SCALING FAIR for M&A and Beyond

Combining **bottom-up** and **top-down** approaches

Cedric De Carvalho – Head of Group Cyber Risk & Advisory

RICHEMONT

September 2022

FAIR22 CONFERENCE

Presentation - Disclaimer

- For confidentiality purpose, data have been anonymized in this presentation
- Figures and Loss Exceedance Curves are for illustration only

Today's Agenda

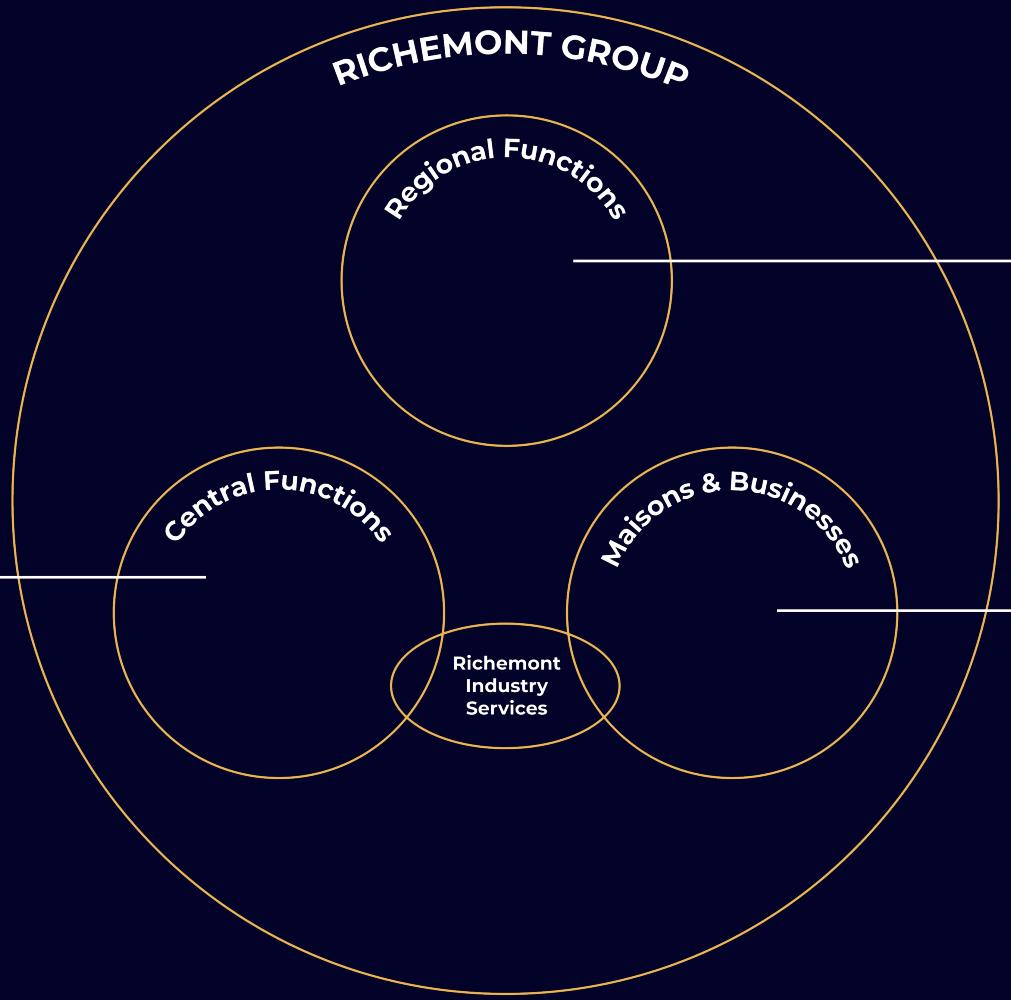
FAIR22 CONFERENCE

Richemont Group – Who are we?

- **26** Maisons and Businesses
- **4** Business Areas (Jewelry, Watchmakers, Online Distributors and Fashion & Accessories)
- **2 297** Monobrand Boutiques
- **35 000+** Colleagues across more than **130** countries

FAIR22 CONFERENCE

Richemont Group – Our organization



Operating behind the scenes, linking all central and regional support to our Maisons.

Provide tools, support teams and development initiatives to our Maisons.

In charge of creation, manufacturing and customer services.

FAIR22 CONFERENCE

Richemont Group – The challenge

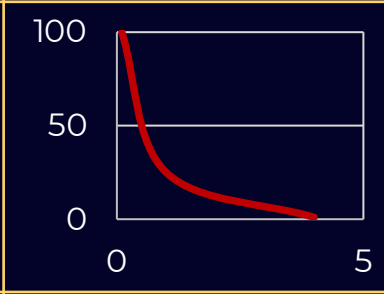
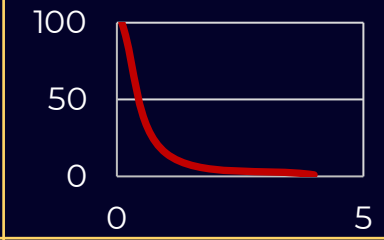
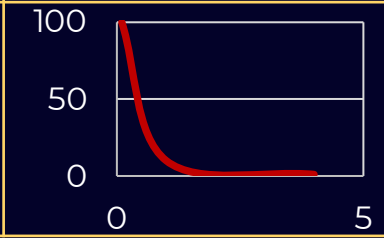
How to enable cost-effective **business decision** by scaling FAIR to companies of different sizes, operations and objectives?

Before

	Low	Minor	Moderate	Major	Extreme
Almost certain					
Likely					
Possible					
Unlikely					
Rare					

Now

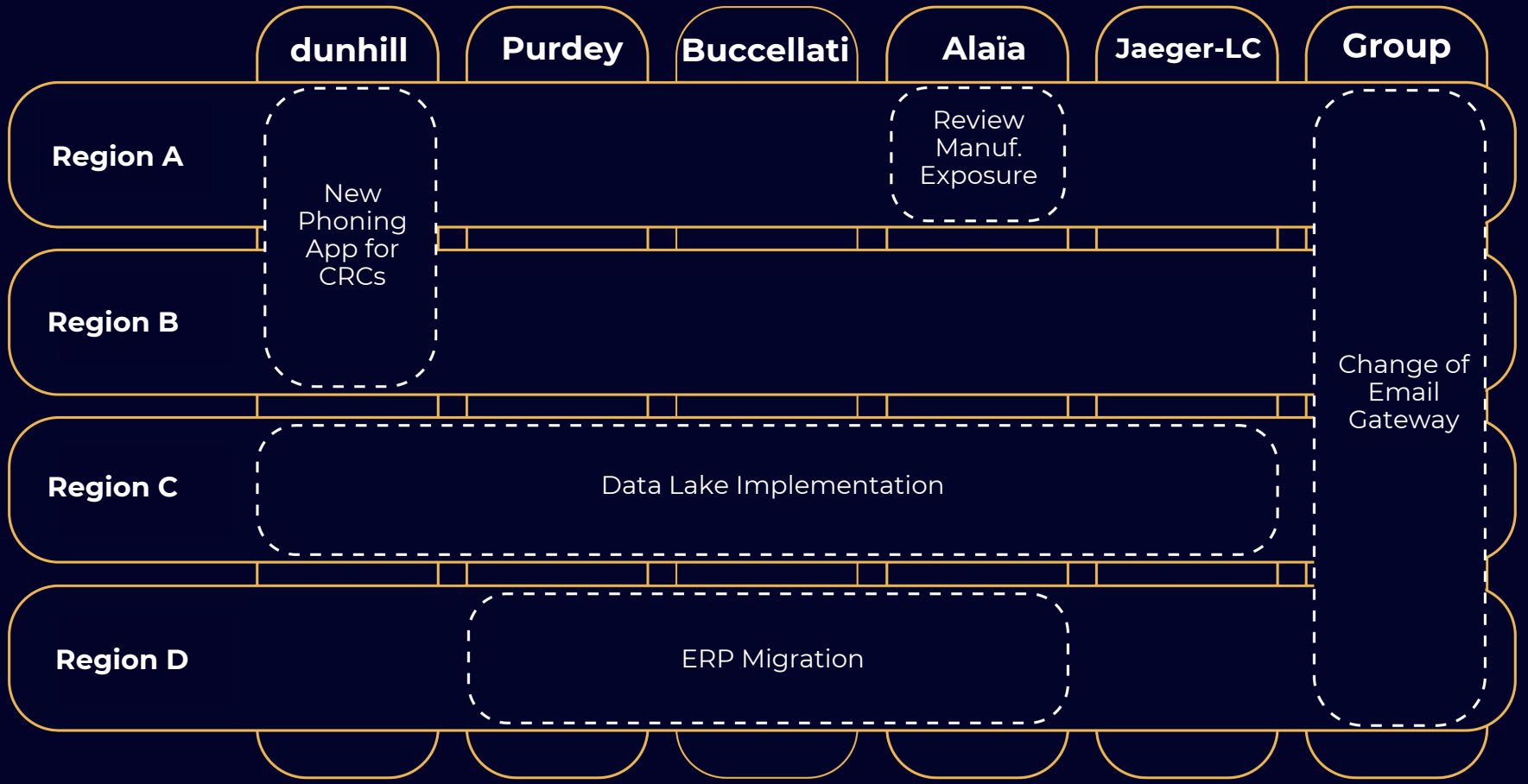
Top-Down Approach – Identify Top Risks

Risk scenario	Average Annualized Loss Exposure	Risk decision	Loss Exceedance Curve
Loss of confidentiality of PII contained in the European Data Lake (ext. threat)	$ 1'480'000	Mitigate	
Loss of Availability of the manufacturing lines (internal error)	$ 1'225'000	Mitigate	
Loss of Integrity of financial data processed in SAP	$ 890'000	Accepted	

FAIR22 CONFERENCE

Top-Down Approach – Support decision making process

Which strategic project should be prioritized?

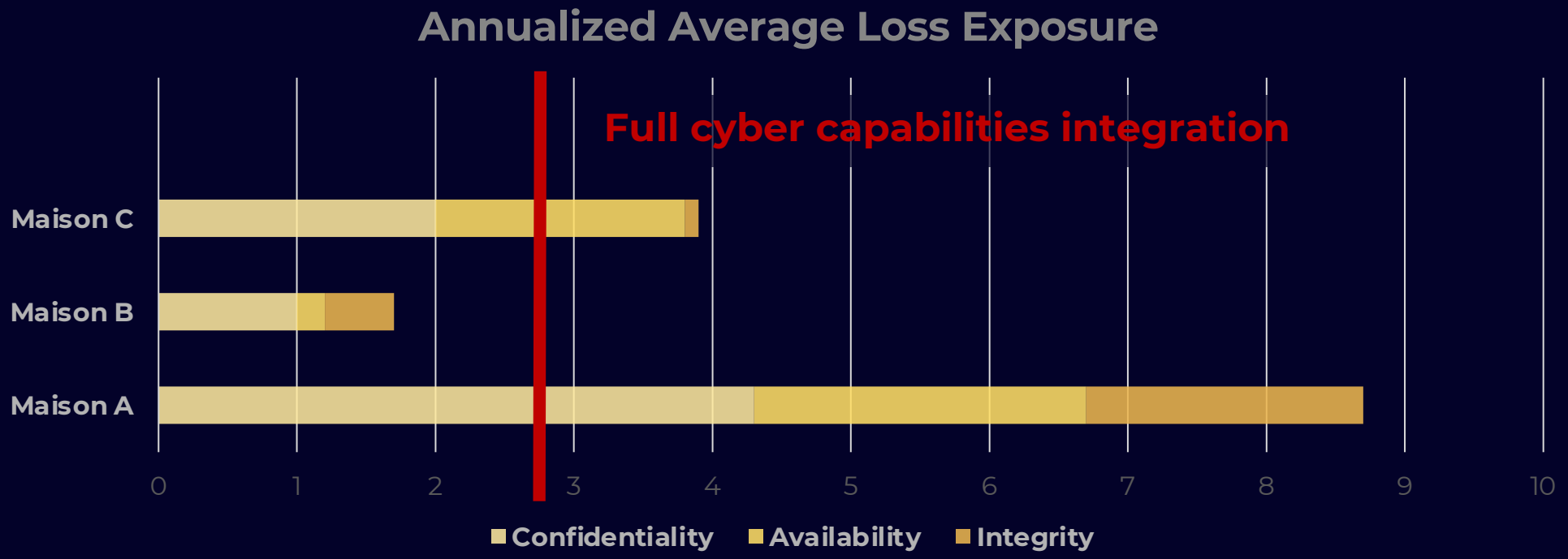


FAIR22 CONFERENCE

Top-Down Approach – Use cases

Merger & Acquisitions

What is the most cost-effective way of managing Cyber Risk of new Maisons?



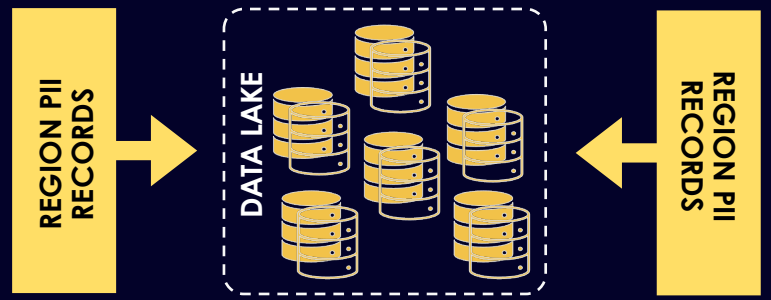
FAIR22 CONFERENCE

Top-Down Approach – Use cases

Technology & Data

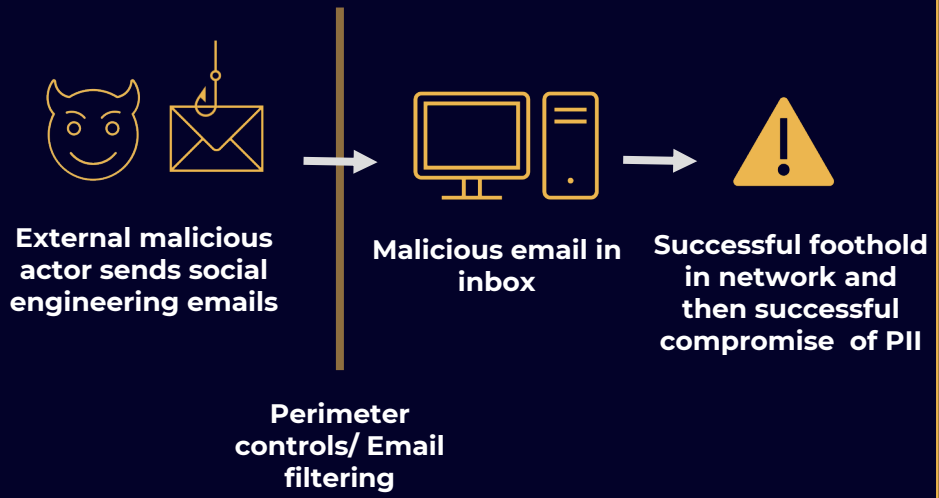
Business-oriented Initiative

Data Lake implementation in a specific region



Technology-oriented Initiative

Email gateway change

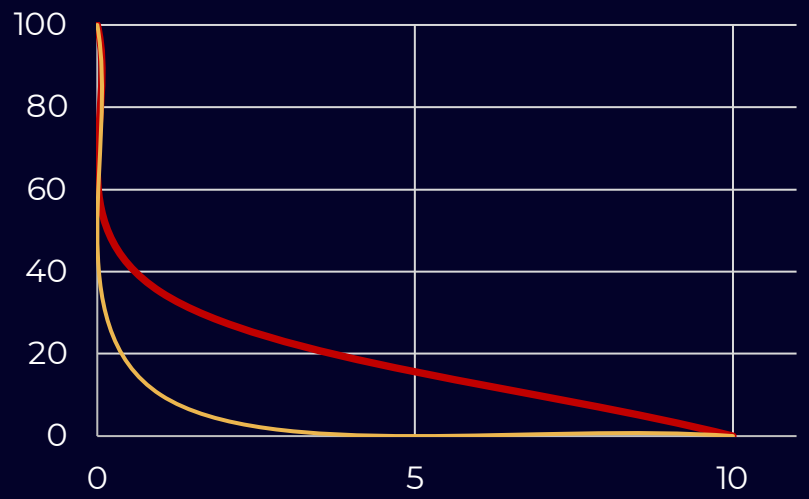


Top-Down Approach – Executive summary

Risk Scenarios	1. Internal Malicious actor exfiltrating PII records from Regional Lake 2. External attacker obtaining a phishing Foothold used to breach PII records in Regional Data Lake

Loss Exceedance Probabilities

The loss exceedance curve is the output of the 50'000 iterations of the Monte Carlo simulations. It helps to visualize the **probability of the loss exceeding** a certain amount.



Average Annualized Loss Exposure

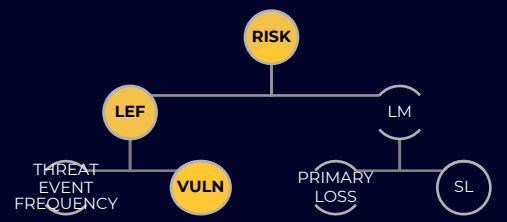
Foreseen annualized amount of risk associated with the hosting of PII in Richemont Regional Data Lake is **CHF 10.2M***, over which CHF 9M are originated by the **malicious insider risk scenario**.

Given the nature of the risk (low frequency and high impact), it was strongly advised to consider that there is a 10% annual probability to suffer a € 62M or greater loss.

**Fictitious values*

FAIR22 CONFERENCE

Top-Down Approach – Cost Benefit



Vulnerability

Baseline

Vulnerability	
Minimum	25%
Most Likely	45%
Maximum	60%

Access is provisioned through Active Directory. This is an SSO solution with no MFA or encryption in place.

Team is responsible for patching monthly.

No proper IAM in place.

Cost Benefit

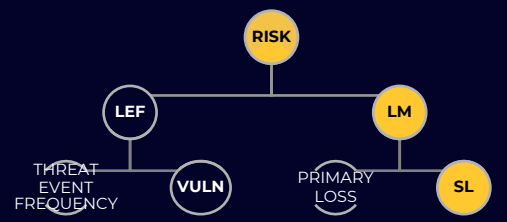
Vulnerability	
Minimum	5%
Most Likely	10%
Maximum	20%

Baseline control environment enhanced with:

- Implementation of **Multi Factor Authentication**;
- Implementation of **proven robust IAM**.

Top-Down Approach – Cost Benefit

Loss event detection/ recognition



Baseline

Loss Event Detection	
Minimum	2%
Most Likely	8%
Maximum	25%

Loss Event Recognition	
Minimum	1%
Most Likely	2%
Maximum	5%

Currently no logging or monitoring in place

Cost Benefit

Loss Event Detection	
Minimum	70%
Most Likely	91%
Maximum	99%

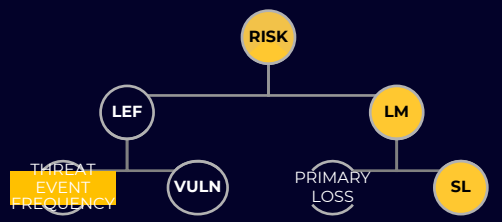
Loss Event Recognition	
Minimum	1%
Most Likely	15%
Maximum	48%

Baseline control environment enhanced with:

- Implementation proper **logging and monitoring** of user's activities;
- Development of **playbooks dedicated to those risk scenarios.**

Top-Down Approach – Cost Benefit

of customer records



Baseline

# of customer records	
Minimum	1M
Most Likely	3.6M
Maximum	5.1M

PII data for all Group is estimated to be a maximum of 5.1M. This represents the maximum number of records with the potential to be breached. However, some users, will only have access to a subset of this data, which means the threat actor would not be able to access this maximum so:

- **Minimum: # of records accessible to data science segregated environment;**
- **Maximum: total # of customer records in data lake.**

Cost Benefit

# of customer records	
Minimum	1M
Most Likely	2.5M
Maximum	5.1M

Sound and proof Identity and Access Management will reduce the number of records that may be breached in the case of an incident.

Assumption is that the Most Likely value will be **reduced by 30%.**

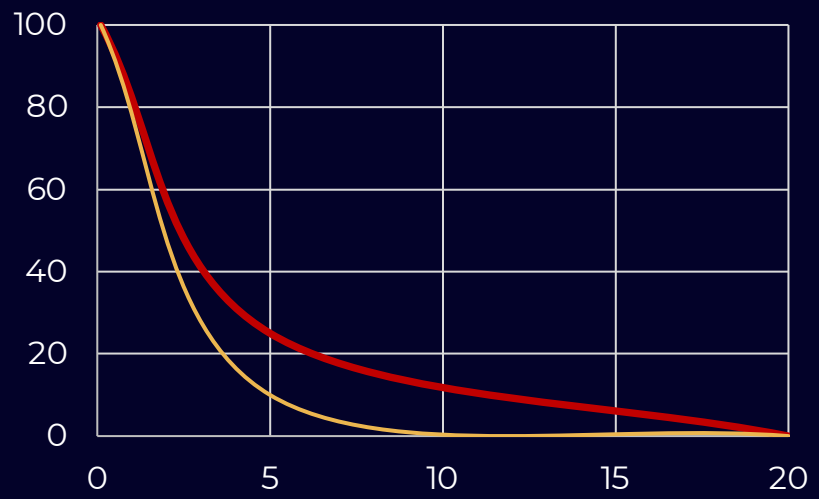
FAIR22 CONFERENCE

Top-Down Approach – Executive summary

Risk Scenarios	External attacker obtaining a **credentialed foothold** to a **specific system** using **phishing,** leading to a **loss of confidentiality**

Loss Exceedance Probabilities

The loss exceedance curve is the output of the 50'000 iterations of the Monte Carlo simulations. It helps to visualize the **probability of the loss exceeding** a certain amount.



Average Annualized Loss Exposure

The quantitative cyber risk assessment demonstrated that Richemont should move forward with the Mail Gateway investment as it will provide an annualized € 10 M risk reduction for the € 0.6 M spent, which provides significant ROI (return on investment) and drives towards core enterprise goals.

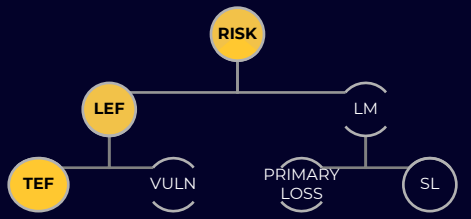
These reductions of expected foothold events reduce the average annualized expected loss from € 25 M to € 6 M.
In terms of loss exceedance, there was an annual probability of ~20% to exceed € 10 M for the current Mail Gateway solution; and has decreased to ~ 5% in the case of implementation of the new solution.

**Fictitious values*

FAIR22 CONFERENCE

Top-Down Approach – Cost Benefit

Threat Event Frequency



Before Project

Number of clicked malware (annually)	
Minimum	26 clicks
Most Likely	96 clicks
Maximum	182 clicks

Threat Event Frequency

Minimum once **every 19 years**

Most Likely once **every 3.5 years**

Maximum once **every 1.3 years**

After Project

Number of clicked malware (annually)	
Minimum	13 clicks
Most Likely	22 clicks
Maximum	40 clicks

Threat Event Frequency

Minimum once **every 38 years**

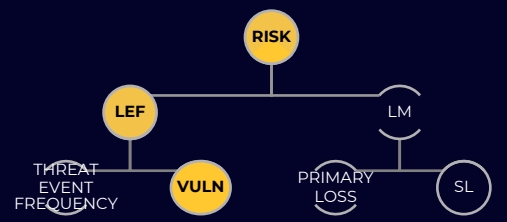
Most Likely once **every 15 years**

Maximum once **every 6.25 years**

FAIR22 CONFERENCE

Top-Down Approach – Cost Benefit

Vulnerability



Effectiveness of controls

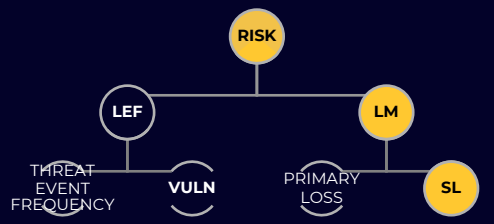
Vulnerability	
Segmentation	Effective
IPS / IDS	Ineffective
IAM Controls	Partially effective
Patching management	Ineffective
Multi-Factor Authentication	Ineffective
Transport security	Effective

Cost Benefit

There is a 60% probability of an external actor compromising specific system being successful

Top-Down Approach – Cost Benefit

Loss Magnitude Factors



Response costs

Number of hours spent by CSIRT	
Minimum	250 hours
Most Likely	550 hours
Maximum	1400 hours

Average employee wage	
Minimum	$ 20
Most Likely	$ 52
Maximum	$ 180

The response cost was estimated based on the historical events as well as on the professional judgment of CSIRT SMEs.

The response cost is split into two variables:
1. Number of hours spent by CSIRT in such a scenario
2. Average employee wage

Reputational impact

Customer's worth over the lifetime of the customer's relationship	
Minimum	$ 300
Most Likely	$ 9'000
Maximum	$ 40'000

The reputational impact involves the present value of the lifetime revenue of an average customer across some Maisons.

Calculation was based on the metrics:
1. # of years of purchasing,
2. # of purchase per year,
3. Amount per purchase.

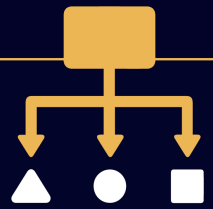
FAIR22 CONFERENCE

Top-Down Approach – Challenges

Takes times to cover entire organization

Creates frustration for decision-makers if the assessment cannot be delivered swiftly

Difficulty to update assessments performed in silos

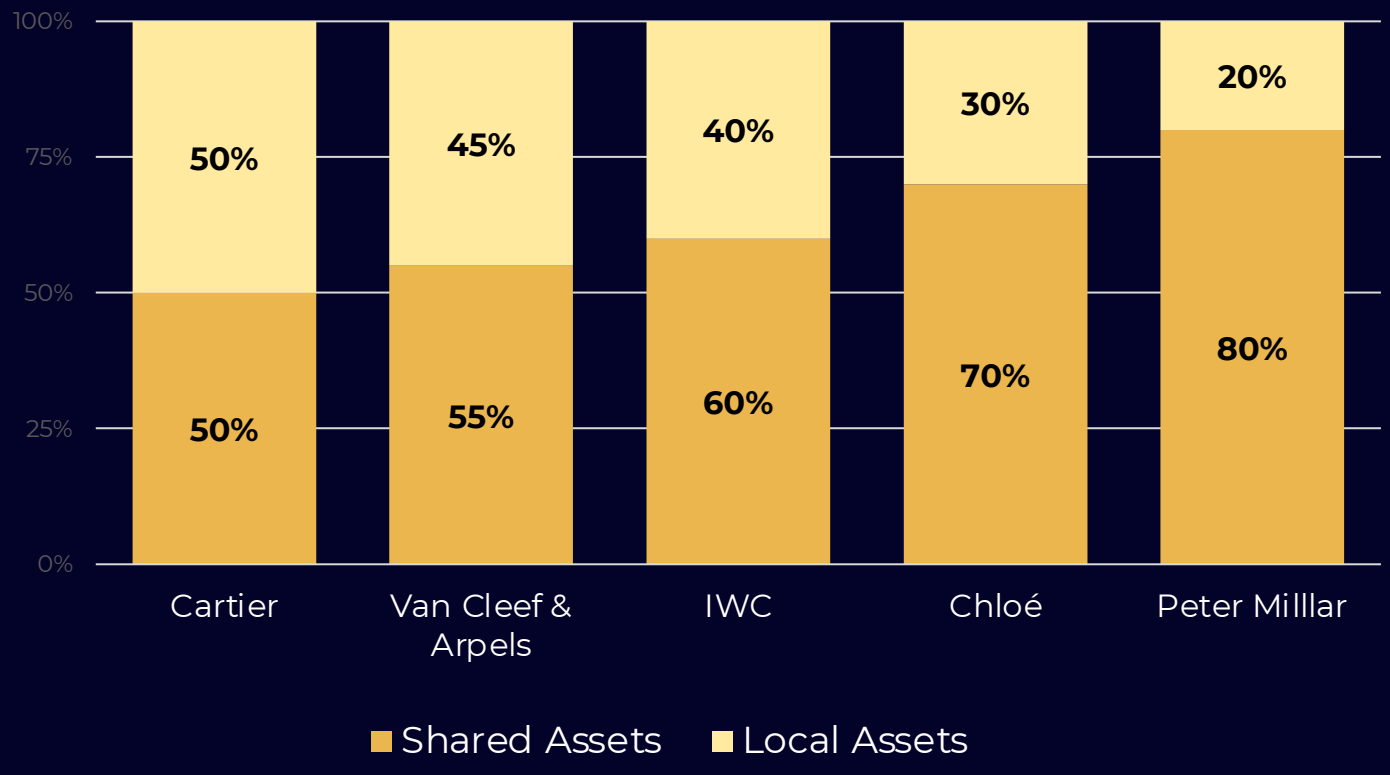


Difficulty to impact all scenarios with new threats or new control in place at once

Bottom-Up Approach – Think differently

When assessing the first entity, we quickly noticed that Group assets were hard to manage

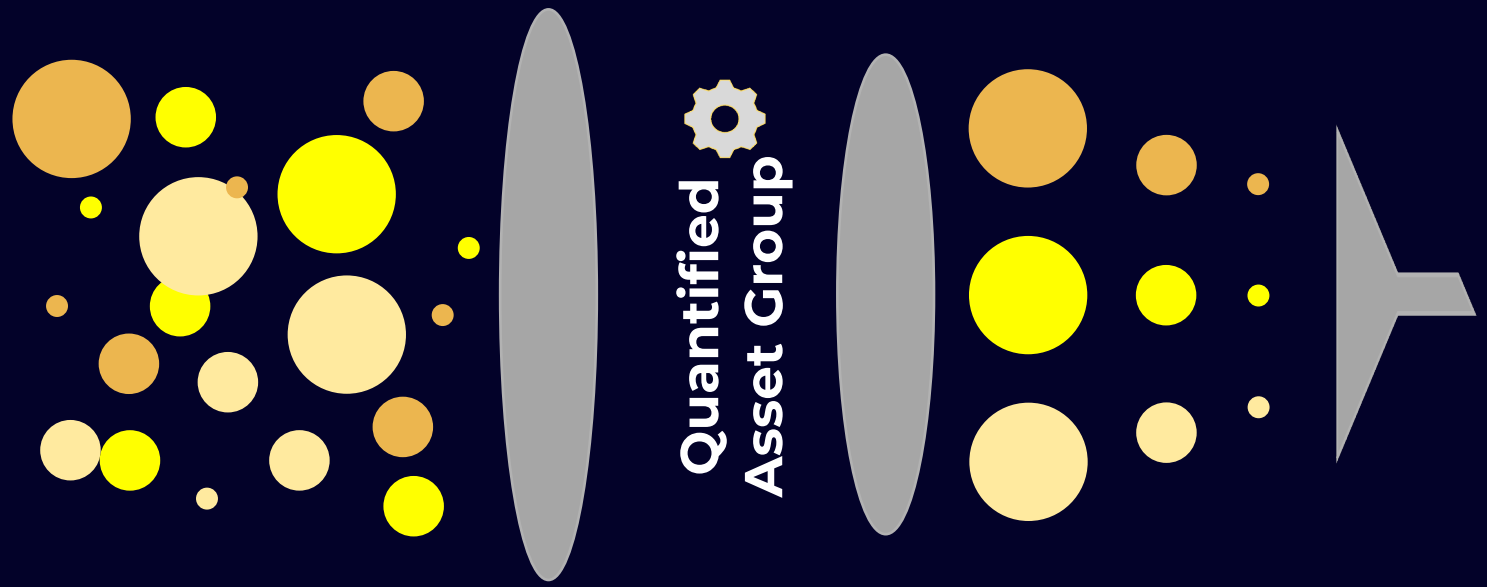
Scoping shifted from vertical to transversal



FAIR22 CONFERENCE

Bottom-Up Approach – How to scale

Challenge -> too many assets, almost impossible to assess and manage



Same:

- Control Environment
- Geographic region
- Type of information
- …

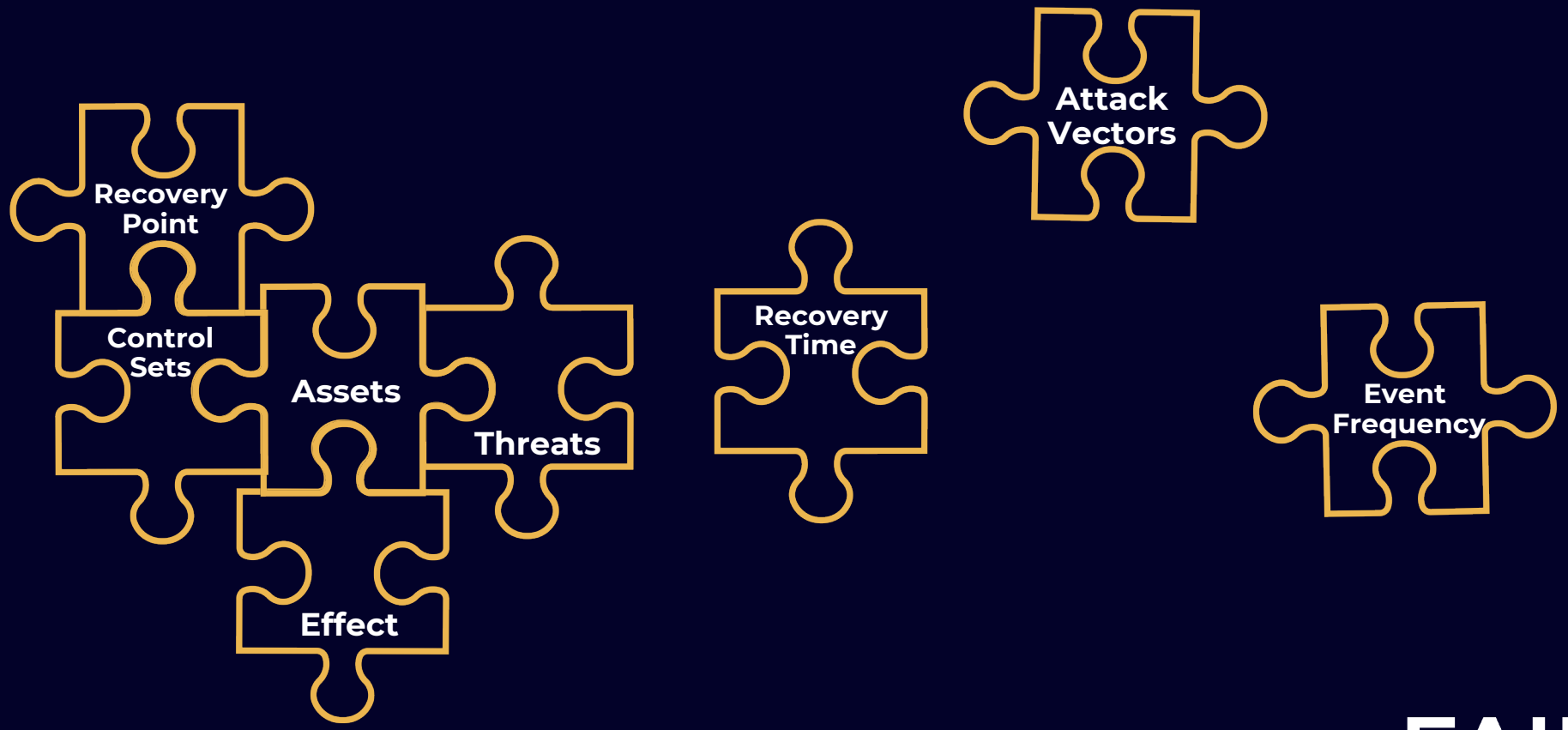
Better ability to select:

Risk Scenarios

- Attack vector
- Potential threat actor
- Data table (i.e. losses)
- …

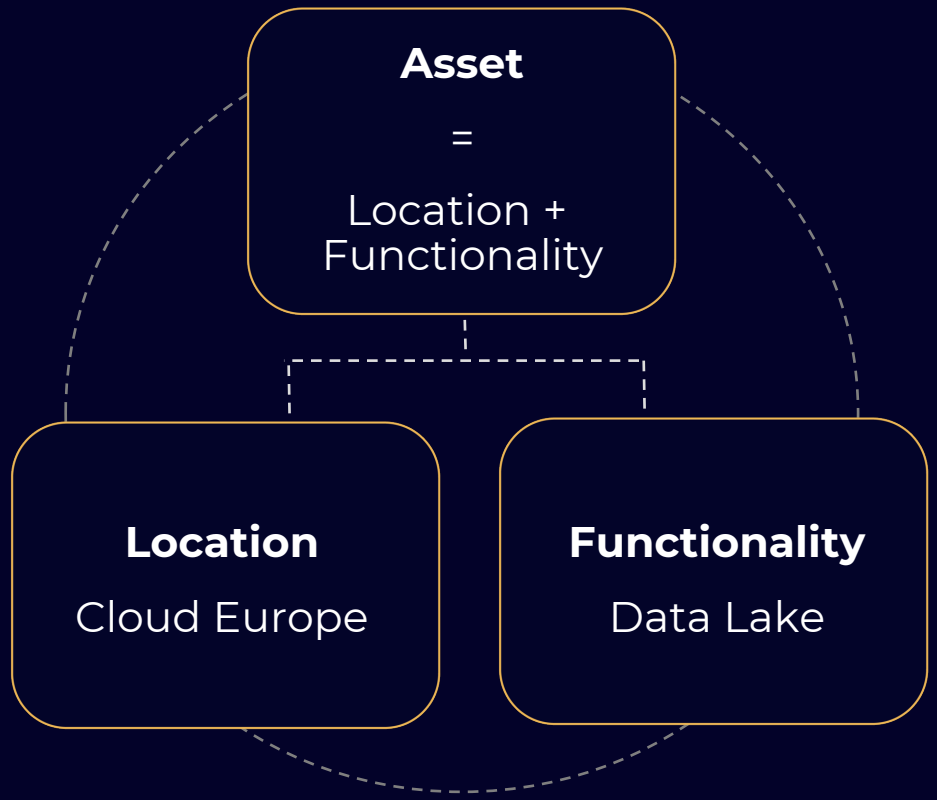
Bottom-Up Approach – How?

Defining reusable blocks to be used across the Ontology



Bottom-Up Approach – Common Control Sets

Once the attack vector is defined, a common control set will help to get faster results for the vulnerability part of the Ontology



Phishing

Identify & Access Mgmt. process
Intrusion Detection System
Authentication process

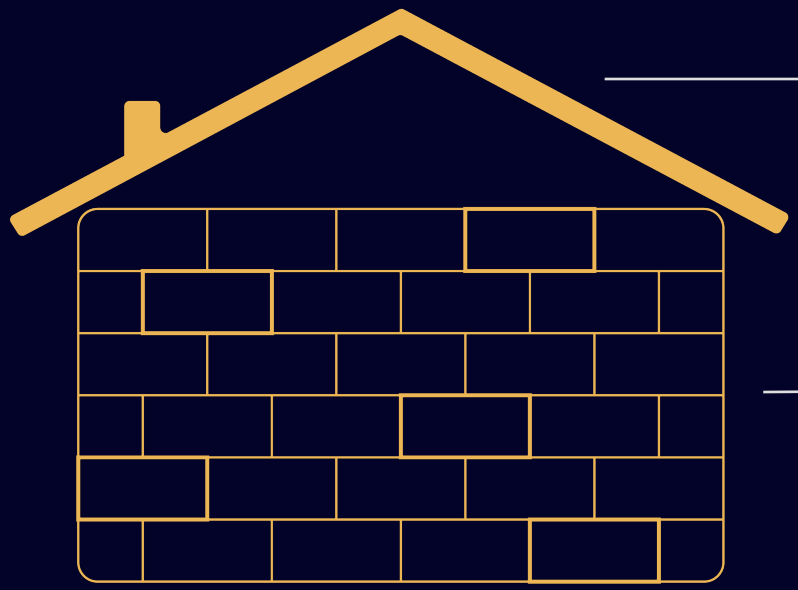
FAIR22 CONFERENCE

Bottom-Up Approach – Scale FAIR

Combine both approach, develop real time quantified risk register

Combined Approach – Filling the gaps

Continuous monitoring of the whole organization



Top-Down Approach

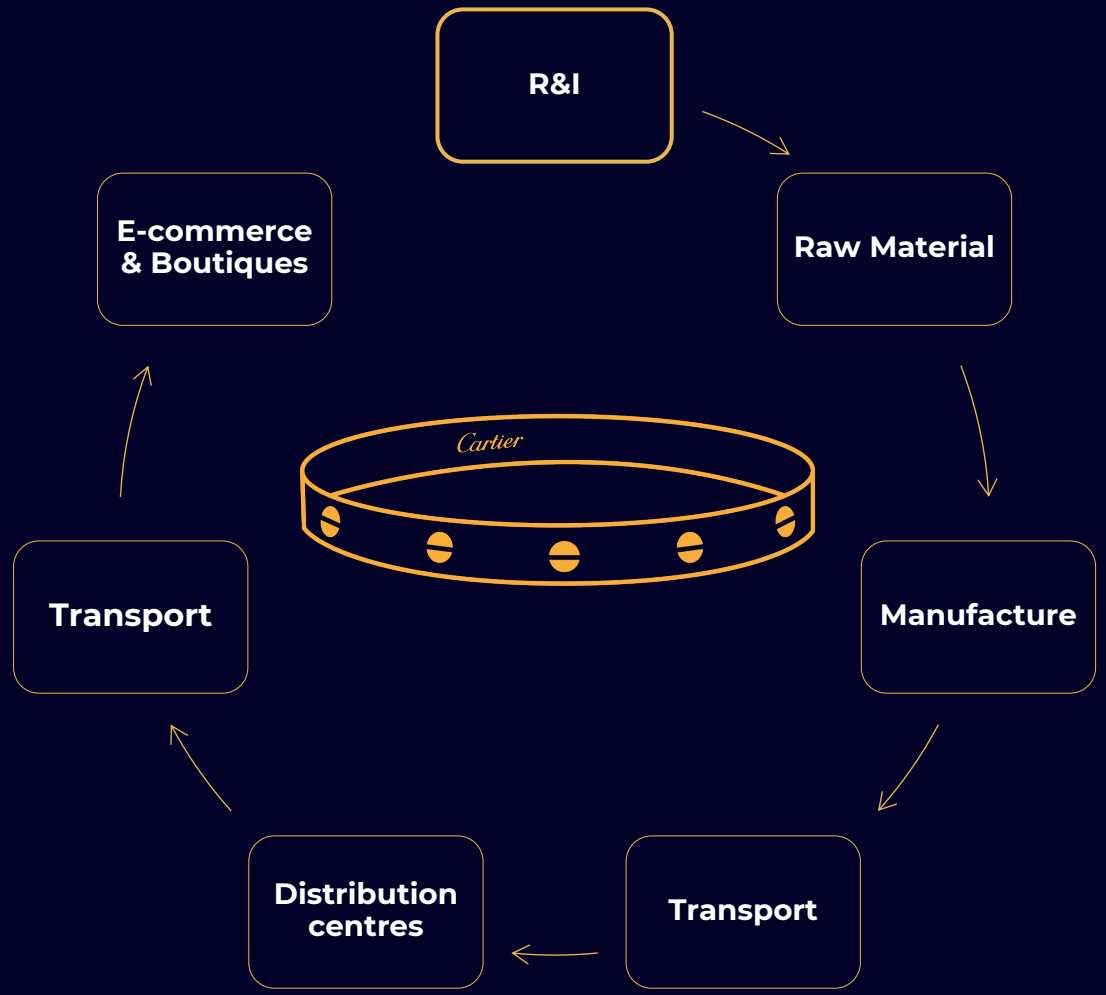
• Identifying the main, and most visible risks

Bottom-Up Approach

• Construct a solid and flexible baseline to complement the Top Down Approach

Combined Approach – Use case

Cartier Love bracelet: how much risk is associated with the entire lifecycle of this product?



Key takeaways

- Traditional scoping from qualitative approach might not be the most effective way to scale FAIR. **Think differently**

- **Enable top management to adopt quantification by**
  - Using critical business decision as first use cases
  - Incrementally showing more and more “insights”

- **Building a cyber quantification factory** is a comprehensive and repeatable way of scaling FAIR, both for strategic and operational assessments

- When ready, **automate operational cyber assessments**

Questions

Scan this QR code if you want to connect with me via LinkedIn

cedric.decarvalho@richemont.com