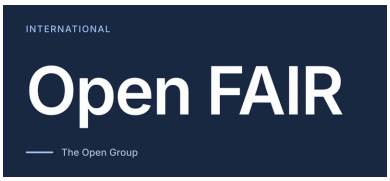
SmartSuite

Framework / Risk Management / Other

Open FAIR – The Open Group Risk Taxonomy (O-RT) Version 3.1 and Risk Analysis (O-RA) Version 2.1 Standards

Open FAIR is The Open Group's pair of standards for quantitative information risk analysis: the Risk Taxonomy (O-RT) Version 3.1 and the Risk Analysis (O-RA) Version 2.1, both of May 2025.



What it is

Open FAIR is The Open Group's pair of standards for quantitative information security risk analysis: the Risk Taxonomy (O-RT) Standard, Version 3.1 (document C251), and the Risk Analysis (O-RA) Standard, Version 2.1 (document C250), both published on May 22, 2025. It is The Open Group's standardization of Factor Analysis of Information Risk (FAIR), and it is voluntary: risk analysts adopt it to express risk in consistent economic terms rather than as high, medium or low ratings. The O-RT provides a standard definition and taxonomy for information security risk and information on how to use the taxonomy; the O-RA provides a set of standards for the aspects of information security risk analysis; each names the other as its companion document.

At a glance

PUBLISHER The Open Group	TYPE Standard	VERSION O-RT Version 3.1 (C251) and O-RA Version 2.1 (C250), May 22, 2025
EFFECTIVE May 22, 2025	DOMAIN Risk Management	FAMILY Other
REGION International	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

Source: opengroup.org/open-fair

Why it matters

- **A shared definition of risk** The O-RT gives risk analysts one standard definition and taxonomy for information security risk, so analysis work from different teams and domains uses the same factors and relationships.
- **Results in economic terms** Open FAIR produces risk statements measured in the same economic terms as the other risks an organization manages, which The Open Group describes as consistent and defensible.
- **A documented process** The O-RA standardizes the aspects of information security risk analysis, and the Risk Analysis Process Guide (G180) and Example Guide (G21A) show how an analysis is performed and reported.
- **Works inside other frameworks** The method is directly applicable with other standards; The Open Group publishes cookbooks for the NIST Cybersecurity Framework (G167) and ISO/IEC 27005 (C103).

Updated Nov 9, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports Open FAIR

Risks Covered by an Open FAIR Analysis

Hold each risk an Open FAIR analysis covers in the Enterprise Risk Management register, rated for inherent and residual likelihood and impact, with the rationale for each rating.

Risk Register, Controls and Mappings

SmartSuite holds the risk register, the controls and the framework mappings for each risk an Open FAIR analysis covers. The analysis itself runs in a FAIR tool.

Loss Exposure as Annual Loss Expectancy

Record the loss exposure calculated in a FAIR tool on each risk as an Annual Loss Expectancy, so it reports beside the rated risks in Enterprise Risk Management.

Framework Risk Assessment Link

Link each risk to the NIST Cybersecurity Framework and ISO/IEC 27005 frameworks and the controls it maps to, the programs the Open FAIR cookbooks describe.

Owners and Assessment Cadence

Name a risk owner and a risk analyst on each risk, set its assessment frequency and next assessment date, and schedule re-analysis in a FAIR tool when the environment or the standards change.

Executive Risk Reporting

Use Enterprise Risk Management to report loss exposure and business-case comparisons to executives and the board in the same economic terms as the organization's other risks.

Common framework mappings

NIST SP 800-30 Rev. 1 · ISO 27005:2022 · ISO 31000:2018 · ISO 31010:2009 · NIST CSF 2.0 · NIST SP 800-39 · COSO ERM 2017 · ISO 27001:2022 · NIST 800-53 Rev.5 · CIS Controls v8.1

Official resources

Open FAIR at The Open Group

The Open Group's Open FAIR page describing the taxonomy and analysis standards, certification, and supporting guides.

opengroup.org/open-fair

Risk Taxonomy (O-RT), Version 3.1 (C251)

The publications entry for the current Risk Taxonomy Standard, published May 22, 2025, superseding Version 3.0.1.

publications.opengroup.org/c251

Risk Analysis (O-RA), Version 2.1 (C250)

The publications entry for the current Risk Analysis Standard, published May 22, 2025, superseding Version 2.0.1.

publications.opengroup.org/c250

Open FAIR Certification for People

The Open Group's certification program for risk analysts based on the O-RT and O-RA standards.

opengroup.org/certifications/openfair

Frequently asked questions

What are the current Open FAIR standards?

The Risk Taxonomy (O-RT) Standard, Version 3.1, document C251, and the Risk Analysis (O-RA) Standard, Version 2.1, document C250, both published by The Open Group on May 22, 2025. The O-RT (42 pages) supersedes C20B, O-RT Version 3.0.1, and the O-RA (48 pages) supersedes C20A, O-RA Version 2.0.1, both of November 2021. The Open Group's Open FAIR page still lists the 2021 versions; the publications catalog entries are current.

What changed in O-RT 3.1 and O-RA 2.1?

The Open Group's announcement of May 22, 2025 says the changes to the standards are limited to addressing the new Governance Function from NIST Cybersecurity Framework 2.0, with other small changes made to ensure consistency between the two documents. The Certification Authority did not anticipate any change to the Open FAIR certification exam, and the Open FAIR Conformance Requirements were being updated separately.

Updated Nov 9, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What is the Open FAIR Body of Knowledge, and is there a certification?

The Body of Knowledge is the O-RA and O-RT standards together. The Open FAIR Certification Program, launched in 2014, is based on it and comprises the Open FAIR Foundation and Open FAIR 2 Foundation certifications, which candidates prepare for through an accredited training course provider or The Open Group's self-study materials. In May 2025 the program had more than 1,700 certified individuals.

Can Open FAIR be used with ISO/IEC 27005 or the NIST Cybersecurity Framework?

Yes. The Open Group says the Open FAIR method is directly applicable with other standards and provides a way to quantify risk within them to inform risk assessments. It publishes the Open FAIR - NIST Cybersecurity Framework Cookbook (G167, October 2016) and the Open FAIR - ISO/IEC 27005 Cookbook (C103, November 2010), the latter written so practitioners can follow by example how to apply Open FAIR to other frameworks of their choice.

Is Open FAIR free to use?

Both standards are available as free PDF editions after login on The Open Group's publications site, and The Open Group says its Open FAIR publications are free to download and use within organizations. A commercial license is available for organizations applying the Open FAIR Body of Knowledge for commercial use. The companion guides, white papers and the Excel-based Risk Analysis Tool are published alongside the standards.

License included / downloadable: No The O-RT and O-RA standards are free PDF editions downloaded from The Open Group's publications site after login, with a commercial license available for commercial use; their text is not included with the platform.

Full framework page and mappings: smartsuite.com/frameworks/open-fair-risk-taxonomy-and-risk-analysis-standards