FAIR RISK MANAGEMENT

Quantification: the Core of Effective Cyber Risk Management

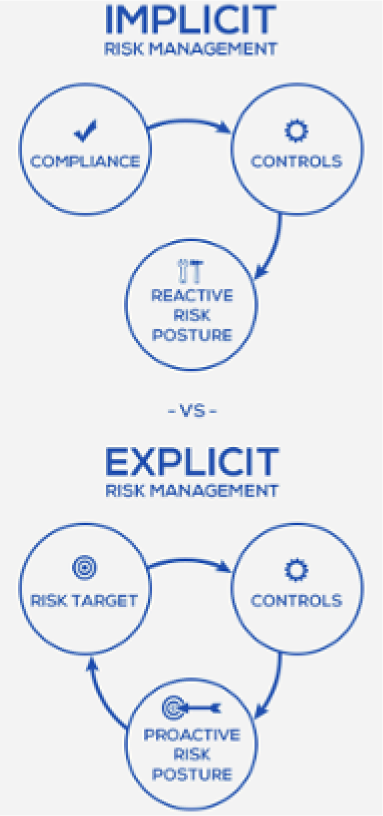
The FAIR framework defines the necessary building blocks for implementing effective cyber risk management programs. Being able to quantify cyber risk is at the core of any such program; after all, "You cannot manage what you don't measure."

Managing Risk Explicitly in Order to be Effective

Your organization already manages risk. The question is whether it is doing it implicitly or explicitly. A risk management program needs to be explicit to be effective.

In an implicit approach to cyber risk management, an organization might have aligned its cybersecurity policies with a framework like NIST CSF, and it might have a NIST CSF-based enterprise risk assessment performed annually. The cybersecurity staff probably prioritizes and works hard to address the findings from that assessment. Where the organization ends up risk-wise however, is a by-product of these efforts.

There is little control of the outcome from a residual loss exposure perspective as it isn't clearly defined within such frameworks, and the measurements are only loosely associated with risk. In order to be explicit, there would need to be a specific and quantified risk target that is actively being managed against.



Defining Risk Management

FAIR defines risk management as "the combination of personnel, policies, processes and technologies that enable an organization to cost-effectively achieve and maintain an acceptable level of loss exposure." A closer look at this definition reveals key take-aways:

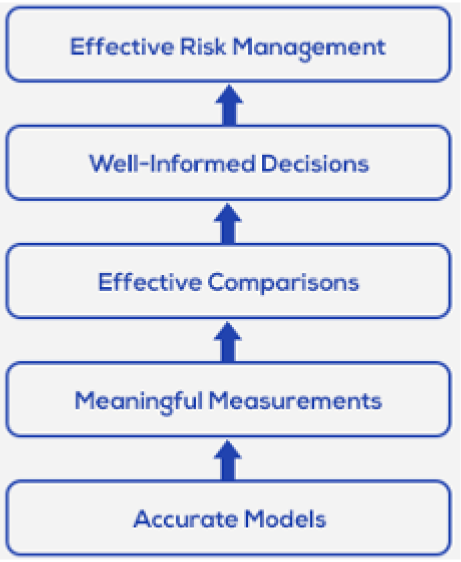
PEOPLE
PROCESS
RISK MANAGEMENT
POLICIES
TECHNOLOGY

- **Cost Effectively:** The responsibility of mature risk professionals is not simply to help their organizations to manage risk, but to manage it cost-effectively. Organizations compete on many levels, and if an organization is able to manage risk more cost-effectively than its competition, then it wins on that level.
- **Achieving and Maintaining:** Achieving an objective suggests that an objective exists. Maintaining a risk (loss exposure) objective over time requires the ability to quantify and compare.
- **An Acceptable Level of Loss Exposure:** Adopting a risk assessment framework, predefined checklists and a set of common practices is a form of implicit risk management and will not enable you to achieve a defined acceptable level of risk. Explicitly managing risk requires that one or more quantitative risk-based objectives exist.

Building the Right Foundation for Effective Risk Management

The foundation required to achieve and maintain effective risk management is comprised of five elements:

- **Cost-effective risk management:** a program that meets the definition of risk management listed above.
- **Well-informed decisions:** every decision involves a choice, and in order for those to be well-informed...
- **Effective comparisons:** a decision-maker has to be able to compare the options before him/her, which requires...
- **Meaningful measurements:** quantitative financial measurements that all stakeholders can understand, which requires...
- **Accurate models:** accurate models of risk and of explicit risk management that can scale in real-life.

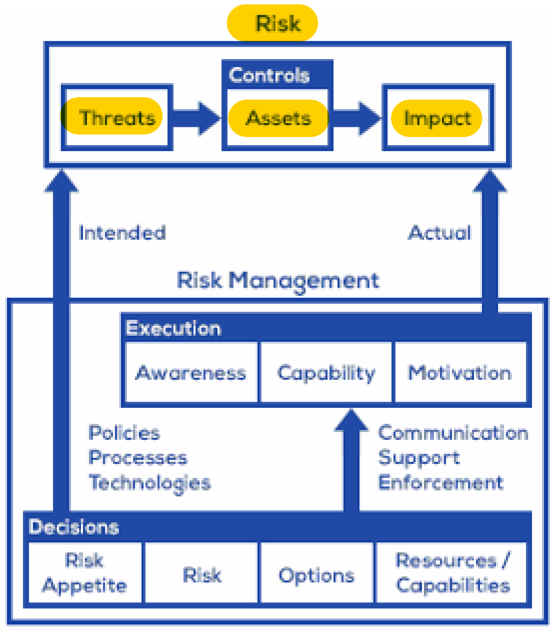


The FAIR methodology was conceived as a way to provide meaningful measurements so that it could satisfy management's desire to make effective comparisons and well-informed decisions. FAIR has become the only international standard Value at Risk (VaR) model for cybersecurity and operational risk.

Implementing an Effective Risk Management System

FAIR tells us that an effective risk management system is comprised of the following elements:

- **Risk**: a function of the threats, assets, controls and impact factors (e.g., laws, etc.) that drive loss exposure.
- **Risk Management:** comprised of decisions and execution. Those decisions are related to the risk governance that the organization decides to implement. What an organization actually gets in terms of risk is a function of execution within the context of those decisions.
- **Feedback Loop:** feedback about the conditions of asset-level controls, metrics related to threat intelligence and losses, metrics regarding conditions that affect execution (e.g., awareness, capabilities) and root-cause analysis data.



LEARN MORE IN THE FAIR BOOK

HOME

ABOUT

GET INVOLVED

LEARN FAIR

EVENTS

AWARDS

ADVISORS

© 2019 FAIR INSTITUTE

TERMS OF USE | PRIVACY | GENERAL MEMBER AGREEMENT | SITE MAP