metricstream

GRC
SUMMIT 2022

LONDON, NOV 8-9

Hosted by MetricStream

C-Risk: The Value of Adopting Cyber Risk Quantification

Tom Callaghan, Co-Founder, C-Risk

Joy Bhowmick, Head of Research and Development, MetricStream

- What is Cyber Risk Quantification?
- CRQ Use cases and adoption
- How to quantify cyber risk in financial terms?
- How to build a CRQ capability?
- Conclusion

What is Cyber Risk Quantificaiton

It is the USE OF quantification techniques, models, and frameworks to CALCULATE an organization's exposure to risk, in monetary terms.

Key Points:

- Not about precision but accuracy.
- A tool for decision making
- A technique which is complimentary to existing risk management appoaches
- Improves objectivity
- We are still modelling uncertainly therefore we work with ranges of data
- Requires a number of tools to implement
- Is not a new scientific discipline
- We advocate the usage of open standards such as FAIR to promote innovation and transparency

What is Cyber Risk Quantificaiton

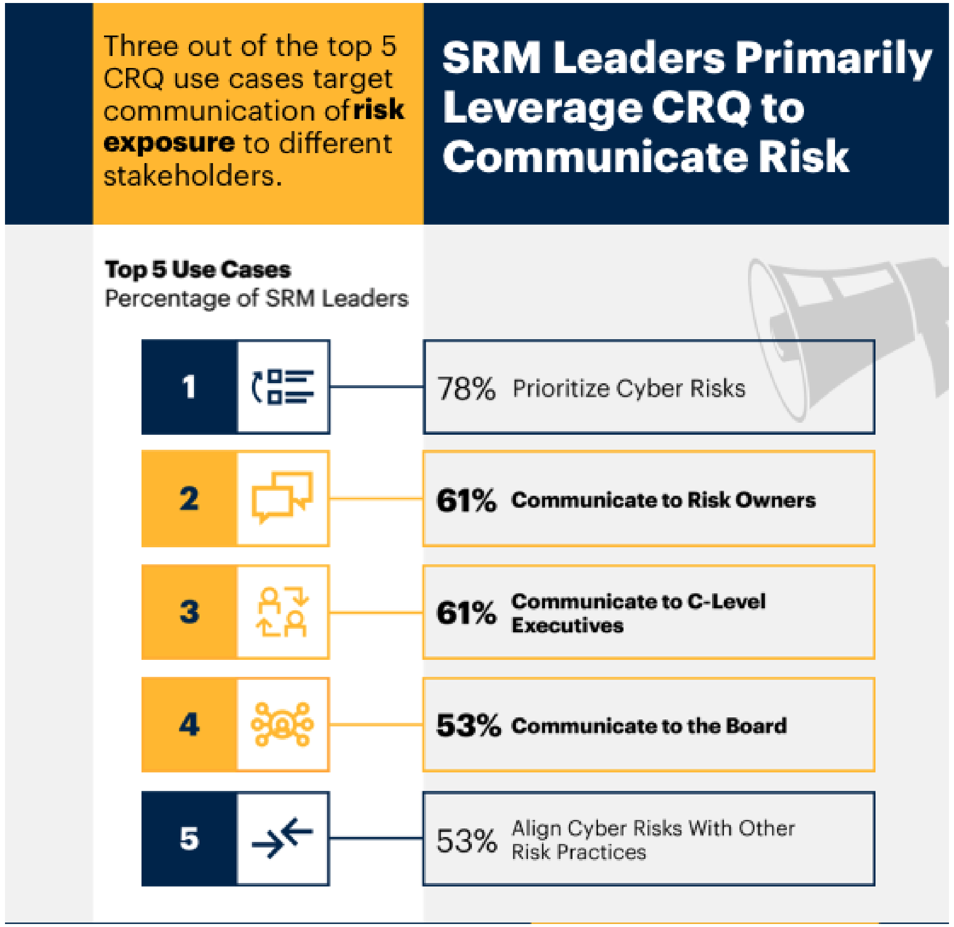
It is the USE OF quantification techniques, models, and frameworks to CALCULATE an organization's exposure to risk, in monetary terms.

Show an example output

An example CRQ assessment.

- Show a simple picture from Metricstream module combined with C-Risk reporting module showing:
  - Loss per event
  - ALE
  - 10 percentile, average, ML, 90% etc..

CRQ Use Cases



Three out of the top 5 CRQ use cases target communication of **risk exposure** to different stakeholders.

SRM Leaders Primarily Leverage CRQ to Communicate Risk

Top 5 Use Cases
Percentage of SRM Leaders

1	78%	Prioritize Cyber Risks
2	**61%**	**Communicate to Risk Owners**
3	**61%**	**Communicate to C-Level Executives**
4	**53%**	**Communicate to the Board**
5	53%	Align Cyber Risks With Other Risk Practices

Source: 2021 Gartner Cyber-Risk Quantification Survey

- Communicate to Board & Exec Management
- Size, Allocate and justify Infosec budget
- Optimize Cyber insurance coverage
- Facilitate regulatory compliance
- Understand 3rd party risk exposure
- Choose an efficient risk reduction strategy
- Merger & Acquisitions

Source: 2019-22 C-Risk most frequent use cases

The Evolution of CRQ Advocacy

International Standards & Frameworks

- NIST National Institute of Standards and Technology
- (ISC)²
- ISO
- ISACA

International Professional Organisations

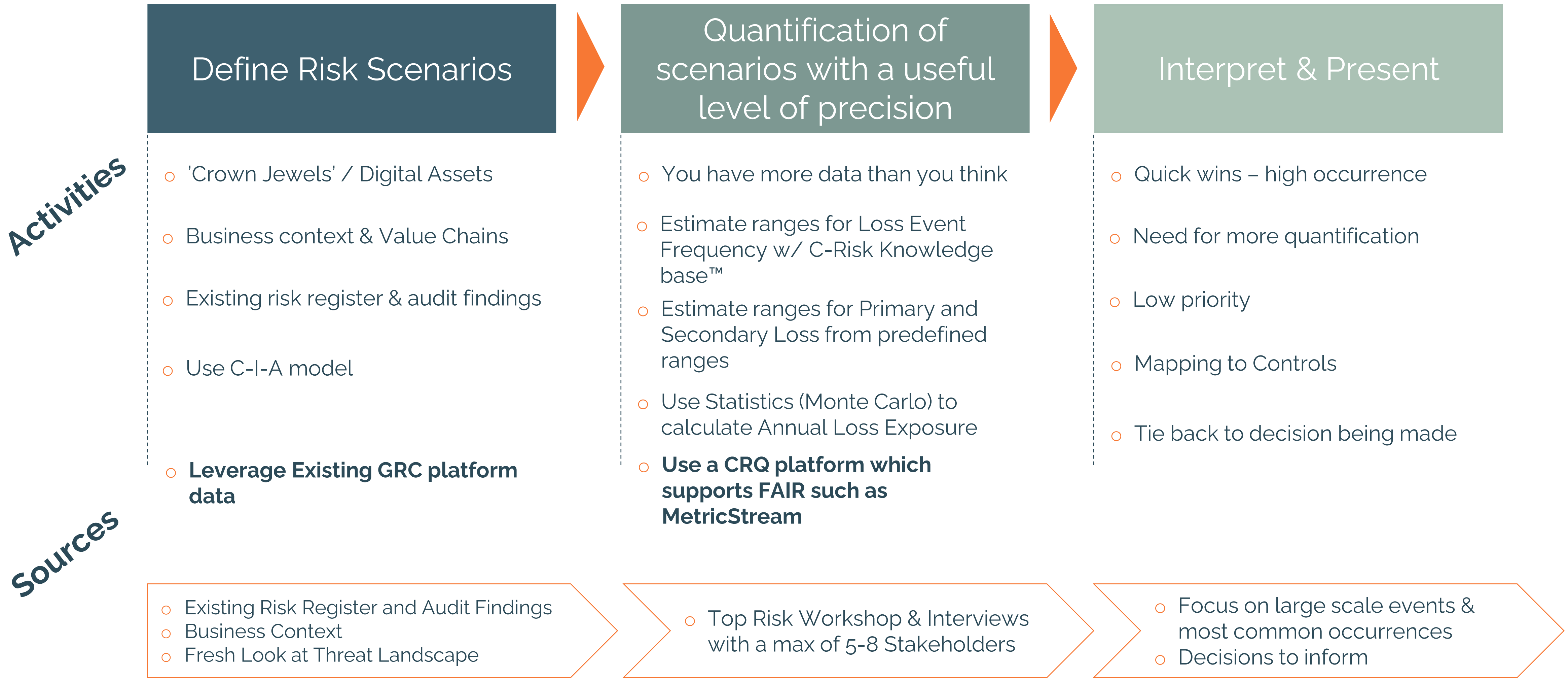
- COSO
- EBA European Banking Authority
- NACD National Association of Corporate Directors
- ecoDa The European Voice of Directors
- World Economic Forum
- International Monetary Fund

Legislation & Compliance Obligations

- U.S. Securities and Exchange Commission MCMXXXIV
- IDW Institut der Wirtschaftsprüfer

Add some analyst data

How to Perform a CRQ Analysis



Activities

Sources

Define Risk Scenarios

- 'Crown Jewels' / Digital Assets
- Business context & Value Chains
- Existing risk register & audit findings
- Use C-I-A model
- **Leverage Existing GRC platform data**

- Existing Risk Register and Audit Findings
- Business Context
- Fresh Look at Threat Landscape

Quantification of scenarios with a useful level of precision

- You have more data than you think
- Estimate ranges for Loss Event Frequency w/ C-Risk Knowledge base™
- Estimate ranges for Primary and Secondary Loss from predefined ranges
- Use Statistics (Monte Carlo) to calculate Annual Loss Exposure
- **Use a CRQ platform which supports FAIR such as MetricStream**

- Top Risk Workshop & Interviews with a max of 5-8 Stakeholders

Interpret & Present

- Quick wins – high occurrence
- Need for more quantification
- Low priority
- Mapping to Controls
- Tie back to decision being made

- Focus on large scale events & most common occurrences
- Decisions to inform

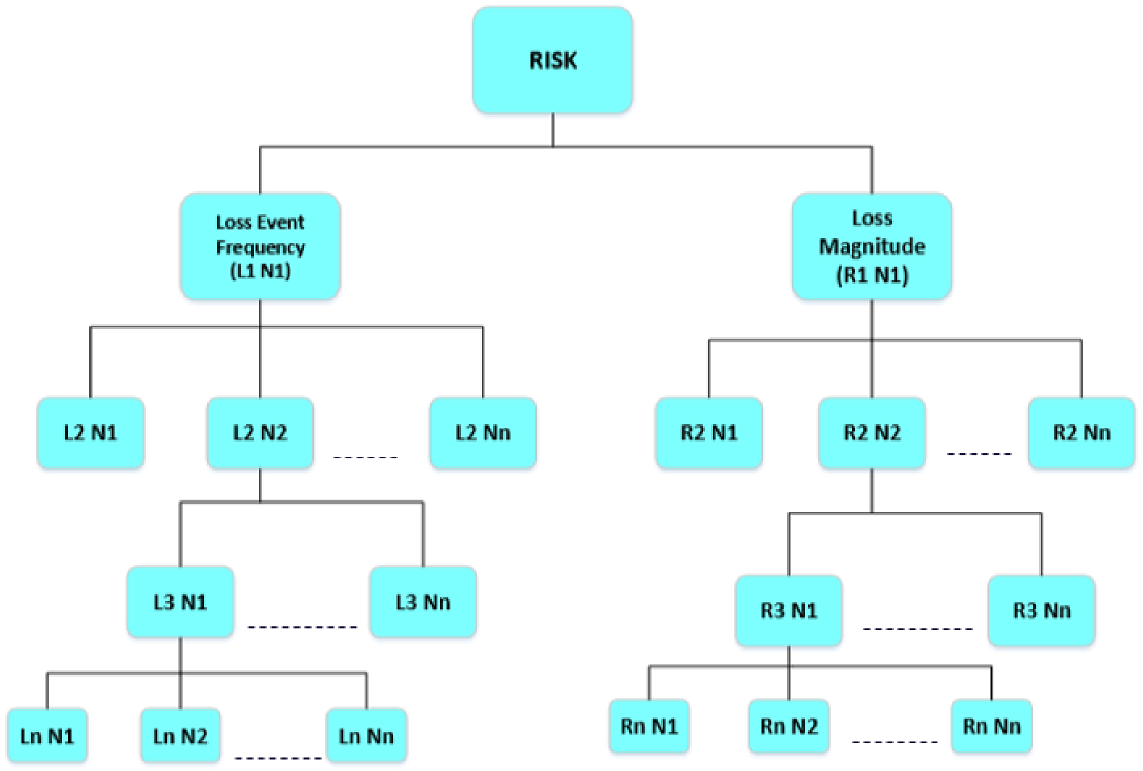
MetricStream's Framework Advantages

Flexible Framework for Quant Models & Toolkit

- Stateless serverless scalable design
- Start simple, add sophistication
- Supports adding Factors and Formulae (Beyond FAIR)
- Add / enhance models without affecting codebase of core modules

Single Vendor Solution

- Seamless reporting/browsing
- Single pane of glass leading to identical user experience
- Avoids customized modifications and reduces long-term costs
- Leverages core strengths (CMDB, Vulnerability Scanners, Threat)

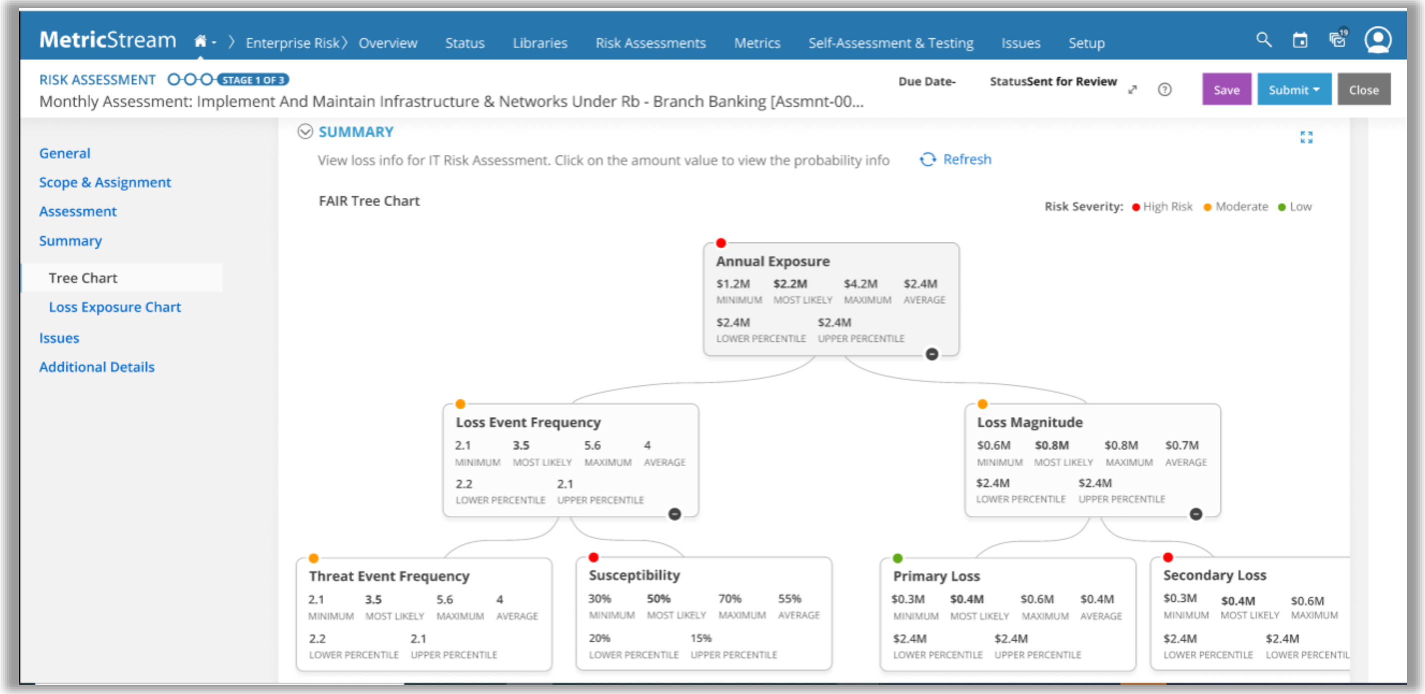


MetricStream Advanced Cyber Risk Quantification and Simulation

- Quantify cyber risk in actual currency, instead of imprecise red, yellow and green heatmaps

- Provides quantification through FAIR®, a standard quantitative model for information security and informational risk, but goes beyond FAIR with added flexibility, variables and multiple models

- Prioritize risk action planning, investments and resources



Monthly Assessment: Implement And Maintain Infrastructure & Networks Under Rb - Branch Banking [Assmnt-00...

Due Date-

StatusSent for Review

View loss info for IT Risk Assessment. Click on the amount value to view the probability info

FAIR Tree Chart

Annual Exposure

$1.2M	$2.2M	$4.2M	$2.4M
MINIMUM	MOST LIKELY	MAXIMUM	AVERAGE
$2.4M	$2.4M		
LOWER PERCENTILE	UPPER PERCENTILE		

Loss Event Frequency

2.1	3.5	5.6	4
MINIMUM	MOST LIKELY	MAXIMUM	AVERAGE
2.2	2.1		
LOWER PERCENTILE	UPPER PERCENTILE		

Loss Magnitude

$0.6M	$0.8M	$0.8M	$0.7M
MINIMUM	MOST LIKELY	MAXIMUM	AVERAGE
$2.4M	$2.4M		
LOWER PERCENTILE	UPPER PERCENTILE		

Threat Event Frequency

2.1	3.5	5.6	4
MINIMUM	MOST LIKELY	MAXIMUM	AVERAGE
2.2	2.1		
LOWER PERCENTILE	UPPER PERCENTILE		

Susceptibility

30%	50%	70%	55%
MINIMUM	MOST LIKELY	MAXIMUM	AVERAGE
20%	15%		
LOWER PERCENTILE	UPPER PERCENTILE		

Primary Loss

$0.3M	$0.4M	$0.6M	$0.4M
MINIMUM	MOST LIKELY	MAXIMUM	AVERAGE
$2.4M	$2.4M		
LOWER PERCENTILE	UPPER PERCENTILE		

Secondary Loss

$0.3M	$0.4M	$0.6M
MINIMUM	MOST LIKELY	MAXIMUM
$2.4M	$2.4M	
LOWER PERCENTILE	LOWER PERCENTIL	

Building a CRQ Capability

Key Points:

- Define Use cases starting with communication and improved objectivity
- Benefits are immediate and will also grow and improve over time
- Invest in initial training and awareness
- Adopt standard open models with publicly available support
- Consider using external services to seed and grow your internal capability
- Leverage existing risk assessment data if in place
- Be cautious about fully automated solutions which may misrepresent risk data or not align to your organisations use case.

Common Objections and how to overcome them

Benefit / What is the use case

Skills

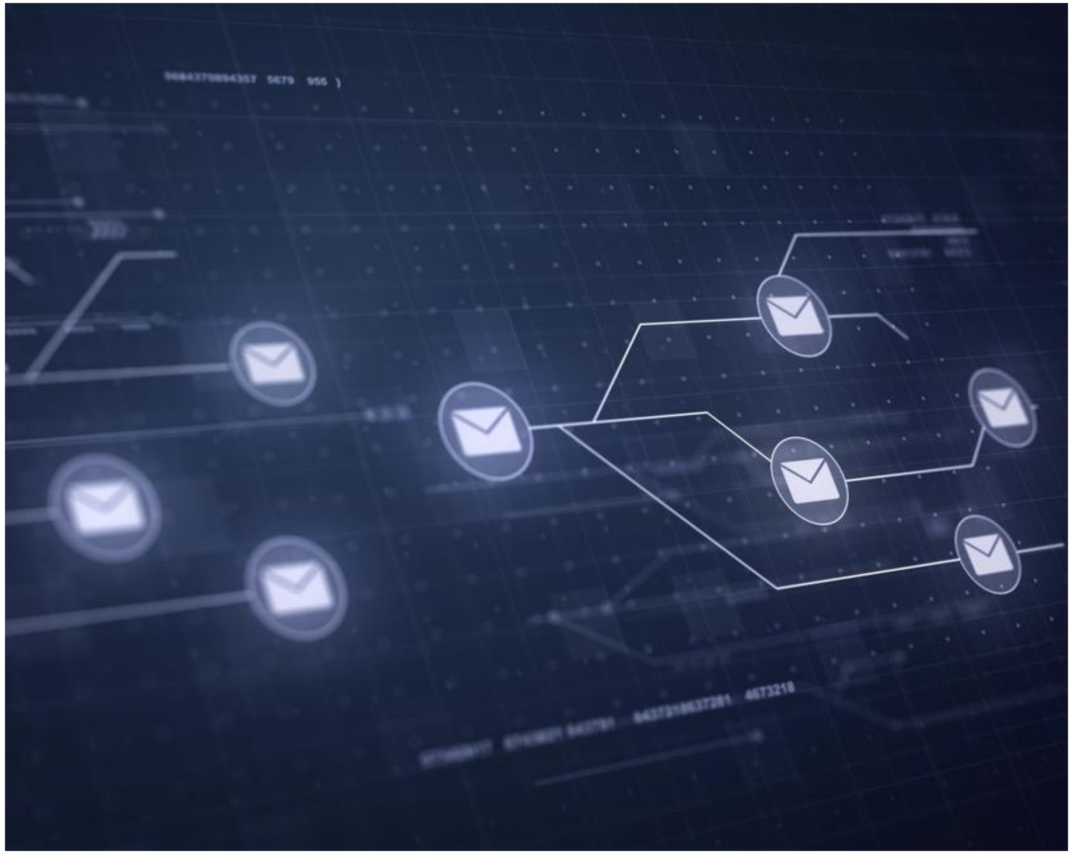
Cost

Lack of Data

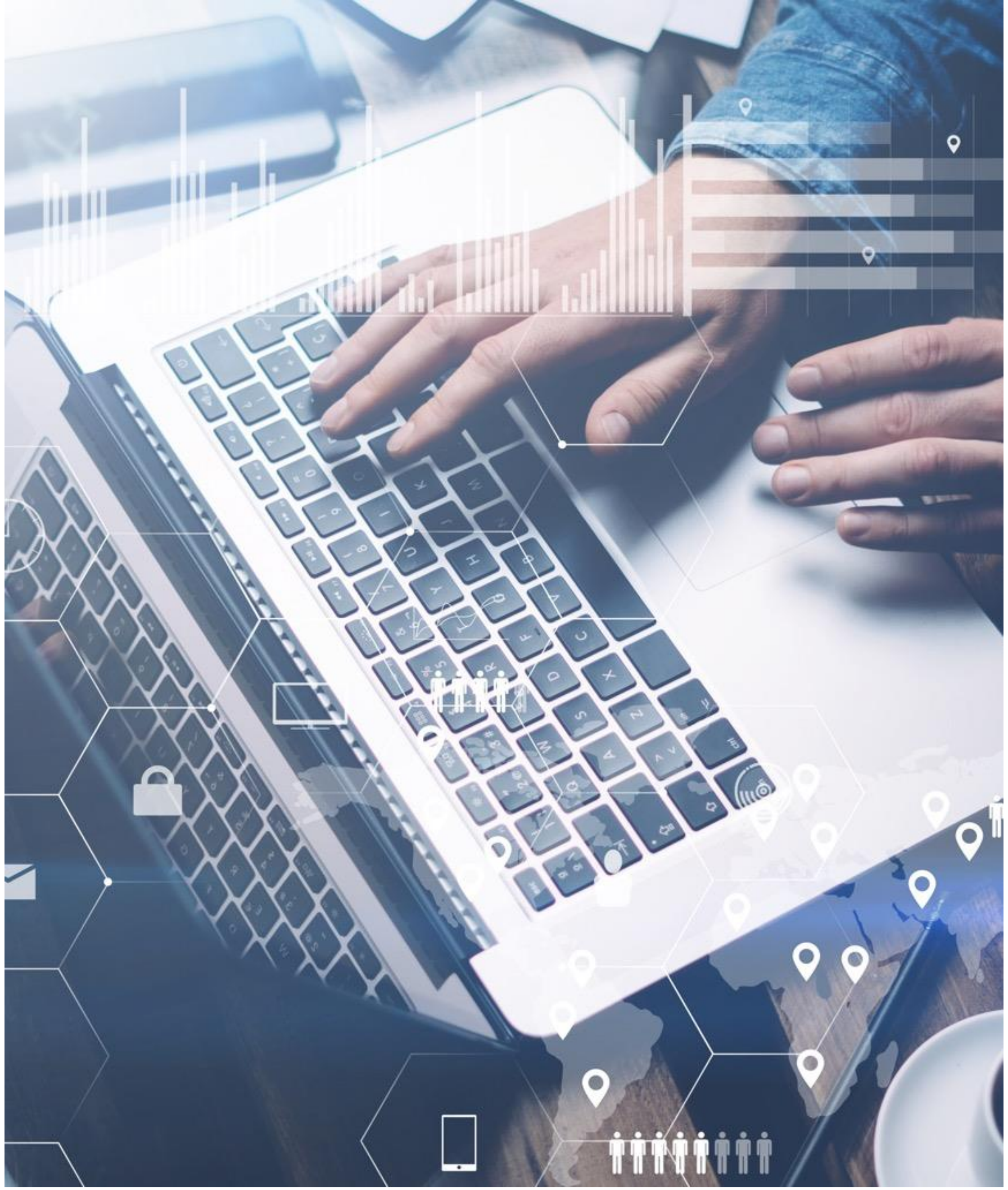
Complexity

Conclusion

- Cyber Risk Quantification in Financial terms vastly improves information security governance.
- There are many established use cases including justification of investments and communication in business terms.
- New use cases are emerging, and regulatory bodies are starting to request the adoption of CRQ in corporate governance.
- CRQ using FAIR is endorsed and recommended by a growing number of standards organizations including NIST, ISACA, CIS and others.
- CRQ analysis using FAIR can be implemented easily and quickly. It is a standalone capability which is not dependent on the overall organizational maturity.



BLOCK 01
NODE 01
NODE 04
NODE 05
NODE 03
BLOCK 01
NODE 01
NODE 02



TELEPHO
TELEPHONE

GRC
SUMMIT 2022
LONDON, NOV 8-9
Hosted by MetricStream

metricstream
thrive on risk™

GRC

SUMMIT 2022

LONDON, NOV 8-9

Hosted by MetricStream

metricstream

thrive on risk™