International Actuarial Association
Association Actuarielle Internationale

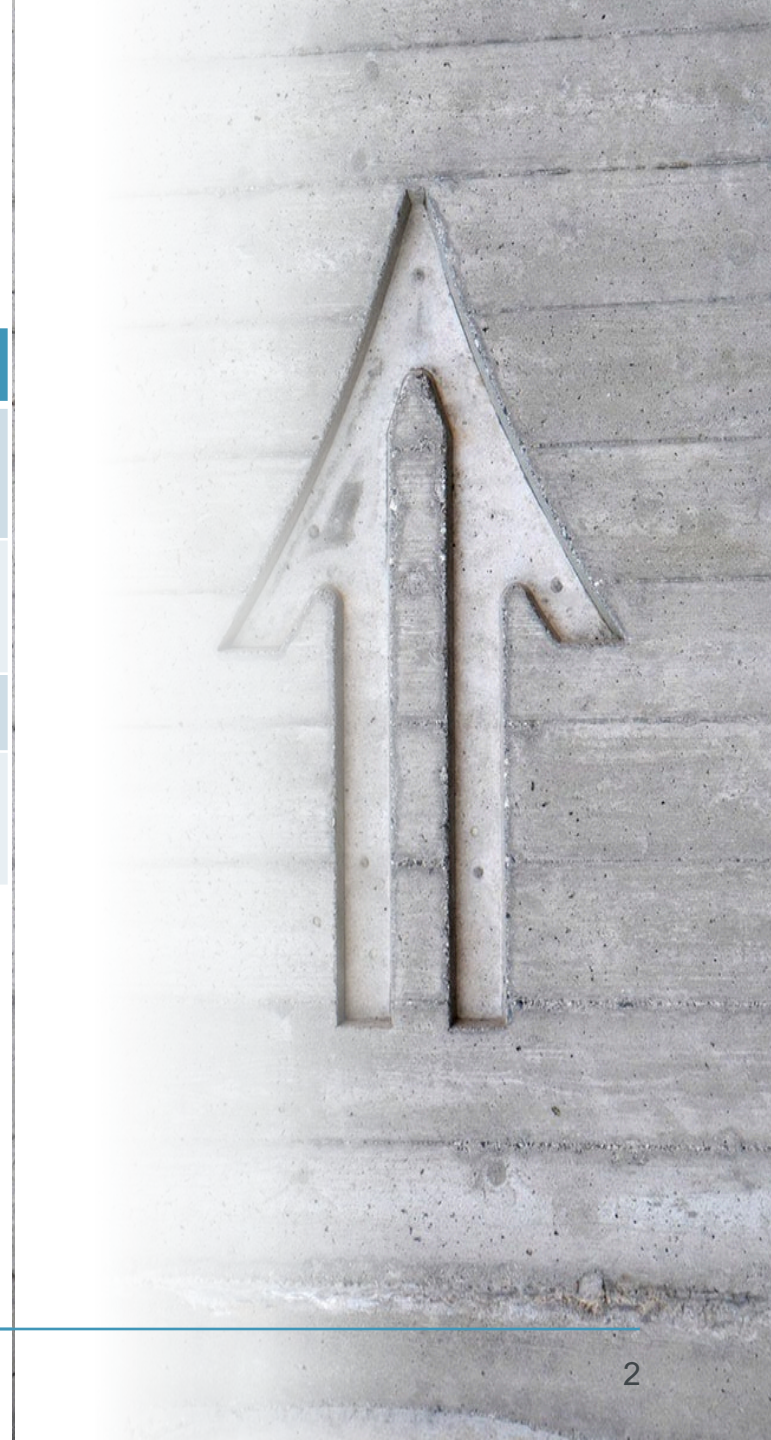
Operational Resilience in the Financial Sector

Presented by the IAA Banking Virtual Forum
5 March 2025

Panelists: Robert Chanon and Lawrence Habahbeh

Sessional event overview (guidance)

Item	Presenter	US EST
Introduction and welcoming remarks	Michael Tichareva	0700-0705
Paper presentation	Robert Chanon and Lawrence Habahbeh	0705-0755
Questions from the floor	All	0755-0810
Closing remarks and close	Michael Tichareva	0810-0815



Agenda

1. Key definitions and principles
2. What matters?
3. Who matters?
4. An operational resilience scenarios framework
5. Conclusion and recommendations

1. Key concepts

- ***Operational Resilience (OR)*** “ability of an organisation to deliver critical operations through disruption”
- ***Important business services (IBS)*** “a service that an organisation provides an external end user” – deemed important if “its disruption would materially impact an organisation’s visibility, cause significant customer harm or impact its ability its strategy”
- ***Impact tolerance*** – a quantification of the level of disruption an IBS can absorb before it materially impacts an organisations viability or causes significant customer harm

2. Key principles

- PRA/FCA guidance on OR. All UK entities subject to the regulations should be “operationally resilient” through prevention, adaptation and recovery mechanisms”
  - Specific statements of policies concerning IT for IBS (2021)
  - OR: Critical 3rd parties to the UK financial sector (2024)
- EU requirements (ICT oriented)
  - NIS2 directive (2022)
  - Digital Operational Resilience Act (DORA)
- Other countries (e.g. Australia, Canada, Singapore)
- International guidelines (ISO 22301, ISO 31000)

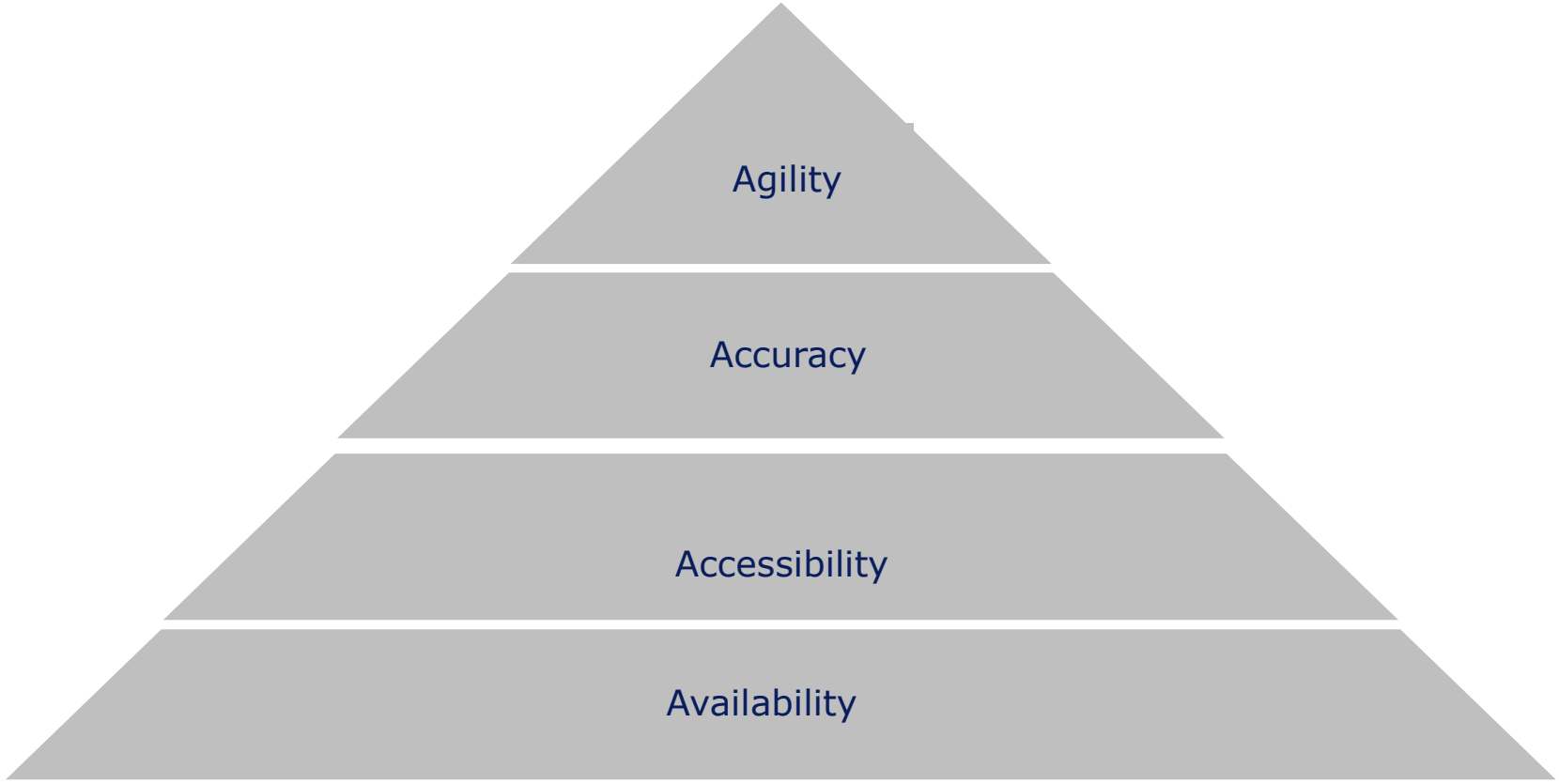
2. What matters? – key issues

- Risk culture – prevailing attitudes, values and behaviours determining how employees approach risk
- Risk appetite – the level of risk an organization is willing to accept in pursuit of its strategic goals
- Building a solid Information Technology foundation for managing IT risk (esp. for DORA compliance)
  - Scenario-based framework (ISACA)

Risk Scenario/Loss Event Structure and Components

I&T Scenario Development (ISACA)

IT Risk Pyramid (Westerman, 2005)



Risk Maturity model (Carnegie Mellon)

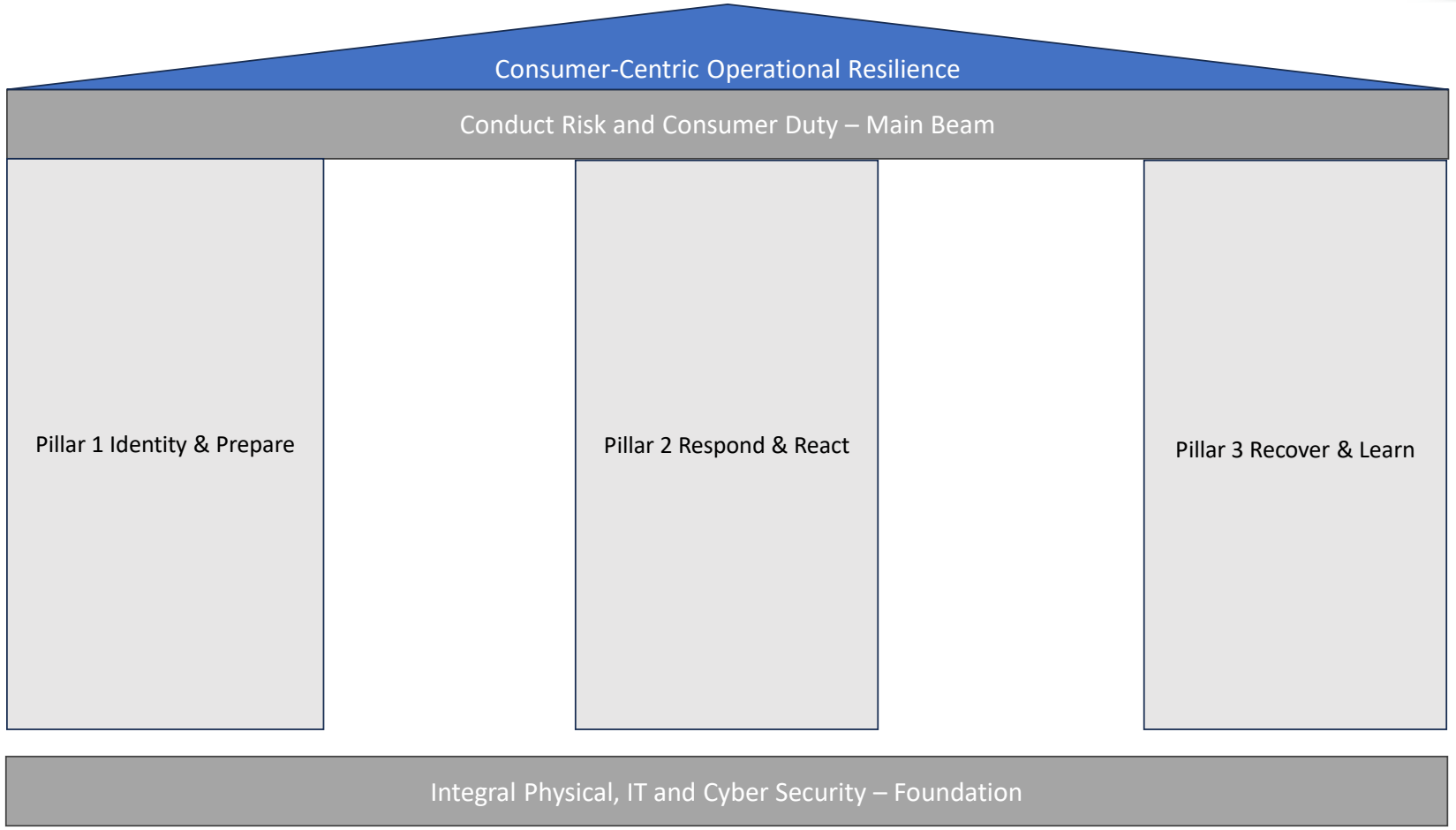
Process Evolution

CONTINUUM	CAPABILITY ATTRIBUTES	METHOD OF ACHIEVEMENT
Optimizing	(Continuous Feedback) Risk management a source of competitive advantage	• Increased emphasis on exploiting opportunities • "Best of class" processes • Knowledge accumulated and shared
Managed	(Quantitative) Risks measured/managed quantitatively and aggregated enterprisewide	• Rigorous measurement methodologies/analysis • Intensive debate on risk/ reward trade-off issues
Defined	(Qualitative/Quantitative) Policies, processes and standards defined and institutionalized	• Process uniformly applied across the organization • Remaining elements of infrastructure in place • Rigorous methodologies
Repeatable	(Intuitive) Process established and repeating; reliance on people continues	• Common language • Quality people assigned • Defined tasks • Initial infrastructure elements
Initial	(Ad Hoc/Chaotic) Dependent on heroics; institutional capability lacking	• Undefined tasks • Relies on initiative • "Just do it" • Reliance on key people

3. Who matters?

- Customer duty and conduct risk: critical elements of OR
  - Consumer duty: refers to the regulatory requirement that financial firms act in the best interest of their customers
  - Conduct risk: involves the risk of inappropriate, unethical or unlawful behaviour by a firm's employees and/or management
- The next slide summarises the inter-relationship between a
  - consumer-centric OR system, conduct risk,
  - three pillars of identity respond and react and recover & learn
  - Foundation: integral physical, IT and cybersecurity

Consumer-centric operational resilience

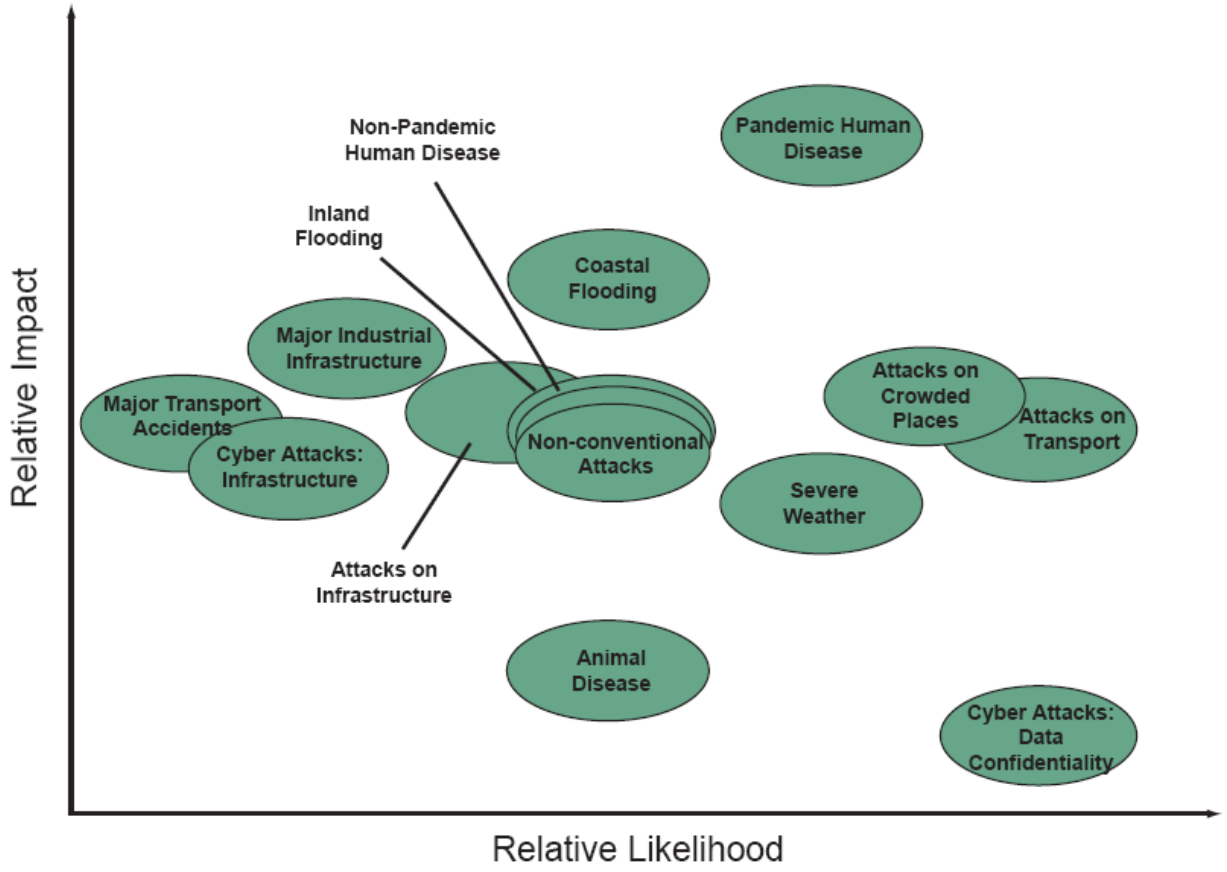


4. An operational resilience scenarios framework

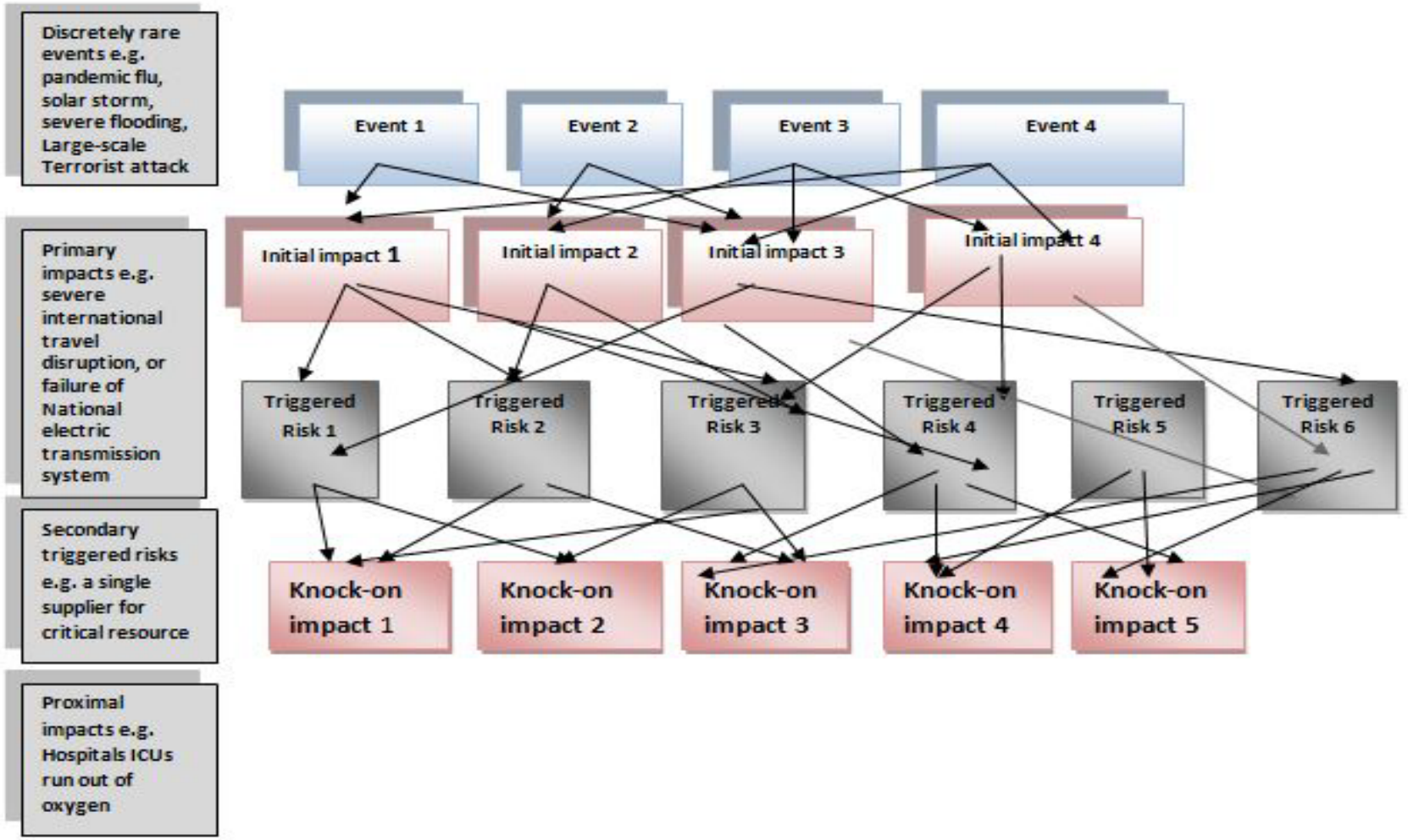
- Classification of risks

Class	Model?	Data?	Example
Known-knowns	Yes	Yes	Easily identified (e.g. business risk)
Emerging	Yes/No	No/Yes	Full extent unknown (e.g. change in interest rates)
Unknown	No	No	Black swan events (e.g. Financial Crisis 2008)

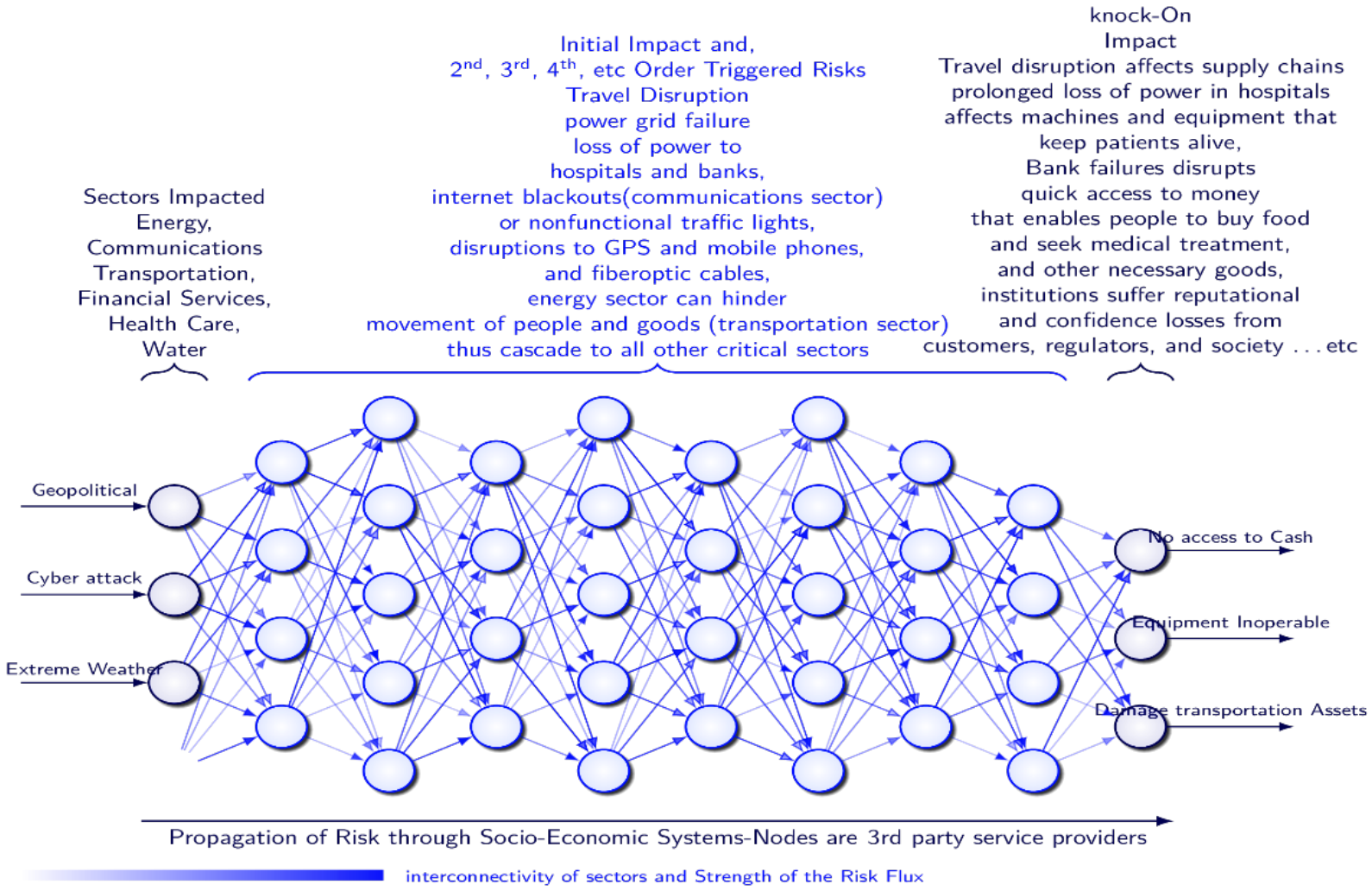
Threats to operational resilience



Risks and common consequences



Propagation of risk through socio-economic systems



Key considerations in building an ORF

- OR profile needs explicit management and a holistic view
- Design of scenario testing proportional to the size, complexity, business and risk profile of the firm
- Consider a range of risks and shocks
- Identifying emerging threats to IBS involves developing a comprehensive framework to understand, assess, model and mitigate systemic risks
- Define levels of disruption potentially caused to customers: (1) medium, (2) high and (3) systemic

6. Conclusion and recommendations

There are several subject areas which can enchance OR and focus attention on the importance of:

- Solid information technology
- Customer-centric organisation
- Operational resilience scenario framework

BOE/PRA now have a robust enforcement framework; thus organisations must identify its level of OR maturity

Issues requiring further examination

- Critical 3rd party risk management
- Climate and nature transition planning issues
- Recovery and resolution

Main references

- R. Chanon, L. Hababheh, P. Klumpes, S. Mann. (2025). Operational Resilience in the Financial Sector: Practical Guidance. *British Actuarial Journal* (forthcoming)
- ------. (2024). Role-playing Resilience. *Enterprise Risk Magazine*, Winter, pp. 23-27. Institute of Risk Management
- Institute of Operational Risk (IRM) (2021). *Operational Resilience: Operational Risk Sound Practice Advice*.
- Prudential Regulatory Authority. :
  - ------. (2021a). *Operational Resilience. Statement of Policy.* London: Bank of England.
  - ------. (2021b). *Operational Resilience: Impact Tolerances for Important Business Services. Policy Statement PS6/21*. London: Bank of England.
  - ----- (2024). *Operational Resilience: Critical Third Parties to the Financial Sector*. London Bank of England

Thank you for joining today's webinar!

Should you have any further questions or comments,

please send them directly to Technical Activities of the IAA

at the following email address:

technical.activities@actuaries.org

International Actuarial Association
Association Actuarielle Internationale
1203-99 Metcalfe, Ottawa ON K1P 6L7 Canada
Tel: +1-613-236-0886 Fax: +1-613-236-1386
Email: secretariat@actuaries.org
www.actuaries.org