



Manage & Quantify **your risks**

# Multi-method approach

Different methodologies tailor made to user's needs and use cases

## GRC methodology

Simple and easy Topline view

**Typology of systems analyzed :**

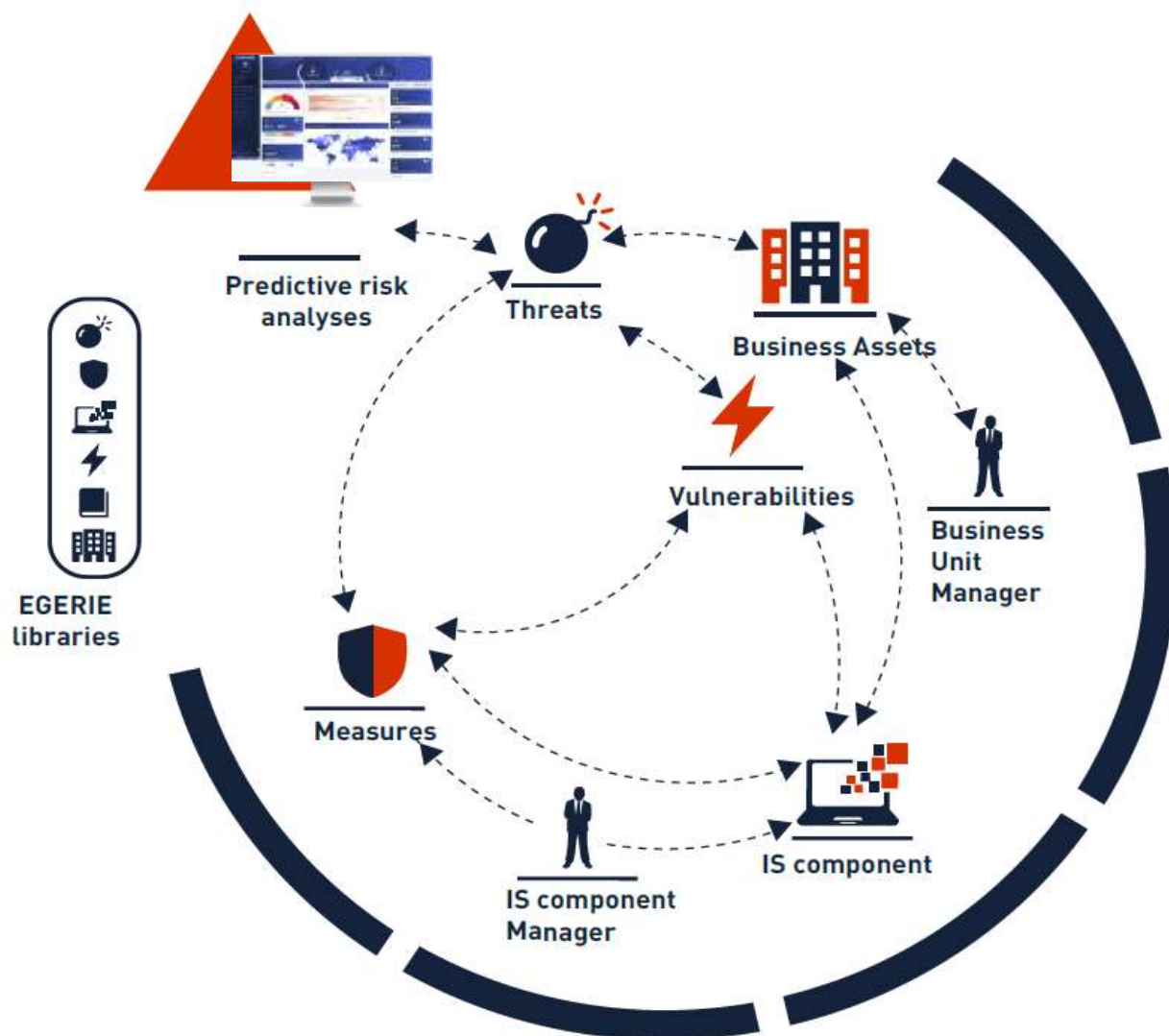
non-susceptible or unexposed systems



## Advanced bottom-up methodology

Approach is made very simple by the EGERIE models





## WHAT IS A RISK

Risk is a matrix of potential harm or loss where the intersecting elements are:

1. **Measures:** The security measures and controls in place to protect assets and business processes.
2. **Vulnerabilities:** Weaknesses or gaps in the security measures, forming rows within the matrix.
3. **Threats:** The potential incidents or attacks that aim to exploit vulnerabilities, forming columns within the matrix.

**Intersection of Elements:** Risks emerge at the intersections of this matrix when threats exploit vulnerabilities despite the presence of security measures. This represents the point where potential harm to business processes and assets becomes a reality.

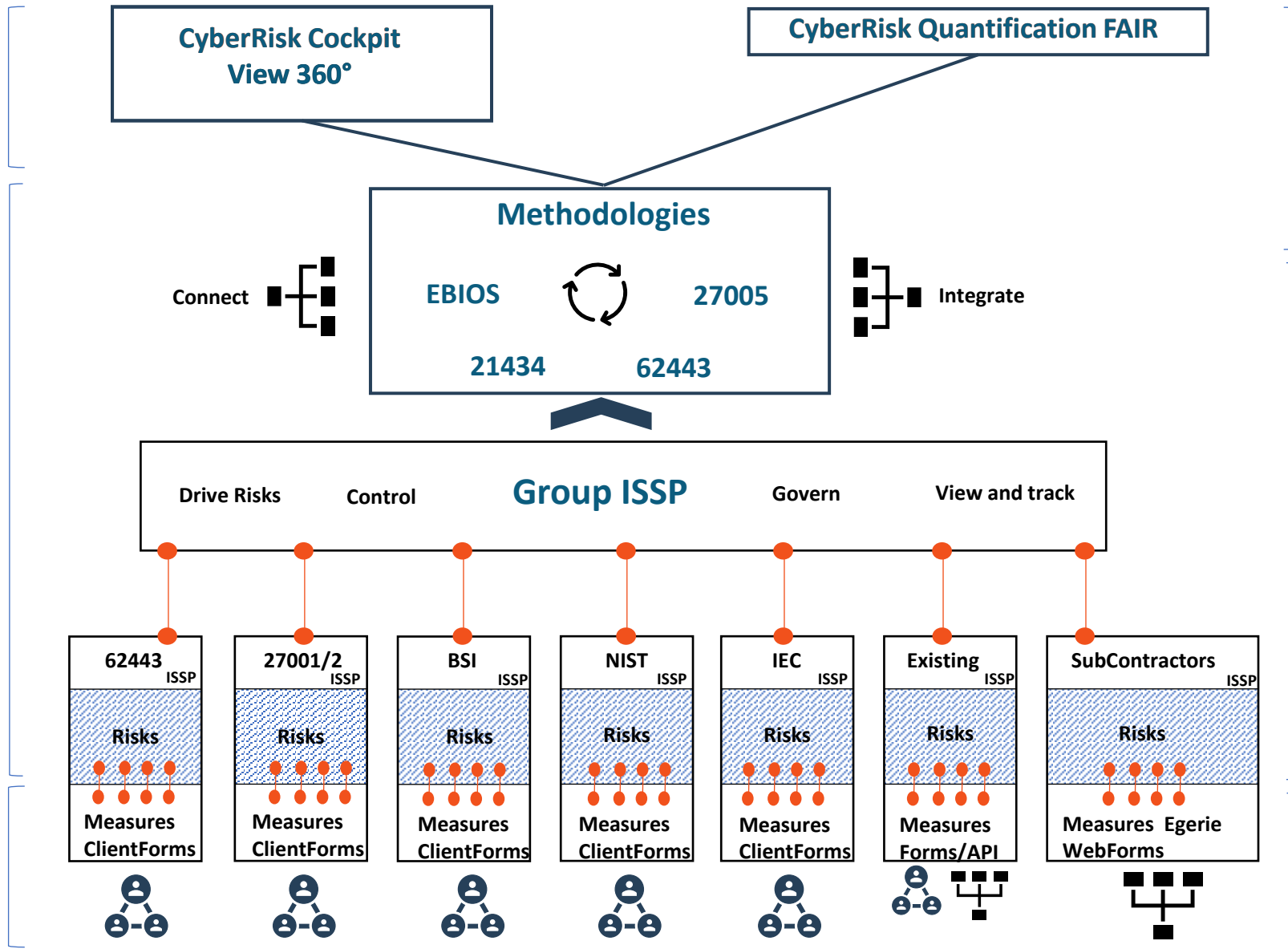
**Impact on Business Processes and Assets:** Risks, once realized, have a direct impact on business processes and assets within the organization, leading to disruptions, financial losses, operational challenges, or damage to reputation.

## Your Organization

CISO x C-Level

CISO Team

Business Team



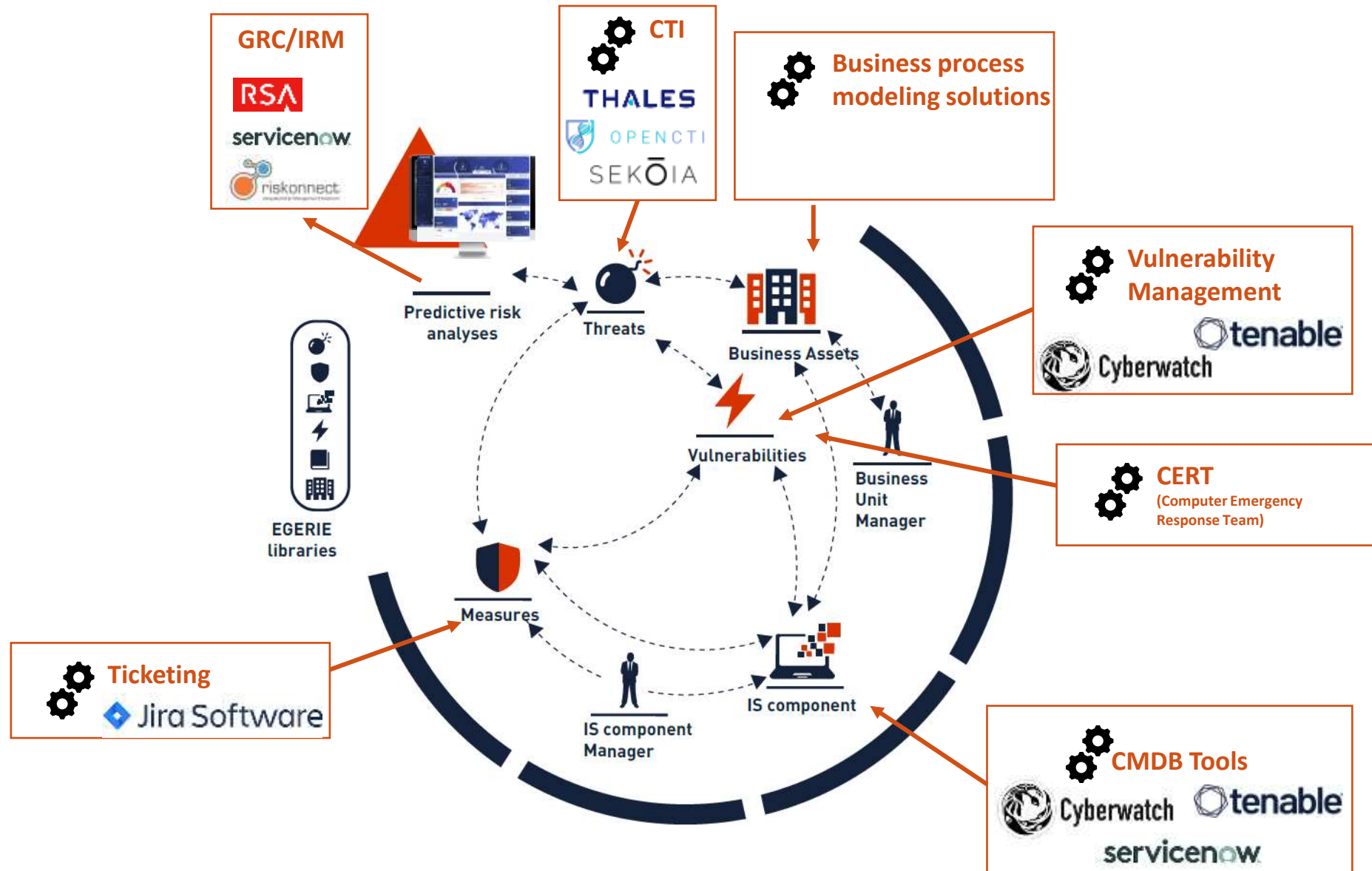
## Egerie & Partners

**Experts**  
Budget – 20%

**Licences**  
**Professional Services**  
Budget – 70%

**Policy Team**  
Budget – 10%

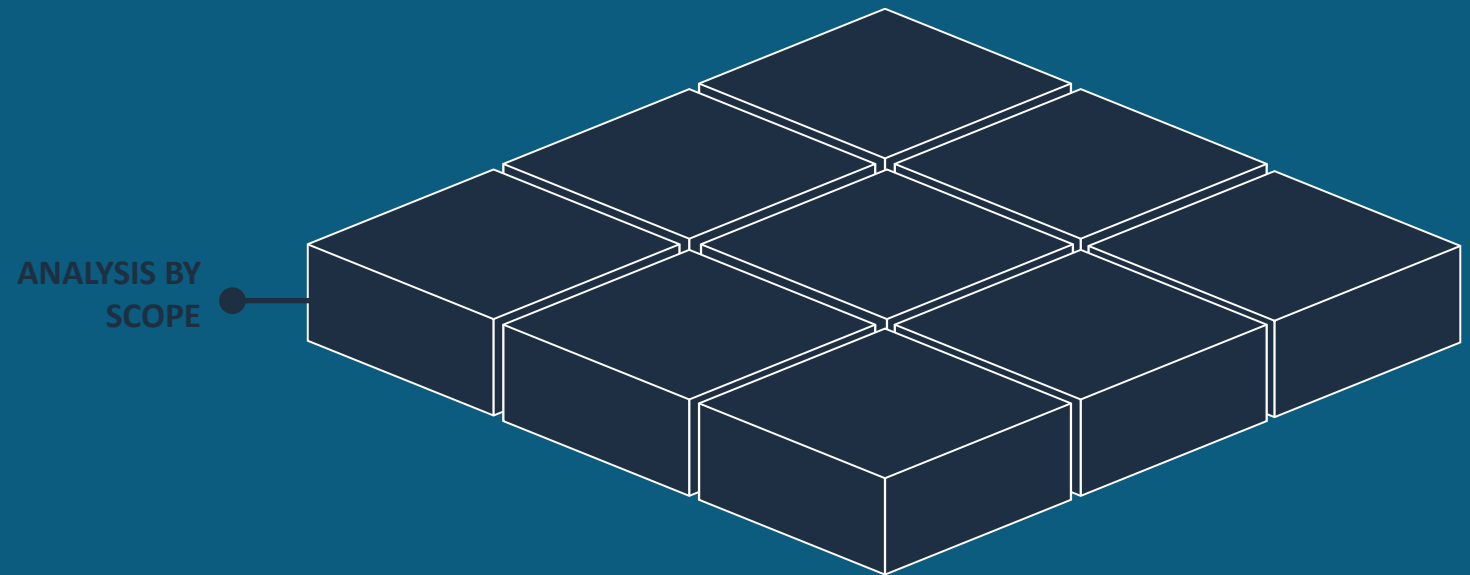
# EGERIE MODELLING & INTERCONNECTIONS





The **CYBER RISK** analysis, mapping and financial quantification platform

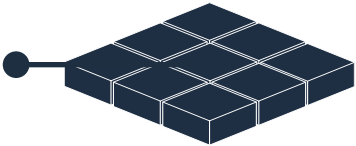
## Bottom-up approach, assets and people



WE PROVIDE A

# Enhanced collaborative approach

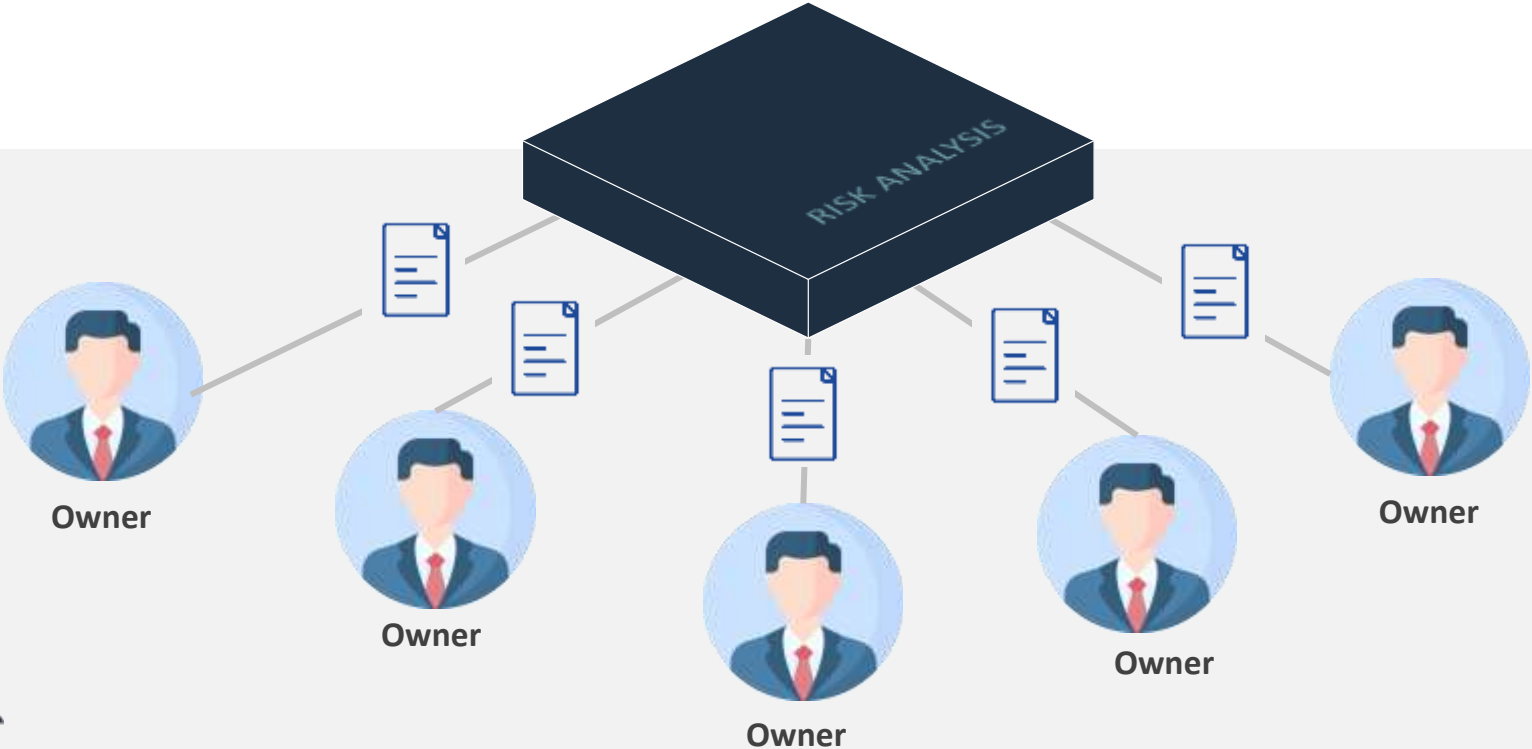
ANALYSIS BY  
SCOPE



Expert Analyst

Oversees risk analysis and treatment plan monitoring

Gain operational efficiencies and eliminate as many manual tasks as possible through centralization, industrialization, and automatic risk reduction.



key business  
stakeholders

Engaged through automated  
questionnaires

We process all the complexity arising from all your risk analyses to provide you with a clear 360° vision

+200

SYSTEMS ASSESSED

125

BUSINESS ASSETS

450

IT ASSETS

8,5K

VULNERABILITIES

8,7K

CONTROLS

11K

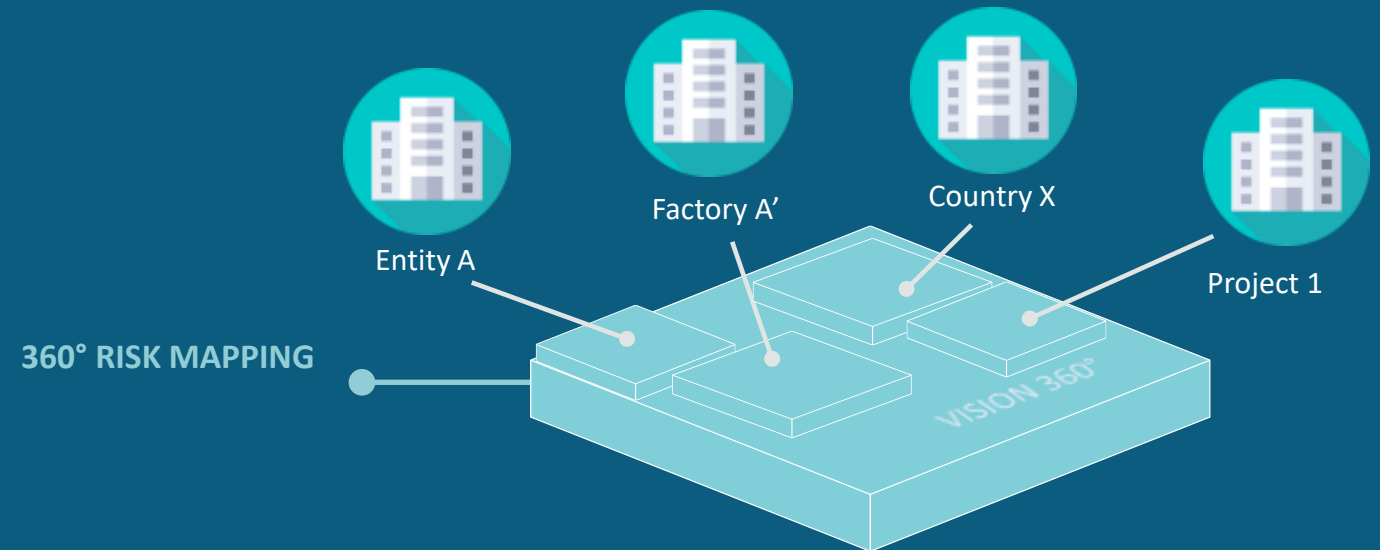
THREATS

9

STRATEGIC RISKS

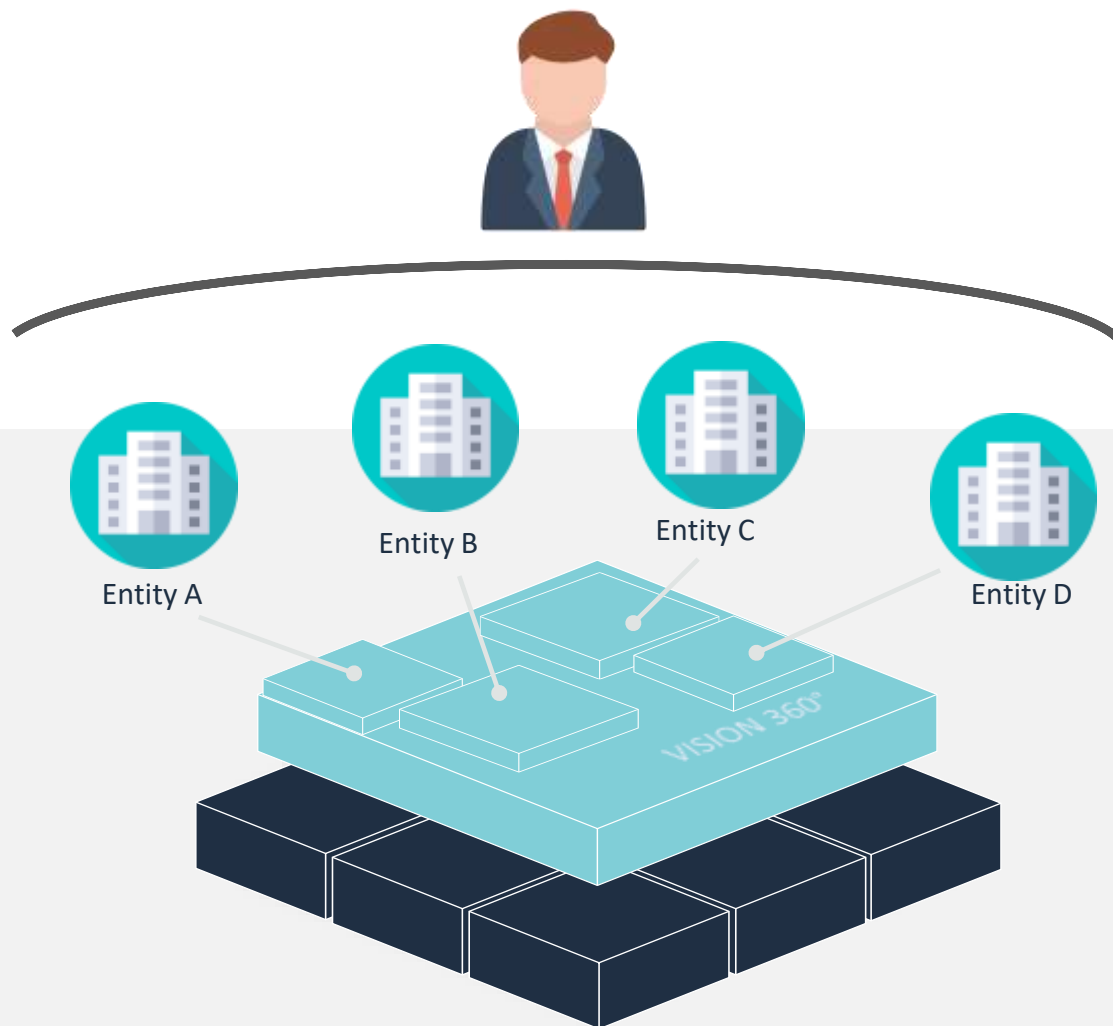
AFTER 2 YEARS IN AN ORGANISATION USING EGERIE

## Granular to 360° vision



WE BUILD AN ORCHESTRATOR

## Granular to 360 vision for all business stakeholders



### CISO

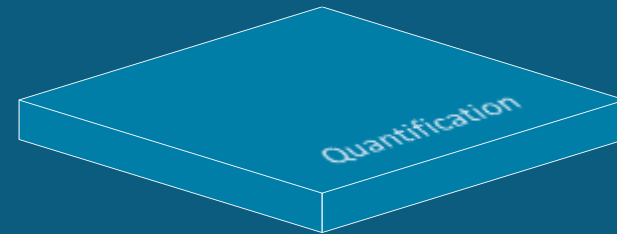
- Maintain a unified view of risks, metrics, and action plans with our 360° view of your cyber program
- Communicate an accurate picture of the state of your cyber security and compliance program performance to your executive committee.

### ENTITIES & RISK OWNERS

Each entity's risk owner has full visibility of its risk mapping, measures and treatment plan.

Dessert

Quantification and Governance



WE HELP YOU

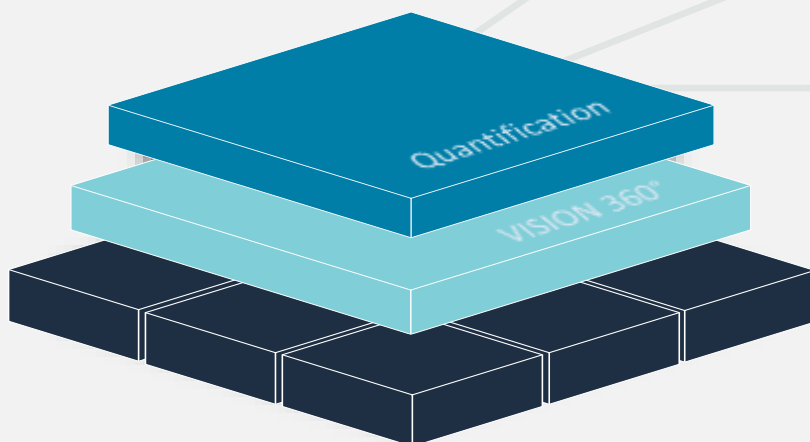
**Quantify risk** to prioritize and improve cybersecurity ROI by investing intelligently

### C LEVELS

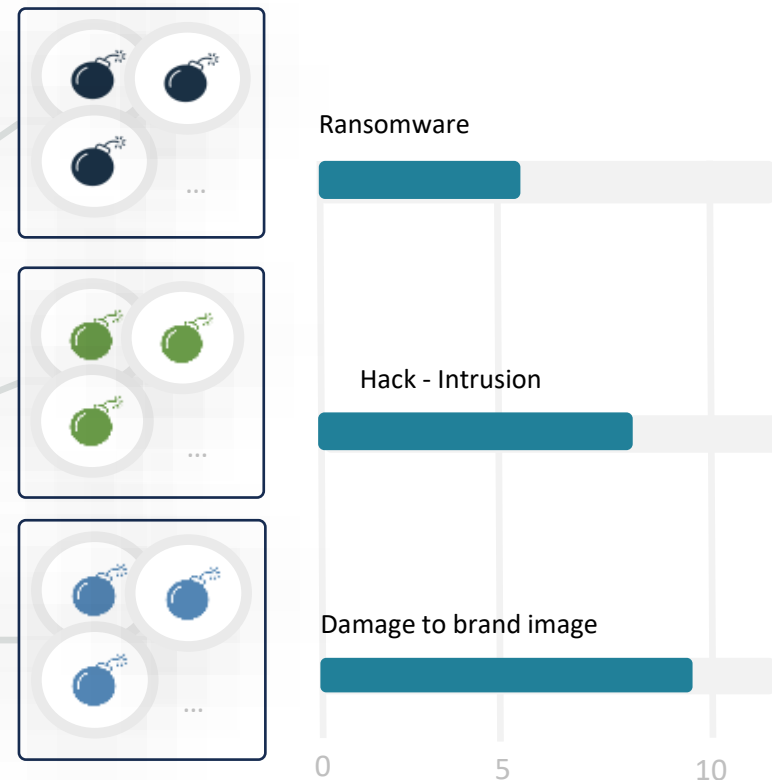
A business intelligence system for your cyber investments



- Gain clear visibility into cyber risk and compliance
- Accelerate decision making
- Governance and control of the cybersecurity program



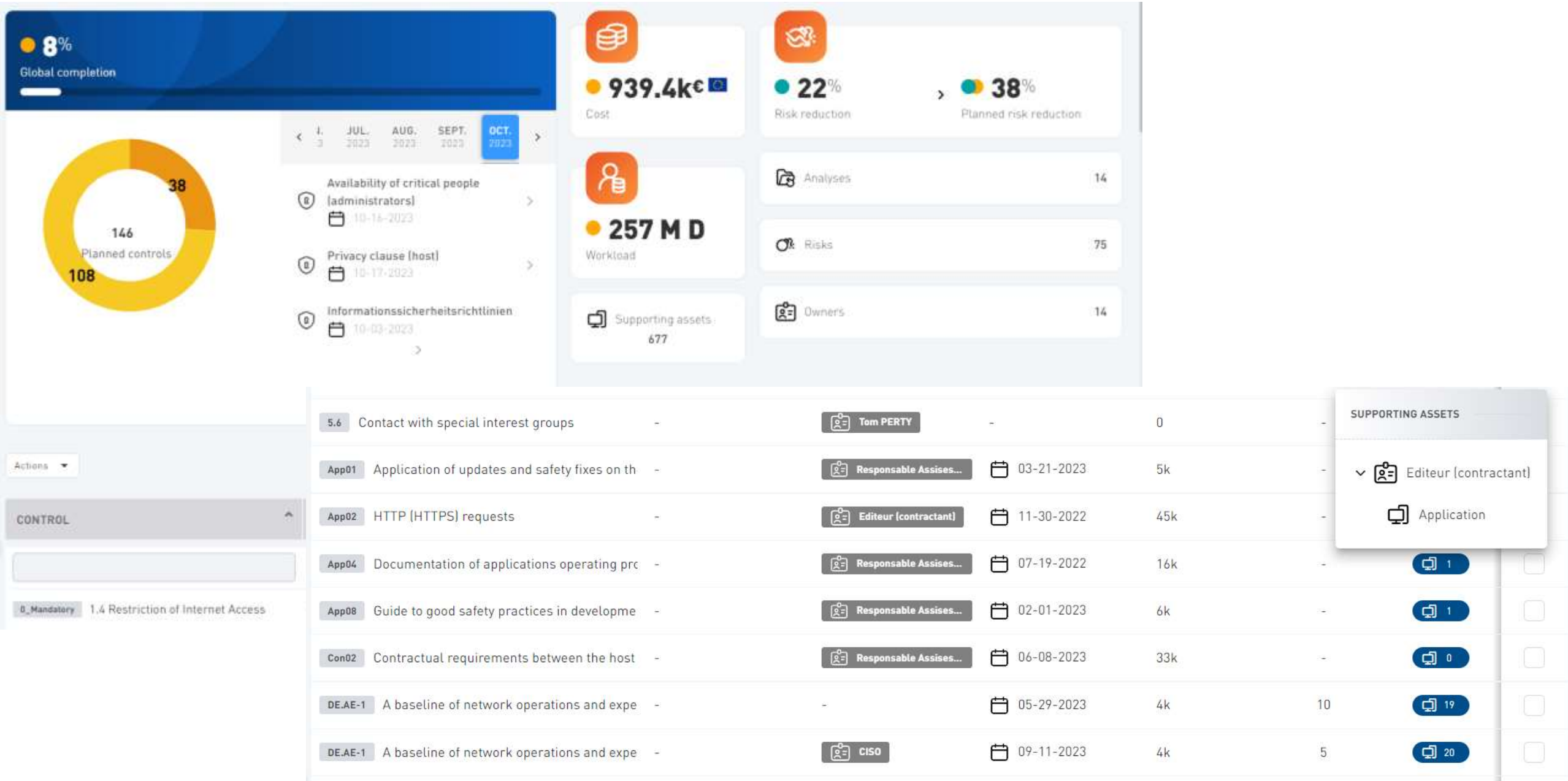
## Risk Universe



**Quantified Risk Exposure with aggregation by risk universe**

MANAGE YOUR TREATMENT PLAN

BUDGET – OWNERS - MANDAYS



# SCHNAPS DIGESTIVE



Sales Forecast By Division



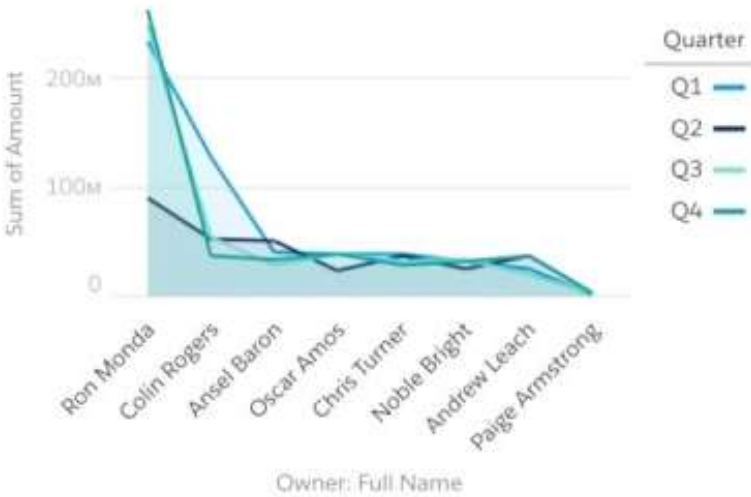
View Report

Sales Forecast-Current Quarter



View Report

Quota Achievement By Sales Rep

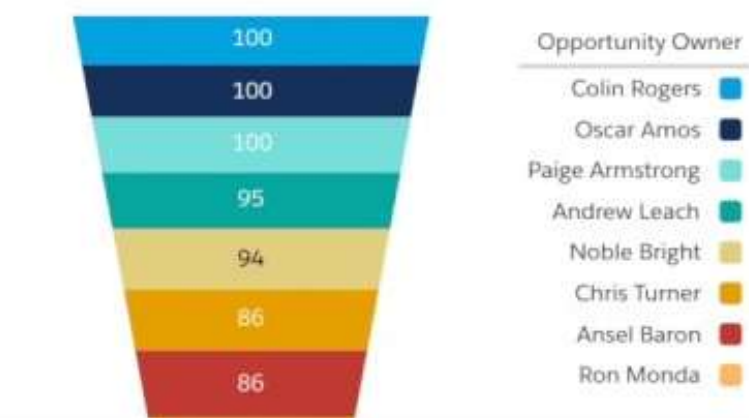


View Report

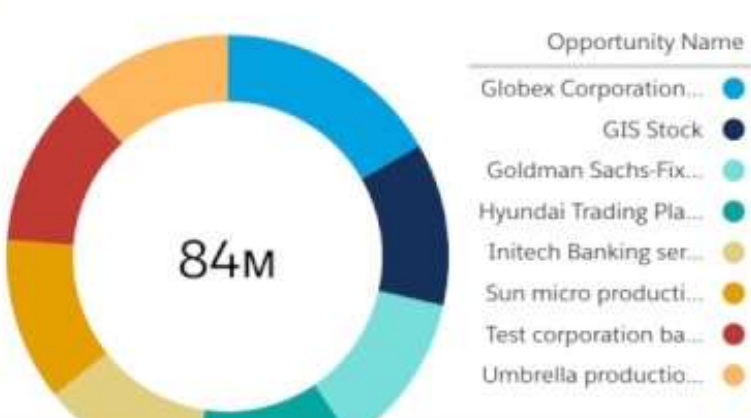
Sales Forecast by Service Line



Win Ratio By Sales Rep



Top Commit Deals



Legislation	Requirement	Applicability	Required?	Last Assessed Date	Next Assessment Date
<a href="#">Anti-terrorism, Crime and Security Act 2001</a>	An Act to amend the Terrorism Act 2000, to make further provision about terrorism and security, to provide for the freezing of assets, to make provision about investigation and detention, to amend or extend the criminal law and powers for preserving public order, to make provision about the control of passports and visas, to provide for the retention of criminal history data, to provide for representation of title of the High Court	Whole the police and security services, including foreign agencies, the power to visit public bodies, including schools, hospitals, customers and third parties to disclose personal records during terrorism and criminal investigations	Yes		
<a href="#">Security Act 2015</a>	An Act to make provision about offences relating to terrorism, and for connected purposes	Full cooperation may be liable for being in contact a person been looking on your behalf but only if that person performs, behaves for you in business. Reassessment of risks determined to be low to be considered	Yes		
<a href="#">Data Protection Act 1998</a>	An Act to provide for the protection of personal information, the power of certain discretionary powers and the supervisory and panel of official scrutiny bodies, in part proceedings, and the connected purposes	Retention of records required for formal investigations	Yes		
<a href="#">Information Act 2006</a>	An Act to reform a company law and make the greater part of the enactments relating to companies, to make other provision relating to companies and other forms of business organisation, to make provision about director disqualification, business names, business and accounts	Adherence to information security related laws such as the Data Protection Act	Yes		
<a href="#">Computer Misuse Act 2000, as amended by the Police and Justice Act 2006 (CMA)</a>	An Act to establish a National Policing Improvement Agency, to make provision about police forces and police authorities and about police powers, to make provision about police powers, and about the powers and duties of community to support the Computer Misuse Act 2000, to make provision about the failure of internet service providers	Full-time provision associated with Computer Misuse Act including increased penalties for "Unauthorized access with intent to impair operation of computer systems and networks" e.g. Penalties have increased from five to ten years imprisonment	Yes		
<a href="#">Copyright and Rights in Databases Regulations 2002</a>	In relation to measures relating to copyright and measures relating to the protection of unauthorised extraction of the contents of a database and of unauthorised re-utilisation of those contents	Data works rights and use of data which are contained and generated under the UK (Data Protection Act)	Yes		
<a href="#">Copyright, Designs and Patents Act 1988 (CDPA)</a>	An Act to amend the law of copyright, with amendments, to make fresh provision as to the rights of performers and others in performances, to confer a design right in original designs, to make a provision with respect to devices designed to circumvent copy protection of works or programs, to make fresh provision relating to the fraudulent acquisition of transmission, to make the fraudulent acquisition of use of a trade mark an offence	Data works rights and use of data which are contained and generated under the UK (Data Protection Act)	Yes		
<a href="#">Copyright, Designs and Patents Act 1988 (CDPA)</a>	An Act to amend the Copyright, Designs and Patents Act 1988 in respect of private offences, certain actions, powers of seizure and orders for forfeiture	Use of data which is contained and generated under the UK (Data Protection Act)	Yes		
<a href="#">General Data Protection Regulation (GDPR)</a>	An Act to confer further powers to gather and share information for counterterrorism and other purposes	Management of information, its retention and destruction also controlled and generated under the UK (Data Protection Act)	Yes		
<a href="#">Information Regulation Act 2017</a>	An Act to reform the law of copyright and make as to offences of disclosure to internet	Retention of records of information records, their retention and	Yes		

Date Complete: 13 <sup>th</sup> Sept 2013	What is being Assessed: Fire Open Day – General Risk Assessment				Ref:	
Date Amended:	Name(s) of Risk Assessor(s): Mike McAdams					
	Practical Advice:			Compliance Advice		
Hazard Identified & Existing control measures:			L	S	R	Plan of Action -- ALARP:
<b>Fire: Injury to Members of the Public &amp; Tree Personnel, &amp; Property damage.</b> <ul style="list-style-type: none"> <li>Area risk assessed via specific Fire Risk Assessment.</li> <li><b>Control Measure</b> <ul style="list-style-type: none"> <li>Testing Regimes for fire protection / detection systems controlled through Tullis Russell Papermakers.</li> <li>Smoking only permitted in a designated area</li> </ul> </li> </ul>			1	5	5	<ul style="list-style-type: none"> <li>As Low As Reasonably Practicable.</li> </ul>
<b>Falls from Height: Associated Injury to Members of the Public &amp; Tree Personnel.</b> <ul style="list-style-type: none"> <li><b>Control Measure</b> <ul style="list-style-type: none"> <li>Handrails &amp; guards provided on high level access routes.</li> <li>Doorway to upper levels of the Airspace to be kept locked at all times during the public visits.</li> </ul> </li> </ul>			1	5	5	<ul style="list-style-type: none"> <li>As Low As Reasonably Practicable.</li> </ul>
<ul style="list-style-type: none"> <li><b>Contact with hot surfaces / substances: Burns &amp; Scolds to members of the Public &amp; TREE Personnel.</b></li> <li><b>Control Measure</b> <ul style="list-style-type: none"> <li>Kitchen restricted to TREE Volunteers by securing the doorways. No access to members of the public</li> <li>Hot drinks only to be given to adults and young persons under the supervision of an adult.</li> <li>No Hot drinks to be provided to children.</li> <li>Children to be supervised by an appropriate adult at all times to ensure correct behaviour.</li> <li>Designated refreshment area.</li> <li>Hot surfaces are either out of reach or lazeed</li> </ul> </li> </ul>			1	4	4	<ul style="list-style-type: none"> <li>As Low As Reasonably Practicable.</li> </ul>
			1	5	5	<ul style="list-style-type: none"> <li>As Low As Reasonably Practicable.</li> </ul>

	A	B	C	D	E	F	G	H	I	J	K
1	Risk Treatment Table implemented from [date] to [date]										
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											
18											
19											

Risk & Opportunity Register											
Identification of			Risk Significance = Impact x Likelihood x Frequency				Risk Level		Response Priority		Compliance Obligation
Ref	Business Objective	Risk Category	Risk Description	A - Impact (1 to 4)	B - Legal (1 to 4)	C - Likelihood (1 to 4)	D - Frequency (1 to 4)	Risk Significance	Risk Level	Response Priority	Compliance Obligation
1	To improve health and safety	OH&S Risk	Incidents and hazardous situations that impact on OH&S	4	4	4	4	24	Very High	Avoid the Risk	Health & Safety at Work Act
2	Improve shareholder value	Market Risk	Changing market trend, requirements and demands	4	2	2	4	16	High	Minimise the Risk	Permanent market requirements and
3	Improve resource optimisation	People Risk	Risk of lack of qualified workers	1	1	1	1	1	Low	Accept the Risk	ISO 9001:2015 (800/275) 8.2.3.2
4	Maximise sustainable growth	Financial Risk	Lack of working capital to meet day to day trading requirements	4	1	2	1	13	Medium	Transfer the Risk	None
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											
18											
19											

BA

BAPTISTEB >



WELCOME

Cockpit

My contributions

360 VISION

Risks

Controls

Treatment plan

RISK MANAGEMENT

Modules

Libraries

RISK MANAGER

CURRENT SITUATION

ACTION PLAN

PLANNED SITUATION

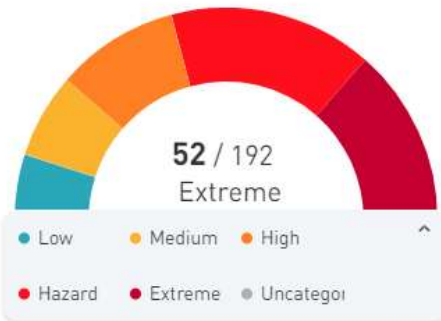


SAVINGS 5M€ ROI 434%

Current risks

CURRENT

RESIDUAL



174 Current risks above the threshold

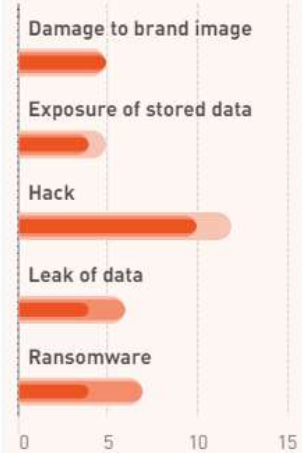
Risk universe

ANNUAL LOSSES



Raw Current Residual

RISKS ABOVE THRESHOLDS



Raw Current Residual



54%

Analyses progress

15 Ongoing analyses



241

Supporting assets

My critical supporting assets

VIELEN DANK

Treffen Sie uns am  
Stand 7-245