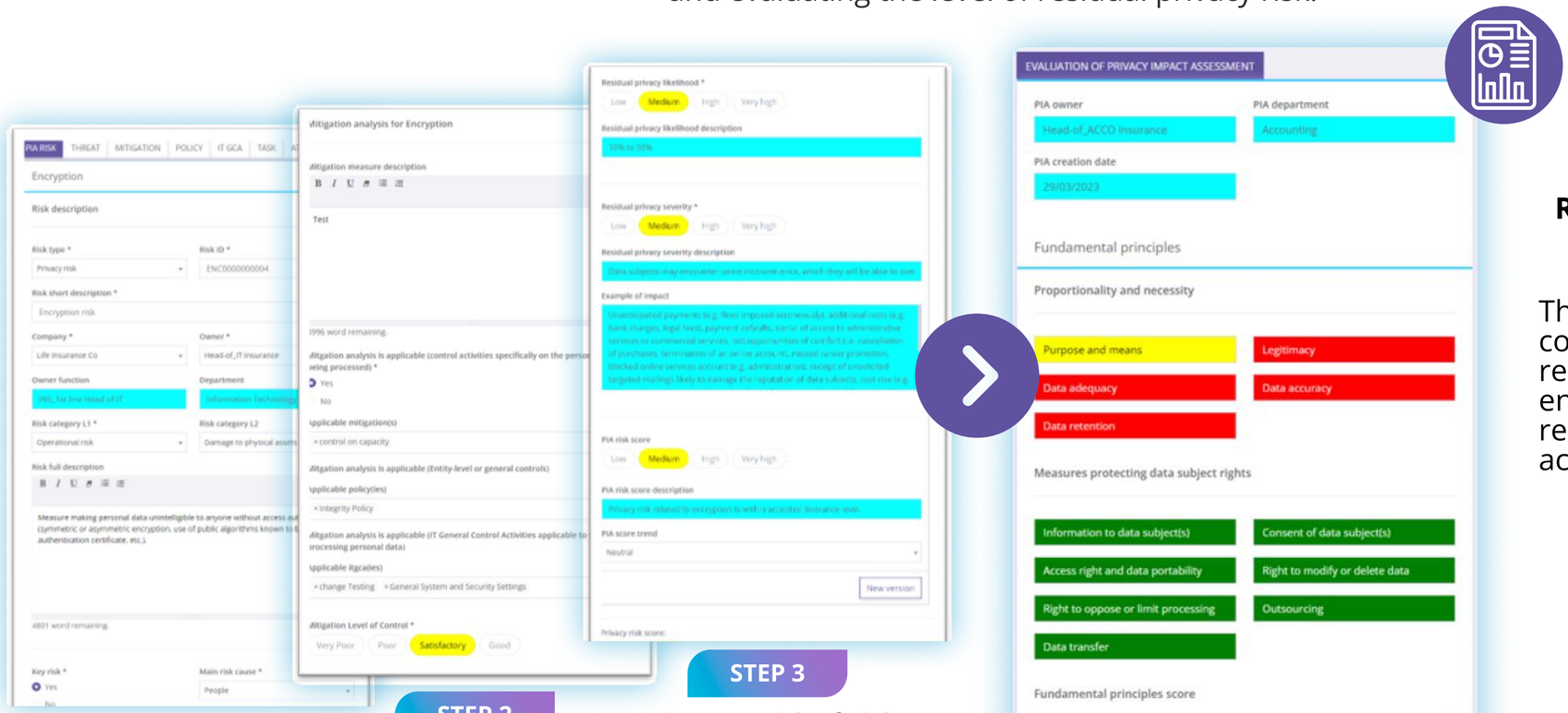
Example of questions raised in the Privacy Risk Register module

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.

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.



STEP 1

PIA inherent risk assessment

STEP 2

Applicable mitigation measures evaluation

STEP 3

Privacy residual risk assessment

Overview of ratings for fundamental principles

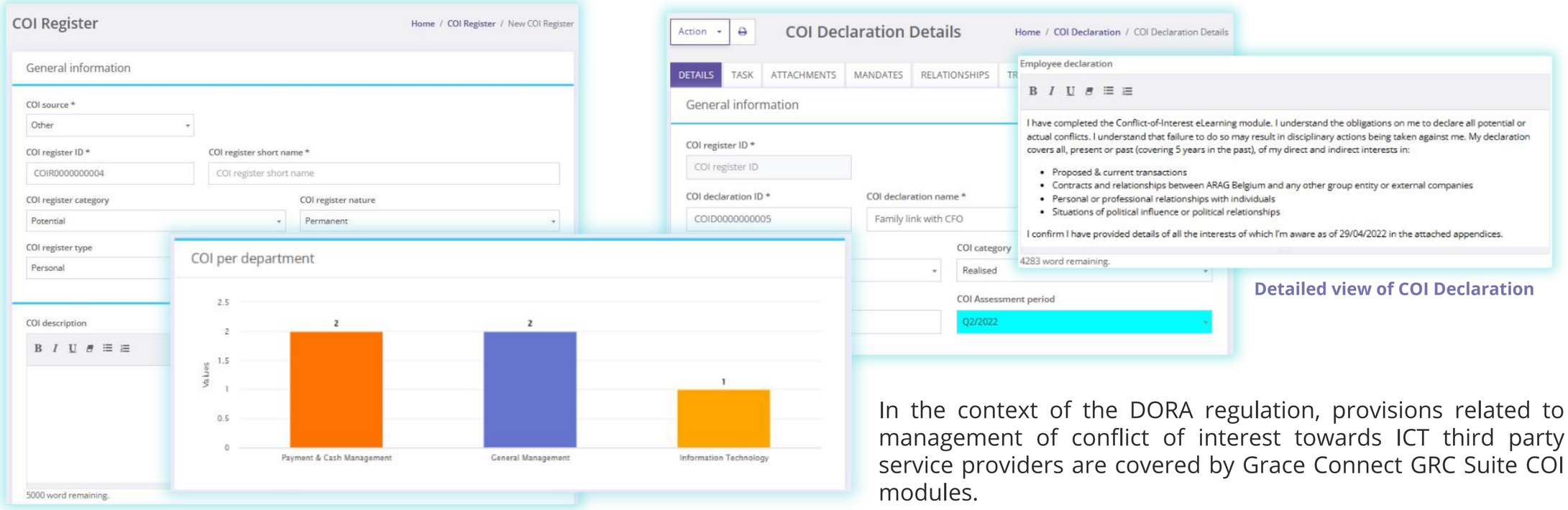
Reporting of residual privacy risks (summary page)

The summary page includes a color-code that illustrate the residual privacy risks for which end-users will have to create or request additional mitigation actions.

Covering
DORA Art. 28.4.e
RTS Risk Art. 2.2.g
RTS TP Art. 7

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.



Detailed and graphical view of COI Register

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

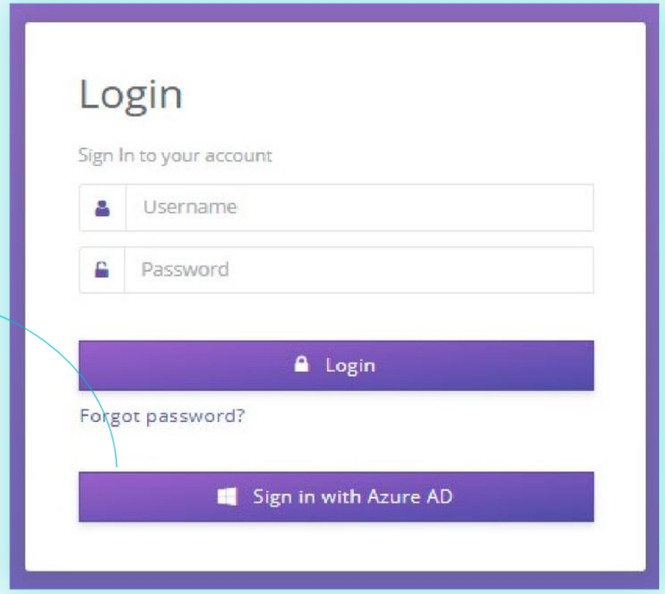
Graph view with number of Actions in the GRC Suite originated by all modules

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.

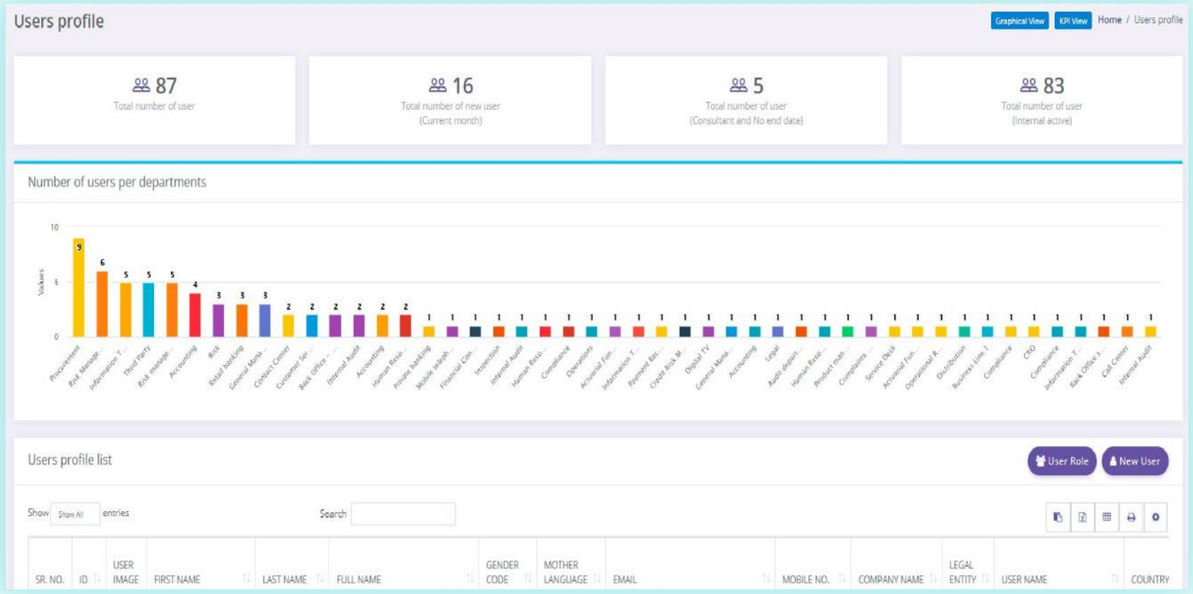
SECURITY EMBEDDED IN GRACE CONNECT GRC SUITE

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.



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.

Grace Connect SARL
is a member of the
LHOFT ecosystem

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.