GRC SUITE

General product presentation

2024

GRACE
CONNECT

KEY CHALLENGES OBSERVED

- **Non—Financial risks** are often managed in Excel, leading to inconsistency in files used to support Risk, Compliance, or Audit Functions.
- **Suboptimal qualitative risk aggregation and data integration.**
- **Time-consuming pivot tables** to manually copy/paste in PPT for management report (This approach is prone to errors).
- **Sub-standard management reporting.**
- **Lack of real time risk monitoring,** especially on most important topics to be handled by Senior Management (e.g. cyber threats).
- **Lack of dedicated resources** to prepare management reporting.
- Recent outbreak of **COVID-19** evidenced the need to have a **risk management approach** also for firms that are not subject to regulatory requirements (e.g. management of business risks).

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 Incapacity to anticipate risks, and usually P&L impacts following occurrence of risks.

3 Ad-hoc or incomplete internal control mechanisms.

4 Inefficiency in meeting changing regulatory requirements

MARKET GAP: RISK MANAGEMENT TOOL

- Based on observations, the best practice is to automate analytics and production of reports (and avoid using manual Excel).

- 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

- Existing GRC tools do not provide reliable solutions covering all domains contributing to a sound management of Non-Financial risks including Operational Risk, Privacy, Business Continuity, Cyber Security, Compliance, 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 GRC Suite has been designed to include all relevant modules supporting a smart and efficient deployment of a risk culture within your organization, while ensuring a smooth adherence to regulatory requirements.

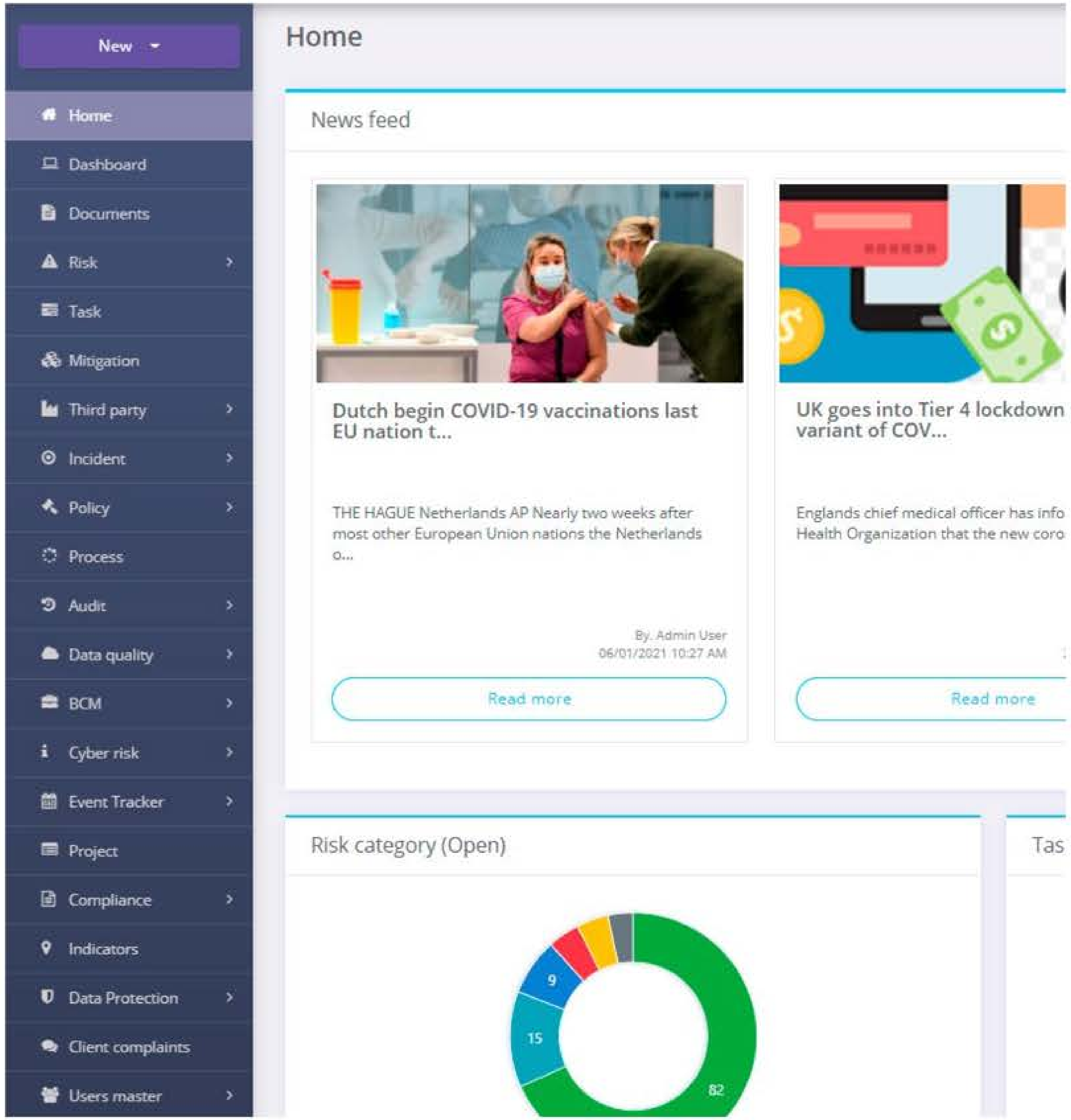
KEY DIFFERENTIATING FACTORS

- 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.
- Time dimension is embedded in the GRC Suite as it is usually better to anticipate risks and delivery dates.
- 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.
- 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	PROJECT
AUDIT & REPORTING	CMMI Capabilities	DATA PROTECTION	MITIGATION	RISK
BCM	COMPLIANCE	DATA QUALITY	NEW PRODUCT	RISK MANAGEMENT Self-Assessment
BCM Self-Assessment	COMPLIANCE QUATERLY REPORTING	DATA QUALITY Self-Assessment	POLICY	SYSTEM
CLIENT COMPLAINTS	COMPLIANCE TRAINING	EVENT TRACKER	PROCESS	THIRD PARTY
CMMI Assessment	CYBER RISK	INCIDENT	TASK	THREAT RADAR



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 o...

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

Read more

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

Englands chief medical officer has info Health Organization that the new coro

Read more

Risk category (Open)

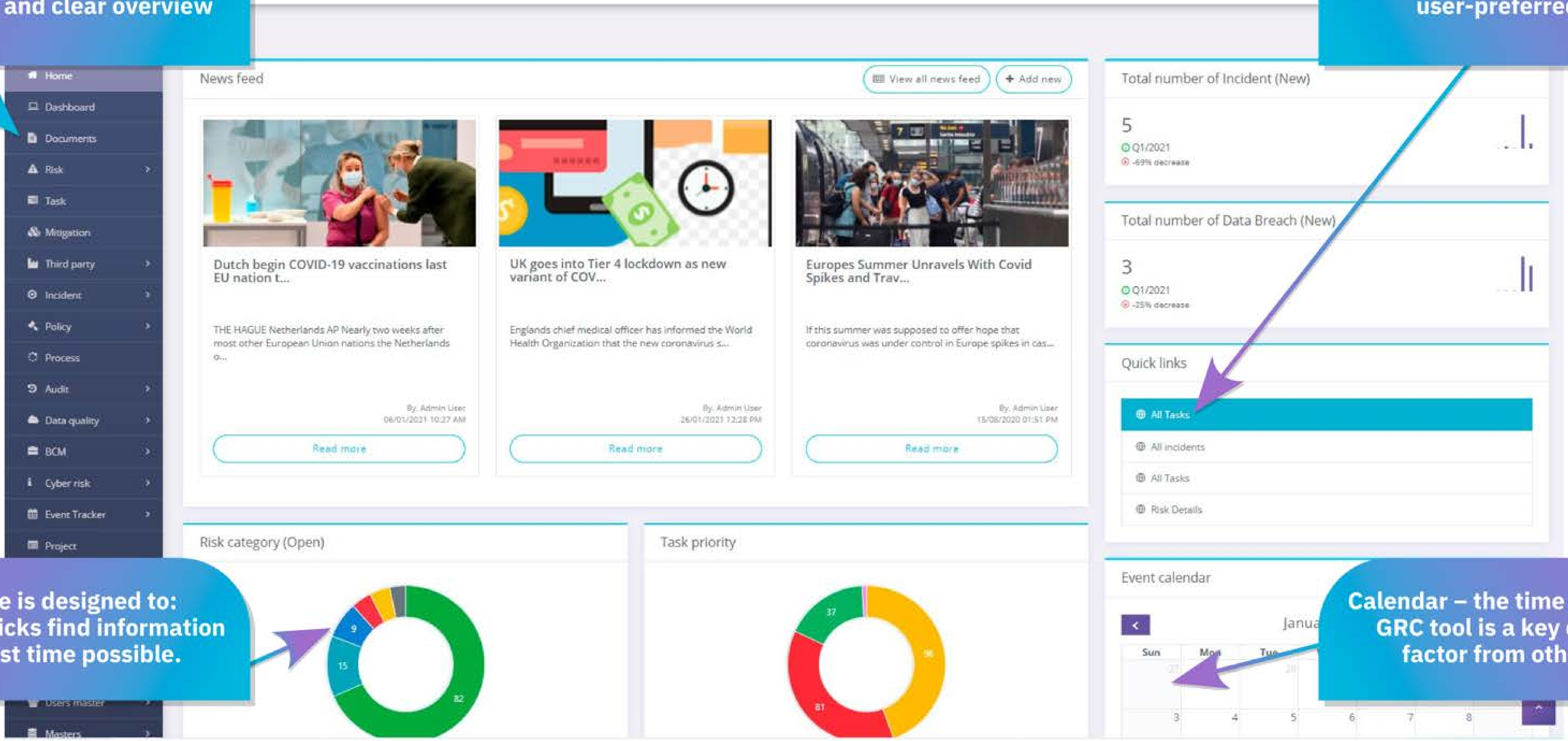
Tas

INTUITIVE TOOL WITH A USER-FRIENDLY LOOK AND FEEL

home page

List of subscribed modules for comprehensive and clear overview

Shortcuts to user-preferred modules



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 o...

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

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

Europes Summer Unravels With Covid Spikes and Trav...

If this summer was supposed to offer hope that coronavirus was under control in Europe spikes in cas...

By. Admin User
15/08/2020 01:51 PM

Total number of Incident (New)

5
Q1/2021
-69% decrease

Total number of Data Breach (New)

3
Q1/2021
-25% decrease

Quick links

Risk category (Open)

Task priority

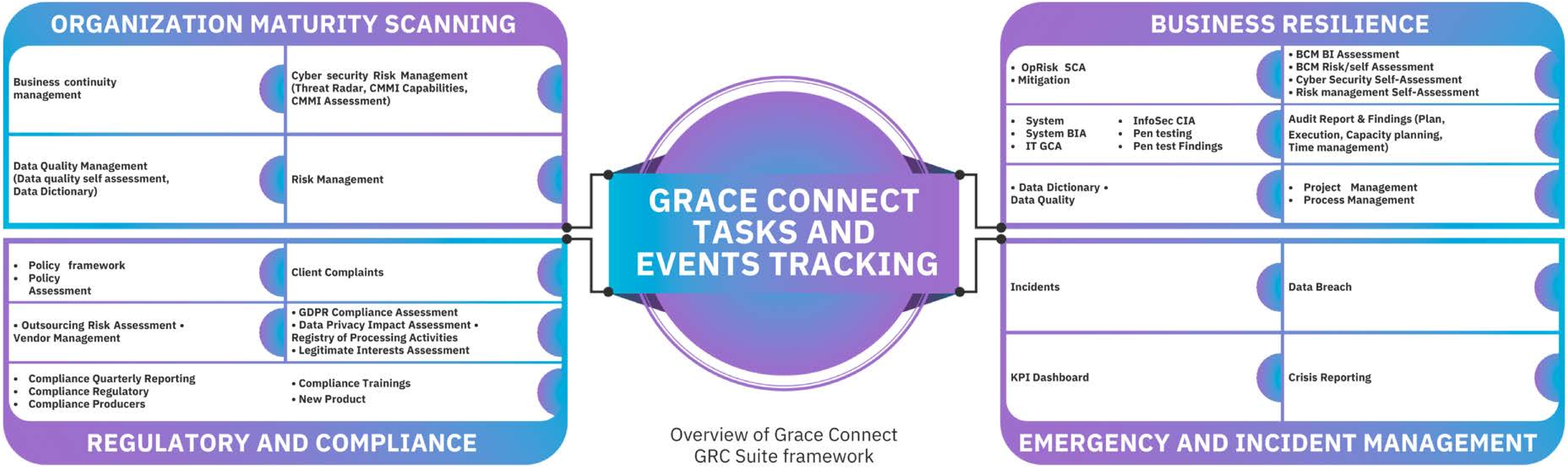
Event calendar

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

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

GRC SUITE ARTICULATED AROUND TASK TRACKING

All modules are designed to feed the Tasks tracking, putting organizations in action and enabling users to easily access their own tasks stored in the GRC Suite, even if they were created by another user and assigned to them.



ORGANIZATION MATURITY SCANNING

- Business continuity management
- Cyber security Risk Management (Threat Radar, CMMI Capabilities, CMMI Assessment)
- Data Quality Management (Data quality self assessment, Data Dictionary)
- Risk Management

REGULATORY AND COMPLIANCE

- Policy framework
- Policy Assessment
- Client Complaints
- Outsourcing Risk Assessment • Vendor Management
- GDPR Compliance Assessment
- Data Privacy Impact Assessment • Registry of Processing Activities
- Legitimate Interests Assessment
- Compliance Quarterly Reporting
- Compliance Regulatory
- Compliance Producers
- Compliance Trainings
- New Product

GRACE CONNECT TASKS AND EVENTS TRACKING

BUSINESS RESILIENCE

- OpRisk SCA
- Mitigation
- BCM BI Assessment
- BCM Risk/self Assessment
- Cyber Security Self-Assessment
- Risk management Self-Assessment
- System
- System BIA
- IT GCA
- InfoSec CIA
- Pen testing
- Pen test Findings
- Audit Report & Findings (Plan, Execution, Capacity planning, Time management)
- Data Dictionary • Data Quality
- Project Management
- Process Management

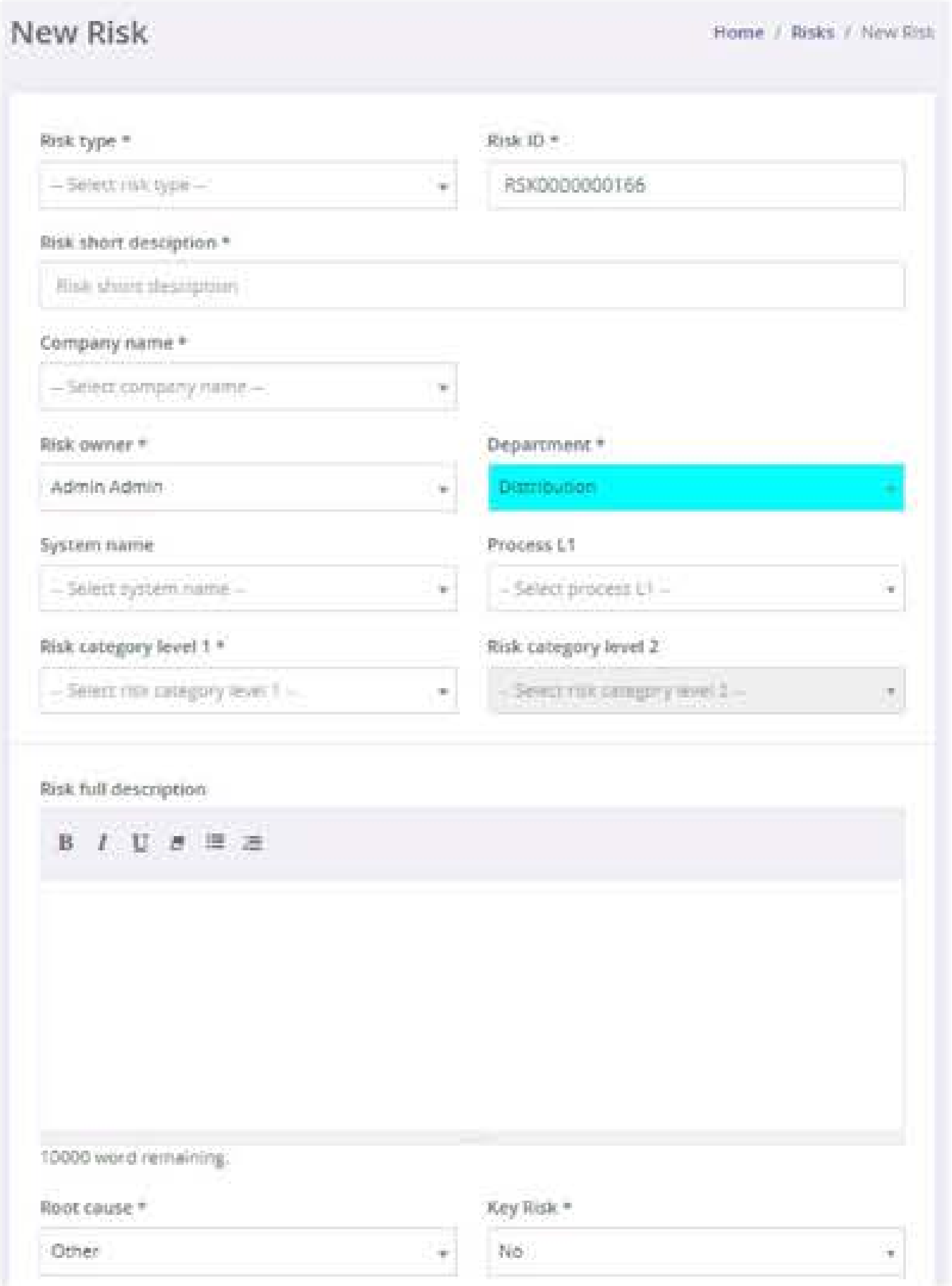
EMERGENCY AND INCIDENT MANAGEMENT

- Incidents
- Data Breach
- KPI Dashboard
- Crisis Reporting

Overview of Grace Connect GRC Suite framework

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.



New Risk

Home / Risks / New Risk

Risk type *: -- Select risk type --

Risk ID *: RSK0000000166

Risk short desciption *: Risk short desciption

Company name *: -- Select company name --

Risk owner *: Admin Admin

Department *: Distribution

System name: -- Select system name --

Process L1: -- Select process L1 --

Risk category level 1 *: -- Select risk category level 1 --

Risk category level 2: -- Select risk category level 2 --

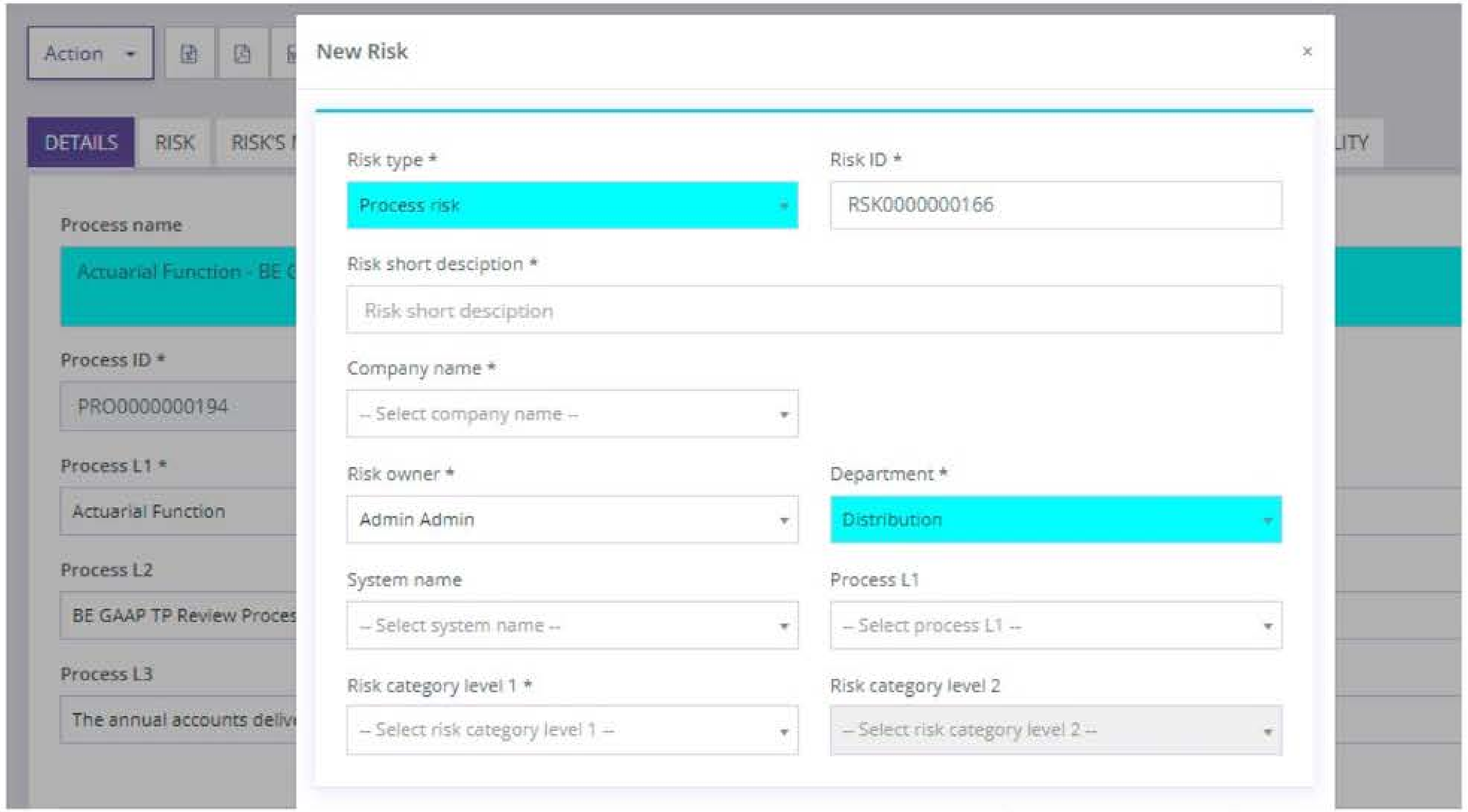
Risk full description

10000 word remaining.

Root cause *: Other

Key Risk *: No

User input form
(New risk)



Process name: Actuarial Function - BE C

Process ID *: PRO0000000194

Process L1 *: Actuarial Function

Process L2: BE GAAP TP Review Proces

Process L3: The annual accounts deliv

New Risk ×

Risk type *: Process risk

Risk ID *: RSK0000000166

Risk short desciption *: Risk short desciption

Company name *: -- Select company name --

Risk owner *: Admin Admin

Department *: Distribution

System name: -- Select system name --

Process L1: -- Select process L1 --

Risk category level 1 *: -- Select risk category level 1 --

Risk category level 2: -- Select risk category level 2 --

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.

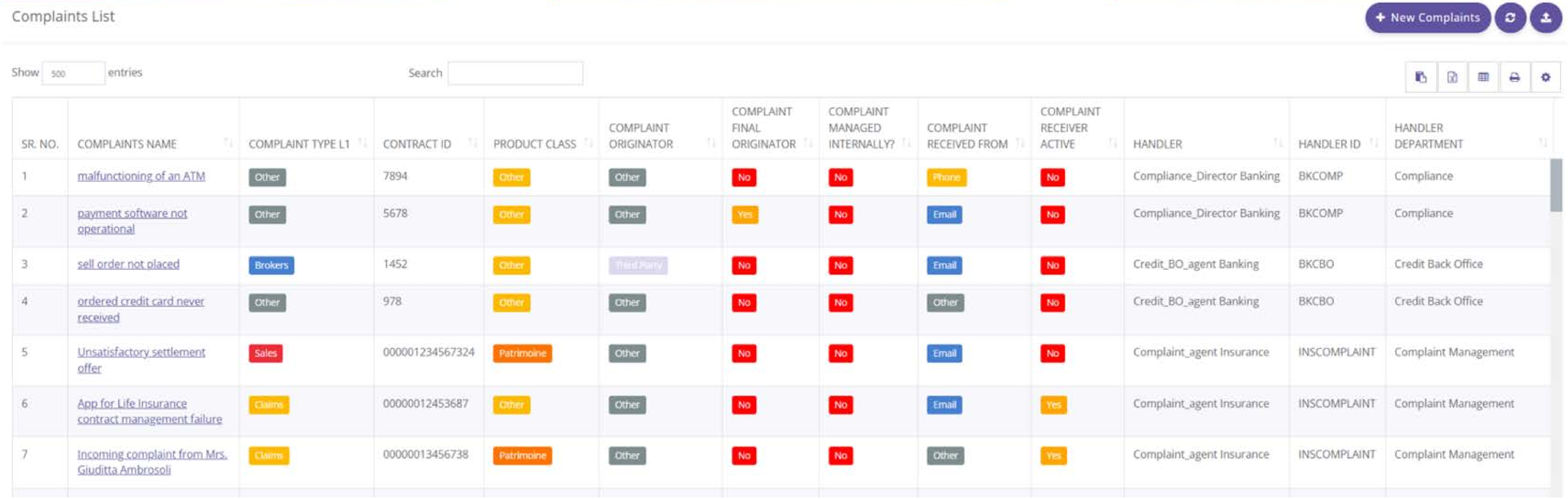
HOMOGENEOUS LIST VIEW THROUGHOUT ALL MODULES

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

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	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.

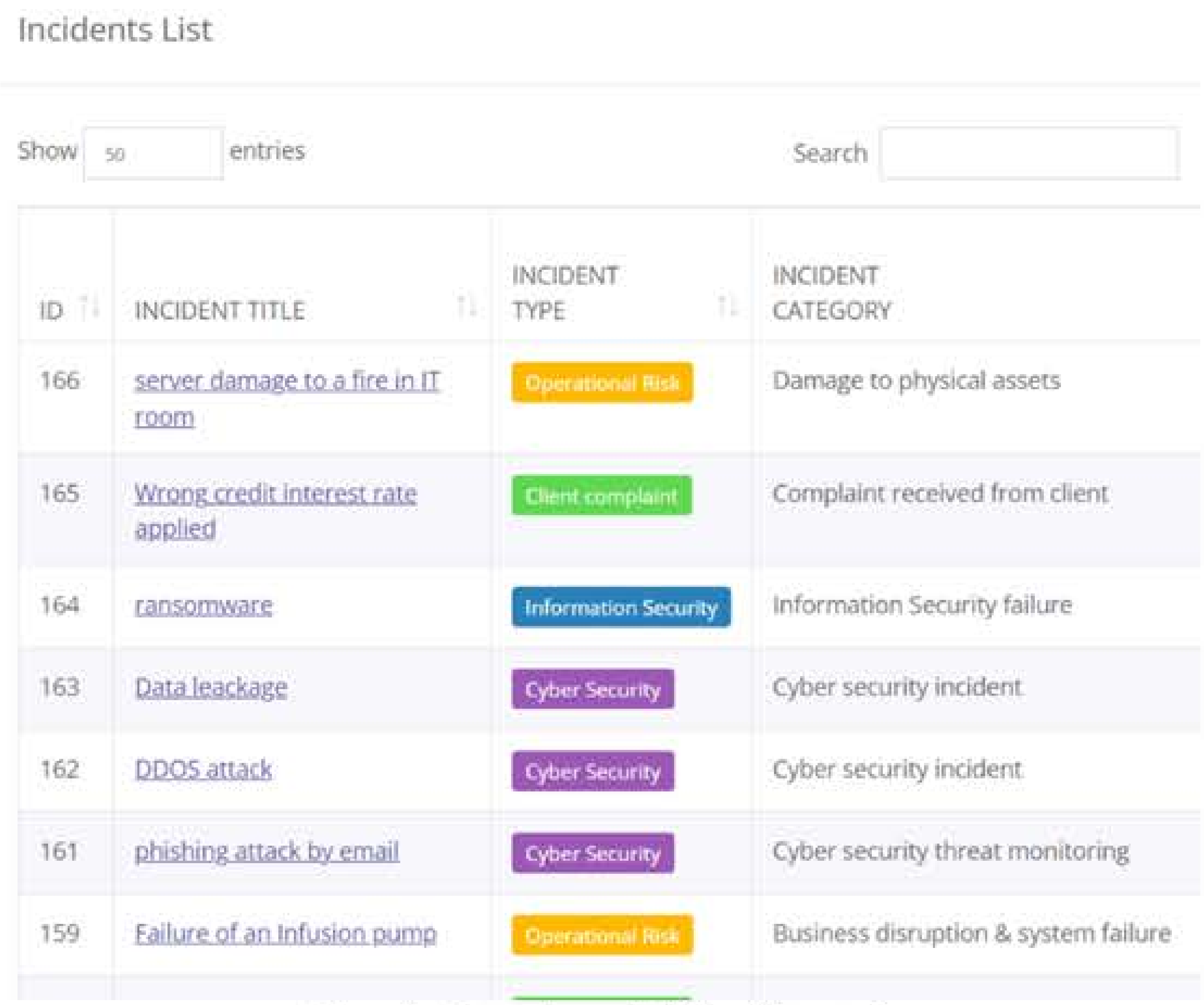
WORKFLOW-BASED INCIDENT MANAGEMENT MODULE

Incident page enables users to record and manage incidents in Grace Connect.
Not only Operational Risk incidents, but also other categories such as:

data quality issues

cyber security incidents

data breaches (GDPR requirement)

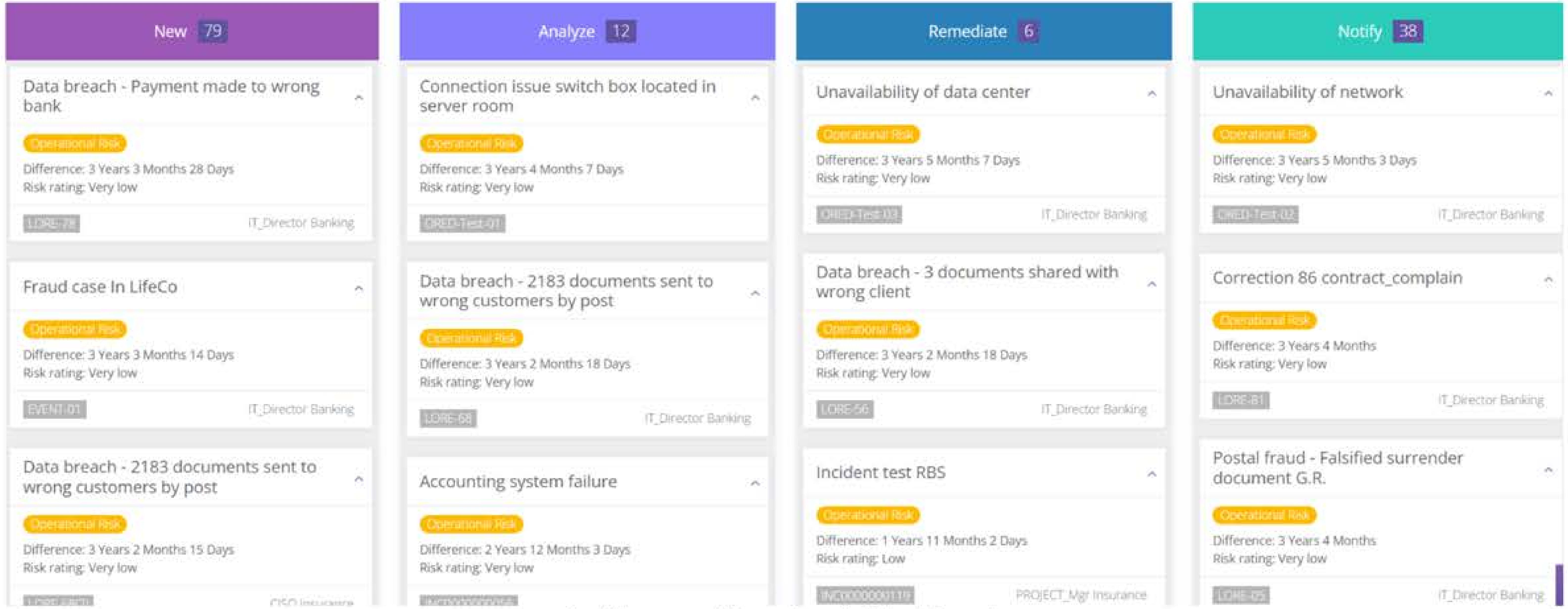


Incidents List

Show 50 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 leackage	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

Simple list view (all incidents)



New 79

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

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 15 Days
Risk rating: Very low
CISO Insurance

Analyze 12

Connection issue switch box located in server room
Operational Risk
Difference: 3 Years 4 Months 7 Days
Risk rating: Very low
ORED-Test-01

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

Accounting system failure
Operational Risk
Difference: 2 Years 12 Months 3 Days
Risk rating: Very low

Remediate 6

Unavailability of data center
Operational Risk
Difference: 3 Years 5 Months 7 Days
Risk rating: Very low
ORED-Test-03 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-56 IT_Director Banking

Incident test RBS
Operational Risk
Difference: 1 Years 11 Months 2 Days
Risk rating: Low
INC000000001119 PROJECT_Mgr Insurance

Notify 38

Unavailability of network
Operational Risk
Difference: 3 Years 5 Months 3 Days
Risk rating: Very low
ORED-Test-02 IT_Director Banking

Correction 86 contract_complain
Operational Risk
Difference: 3 Years 4 Months
Risk rating: Very low
LORE-81 IT_Director Banking

Postal fraud - Falsified surrender document G.R.
Operational Risk
Difference: 3 Years 4 Months
Risk rating: Very low
LORE-05 IT_Director Banking

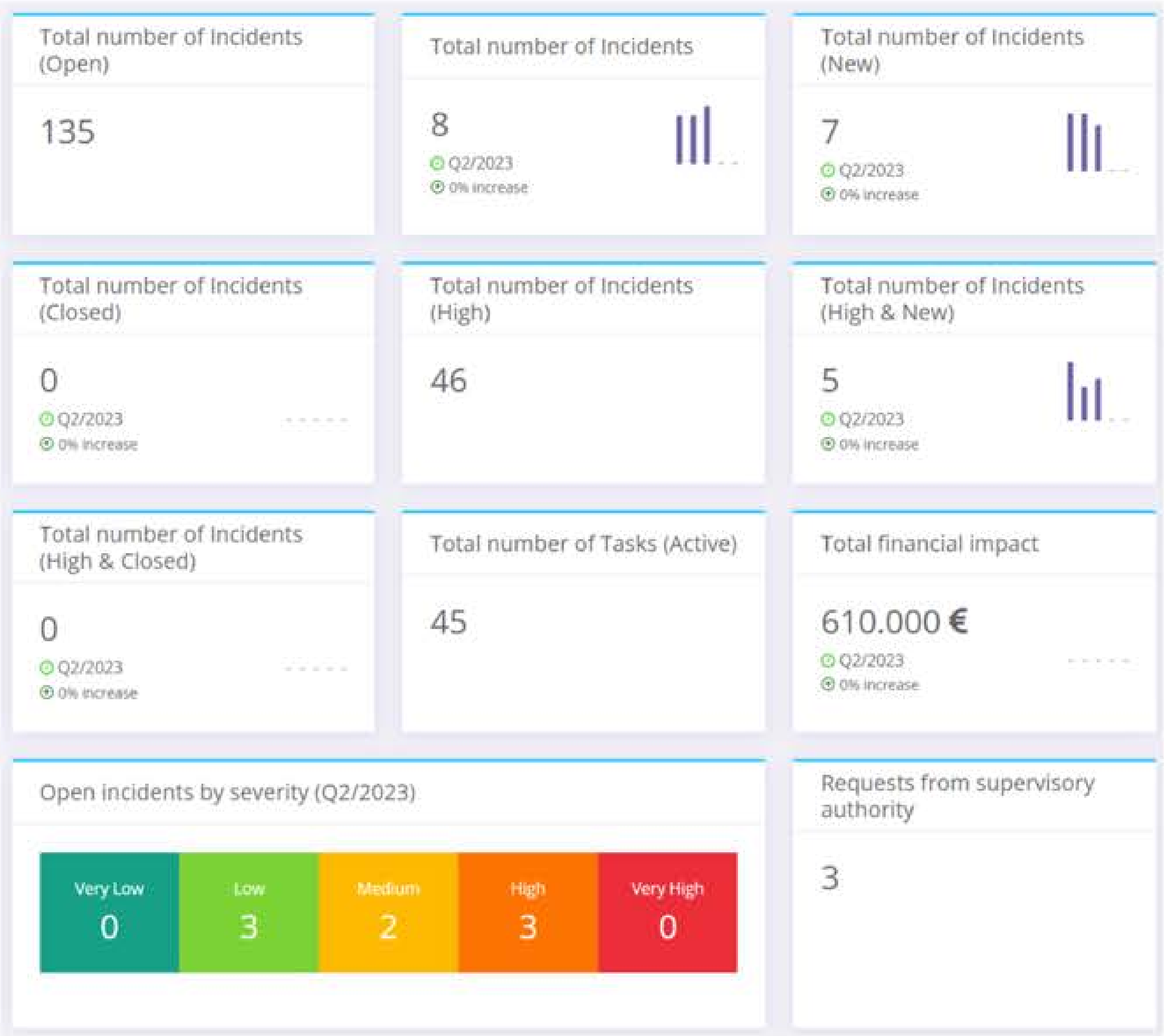
Incident tracking view (all incidents)

Incidents are listed and illustrated with predefined graphs and are an input to Key Performance indicators.
This allows users to have a direct views on burning issues with possible P&L impacts.

Possible connection with JIRA (through API)

WORKFLOW-BASED INCIDENT MANAGEMENT MODULE

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



Total number of Incidents (Open)
135

Total number of Incidents
8
Q2/2023
0% increase

Total number of Incidents (New)
7
Q2/2023
0% increase

Total number of Incidents (Closed)
0
Q2/2023
0% increase

Total number of Incidents (High)
46

Total number of Incidents (High & New)
5
Q2/2023
0% increase

Total number of Incidents (High & Closed)
0
Q2/2023
0% increase

Total number of Tasks (Active)
45

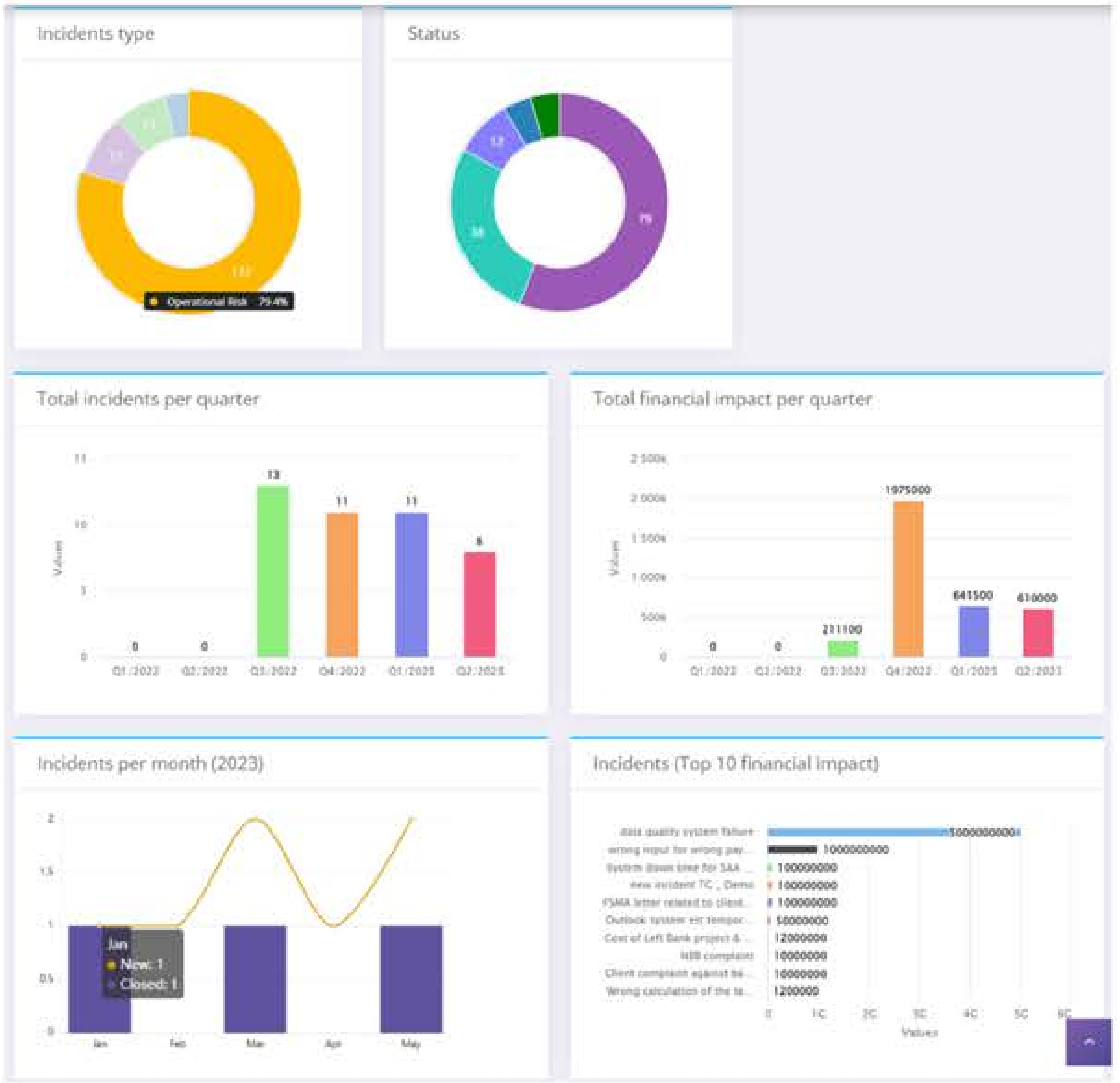
Total financial impact
610.000 €
Q2/2023
0% increase

Open incidents by severity (Q2/2023)

Very Low	Low	Medium	High	Very High
0	3	2	3	0

Requests from supervisory authority
3

KPI's view (all incidents)

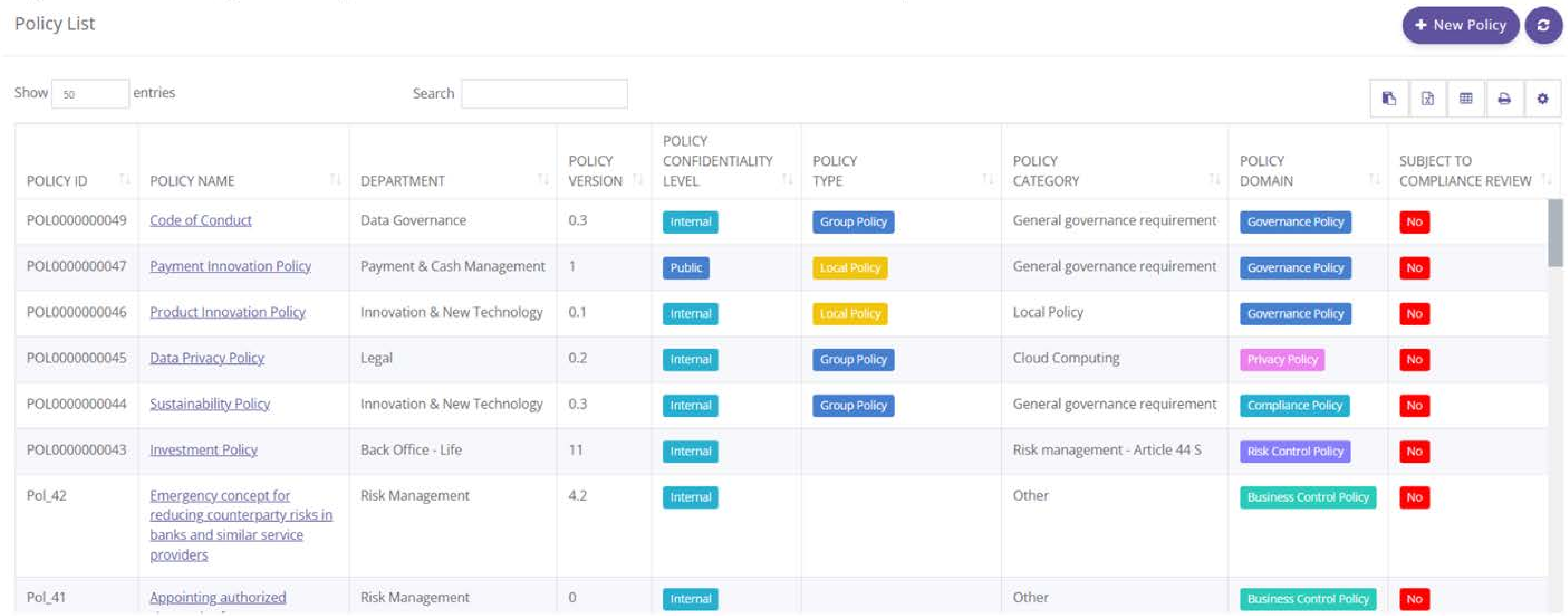


Graph view (all incidents)

KPI's and graphs uploaded in the GRC Suite provide a comprehensive view on **incidents.**
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

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).

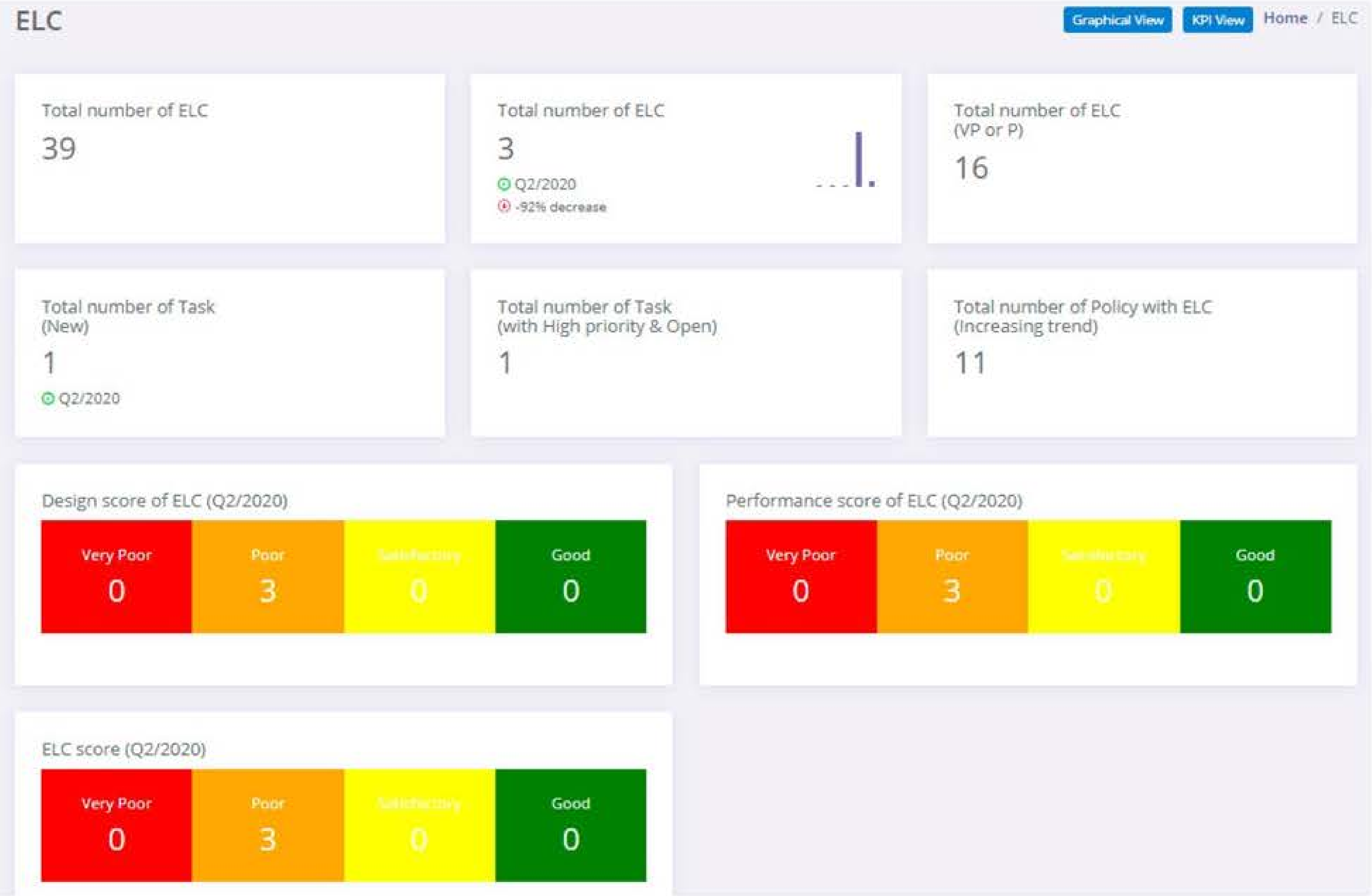
POLICIES ASSESSMENT (PART OF INTERNAL CONTROL)

“Entity-level Control” assessment module

To ensure compliance with local regulatory requirements

and/
or expectations from a parent company, an **“Entity-level Control” assessment module** is available in the GRC Suite.

This module will allow policy owners to assess the design of their policies and the extent to which they are operationally and by design effective in their organization.



Total number of ELC
39

Total number of ELC
3
Q2/2020
-92% decrease

Total number of ELC (VP or P)
16

Total number of Task (New)
1
Q2/2020

Total number of Task (with High priority & Open)
1

Total number of Policy with ELC (Increasing trend)
11

Design score of ELC (Q2/2020)

Very Poor	Poor	Satisfactory	Good
0	3	0	0

Performance score of ELC (Q2/2020)

Very Poor	Poor	Satisfactory	Good
0	3	0	0

ELC score (Q2/2020)

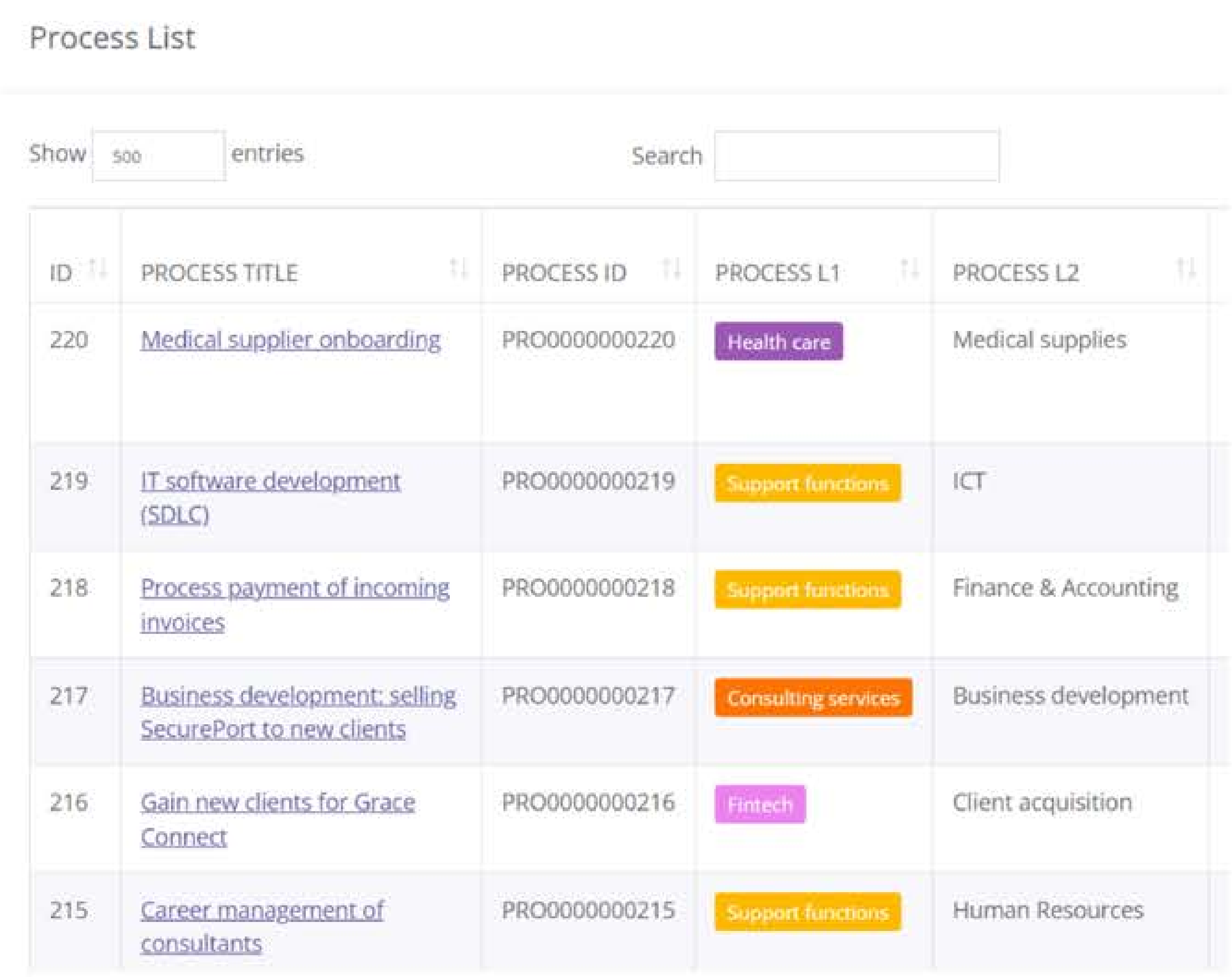
Very Poor	Poor	Satisfactory	Good
0	3	0	0

Graph view (all incidents)

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.

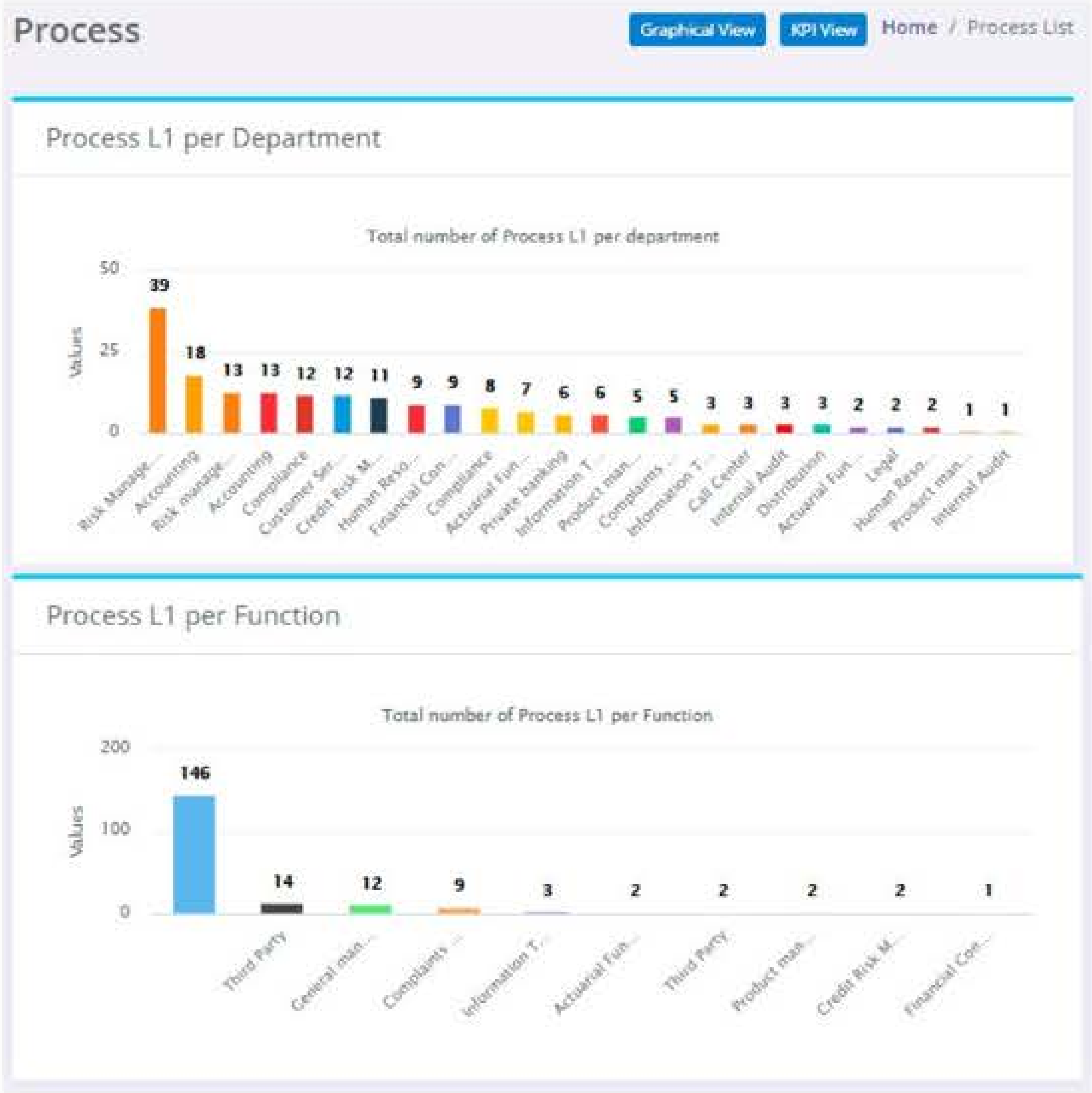
The GRC Suite is designed to integrate a Process view enabling users to map out:
risks, controls, incidents | BCM business impact analysis | data quality issues | audit findings linked to business processes



Process List

Show 500 entries Search

ID	PROCESS TITLE	PROCESS ID	PROCESS L1	PROCESS L2
220	Medical supplier onboarding	PRO0000000220	Health care	Medical supplies
219	IT software development (SDLC)	PRO0000000219	Support functions	ICT
218	Process payment of incoming invoices	PRO0000000218	Support functions	Finance & Accounting
217	Business development: selling SecurePort to new clients	PRO0000000217	Consulting services	Business development
216	Gain new clients for Grace Connect	PRO0000000216	Fintech	Client acquisition
215	Career management of consultants	PRO0000000215	Support functions	Human Resources

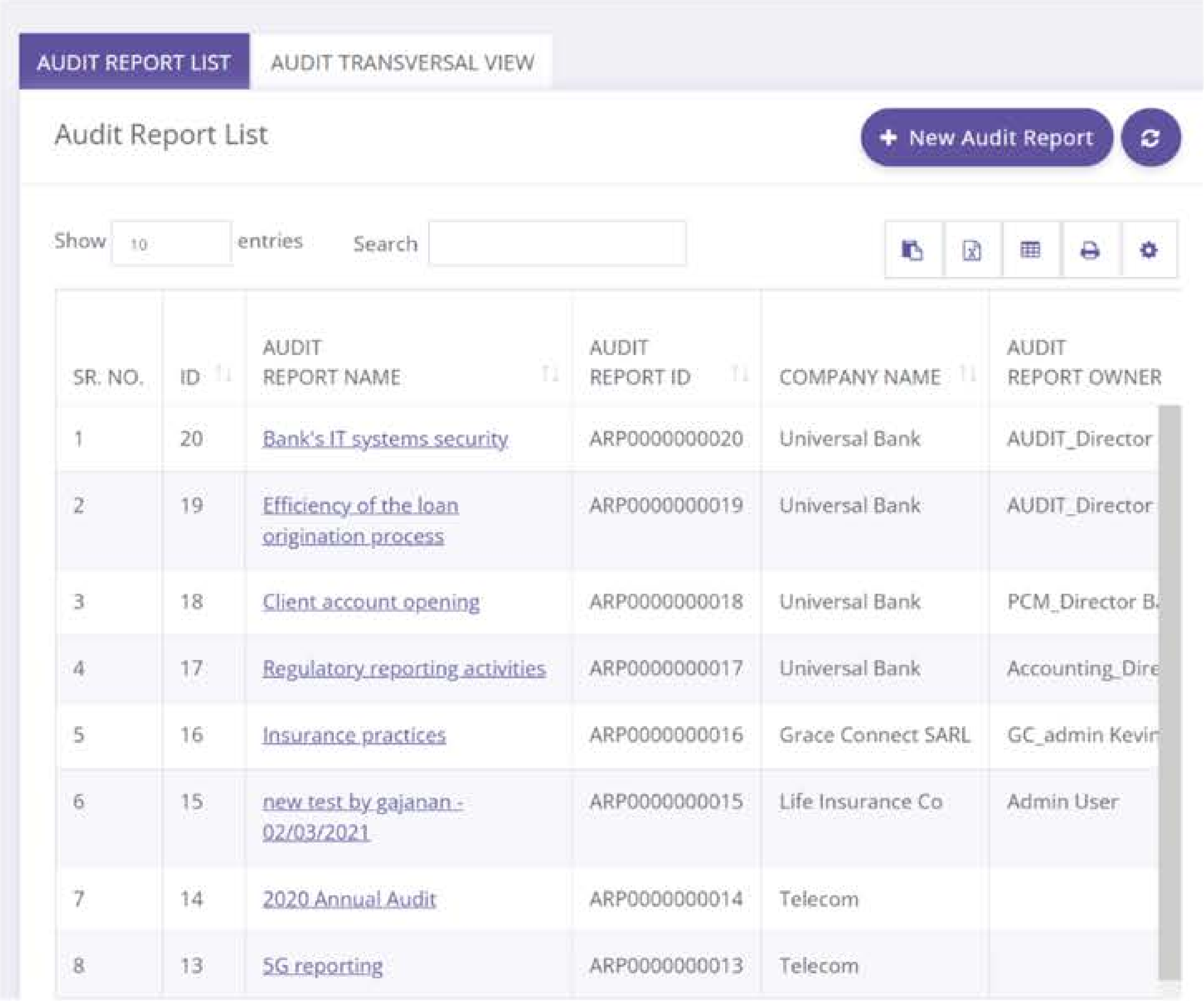


The purpose of the GRC Suite is not to design processes, it is to ensure that GRC related modules are linked to processes. This will allow users to have a consolidated view on all related items cutting through a process.

For smaller organization, a view per department is designed by default.

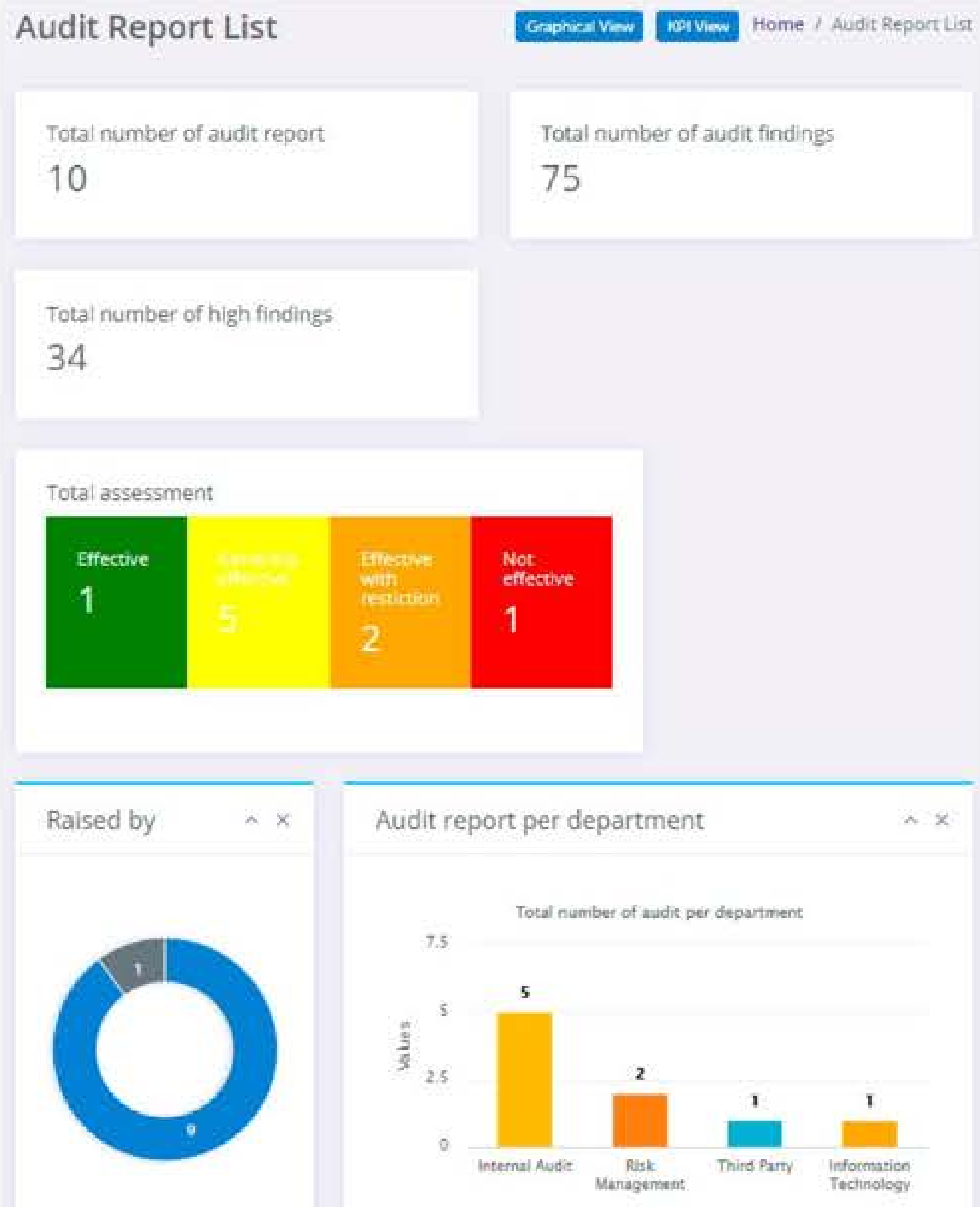
AUDIT REPORTS AS A CORNERSTONE OF THE GRC SUITE

As third line of defense, **Internal Audit** is testing the operating effectiveness of control activities embedded in business operations. These tests are formalized in audit reports stored in the GRC Suite and linked to 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 Kevir
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



Total number of audit report
10

Total number of audit findings
75

Total number of high findings
34

Total assessment

Effective	[illegible]	Effective with restiction	Not effective
1	5	2	1

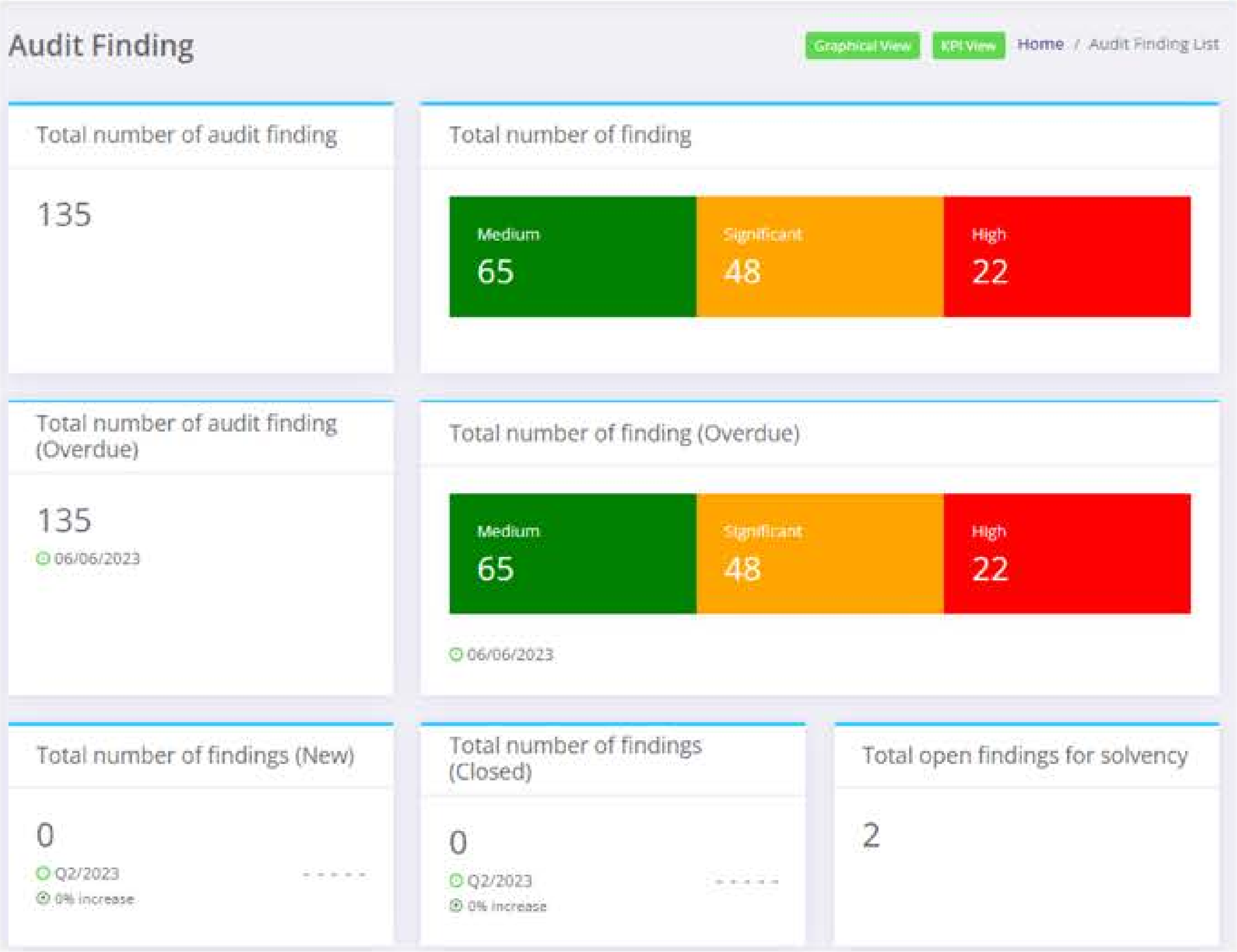
Graphs and KPI's for Audit reports

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.

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.

Calendar can be synchronized with MS Outlook



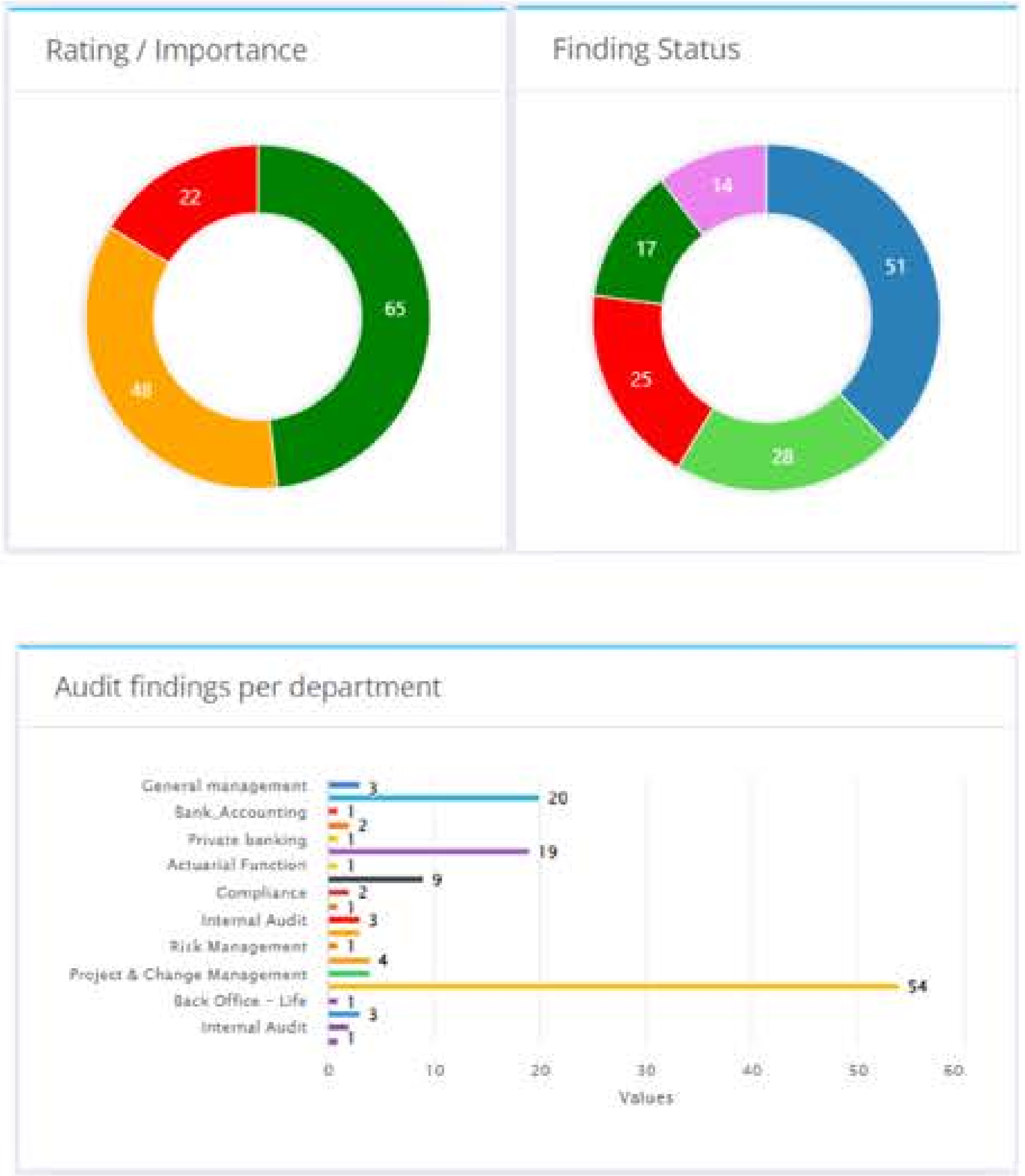
Audit Finding

Graphical View | KPI View | Home / Audit Finding List

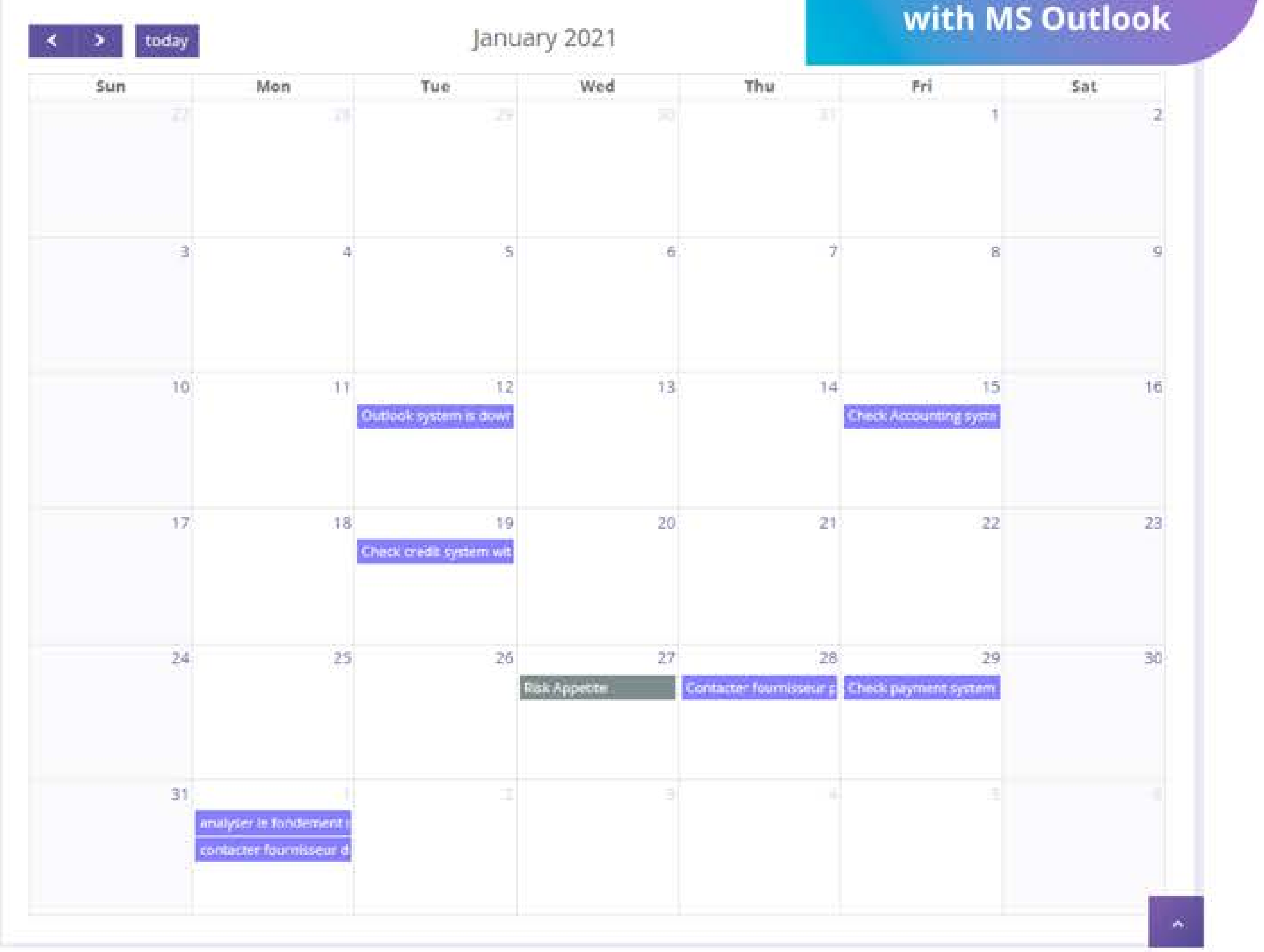
Total number of audit finding 135	Total number of finding Medium 65 · Significant 48 · High 22
Total number of audit finding (Overdue) 135 06/06/2023	Total number of finding (Overdue) Medium 65 · Significant 48 · High 22 06/06/2023

Total number of findings (New) 0 Q2/2023 0% increase	Total number of findings (Closed) 0 Q2/2023 0% increase	Total open findings for solvency 2

KPI's on Audit findings



Graphs on Audit findings



< > today

January 2021

Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12 Outlook system is dowr	13	14	15 Check Accounting syste	16
17	18	19 Check credit system wit	20	21	22	23
24	25	26	27 Risk Appetite	28 Contacter fournisseur p	29 Check payment system	30
31	1 analyser le fondement r contacter fournisseur d	2	3	4	5	6

Calendar view of Audit findings (High)

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.

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 such as:

description

root cause

categories

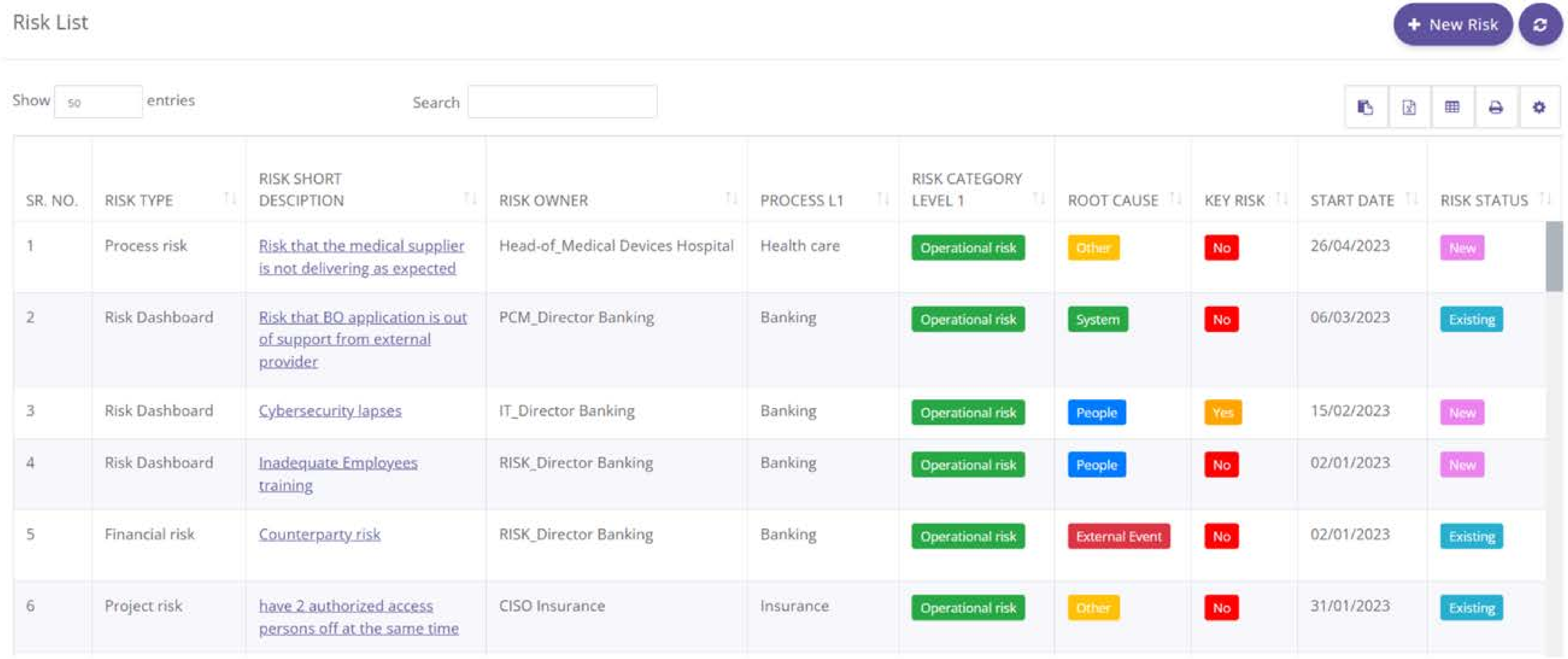
owners

impacted process

likelihood, impact

score, etc.

are stored and updated.



Show 50 entries Search

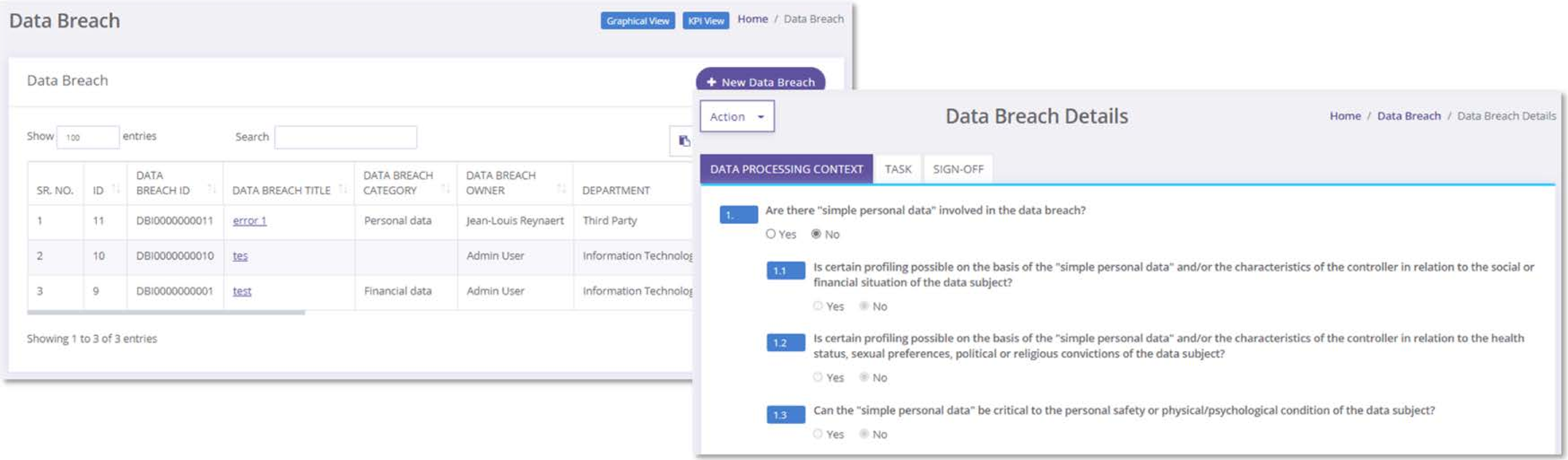
SR. NO.	RISK TYPE	RISK SHORT DESCIPTION	RISK OWNER	PROCESS L1	RISK CATEGORY LEVEL 1	ROOT CAUSE	KEY RISK	START DATE	RISK STATUS
1	Process risk	Risk that the medical supplier is not delivering as expected	Head-of_Medical Devices Hospital	Health care	Operational risk	Other	No	26/04/2023	New
2	Risk Dashboard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

List view of all documents stored in the GRC Suite

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.

DATA BREACH MODULE IN GRC SUITE

The list view of the Data Breach modules provide 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.



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

Showing 1 to 3 of 3 entries

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

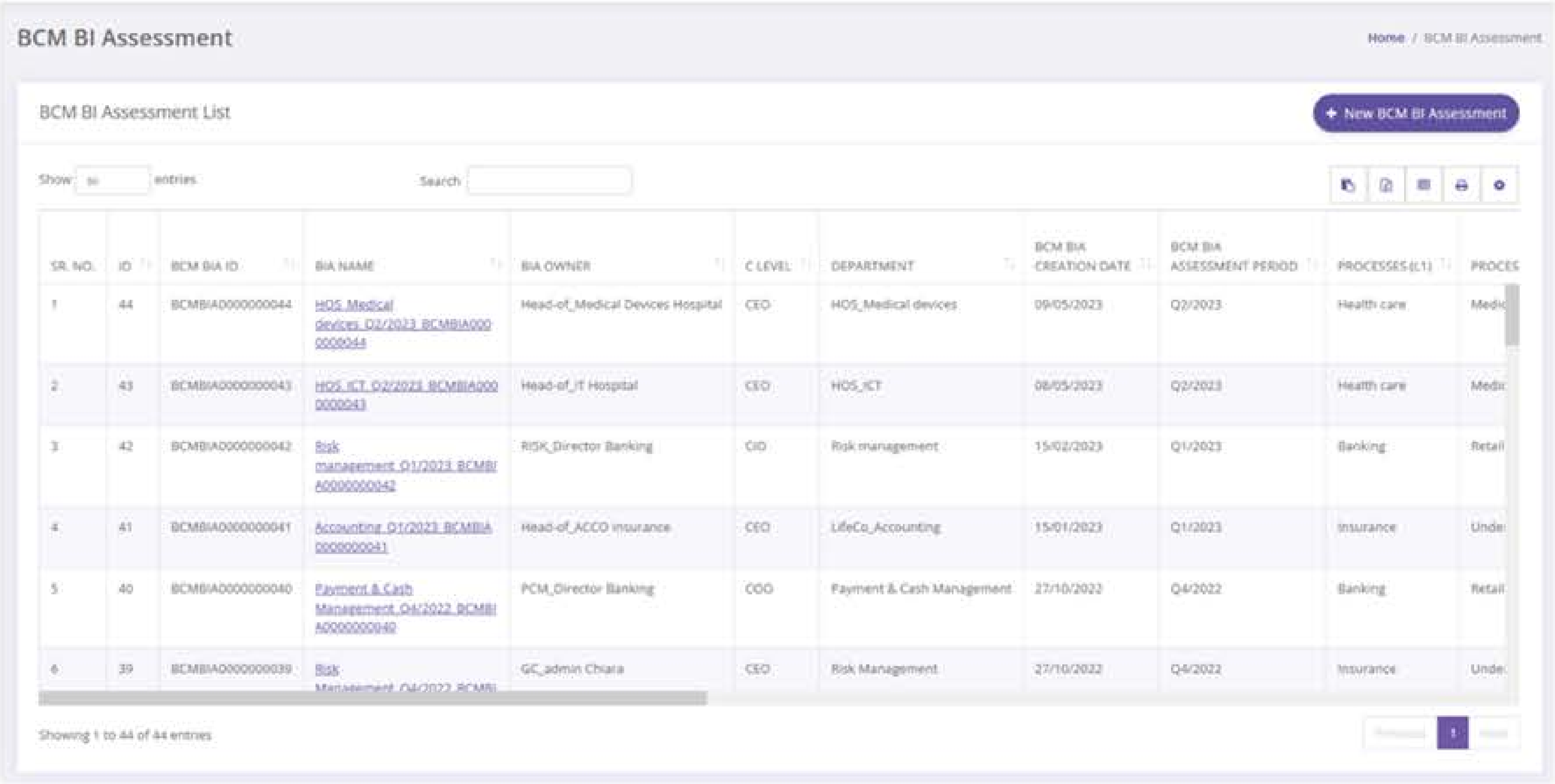
1.2 Is certain profiling possible on the basis of the "simple personal data" and/or the characteristics of the controller in relation to the health status, sexual preferences, political or religious convictions of the data subject?
○ Yes ● No

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.

BIA MODULE IN GRC SUITE

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



BCM BI Assessment

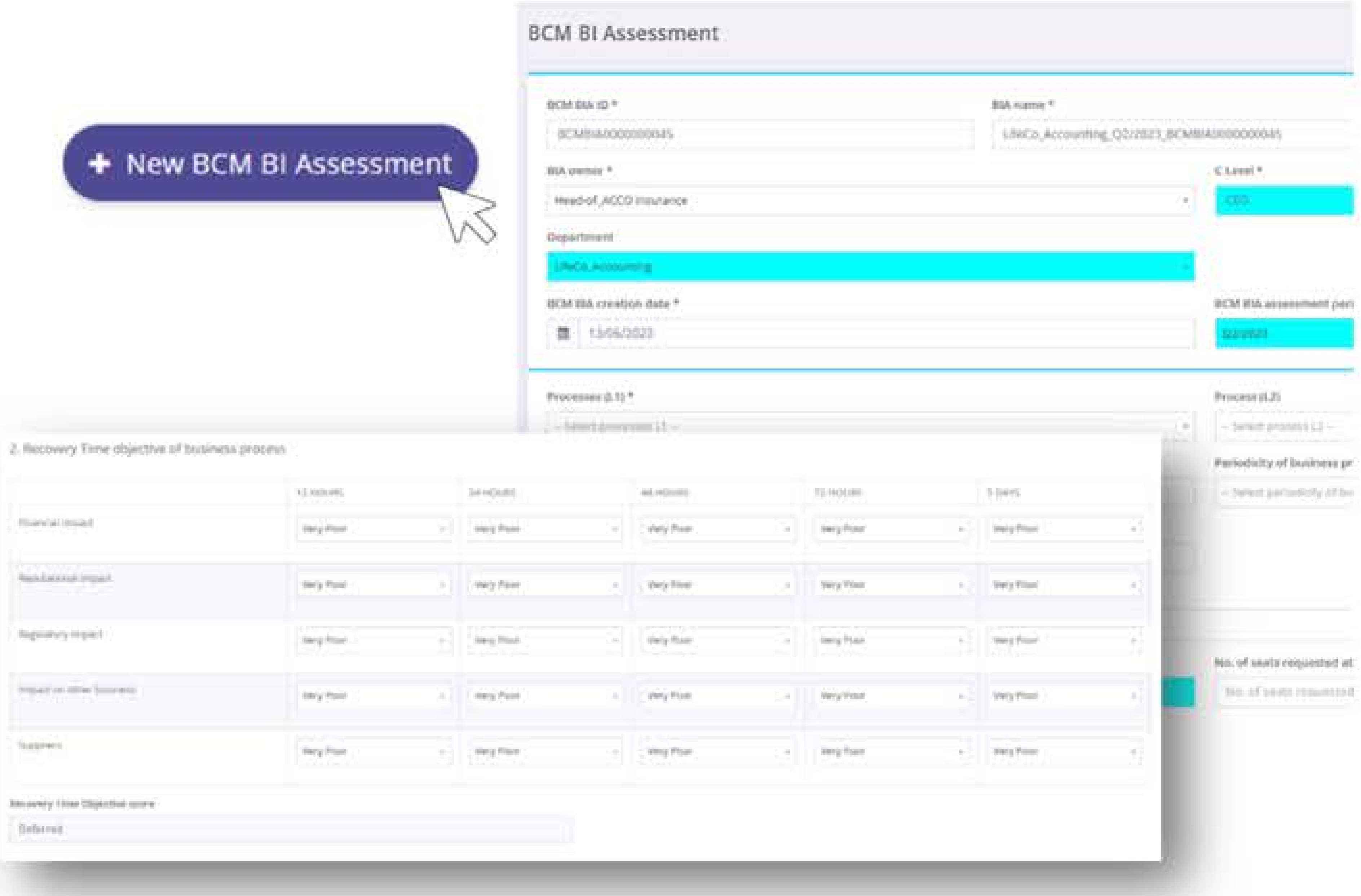
Home / BCM BI Assessment

BCM BI Assessment List

Show 50 entries Search

SR. NO.	ID	BCM BIA ID	BIA NAME	BIA OWNER	C LEVEL	DEPARTMENT	BCM BIA CREATION DATE	BCM BIA ASSESSMENT PERIOD	PROCESSES (L1)	PROCES
1	44	BCMBIA000000044	HOS_Medical devices_Q2/2023_BCMBIA0000000044	Head-of_Medical Devices Hospital	CEO	HOS_Medical devices	09/05/2023	Q2/2023	Health care	Medic
2	43	BCMBIA000000043	HOS_ICT_Q2/2023_BCMBIA0000000043	Head-of_IT Hospital	CEO	HOS_ICT	08/05/2023	Q2/2023	Health care	Medic
3	42	BCMBIA000000042	Risk management_Q1/2023_BCMBIA000000042	RISK_Director Banking	CIO	Risk management	15/02/2023	Q1/2023	Banking	Retail
4	41	BCMBIA000000041	Accounting_Q1/2023_BCMBIA000000041	Head-of_ACCO insurance	CEO	LifeCo_Accounting	15/01/2023	Q1/2023	Insurance	Unde
5	40	BCMBIA000000040	Payment & Cash Management_Q4/2022_BCMBIA000000040	PCM_Director Banking	COO	Payment & Cash Management	27/10/2022	Q4/2022	Banking	Retail
6	39	BCMBIA000000039	Risk Management_Q4/2022_BCMBI	GC_admin Chiara	CEO	Risk Management	27/10/2022	Q4/2022	Insurance	Unde

Showing 1 to 44 of 44 entries



BCM BI Assessment

BCM BIA ID * BCMBIA000000045

BIA name * LifeCo_Accounting_Q2/2023_BCMBIA000000045

BIA owner * Head-of_ACCO insurance

C Level * CEO

Department LifeCo_Accounting

BCM BIA creation date * 13/06/2023

BCM BIA assessment peri Q2/2023

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

Process (L2) -- Select process L2 --

Periodicity of business pr -- Select periodicity of bu

No. of seats requested at No. of seats requested

2. Recovery Time objective of business process

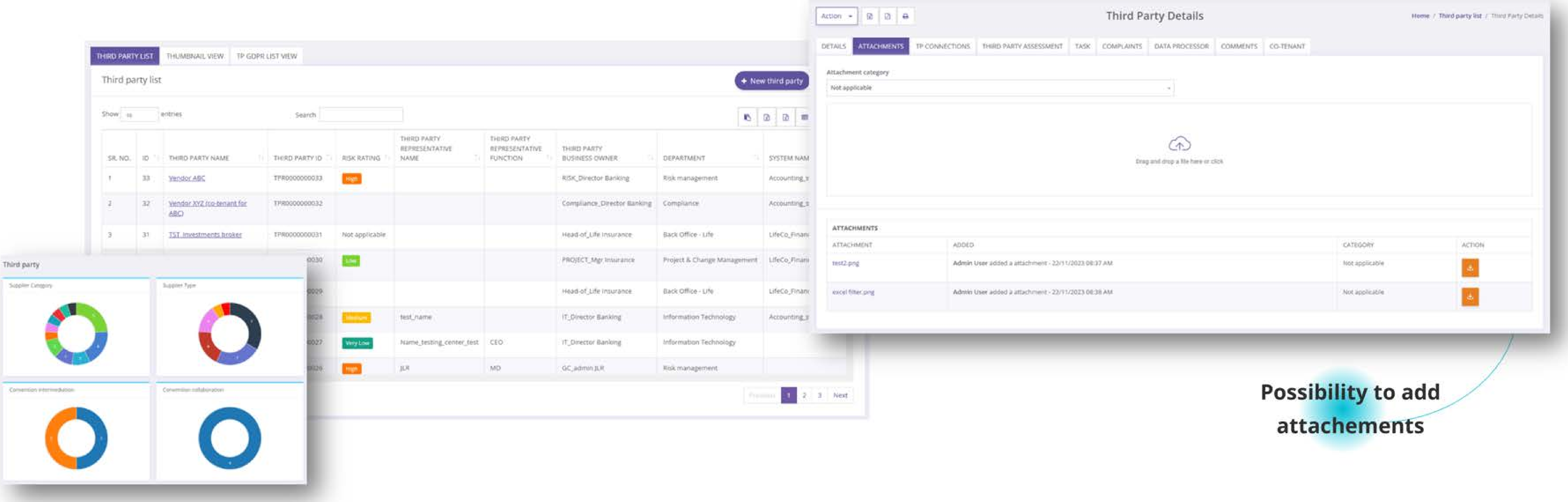
	12 HOURS	24 HOURS	48 HOURS	72 HOURS	5 DAYS
Financial impact	Very Poor	Very Poor	Very Poor	Very Poor	Very Poor
Reputational impact	Very Poor	Very Poor	Very Poor	Very Poor	Very Poor
Regulatory impact	Very Poor	Very Poor	Very Poor	Very Poor	Very Poor
Impact on other business	Very Poor	Very Poor	Very Poor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

Recovery Time Objective score Deferred

The detailed form is used to create new BCM BIA entry with all relevant information to be introduced by users.

THIRD PARTY MODULE IN GRC SUITE

Third Party Risk Management (TPRM) Tool helps to fortify your organization against unforeseen risks while fostering secure and productive partnerships with your external service providers



THIRD PARTY LIST | THUMBNAIL VIEW | TP GDPR LIST VIEW

Third party list

+ New third party

Show 10 entries Search

SR. NO.	ID	THIRD PARTY NAME	THIRD PARTY ID	RISK RATING	THIRD PARTY REPRESENTATIVE NAME	THIRD PARTY REPRESENTATIVE FUNCTION	THIRD PARTY BUSINESS OWNER	DEPARTMENT	SYSTEM NAM
1	33	Vendor ABC	TPR0000000033	High			RISK_Director Banking	Risk management	Accounting_s
2	32	Vendor XYZ (co-tenant for ABC)	TPR0000000032				Compliance_Director Banking	Compliance	Accounting_s
3	31	TST_Investments broker	TPR0000000031	Not applicable			Head-of_Life Insurance	Back Office - Life	LifeCo_Financ
			0030	Low			PROJECT_Mgr Insurance	Project & Change Management	LifeCo_Financ
			0029				Head-of_Life Insurance	Back Office - Life	LifeCo_Financ
			0028	Medium	test_name		IT_Director Banking	Information Technology	Accounting_s
			0027	Very Low	Name_testing_center_test	CEO	IT_Director Banking	Information Technology	
			0026	High	JLR	MD	GC_admin JLR	Risk management	

Previous 1 2 3 Next

Third party

Third Party Details

Action | Home / Third party list / Third Party Details

DETAILS | ATTACHMENTS | TP CONNECTIONS | THIRD PARTY ASSESSMENT | TASK | COMPLAINTS | DATA PROCESSOR | COMMENTS | CO-TENANT

Attachment category: Not applicable

Drag and drop a file here or click

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	⭳

Possibility to add attachements

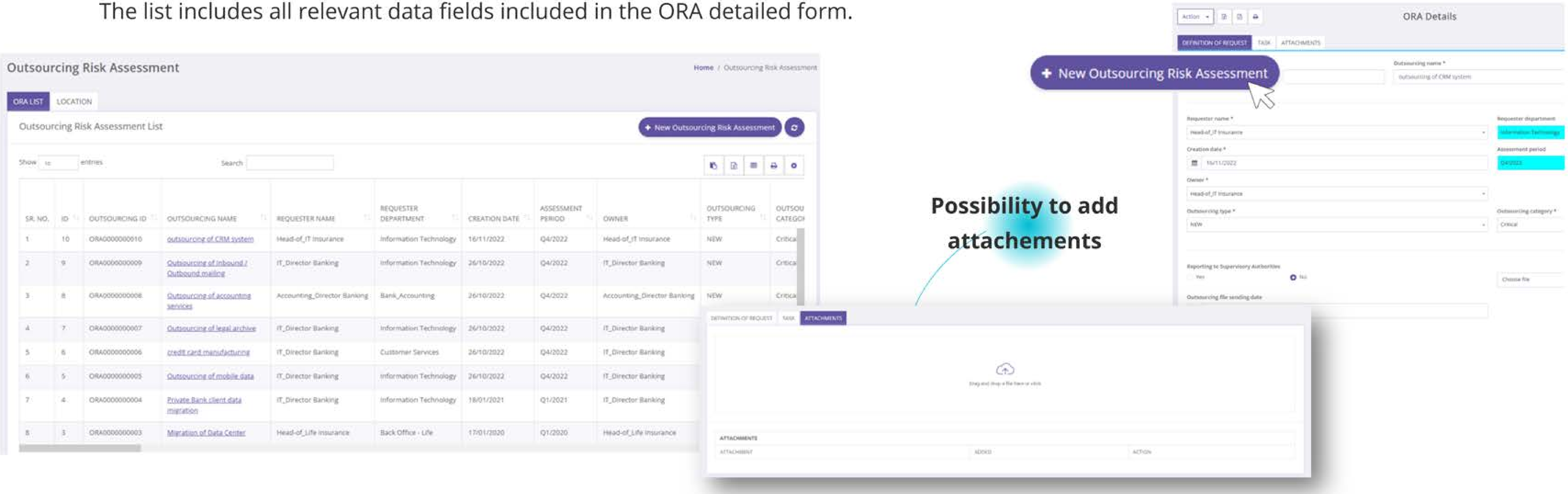
Key Features and Benefits:

Enhanced Risk Visibility, Improved Compliance for Outsourcing Services, Cost Reduction, Reputation Protection and Strategic Decision-Making

OUTSOURCING RISK ASSESSMENT MODULE IN GRC SUITE

The list view of the Outsourcing Risk Assessment (ORA) module provide users with all entries recorded. This enables to update graphs and KPI's.

The list includes all relevant data fields included in the ORA detailed form.



Outsourcing Risk Assessment

Home / Outsourcing Risk Assessment

ORA LIST | LOCATION

Outsourcing Risk Assessment List

+ New Outsourcing Risk Assessment

Show 10 entries Search

SR. NO.	ID	OUTSOURCING ID	OUTSOURCING NAME	REQUESTER NAME	REQUESTER DEPARTMENT	CREATION DATE	ASSESSMENT PERIOD	OWNER	OUTSOURCING TYPE	OUTSOU CATEGOI
1	10	ORA0000000010	outsourcing of CRM system	Head-of_IT Insurance	Information Technology	16/11/2022	Q4/2022	Head-of_IT Insurance	NEW	Critica
2	9	ORA0000000009	Outsourcing of Inbound / Outbound mailing	IT_Director Banking	Information Technology	26/10/2022	Q4/2022	IT_Director Banking	NEW	Critica
3	8	ORA0000000008	Outsourcing of accounting services	Accounting_Director Banking	Bank_Accounting	26/10/2022	Q4/2022	Accounting_Director Banking	NEW	Critica
4	7	ORA0000000007	Outsourcing of legal archive	IT_Director Banking	Information Technology	26/10/2022	Q4/2022	IT_Director Banking		
5	6	ORA0000000006	credit card manufacturing	IT_Director Banking	Customer Services	26/10/2022	Q4/2022	IT_Director Banking		
6	5	ORA0000000005	Outsourcing of mobile data	IT_Director Banking	Information Technology	26/10/2022	Q4/2022	IT_Director Banking		
7	4	ORA0000000004	Private Bank client data migration	IT_Director Banking	Information Technology	18/01/2021	Q1/2021	IT_Director Banking		
8	3	ORA0000000003	Migration of Data Center	Head-of_Life Insurance	Back Office - Life	17/01/2020	Q1/2020	Head-of_Life Insurance		

+ New Outsourcing Risk Assessment

Action ▾

ORA Details

DEFINITION OF REQUEST | TASK | ATTACHMENTS

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

Choose file

Outsourcing file sending date

Possibility to add attachements

DEFINITION OF REQUEST | TASK | ATTACHMENTS

Drag and drop a file here or click

ATTACHMENTS

ATTACHMENT	ADDED	ACTION

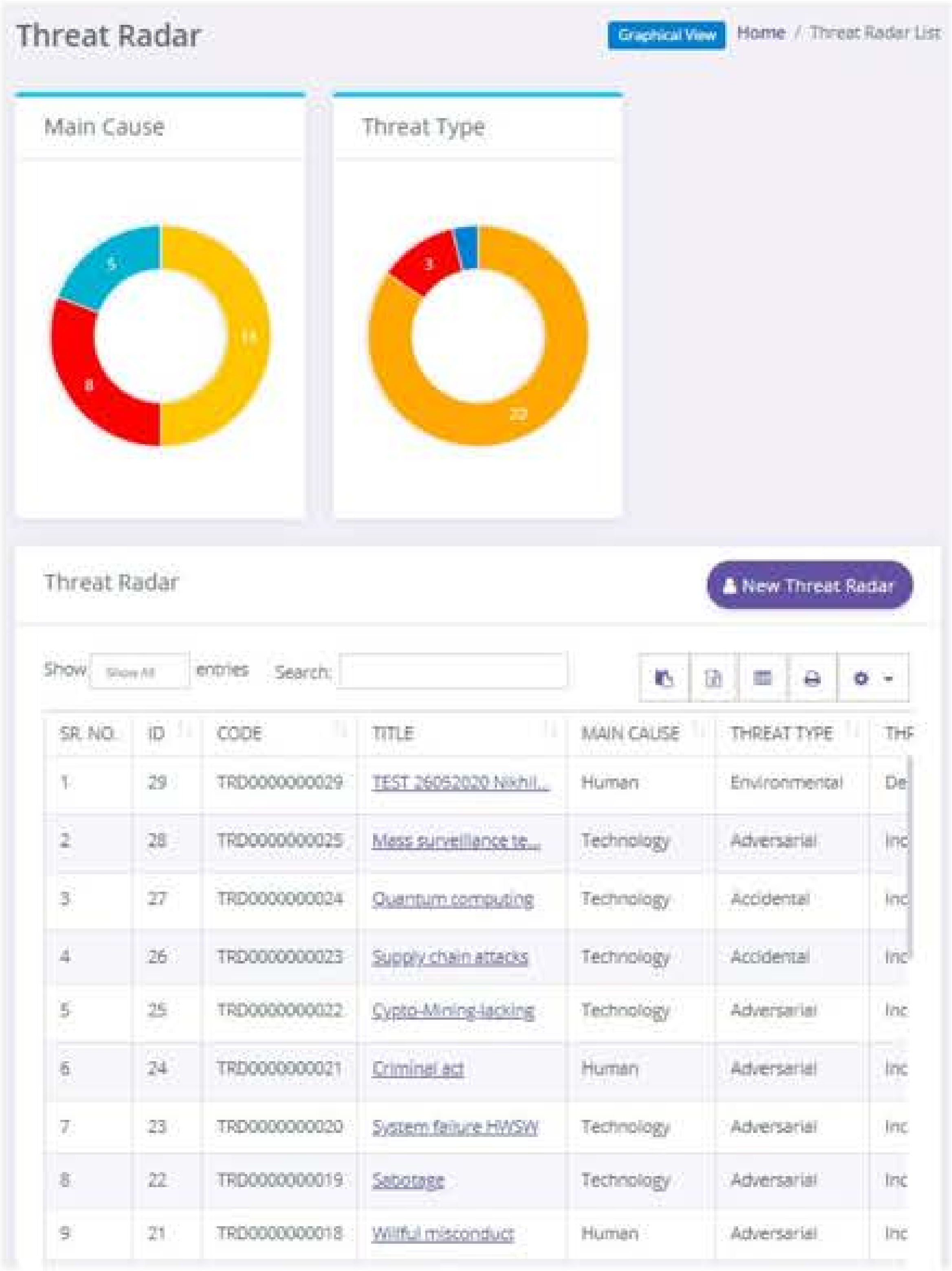
The detailed form is used to create new Outsourcing risk assessment entry with all relevant information to be introduced by users.

CYBER SECURITY MODULE IN GRC SUITE

Grace Connect GRC Suite includes a set of modules dedicated to the **management of Cyber Security risks.**

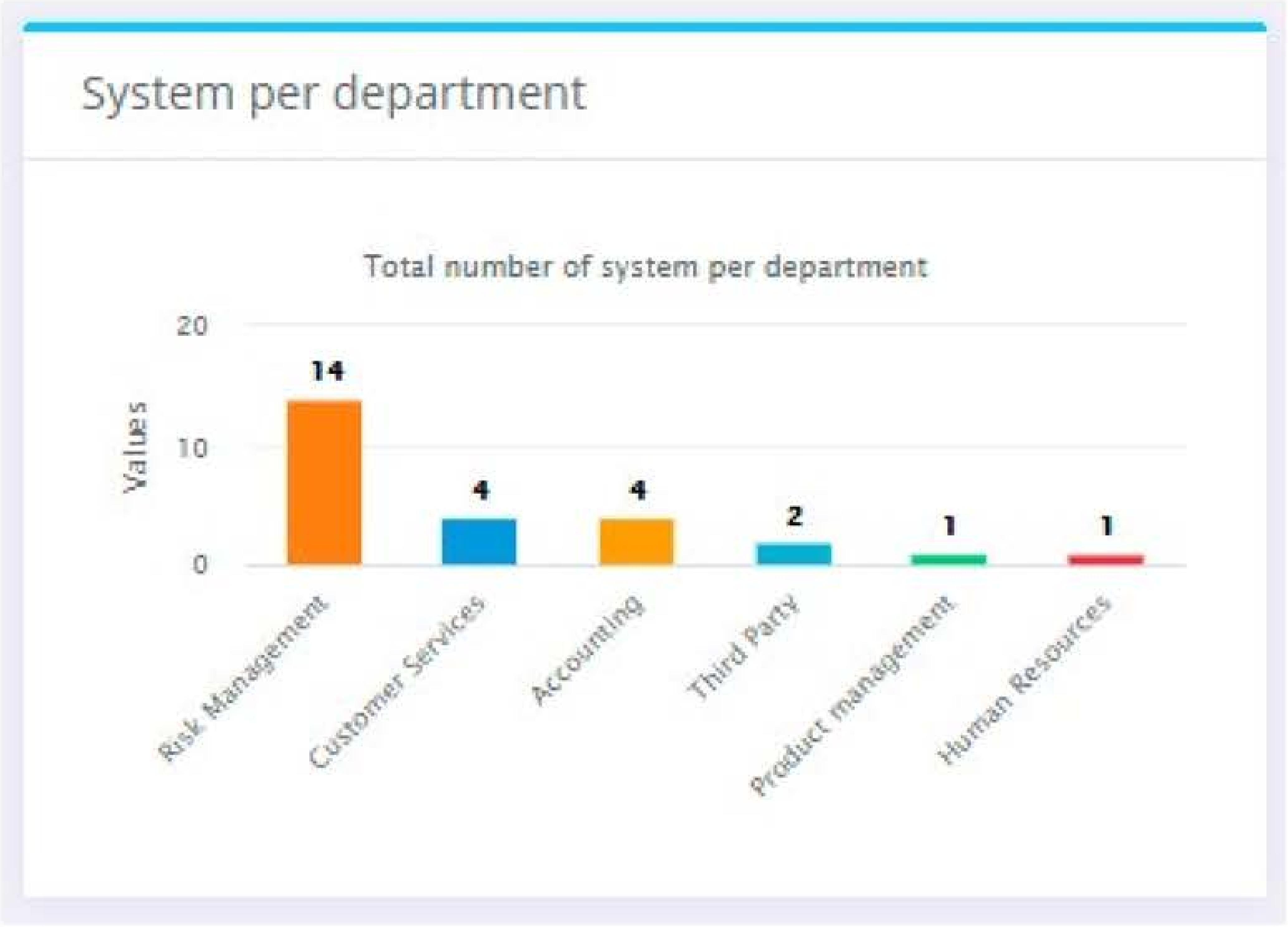
A maturity assessment enables to focus on areas to reinforce in the short term and design a roadmap to increase the maturity for Cyber security in the long term.

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.



Threat Radar

SR. NO.	ID	CODE	TITLE	MAIN CAUSE	THREAT TYPE	THR
1	29	TRD0000000029	TEST 26052020 Nikhil...	Human	Environmental	De
2	28	TRD0000000025	Mass surveillance te...	Technology	Adversarial	Inc
3	27	TRD0000000024	Quantum computing	Technology	Accidental	Inc
4	26	TRD0000000023	Supply chain attacks	Technology	Accidental	Inc
5	25	TRD0000000022	Cypto-Mining-Jacking	Technology	Adversarial	Inc
6	24	TRD0000000021	Criminal act	Human	Adversarial	Inc
7	23	TRD0000000020	System failure HWSW	Technology	Adversarial	Inc
8	22	TRD0000000019	Sabotage	Technology	Adversarial	Inc
9	21	TRD0000000018	Willful misconduct	Human	Adversarial	Inc



List of all Systems stored in the GRC Suite

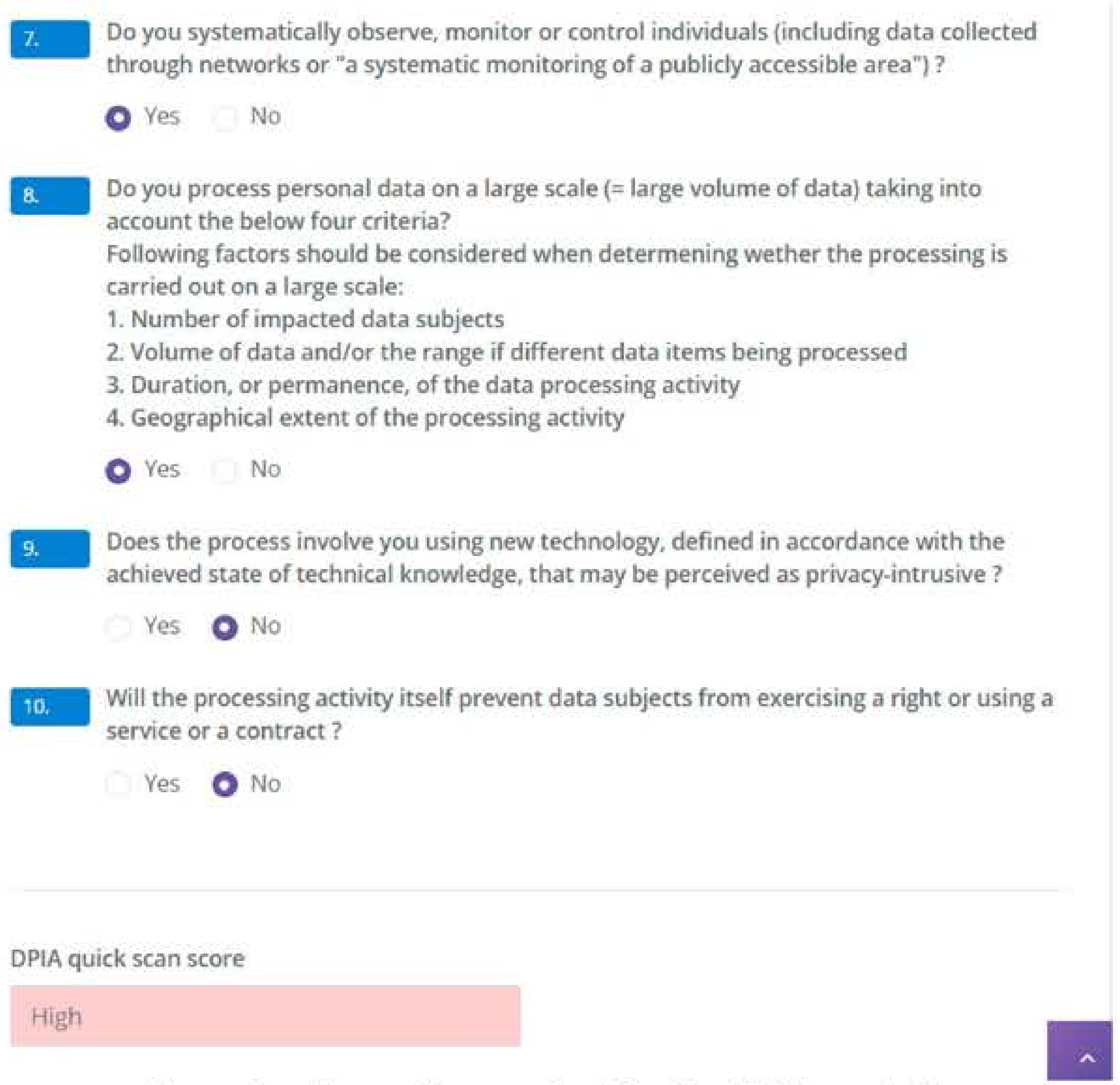
- The Cyber security module is fully aligned with Information Security CIA classification and is applicable to all systems stored in the GRC Suite.
- Possibility to have a Cyber Security maturity assessment stored and mapped out with Grace Connect Task tracking module.

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

DATA PROTECTION MODULES IN GRC SUITE

Grace Connect GRC Suite includes a full set of modules dedicated to the **management of Data Privacy risks.**

A Registry of Processing Activities (“ROPA”) is included in the GRC Suite, with the aim to collect all relevant information on data processed on main activities. A module is designed to perform a Data Protection Impact Assessment (“DPIA”), which is required any time a new project is started to identify and assess risks related to sensitive information. A specific GDPR compliancy assessment module is also integrated in the GRC Suite.



7. Do you systematically observe, monitor or control individuals (including data collected through networks or "a systematic monitoring of a publicly accessible area") ?

● Yes ○ No

8. Do you process personal data on a large scale (= large volume of data) taking into account the below four criteria?
Following factors should be considered when determening wether the processing is carried out on a large scale:
1. Number of impacted data subjects
2. Volume of data and/or the range if different data items being processed
3. Duration, or permanence, of the data processing activity
4. Geographical extent of the processing activity

● Yes ○ No

9. Does the process involve you using new technology, defined in accordance with the achieved state of technical knowledge, that may be perceived as privacy-intrusive ?

○ Yes ● No

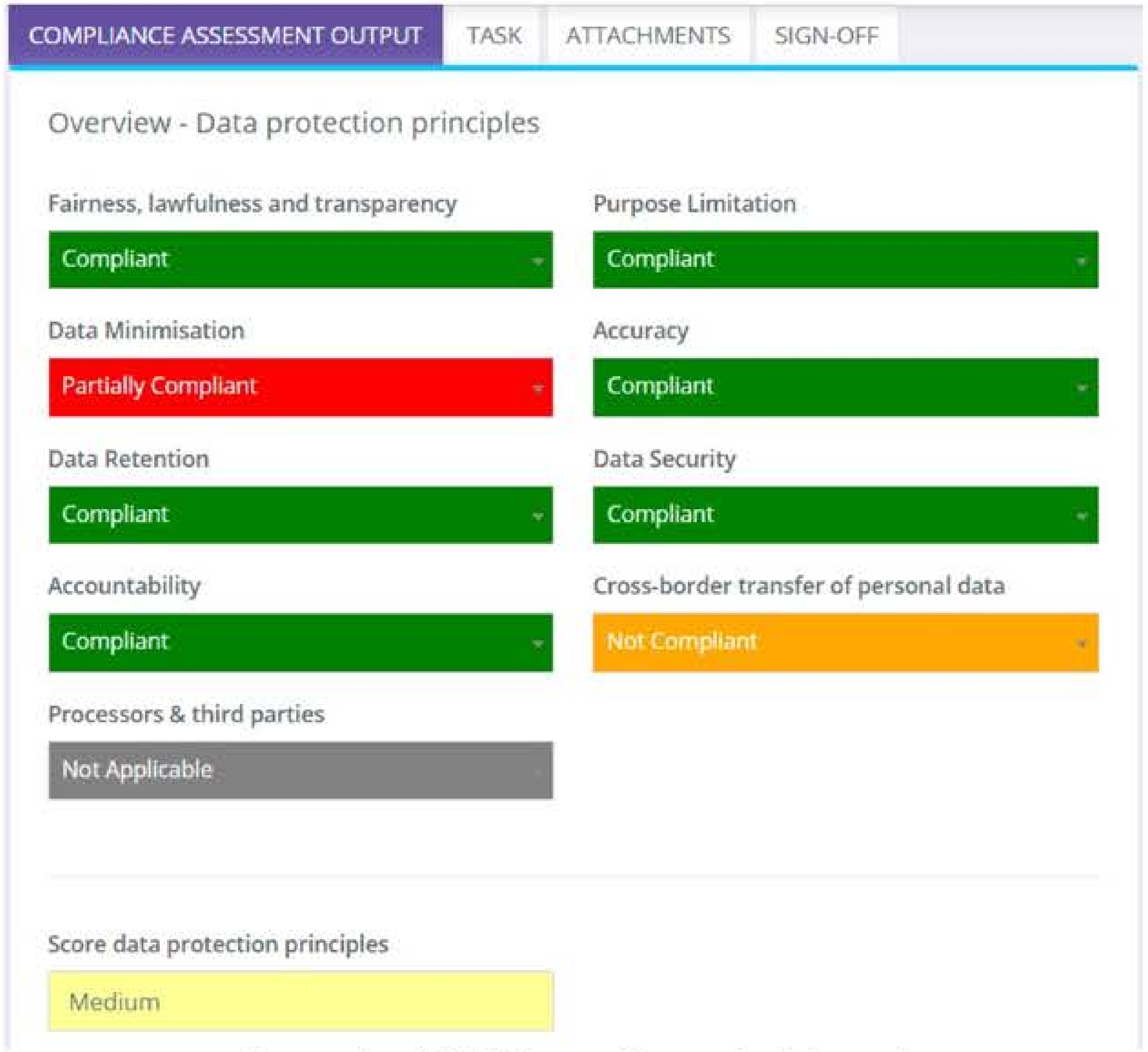
10. Will the processing activity itself prevent data subjects from exercising a right or using a service or a contract ?

○ Yes ● No

DPIA quick scan score

High

Example of questions raised in the DPIA module



Overview - Data protection principles

Fairness, lawfulness and transparency: Compliant

Purpose Limitation: Compliant

Data Minimisation: Partially Compliant

Accuracy: Compliant

Data Retention: Compliant

Data Security: Compliant

Accountability: Compliant

Cross-border transfer of personal data: Not Compliant

Processors & third parties: Not Applicable

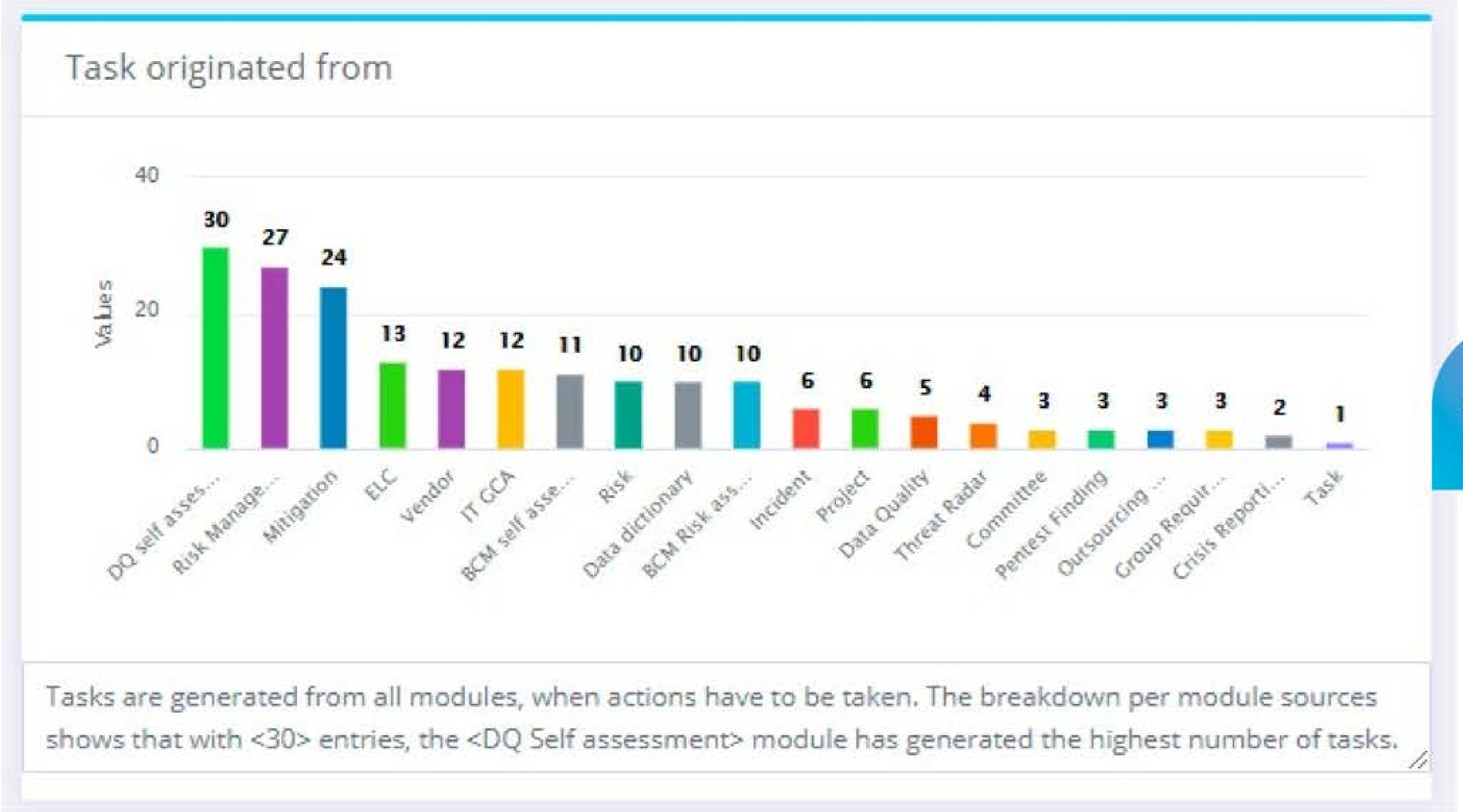
Score data protection principles: Medium

Example of GDPR compliance dashboard

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.



Tasks are generated from all modules, when actions have to be taken. The breakdown per module sources shows that with <30> entries, the <DQ Self assessment> module has generated the highest number of tasks.

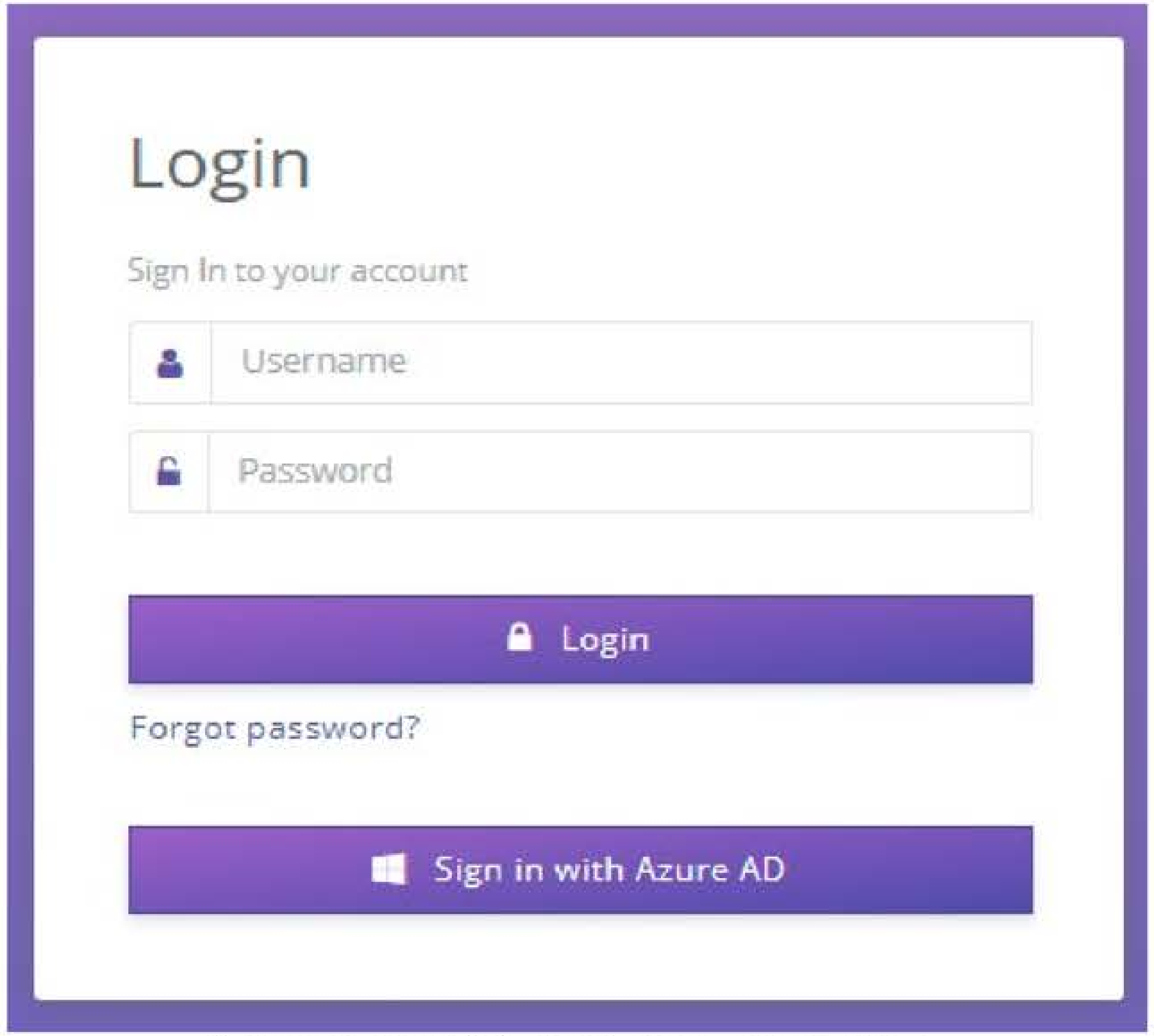
Task module synchronized with MS-Outlook tasks

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.



Login

Sign In to your account

Username

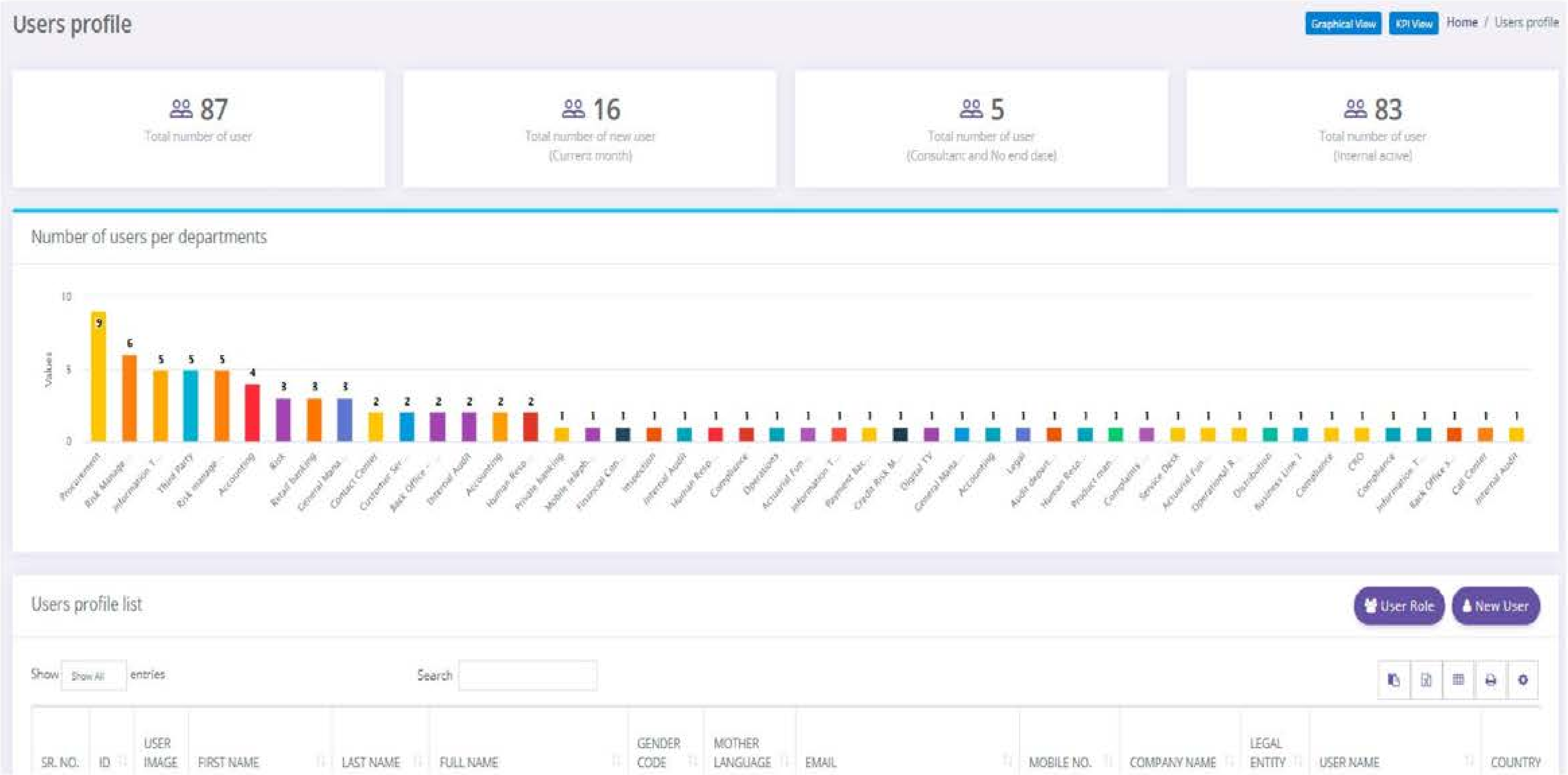
Password

🔒 Login

Forgot password?

Sign in with Azure AD

Entry screen with individual user recognition



Users profile

Graphical View | KPI View | Home / Users profile

87	16	5	83
Total number of user	Total number of new user (Current month)	Total number of user (Consultant and No end date)	Total number of user (Internal active)

Number of users per departments

Users profile list

User Role | New User

Show Show All entries

Search

SR. NO.	ID	USER IMAGE	FIRST NAME	LAST NAME	FULL NAME	GENDER CODE	MOTHER LANGUAGE	EMAIL	MOBILE NO.	COMPANY NAME	LEGAL ENTITY	USER NAME	COUNTRY

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 9, rue du Laboratoire, 1911 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.