

# Security Forum

## Open FAIR™ Risk Analysis Example Guide

### Project Charter

Status: Final

Revision level: V1.0

Date: 01 Sep. 2020

#### A. Project Description

The Open FAIR™ Risk Analysis Example Guide Project will seek to create a guide in The Open Group format to walk through example Open FAIR risk analyses. In revising the Open FAIR™ Standard, the previous qualitative example was removed to ensure the standard documents only emphasize materials that can be included in an exam—instead of trying to offer guidance. This Example Guide will fill the guidance role. It will walk readers through the qualitative example originally in O-RA V1.0 and O-RT V2.0 before providing a quantitative version of the same example. The quantitative version will include the rationale for any and all calibrated estimates used and will present results from the Open FAIR™ Risk Analysis Tool. The Example Guide will contrast the results of the qualitative and quantitative analyses to demonstrate the value of the Open FAIR quantitative approach.

The Example Guide will be designed to include additional/different classes of examples of analyses and examples of communicating results—it will be a *living document* to be updated over time with new examples of analyses and reports.

The Example Guide will also consider communicating results from an Open FAIR risk analysis within other frameworks, such as the NIST CSF or ISO 27005, to demonstrate examples of how the results might be presented to satisfy the requirements of management/decision-makers.

#### B. Goals of this Project

This project will create an Open FAIR™ Risk Analysis Example Guide that will primarily demonstrate the benefit of a quantitative risk analysis (over a qualitative risk analysis) and provide guidance and rationale for using calibrated estimates as well as examples of reports and communicating results.

#### C. Project Deliverables

- A. Open FAIR™ Risk Analysis Example Guide

#### D. Project Value Proposition

- A. Separation of guidance from the normative Open FAIR™ Standard
- B. Additional room to expand on and explain the rationale for calibrated estimates
- C. Demonstration of the Open FAIR™ Risk Analysis Tool
- D. Provide examples of reports and communicating results

#### E. Project Personnel

- A. Stakeholders
  - a. The governing stakeholders of the project are:
    - i. The Open Group
- 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 will be Chris Carlson (C T Carlson LLC).

## F. Project Methodology

This final section describes the project methodology, which includes:

- A. Approach
  - a. Chris Carlson has prepared a draft document for a Working Group within the Security Forum to review, revise, restructure, and refine.
  - b. The Open FAIR Risk Analysis Example Guide Working Group will ensure the draft document follows updates to the Open FAIR™ Standard before making a consensus decision to enter it into the publication process as The Open Group Guide.
- B. Roadmap
  - a. This Project will meet every other week on Tuesdays at 2:00PM EDT for 1-hour per meeting with an *initial goal* of completing a first draft of the document by the end of March 2021.
    - i. The first meeting will be on Tuesday, Sep. 1, 2020 at 2:00PM EDT.
  - b. After completing the first draft, the Working Group will determine what additional changes are needed for the Open FAIR™ Risk Analysis Example Guide before it can be entered into the publication process, following [The Open Group Standards Process](#) for guides.
- C. Governance
  - a. Governance of the initiative will be The Open Group standard policy and procedures.
- 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.