Security Forum
Open FAIR Model Mathematical Description
Project Charter

Status: Approved
Revision level: V1.0
Date: 3 Dec. 2021

Project Description
Current documents available describing the Open FAIR methodology have focused on the flow of logic and parameters of an Open FAIR model. There is a pressing need to describe how these parameters should be interpreted mathematically so that users can produce Open FAIR analyses in a consistent and defensible fashion. Currently, taken to extremes, any mathematical model that incorporates all Open FAIR parameters could claim to follow the Open FAIR method.

There is some flexibility in using the Open FAIR parameters to produce a model that most accurately reflects the circumstances that the IT risk manager needs to evaluate, but there are also certain probabilistic rules that need to be respected. These rules are simple to follow once understood, but a risk modeler is very often unaware of them which can unintentionally lead to highly inaccurate results. Inconsistencies in results from different models with the same input data would undermine the validity of the Open FAIR method.

The aim of this project is to provide a reference document that explains to the user how to build an Open FAIR risk analysis model, how to interpret its results, and offer guidance on statistical methods that can be used in the estimation of Open FAIR parameters where data are available.

Goals of this Project
The goals of this project are to:

- Provide a Guide explaining how an Open FAIR model can be interpreted mathematically
- Explain the range of appropriate probabilistic interpretations that can be applied
- Make appropriate statistical techniques easily accessible where data are available to inform the model parameters
- Offer some test case scenarios with results against which a model can be checked

Project Value Proposition
A. Increase confidence in the use of the Open FAIR methodology
B. Assist users in developing and adapting their own Open FAIR models
C. Educate readers in the application of probabilistic analysis to IT risks
D. Provide a ‘cookbook’ for certain scenarios for Open FAIR analyses and the mathematics behind them
E. Provide an authoritative reference that can be used to validate a model is following the Open FAIR methodology, avoiding prescribing a specific way to model Open FAIR and instead offering advice on options
Project Deliverables
The Open Group Guide, of no more than 40 pages of content (excluding The Open Group template materials), containing:

A. An overview of the mathematical concepts inherent in the Open FAIR methodology
B. Explanation of how the parameters are used within the model
C. Description of the mathematical options in parameter use that allow one to describe different scenarios, providing easy access to a range of techniques available
D. Review of the risk modeling common mistakes for this type of model and how to avoid them
E. An appendix of example model scenarios with test input and output values to assist model validation, providing a range of outcomes to allow checking whether a model produces results within the range at various percentiles

Project Personnel
A. Stakeholders
    a. The governing stakeholders of the project are:
       i. The Open Group
       ii. The Security Forum
B. Team
    a. The project team will be drawn from members of The Open Group Security Forum. The project leadership will be selected through the normal procedures of The Open Group.
    b. The Project Facilitator(s) will be David Vose.

Project Methodology
This section describes the project methodology, which includes:

A. Approach
    a. Project Facilitator David Vose will produce an initial draft document description, including an overview of the problem being solved and the purpose of the document and providing an overview of the content of each section for initial approval by the Project Team.
    b. After receiving initial approval by the Project Team, David and co-author(s) will produce a complete document for review and revision by the Project Team.
    c. After review and revision by the Project Team, David and co-author(s) will apply any final changes before the document goes through formal Security Forum Review.
B. Roadmap
    a. Draft document description (9+ weeks)
       i. 1 week – Initial draft document description creation
       ii. 2 week – Initial Project Team input
       iii. 4 weeks – Complete draft document preparation
       iv. 2-6+ weeks – Project Team review and revision
    b. The Open Group publication process
       i. Forum Review (8+ weeks)
          1. 1 Week – Announcement
          2. 2 Weeks – Review
3. 1-3+ Weeks – Resolve Change Requests (CRs), implement revisions, and ballot to approve for publication (or to approve to proceed to Company Review)
   a. 75% approval required (If White Paper/Guide)
   b. Potential for more time needed if many CRs submitted

4. 4+ Weeks – Publication
   a. Technical Editor review and editing
   b. VP Approval for document to proceed to Executive Approval
   c. Executive Approval
   d. Publication

C. Governance
   a. Governance of the initiative will be The Open Group standard policy and procedures.
   b. The Project will reside within the Security Forum’s Security and Risk Management Working Group.

D. Approval
   a. Project deliverables will be approved by The Open Group. The Project Charter will be approved through the normal mechanism of The Open Group.