The Open Group Security Forum Project Charter
Calculating Reserves for Cyber Risk: An Open FAIR Approach

Status: Final
Revision level: V1.0
Date: Mar. 09, 2021
Proposed by: Mike Jerbic

A. Project Description

To comply with international regulations, financial institutions must model, estimate, measure and prudentially manage their financial risk exposure associated with their financial assets and operations. The risk associated with the information technology operating a financial institution, however, is rarely modeled, estimated, measured and managed in a way that can be compared to the risk exposures of financial asset portfolios.

The contributed White Papers will show how the risk associated with information and information technology can be measured in a commensurate way as financial asset risk, so much so that capital requirements can be applied to it.

This work is significant and timely now, especially with the COVID-19 pandemic and with CISOs needing to cross the financial risk management chasm.

Key Points or content

- Demonstrate by analogy to an underlying security (loan portfolio, stock, or bond) and the risk associated with a cyber event, such as ransomware, how the concepts of risk analysis are the same between the two.
- Translate risk terms between the risk management community in financial institutions and Open FAIR cyber risk community to show what appears to be a concept and language gap really is not one.
- Show how cyber risk once measured in bank risk terms can have a BASEL capital requirement applied to it.
- By hypothetical example, quantify a bank's risk associated with ransomware and apply capital requirements against it.
- Emphasize that while detailed models will differ between those in the financial risk community and the cyber risk modeling community, they are all conceptually based upon the same fundamentals: probable loss event frequency and probable loss magnitude, expressed as distributions.
- Point out (to head off financial risk professionals' unnecessary objections) that in these White Papers, the financial asset risks modeled are for underlying tangible assets such as stocks, bonds, loan portfolios, not for derivatives. Those assets best mirror cyber assets: information, information systems, etc. There is no (currently identified) equivalent "derivative" asset in cyberspace.
- Open FAIR is an accepted, industry standard way of quantifying cyber risk in economic risk terms and is unique in that it quantifies risk in economic terms.

B. Goals of this Project

The purpose of these White Papers is to connect cyber risk as discussed in the Security Forum (as standardized in Open FAIR) in a way that risk managers and analysts in financial institutions can understand and accept within their frame of understanding risk and its management within a financial institution such as a bank or trading desk. Key to accomplishing this goal is that The Open Group stands by these White Papers as authoritative from the perspective of the high technology industry.

- Connect the financial risk management community and cyber risk community such that a bank audience grasps that cyber risk can be measured and have capital reserved against it.
- Provide guidance for cyber risk managers in a bank to be able to communicate cyber risk to financial risk management in a bank more effectively.
- Have the cyber audience grasp how cyber risk fits within an overall holistic enterprise risk picture that the bank audience. This gives the foundation for a CISO to influence a bank's decisions up to and including capital requirements.
- Show that the Open FAIR standards are fit for purpose as an approach to evaluate and quantify cyber risk in a financial institution.

Questions these White Papers answer:

We do not know the capital requirements on cyber risk, but we are afraid of them, and regulators are asking for them. Capital requirements for a bank can be defined in two ways: economic capital (actual amount of capital held in reserve to cover cyber risk) and regulatory capital (the capital regulators demand to be held in reserve to cover cyber risk). These White Papers would help banks do that.

- How much is that risk?
- How important is it compared to other financial institution enterprise risks?

The authors Dr. Bob Mark and Mike Jerbic envision that they will write a companion document based upon these White Papers aimed at the Banking Risk management community. *Operational risk, which includes cyber risk, has a tight, very specific meaning in Financial Risk world.* We feel that authoritative guidance approved and supported by the technical community is perquisite to a derivative work for the banking community. Bob knows that community well and can navigate terminology minefields and other sensitive "hot buttons" that must be overcome to get that audience to understand Open FAIR and its role in quantitative cyber risk analysis. That said, we want an authoritative, approved foundational document as a reference.

C. Project Deliverables

A. Two White Papers
    a. The first to describe the method for applying capital requirements to cyber risk
    b. The second to provide evidence and support for the method, justifying its applicability

D. Project Value Proposition

A. These White Papers demonstrate how cyber risk can be measured in the same units of measure as other financial services risks. The financial services industry has the most mature risk management models and staff. That staff may not know about Open FAIR, and seeing how Open FAIR can measure cyber risk in substantially similar terms to other risks

such as credit risk, market risk, etc., will build credibility for Open FAIR as a standard and approach and will open Open FAIR up to adoption by the Financial Services and regulatory communities.

E. Project Personnel

A. Stakeholders
    a. The governing stakeholders of the project are:
        i. The Open Group Security Forum (Steering Committee)
B. Team
    a. The primary authors are Mike Jerbic and Dr. Bob Mark. Dr. Mark will be an Invited Contributor to the project so that he can interact directly with the Security Forum.
    b. The project review team will be drawn from members of The Open Group Security Forum, most likely the majority of which will come from the Open FAIR working group.
    c. Mike Jerbic will be the Project Facilitator.

F. Project Methodology

This final section describes the project methodology, which includes:

A. Approach
    a. These White Papers would follow The Open Group Contributor process. Bob Mark would be the Contributor of the document, offering draft complete White Papers for Security Forum Member review and revision, with Bob Mark participating in discussions as an Invited Contributor. Members would eventually review and submit Change Requests to the draft that Mike would respond to using The Open Group review processes.
B. Roadmap
    a. The draft contributed will originate from Mike Jerbic and Bob Mark.
    b. Members review the draft and discuss it with Bob and Mike during scheduled meetings, either as its own working group or during another established meeting series.
    c. The Open FAIR BoK Update working group will act as the initial review and discussion group, followed by a Forum Review with the Security Forum.
    d. Estimate of six months/White Paper for a draft ready for Forum Review.
C. Governance
    a. Governance of the initiative will be the Open Group standard policy and procedures.
D. Approval
    a. The project charter will be approved by The Open Group Security Forum Steering Committee.
    b. Project deliverables will be approved by The Open Group Security Forum Members.