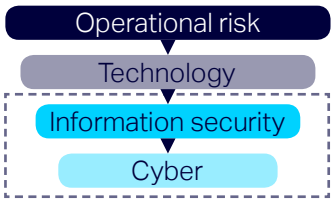
ORX CISR Initiative: Definitions

CISR Definitions

Working with participants of the ORX cyber and information security risk (CISR) initiative, we have developed the definitions below. These definitions define the scope of the project, ensure participants are talking the same language and allow consistent data sharing and collection. They are not intended to replace industry standards.

Term	Definition
Cyber and information security risk (CISR)	Cyber and information security risk (CISR) is the risk of loss (financial/non-financial) arising from digital events caused by external or internal actors or third parties, including: • Theft of information/technology assets • Damage to information/technology assets • Compromised integrity of information/technology assets • External and internal fraud • Business disruption The events may impact the confidentiality, integrity and/or availability of data. Implicit in this definition are elements of privacy risk where relevant.
Cyber and information security risk taxonomy	The majority of our community consider cyber and information security to be part of operational risk, treated as a distinct risk type within technology risk. Taxonomy structure: 
Indicator	A metric used to measure the status of something an organisation needs to know to support its day-to-day operations.
Early warning indicator	An early warning indicator is a metric that can provide a signal of a risk event before it occurs.
Key risk indicator	A key risk indicator is a metric that provides insight into the level of risk an organisation is exposed to, as well as to provide an early warning of potential loss.
Key control indicator	A key control indicator is a metric that provides information on the effectiveness and performance of an institution's key controls.
Key control	A key or critical control is fundamental to reducing the level of material risk an institution faces. Typically, it has these characteristics: • Proven to be effective; often described as particularly relevant for a specific material risk • Often has a mitigating impact on other, less severe risks • Failure of a key control could have substantial financial or non-financial impacts for an organisation

ORX CISR Initiative: Definitions

About the CISR initiative

Financial firms are increasingly focusing on managing risk in addition to measuring its impact. To support them, we are expanding our activities and developing a blend of services that will better meet the changing needs of the operational risk industry. As part of this, we are exploring what support we can provide in the management of the most material risk types identified in the Operational Risk Horizon 2019 study. We have started with cyber and information security risk (CISR), which was identified as one of the most concerning material risks.

The CISR initiative combines our established research services and information sharing capabilities with the input of our community of experts. We are focusing on three key areas:

- **Information sharing** – Helping firms understand their cyber and information security risk exposure, including data sharing, allowing for peer comparison and benchmarking.
- **Governance and management practice standards** – Helping firms improve their management of cyber and informations security risks. This may include the future development of risk management standards and benchmarking.
- **Collaboration** – Building a community of second line CISR specialists.

How will these definitions help?

We needed to develop and share a set of definitions and a common language to be used throughout the ORX CISR initiative. These definitions will underpin the work we do across the initiative, including information sharing and practice standards. There are many approaches to managing CISR, so a common language is essential. This ensures that the information we collect and share is clear and consistent, and enables meaningful peer comparison.

We developed the definitions in partnership with our community of cyber and information security experts. Twenty five firms participated in this part of the initiative, and a working group of five firms provided further input. The definitions have been created for use in the CISR initiative, and are not currently intended to replace external standards or definitions.

We will continue to reference these definitions throughout the project. We will also review the definitions during the project to capture changes in the industry and ensure they continue to reflect the activities.

Definitions have been agreed for the following terms:

- Cyber and information security risk (CISR)
- CISR taxonomy
- Indicator and indicator types (early warning indicator, key risk indicator, key control indicator)
- Key control

During the creation of these definitions, we also collected some information on terminology, indicators and risk appetite that will be used to inform later work. Further information is available to project participants in the ORX CISR Initiative Definitions Appendix.

For more information about the ORX CISR initiative contact Melanie Lavallin:
melanie.lavallin@orx.org

Stay up to date with our work on cyber

Visit our website:
www.orx.org

Follow on LinkedIn:
@ORX_Association

Follow on Twitter:
@ORX_association