Is risk still risky when you see it coming?

Is your Cyberrisk appetite and tolerance in line with your business strategy?

89%

say their Cybersecurity function does not fully meet their organization's needs.

Is your Cybersecurity function managing risks within your corporate's risk capacity? When done well, defining risk appetite establishes internal boundaries for prudent decision making, risk taking and highly efficient governance.

Managing Cyberrisk is a continuous process to keep the organization vital and protected from evolving attacks from the Cyberspace

Enterprise risk managers (e.g. CRO) need to compare Cyberrisks to other risks using the same financial and probability benchmarks, so that investment on Cyberrisk prevention and remediation can be considered simultaneously with other pressing enterprise risks.

The board is expected to maintain oversight over the enterprise-wide Cyberrisk management strategy, including an appropriately set appetite for Cyberrisks, and to define the risk an organization is willing to assume within its risk capacity. It also has to validate that Cyberrisk management strategies and Cyberrisk appetites have been integrated into strategic plans and risk management structures in other areas of the enterprise.

Monitoring Cyberrisk should be done based on a defined set of Cyberrisk metrics indicating trends of an increased level of risk. However, specifying Cyberrisk appetite and tolerance poses often challenges to an organization due to the unclear definition of the terms itself including the definition of Cyberrisk and Cybersecurity.

Why is risk appetite important?

Informs strategy

- A constant in an ever-changing environment
- Sets the boundaries for the firm
- A framework for evaluating opportunities

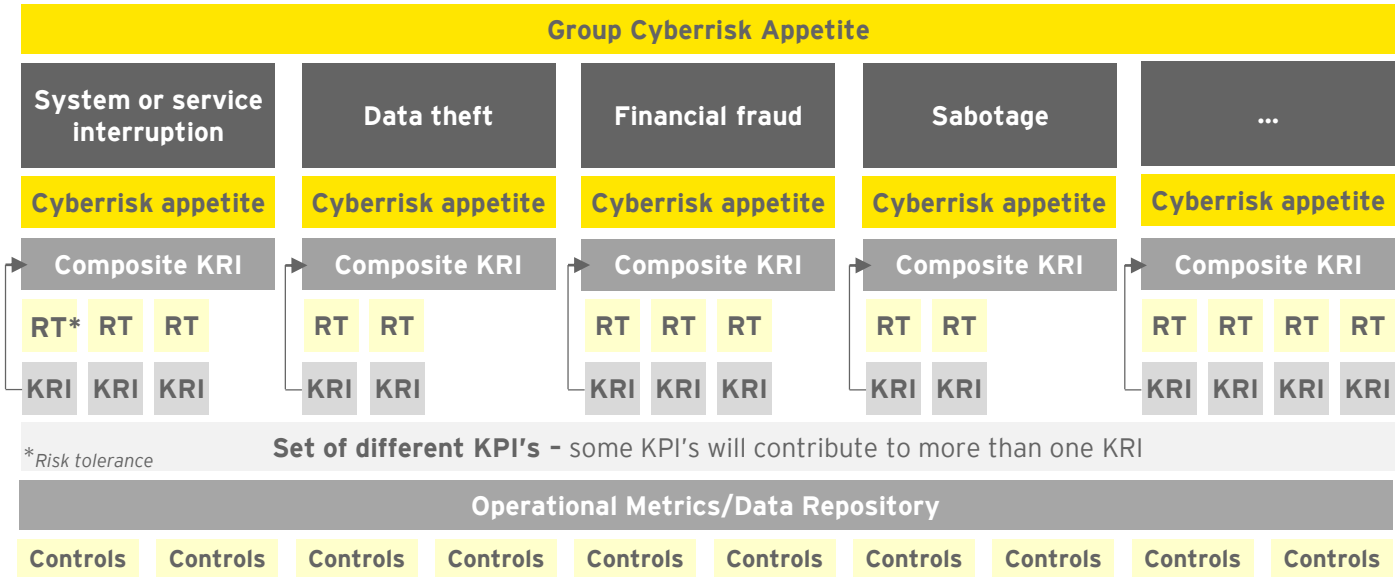
Makes risk culture tangible

- A mechanism for articulating and measuring the behaviors of the firm
- Underpins individual accountabilities

EY's approach to define Cyberrisk appetite and tolerance

1	2	3	4
Collect information and review existing framework	**Establish risk appetite principles and statements**	**Define and validate risk appetite (KRI/KPI discussion)**	**Sustain and monitor risk appetite process**
Collect information about the existing frameworks used at the organization through interviews key stakeholder e.g. CRO, CISO, CIO and study of relevant documents.	Develop risk appetite principles and define the Cyberrisk appetite and tolerance by conducting workshops with relevant stakeholders from CISO, CRO, IT, Audit and governance functions.	Verify Cyberrisk appetite and tolerance with various representatives of the organization. Develop and verify the approach on how to define risk metrics (KPI and KRI).	Develop and implement governance principles to review Cyberrisk appetite on a regular basis to be in line with the organization overall risk appetite and strategy.

The definition of Key Risk Indicators (KRI's) is an important step as this is the bridge between risk management and operations (Key Performance Indicators - KPI)



How can we help you

Current State Assessment

Conduct a current state assessment to understand your needs and maturity with regard to Cyberrisk management and ERM/ORM integration.

Cyberrisk Statement Advisory

We will provide you guidance on the definition of your Cyberrisk appetite and tolerance and support you to define your KRI's inline with your KPI's.

Cyberrisk Framework & Metrics Definition

We will help you to define a holistic Cyberrisk management framework – fully integrated into your ERM/ORM and support with regard to your Cyberrisk metrics & reporting.

Question you should ask yourself

- Do you know your Cyberrisk tolerance – and what do you do if your tolerance is exceeded?
- Are your Key Risk Indicators inline with your Key Performance Indicators?
- Do your Cyberrisk metrics provide enough insights to understand certain Cyberrisk trends?

Your EY Team

Tom Schmidt
Partner
+41 58 286 64 77
tom.schmidt@ch.ey.com

Reto Aeberhardt
Associate Partner
+41 58 286 67 40
reto.aeberhardt@ch.ey.com

Marc Minar
Manager
+41 58 286 43 81
marc.minar@ch.ey.com