Addressing Cyber Resilience beyond Compliance

October 17th, 2023

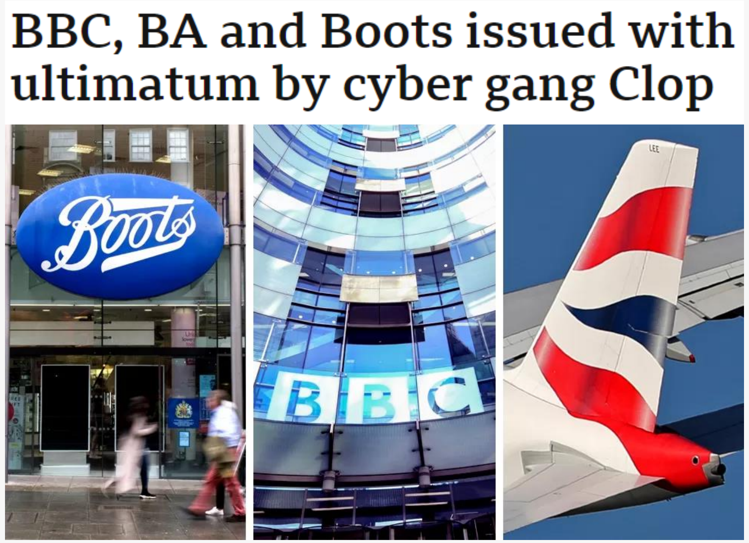
Context & Goals of the Cyber Regulations

DORA & NIS2 vis-à-vis broad Cyber Resilience

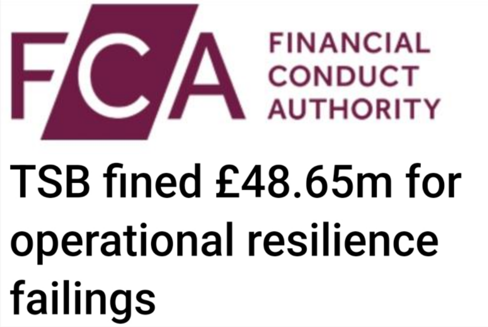
Cyber Readiness with GRC Technology

Impulse for addressing Cyber Resilience

The Problem: IT Resilience is a concern in several industries

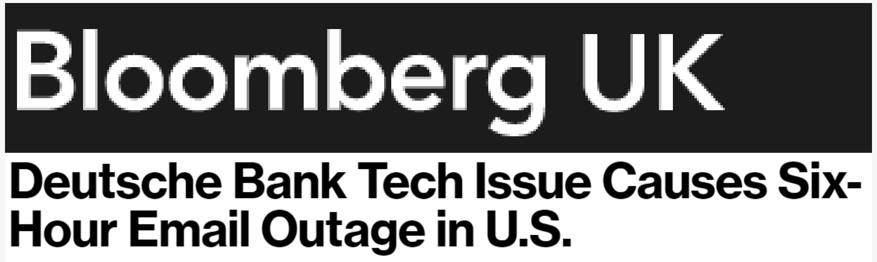


BBC, BA and Boots issued with ultimatum by cyber gang Clop



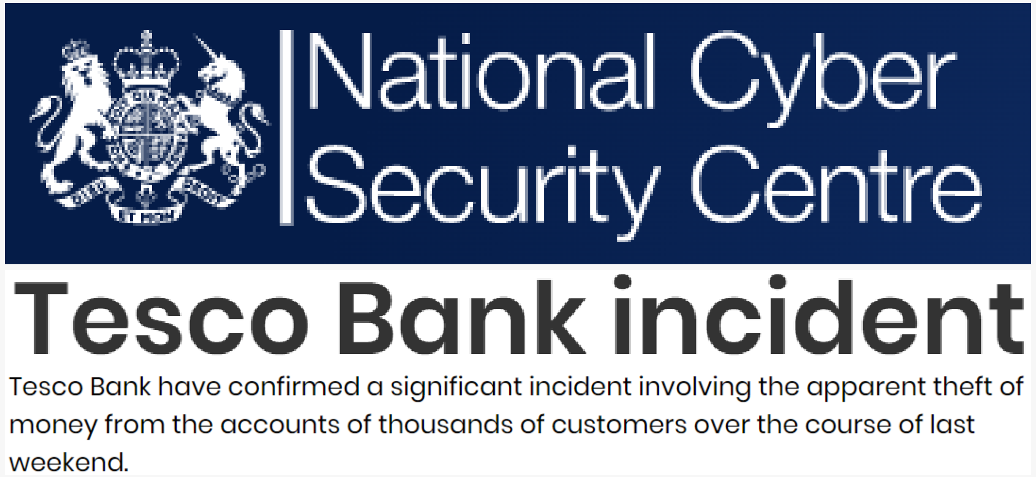
FCA FINANCIAL CONDUCT AUTHORITY

TSB fined £48.65m for operational resilience failings



Bloomberg UK

Deutsche Bank Tech Issue Causes Six-Hour Email Outage in U.S.



National Cyber Security Centre

Tesco Bank incident

Tesco Bank have confirmed a significant incident involving the apparent theft of money from the accounts of thousands of customers over the course of last weekend.

The Risk Recognition & Prioritisation

***Bank of England Survey Results:**

Risk with the greatest impact

74% Cyber Attack

Number one risk

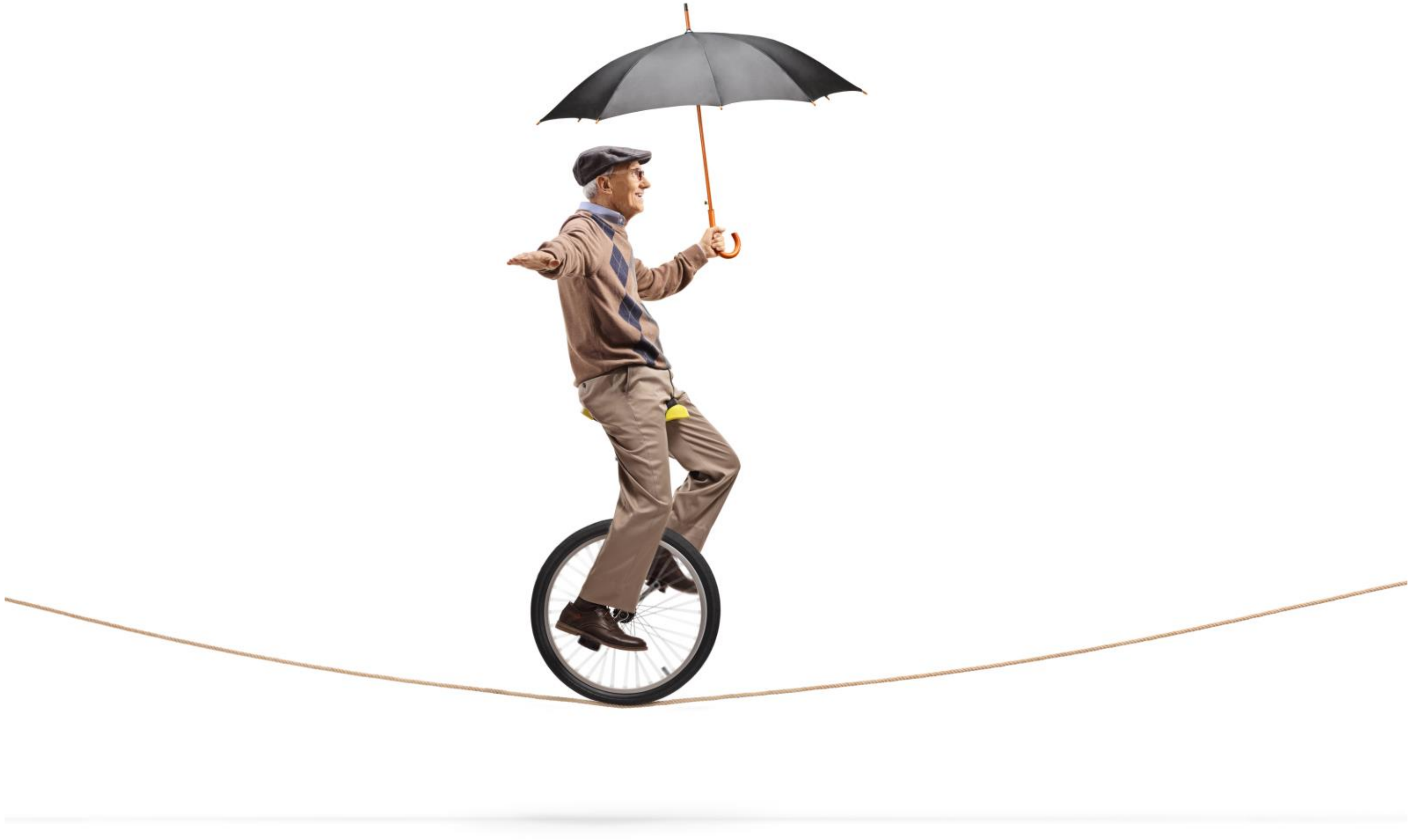
17% Cyber Attack

Source: *Systemic Risk Survey Results - 2022 H2; Survey of Risk Management and Treasury leadership Bank of England

Why protect assets when nothing happens?

We protect assets so that nothing happens.

We are insured. So is he.



The Regulatory Response

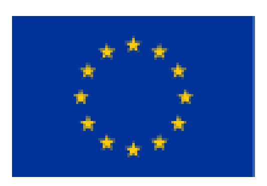
Digital Operational Resilience Act and NIS2

“…uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector as well as critical third parties.*”

Source: *Council of the European Union

DORA and NIS2 Requirements

- Board sign off on ICT Governance
- ICT Third-Party Risk Management
- Incident Reporting & Sharing
- Operational Resilience Testing
- ESA Oversight and NCA Enforcement



EU DORA & NIS2 Predecessors

- The Norwegian National Security Act
- PRA Policy Statement on Operational Resilience
- Basel Committee Principles for Operational Resilience
- MaRisk-Minimum risk management requirements

Complicating business context:

Third-Party treatment in Open Banking

Third-Party treatment in DORA

DORA & NIS2 vis-à-vis broad Cyber Resilience

At bare minimum, compliance with DORA & NIS2 requires visibility of…

….ICT risks, critical vendors, incidents, BCM/P etc.

DORA & NIS2 compliance is not enough -widen your risk lens.

See more risks→ Preempt Losses

Monitor emerging threats i.e., CISA, MITRE ATT&CK

Look beyond DORA & NIS2→ broader Incident Management

Compliance Management < Business Risk Management

The Spirit of the Regulations

EU DORA Article 6:
ICT Risk Management Framework

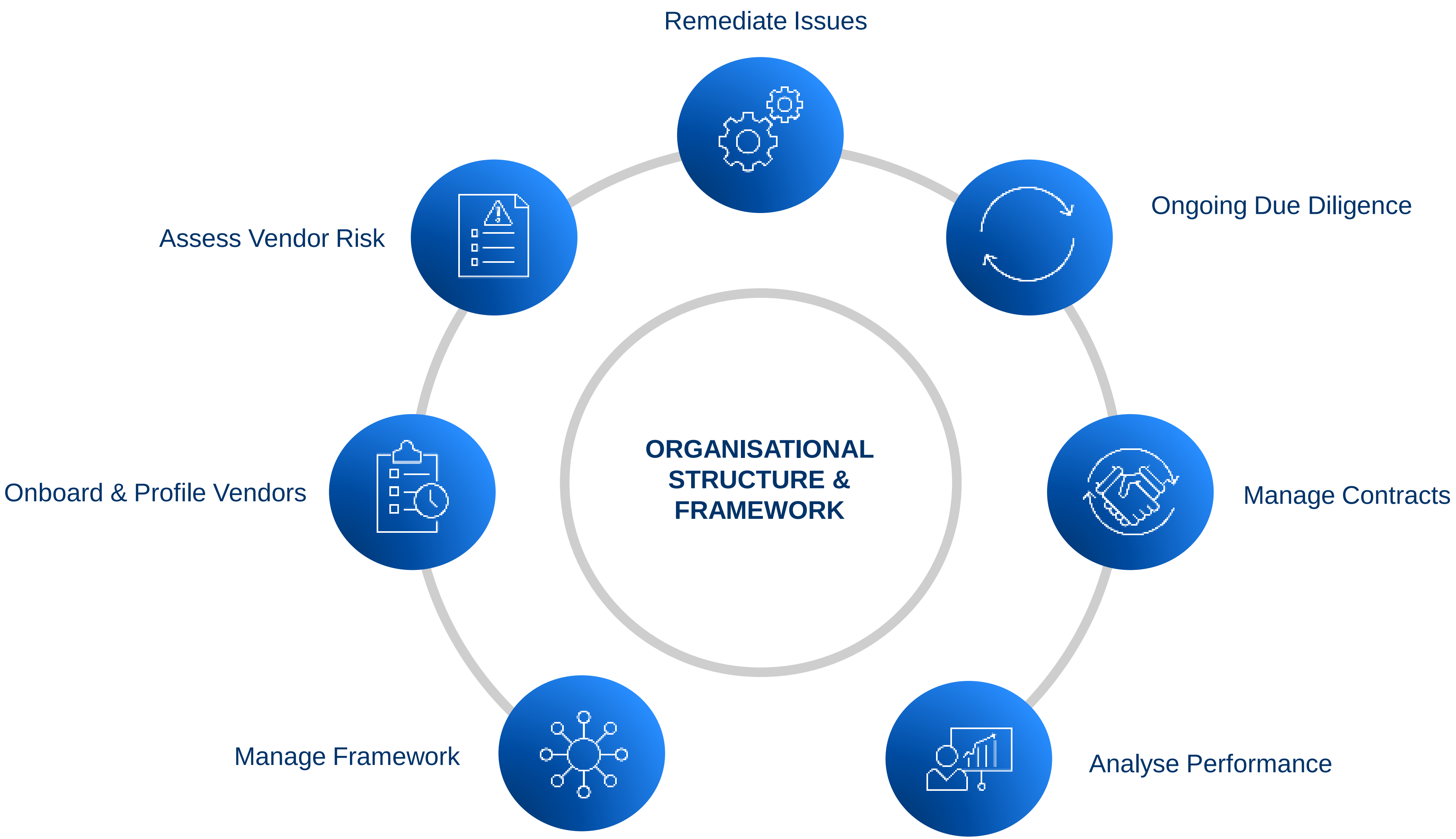
“Financial entities shall have a sound, comprehensive and well-documented ICT risk management framework as part of their overall risk management system…”

Source: *Official Journal of the European Union: EU DORA; REGULATION (EU) 2022/2554

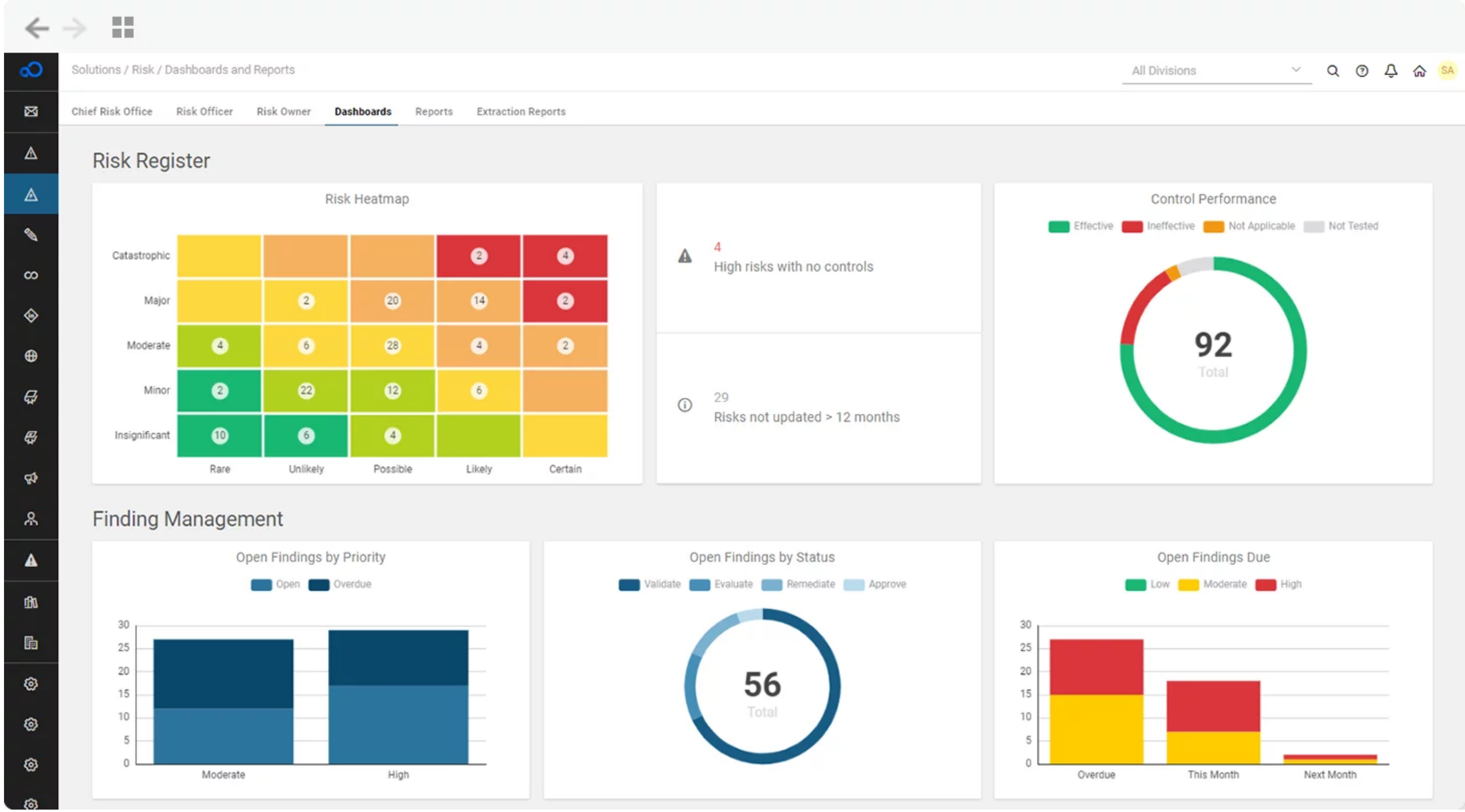
Cyber Readiness with Technology

Determine Critical Third-Parties for comprehensive risk mapping

Automate & coordinate Risk Management to handle the workload



Clarity on the ICT Framework performance before Management Sign Off



Solutions / Risk / Dashboards and Reports

Risk Register

Risk Heatmap

	Rare	Unlikely	Possible	Likely	Certain
Catastrophic				2	4
Major		2	20	14	2
Moderate	4	6	28	4	2
Minor	2	22	12	6	
Insignificant	10	6	4		

4
High risks with no controls

29
Risks not updated > 12 months

Control Performance

Finding Management

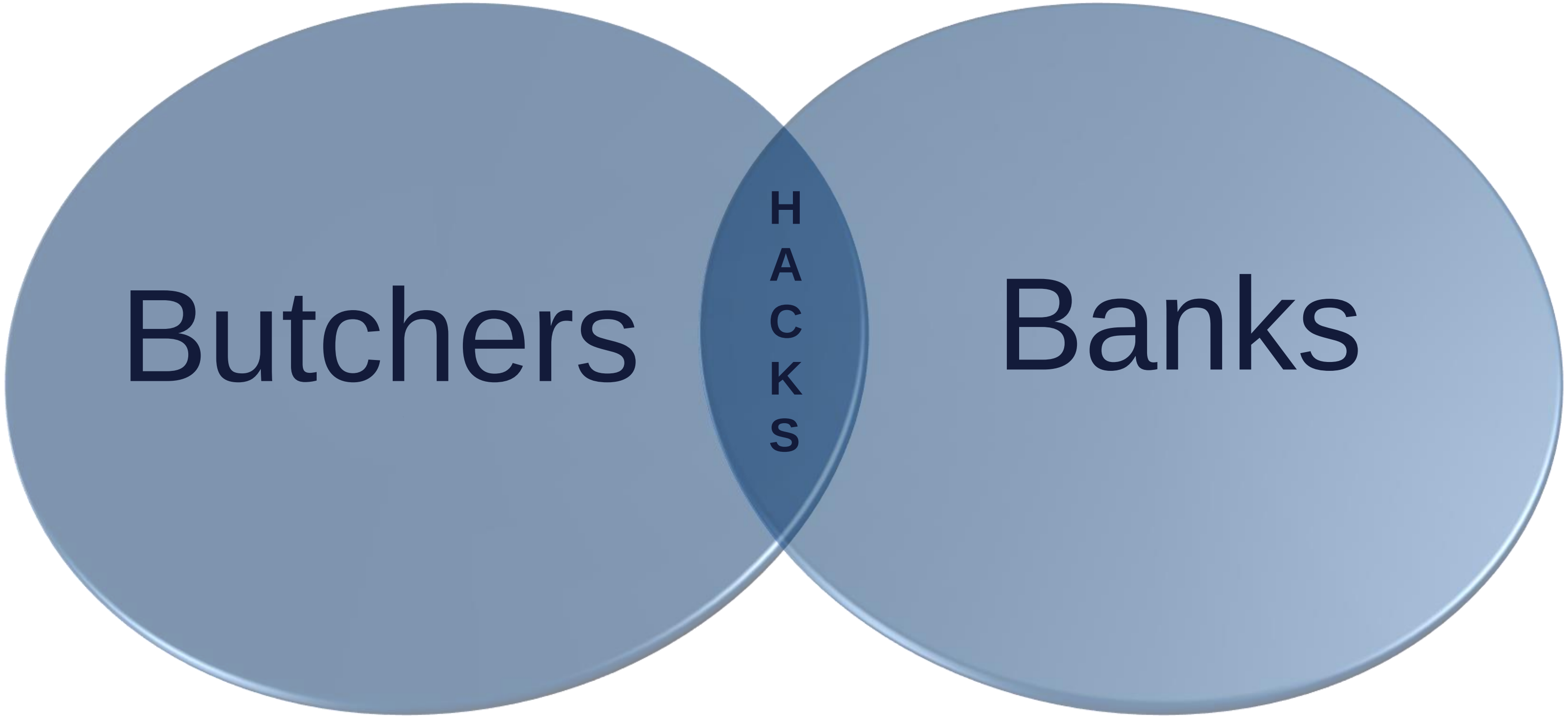
Open Findings by Priority

Open Findings by Status

Open Findings Due

Impulse for addressing Cyber Resilience

What do butchers and banks have in common?



Butchers

HACKS

Banks

Preempt Cyber Criminals who are casting a wider net*.

Source: *MIT Technology Review “Protecting your business in the age of ransomware.”

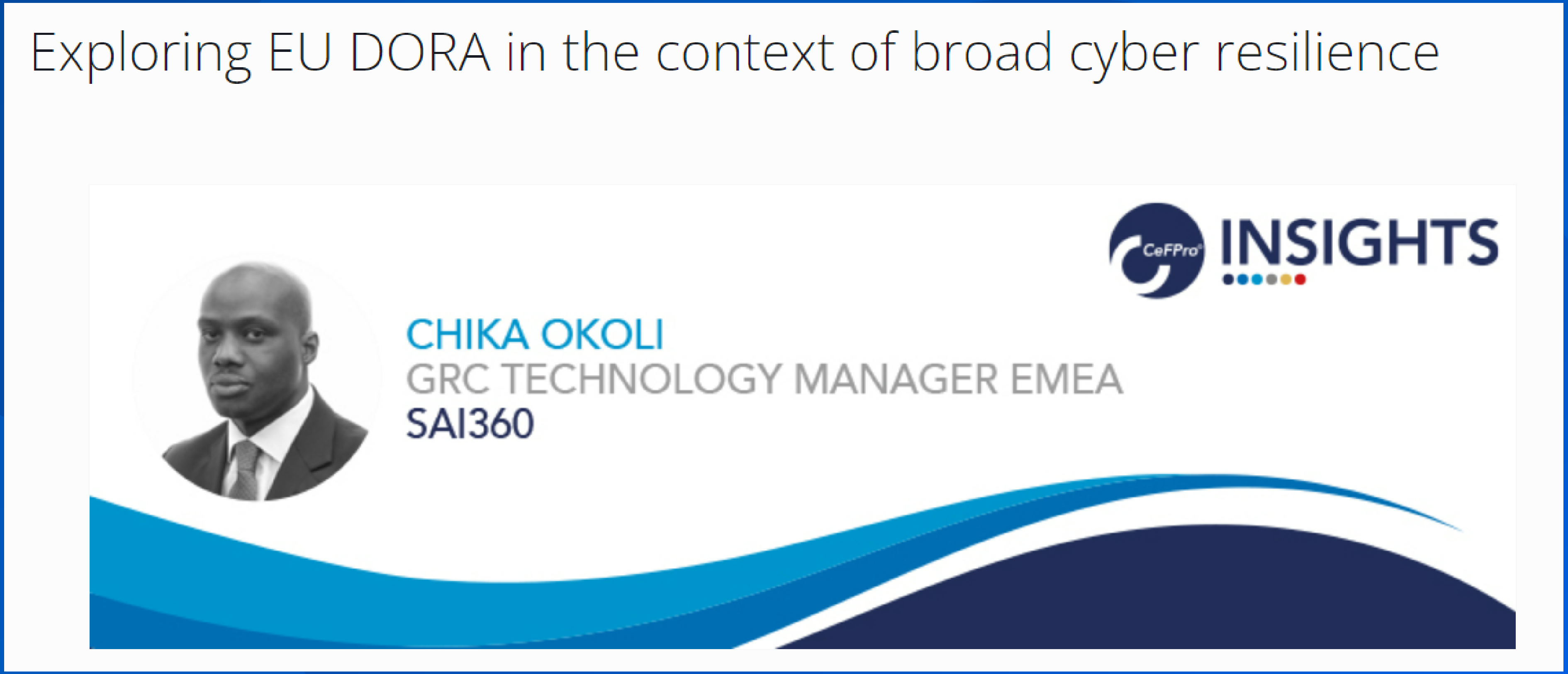
Let’s keep the conversation on operational resilience going:

Chika Okoli

GRC Technology Manager
SAI360

chika.okoli@sai360.com
www.linkedin.com/in/chika-o-n

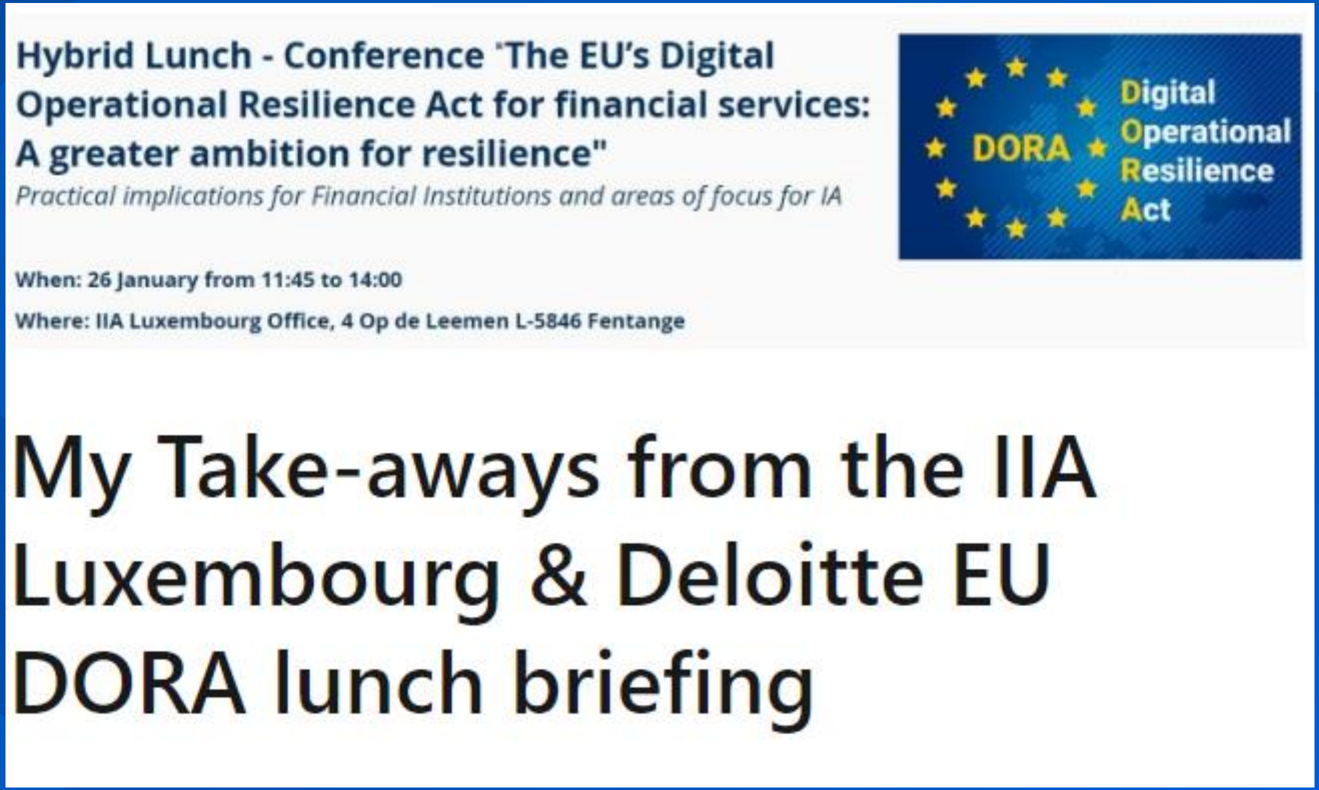
Further Information:



Exploring EU DORA in the context of broad cyber resilience

CHIKA OKOLI
GRC TECHNOLOGY MANAGER EMEA
SAI360

www.linkedin.com/pulse/exploring-eu-dora-context-broad-cyberresilience-chika-o-/



Hybrid Lunch - Conference 'The EU's Digital Operational Resilience Act for financial services: A greater ambition for resilience"

Practical implications for Financial Institutions and areas of focus for IA

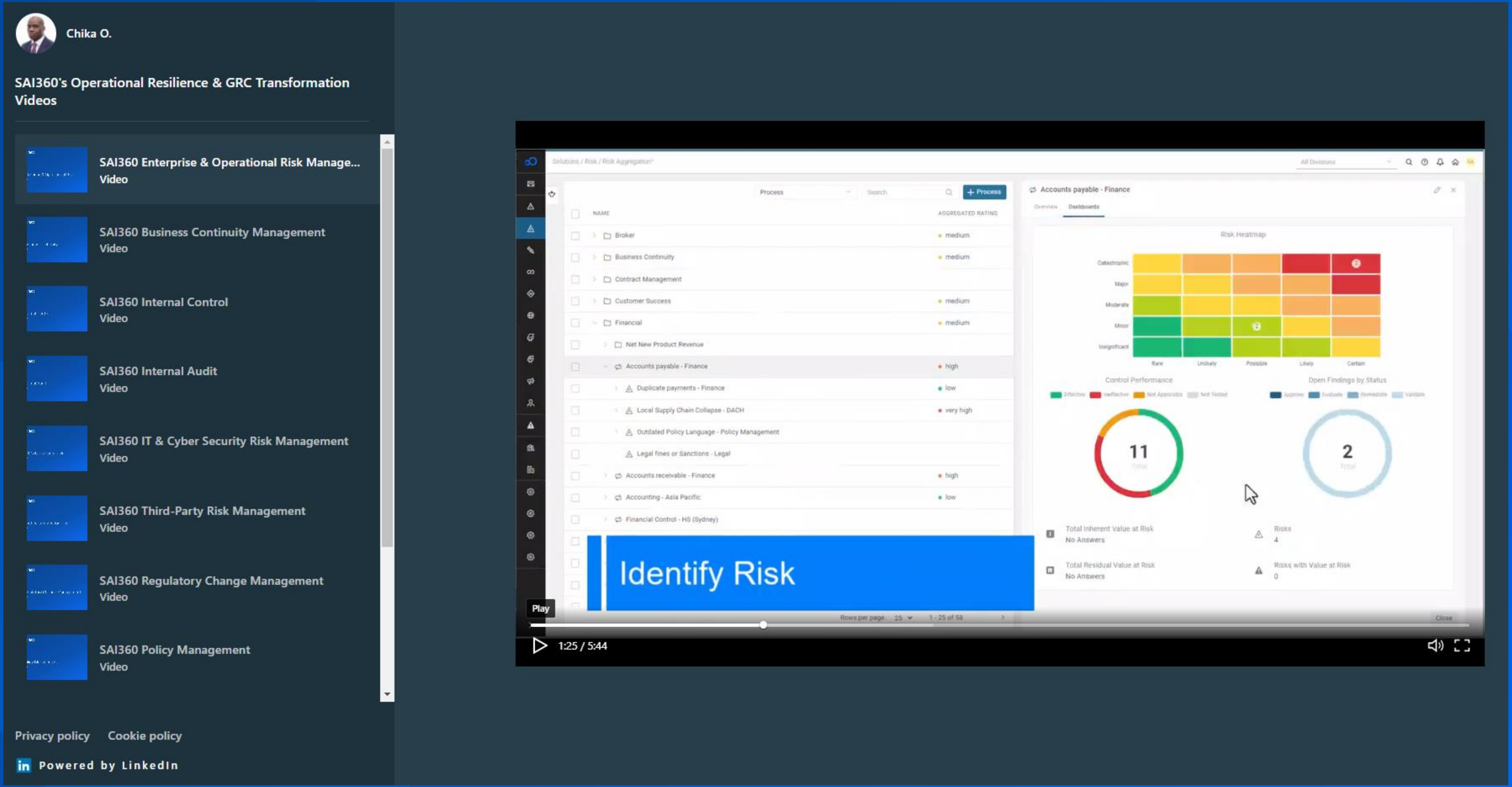
When: 26 January from 11:45 to 14:00

Where: IIA Luxembourg Office, 4 Op de Leemen L-5846 Fentange

My Take-aways from the IIA Luxembourg & Deloitte EU DORA lunch briefing

www.linkedin.com/pulse/my-take-aways-from-iia-deloitte-dora-lunch-briefing-chika-o-

GRC Platform Preview Videos:
https://www.linkedin.com/smart-links/AQHmt4-tepeaXw



Chika O.

SAI360's Operational Resilience & GRC Transformation Videos

- SAI360 Enterprise & Operational Risk Manage… Video
- SAI360 Business Continuity Management Video
- SAI360 Internal Control Video
- SAI360 Internal Audit Video
- SAI360 IT & Cyber Security Risk Management Video
- SAI360 Third-Party Risk Management Video
- SAI360 Regulatory Change Management Video
- SAI360 Policy Management Video

Privacy policy Cookie policy

Powered by LinkedIn

Solutions / Risk / Risk Aggregation
All Divisions
Process
Search
+ Process
NAME
AGGREGATED RATING
Broker medium
Business Continuity medium
Contract Management
Customer Success medium
Financial medium
Net New Product Revenue
Accounts payable - Finance high
Duplicate payments - Finance low
Local Supply Chain Collapse - DACH very high
Outdated Policy Language - Policy Management
Legal fines or Sanctions - Legal
Accounts receivable - Finance high
Accounting - Asia Pacific low
Financial Control - HS (Sydney)
Accounts payable - Finance
Overview
Dashboards
Risk Heatmap
Catastrophic
Major
Moderate
Minor
Insignificant
Rare
Unlikely
Possible
Likely
Certain
Control Performance
Open Findings by Status
11
2
Total Inherent Value at Risk
No Answers
Risks
4
Total Residual Value at Risk
No Answers
Risks with Value at Risk
0
Identify Risk
Rows per page 25
1 - 25 of 58
Close
Play
1:25 / 5:44