# Cyber Risk Framework

Measuring how efficient and effective cybersecurity frameworks are towards managing real-life cyber risks is crucial to understanding its economic impact on any organization. Organizations are required to take a systematic approach when implementing a risk management framework.

Some studies, investigated the top cyber risk frameworks available and described their effectiveness and challenges. The cybersecurity frameworks investigated were: NIST SP 800-53 Rev. 4. (NIST, 2014a); NIST CSF version 1.0 (NIST, 2014b); Control Objectives for Information and Related Technologies - COBIT5, (ISACA, 2012); ISO/IEC 27001:2013 - published by International Organization for Standardization and the International Electrotechnical Commission (ISO, 2013); International Society of Automation (ISA) 62443-2-1:2009 (ISA, 2009); and ISA 62443-3-3:2013 (ISA, 2012).

NIST CSF is one of the top preferred frameworks used by organizations because its structure was designed to evolve with changes in cybersecurity threats, processes, and technologies. These organizations usually develop their custom assessment tools based on the NIST CSF model, because of its ease of use and flexibility in targeting individual areas of an organization to measure the risk level. The primary function of such a tool is to determine the level of security compliance of any unit in the organization, and it can also evaluate the organization’s system to identify the risks/possible threat areas.

# Qualitative Assessment

In practice, a qualitative risk assessment is a process of using ordinal rating scales (e.g., green-yellow-red, low-medium-high) to determine risks based on their likelihood of occurrence and impact of loss to the organization. Going by this, organizations can visually represent the relative severity of the various risks the organization faces.

One major downfall of this type of approach is that the range of values in a qualitative assessment is usually small, this makes different experts rely on their personal experiences to produce meaningful but inconsistent results from them.

Qualitative risk assessment is efficient, useful in making quick decisions, and easy to communicate. However, the downsides associated with this approach are bias and inconsistencies in risk assessment results, as well as ambiguity in meaning (what does "red/high" really mean?).

Another issue lies with risk prioritization and mitigation. When there are multiple red risks, how does an analyst decide which to mitigate first? Which one is "reddest"? Succinctly, the qualitative approach presents a systematic analysis that provides ordinal results rather than a numerical result. Although the results are reliable, in many cases, the ordinal results are not detailed enough to make clear decisions.

# Quantitative Assessment

Quantitative assessment depends on probabilistic and statistical approaches towards an uncertain event. Quantitative risk assessment minimizes the tendency towards bias and inconsistencies if integrated with a well-defined model to evaluate risk. Moreover, it addresses the prioritization problem by utilizing economic terms (e.g., dollars and cents) as its measurement, rather than an ordinal or relative scale.

Quantitative method enhances analysis by scoring the effectiveness of current and potential security solutions. The objective of the quantitative assessment is to utilize probability theory and statistics to assign probabilistic numerical values to threat likelihood. Although this method provides clear guidance about the threat, it usually has a high level of difficulty in implementation and ambiguity evaluation.

One of the most popular frameworks for the quantitative cyber risk assessment is the Factor Analysis of Information Risk (FAIR) model (Wang, Neil & Fenton, 2019).

FAIR’s definition of risk states that « Risk is the possibility of an unfortunate occurrence ».

Hybrid Assessment