London, HQ Bloomsbury
4/4a Bloomsbury Square
London WC1A2RP

Training catalog 2026

FAIR™ Framework
(Factor Analysis of Information Risk™)
& Cyber Risk Quantification

c·risk

C-Risk Education offers training in Data-Driven Cyber Risk Management using the FAIR™ (Factor Analysis of Information Risk) standard. Our programs enable executives, managers, and practitioners to integrate financial Cyber Risk Quantification into their strategic and operational decision-making.

All our training courses (excluding e-learning) are subject to a training agreement to be signed by the customer.

Table of contents

OUR TRAINING COURSES

ED-IN-01 – Introduction to Data-Driven Cyber Risk Management with the FAIR™ Standard

This course introduces the principles of financial risk quantification. It provides an overview of the FAIR™ taxonomy and analysis method and learn how to define risk scenarios and then quantify them in financial terms. Participants are guided in the practical next steps for themselves and their organization in adopting cyber risk quantification.

Duration: ½ day (3 hours)

Format: Instructor-led training (on-site or virtual classroom)

CPE: 3

Pricing:

€595 excl. VAT / person (public session) ED-IN-01.1

€3 500 excl. VAT / group of 8 (private session) ED-IN-01.2

Learning Objectives

- Overview of risk and risk management definitions
- Understand the objectives of risk management and the limitations of current qualitative approaches to risk analysis
- Understand how the FAIR™ standard quantifies cyber risk and supports decision-making in cybersecurity strategy

Target Audience: Managers and department heads interested in implementing quantitative cyber risk management approaches

Prerequisites: None, though some basic knowledge of cybersecurity may be helpful

ED-EL-01 – Introduction to Data-Driven Cyber Risk Management with the FAIR™ Standard - e-Learning

This course introduces the principles of financial risk quantification. It provides an overview of the FAIR™ taxonomy and analysis method and learn how to define risk scenarios and then quantify them in financial terms. Participants are guided in the practical next steps for themselves and their organization in adopting cyber risk quantification.

Pricing:

€195 excl. VAT / person ED-EL-01.1

€780 excl. VAT / 5 people ED-EL-01.2

€1,170 excl. VAT / 10 people ED-EL-01.3

CPE: 3

Unlimited access for 3 months

Learning Objectives

- Overview of risk and risk management definitions
- Understand the objectives of risk management and the limitations of current qualitative approaches to risk analysis
- Understand how the FAIR™ standard quantifies cyber risk and supports decision-making in cybersecurity strategy

Target Audience: Managers and department heads interested in implementing quantitative cyber risk management approaches

Prerequisites: None, though some basic knowledge of cybersecurity may be helpful

ED-IN-02 – Data-Driven Cyber Risk Management with the FAIR™ Standard for Practitioners

This course prepares participants to quantify risk in financial terms by providing a detailed explanation of the FAIR™ taxonomy and analysis method, supported by practical exercises and applied analysis. Participants will learn how to define risk scenarios, model them using FAIR™, identify and estimate the data required for financial quantification, and interpret results in context. The course also prepares participants for the Open FAIR™ 2 certification exam. *The exam is not included in the training fee, and additional study may be required before taking the certification test.*

Duration: 2 days (12 hours)

CPE:12

Format: Instructor-led training (on-site or virtual classroom)

Pricing:

€1,850 excl. VAT / person (public session) ED-IN-02.1

€9,000 excl. VAT / group of 8 (private session) ED-IN-02.2

Learning Objectives:

- Understand the limitations of qualitative risk management approaches
- Understand the decision-making process and decision support
- Understand how the FAIR™ standard helps quantify cyber risk to support decisions in cybersecurity strategy
- Practice financial quantification through a use case based on a real-world situation
- Prepare for the Open FAIR™ certification with practice on multiple-choice exam-style questions

Target Audience: CISOs, consultants, cybersecurity analysts, risk managers

Prerequisites: None, though some basic knowledge of cybersecurity may be helpful

ED-EL-02 – Data-Driven Cyber Risk Management with the FAIR™ Standard for Practitioners - e-Learning

This course prepares participants to quantify risk in financial terms by providing a detailed explanation of the FAIR™ taxonomy and analysis method, supported by practical exercises and applied analysis. Participants will learn how to define risk scenarios, model them using FAIR™, identify and estimate the data required for financial quantification, and interpret results in context. The course also prepares participants for the Open FAIR™ 2 certification exam. *The exam is not included in the training fee, and additional study may be required before taking the certification test.*

Pricing:

€495 excl. VAT / person ED-EL-02.1

€1,980 excl. VAT / 5 people ED-EL-02.2

€2,970 excl. VAT / 10 people ED-EL-02.3

CPE:12

Unlimited access for 3 months

Learning Objectives :

- Understand the limitations of qualitative risk management approaches
- Understand the decision-making process and decision support
- Understand how the FAIR™ standard helps quantify cyber risk to support decisions in cybersecurity strategy
- Prepare for the Open FAIR™ 2 certification with a practice exam

Target Audience: CISOs, consultants, cybersecurity analysts, risk managers

Prerequisites: None, though some basic knowledge of cybersecurity may be helpful

ED-IN-03 – Maximize your chances of success with Data-Driven Cyber and Technology Risk Governance - Module for executives

This course helps executives recognize the importance of objective, data-driven risk analysis for making informed decisions and increasing their chances of success. This one-hour course underscores the limitations of purely qualitative approaches and demonstrates how the FAIR™ methodology enhances the evaluation and quantification of cyber risks, strengthening corporate governance and strategy.

Duration: 1 hour

CPE:1

Format: Instructor-led training
(on-site or virtual classroom)

Pricing:
€495 excl. VAT / person ED-IN-03.1

Learning Objectives :

- Identify the limitations of current qualitative analyses and understand how to improve them with FAIR™
- Understand the value of cyber risk quantification for strategic decision-making
- Explore the FAIR™ methodology and its taxonomy for better risk management

Target Audience: Executives, members of the executive committee, strategic decision-makers involved in risk governance

Prerequisites: None

ED-IN-04 – Turning Controls into Measurable Risk Reduction with FAIR-CAM

This advanced course focuses on how cybersecurity controls influence risk and how to model the effectiveness of cybersecurity controls usingFAIR-CAM (Controls Analytics Model). The course is based on real-world cases. Participants will analyze attack chains, identify relevant control functions, and estimate their operational effectiveness using measurable criteria (efficacy, coverage, reliability). By the end of the course, participants will be able to use FAIR-CAM to support FAIR™ risk analyses and optimize risk reduction strategies.

This course is an excellent follow-up to CRQ-02 and provides a deeper understanding of controls in a quantitative risk management approach.

Duration: 4 hours

Format: Instructor-led training
(on-site or virtual classroom)

CPE:4

Pricing:
€1,200 excl. VAT / person (public session) ED-IN-04.1
€6,500 excl. VAT / group of 8 (private session) ED-IN-04.2

Learning Objectives:

- Understand how security controls influence the frequency and magnitude of losses
- Identify the functions of security controls in an attack chain
- Evaluate the operational effectiveness of security controls based on measurable criteria
- Model the aggregated effect of security controls on loss probability using FAIR-CAM
- Incorporate FAIR-CAM results into FAIR™ analyses

Target Audience: CISOs, risk or cybersecurity analysts, GRC consultants, technical auditors

Prerequisites: Completion of CRQ-02, ELC-02, or practical knowledge of the FAIR™ model.

ED-EL-04 – Turning Controls into Measurable Risk Reduction with FAIR-CAM – e-Learning

This advanced e-learning course focuses on how cybersecurity controls influence risk and how to model the effectiveness of cybersecurity controls using FAIR-CAM (Controls Analytics Model). The course is based on real-world cases. Participants will analyze attack chains, identify relevant control functions, and estimate their operational effectiveness using measurable criteria (efficacy, coverage, reliability). By the end of the course, participants will be able to use FAIR-CAM to support FAIR™ risk analyses and optimize risk reduction strategies.

Pricing:
€695 excl. VAT / person ED-EL-04.1
€2,780 excl. VAT / 5 people ED-EL-04.2
€4,170 excl. VAT / 10 people ED-EL-04.3

CPE:10

Unlimited access for 3 months

Learning Objectives :

- Understand the role of controls in reducing cyber risk
- Grasp the key dimensions of control effectiveness (intention, coverage, reliability)
- Model an attack chain and identify relevant control functions
- Apply FAIR-CAM™ results within a FAIR™ analysis
- Strengthen quantification skills through a practical case study

Target audience: CISOs, risk or cybersecurity analysts, GRC consultants, technical auditors.

Prerequisites: Completion of ELC-02, CRQ-02, or practical knowledge of the FAIR™ model.

ED-EL-05 – Building a Data-Driven Third-Party Risk Management (TPRM) Program with FAIR – e-Learning *(available soon)*

This advanced e-learning course provides a practical, scenario-driven approach to managing third-party cyber and operational risks using the FAIR™ standard. Participants will learn how to identify vendor exposures, construct high-quality third-party risk scenarios, and quantify their financial impact using data-driven methods. The course covers the full TPRM lifecycle and shows how to integrate quantitative insights into due diligence, contracting, onboarding, and ongoing monitoring. By the end of the course, participants will be able to apply FAIR™ to build a measurable, defensible TPRM program, prioritize vendor remediation efforts, and communicate third-party risks clearly and effectively to business leaders.

Pricing:
€695 excl. VAT / person ED-EL-05.1
€2,780 excl. VAT / 5 people ED-EL-05.2
€4,170 excl. VAT / 10 people ED-EL-05.3

CPE:10

Unlimited access for 3 months

Learning Objectives :

- Understand the unique risk challenges introduced by third-party relationships.
- Identify assets, threats, and loss events involved in third-party risk scenarios.
- Construct high-quality FAIR™ scenarios tailored to vendors and supply-chain contexts.
- Quantify third-party risks using data-driven ranges and Monte Carlo simulation.
- Integrate quantitative insights into due diligence, contracting, onboarding, and ongoing monitoring.
- Communicate vendor risk in financial terms to support decision-making and prioritization.

Target audience: CISOs, cybersecurity or risk analysts, TPRM practitioners, GRC consultants, vendor management teams, procurement professionals, and technical auditors.

Prerequisites: Completion of ED-EL-02, ED-IN-02, or equivalent practical knowledge of the FAIR™ model and basic TPRM concepts.

BS-00 – Bespoke / On Demand

On request, C-Risk Education will design and deliver customized training courses tailored to the specific needs of your organization. Whether you are looking to focus on a particular topic, address a unique risk context, or align the content with your internal frameworks and practices, we will work with you to build a training course that meets your objectives. These bespoke sessions can be delivered on-site or remotely and are suitable for both executive and practitioner audiences. Pricing is available upon request.

Bespoke courses are also eligible for Continuing Professional Education (CPE) credits, with a certificate of completion automatically provided to all participants.

TRAINING COURSE TERMS & CONDITIONS

Purpose and General Provisions

C-Risk Education is a training organization specialized in cyber risk quantification using the FAIR™ standard. C-Risk Education designs, develops, and delivers public and private training programs in Paris, across France, and in Europe, either on-site or remotely.

In the following paragraphs, the following terms are defined as:

- Customer: any natural or legal person who registers or orders training from C-Risk Education.
- Trainee: the individual participating in training.
- Inter-company training: training courses listed in the C-Risk catalogue which bring together trainees from different organizations.
- Intra-company training: tailor-made training by C-Risk on behalf of a specific client or a group of clients.
- CGV: the general conditions of sale, detailed below.
- OPCA: French organization responsible for the financial oversight of employee training within France.

These general conditions of sale apply to inter-company and intra-company training orders placed with C-Risk SAS. This implies the unconditional acceptance by the buyer and their full acceptance of these general conditions of sale. C-Risk provides guidelines for the requirements to follow the training courses it offers. It is up to the client to assess their needs and check whether their employees have the expected prerequisites to follow C-Risk Education training.

CPE Credits

Our training courses are eligible for Continuing Professional Education (CPE) credits recognized by organizations such as (ISC)² and ISACA. The number of credits depends on the actual duration of the training and the relevance of the content to the participant's certification domain. It is the responsibility of each participant to self-report their earned CPEs to the relevant certification body, in accordance with its guidelines.

At the end of the course, participants will receive a certificate of completion stating:

- the title of the training program
- the total number of training hours
- the date of completion
- the participant's name
- the learning objectives of the course

Registration

Registration becomes effective only upon receipt by C-Risk of the training agreement or quote, duly completed and stamped by the client. For regional or international sessions, documents must be received at least 15 days before the training begins.

C-Risk will send a training confirmation by email no later than three days before the session, summarizing logistical details: date, location, time, and access instructions, to the contact(s) indicated in the registration documents. C-Risk cannot be held responsible for non-receipt of the confirmation, especially in case of participant absence. After the training, an individual certificate of attendance and the related invoice will be sent by email.
Orders are valid only after formal acceptance by C-Risk within eight days. Any subsequent modification by the client must be approved in writing by C-Risk.

Billing

All prices are quoted in euros, excluding VAT, which will be added at the prevailing rate.
For private training courses held at the client's premises, prices do not include trainer travel expenses.
For public sessions attended by at least five participants and held on-site at C-Risk, accommodation and catering costs are not included in the course fees.
Training fees include participation, training materials, and coffee breaks. Any training begun is due in full.

Payment must be made at least one week before the first training day.
Without payment, C-Risk may deny access to the course.
The invoice will be issued after the training.

The payment deadline is stated on the quote. Any late payment (partial or total) will, unless a formal extension has been granted by C-Risk, incur late fees automatically without the need for reminder, starting the day after the due date, calculated at three times the legal interest rate.
C-Risk may also charge a fixed €40 recovery fee, plus any justified additional recovery costs.

Cancellation, absence or interruption of training

Any training module started is fully due and will be invoiced to the client.
In the event of absence, interruption, or cancellation, C-Risk will distinguish between days attended and days missed.
Amounts due for absences or interruptions are not eligible for OPCO coverage. In this case, the client agrees to pay the outstanding balance directly to C-Risk.

In case of cancellation by the client, C-Risk reserves the right to charge cancellation fees as follows:

- If cancellation occurs more than 15 working days before the course start: no fee.
- If cancellation occurs between 15 and 7 working days before: 50% of the training cost excl. VAT.
- If cancellation occurs less than 7 working days before: 100% of the training cost excl. VAT.

However, a participant may be replaced by a colleague from the same company.
The replacement's name and contact details must be confirmed in writing to C-Risk.
In case of absence due to a force majeure event recognized by courts, and upon validation of this condition by C-Risk, the client may reschedule the same training within 12 months.

C-Risk reserves the right to cancel or postpone any course without compensation if the number of participants is insufficient or in the event of force majeure. The client may then choose another session from the training calendar. C-Risk cannot be held liable for any costs or damages resulting from a cancellation or rescheduling.

OPCO Funding

If the client requests funding from an OPCO, it is their responsibility to:

- Submit the request in a timely manner and ensure its approval
- Indicate this explicitly upon registration

If OPCO confirmation is not received at least one week before the course start, subrogation will not be accepted. The client may then:

- Cancel or reschedule the registration
- Or provide, before the course, a formal purchase order committing to payment

Intellectual Property

Each training includes documentation for the client's internal use only. Any reproduction, modification, or sharing with third parties, in whole or in part, in any form, is prohibited without prior written consent from C-Risk.

Arbitration in the event of a dispute

These general conditions of sale are governed by French law. Any dispute arising from their interpretation or application comes under the exclusive jurisdiction of the courts of Hauts-de-Seine (92).
General conditions applicable on January 3, 2023 and subject to change without notice.

ACCESSIBILITY FOR PERSONS WITH DISABILITIES

C-Risk Education is committed to making its training accessible to all. For any accessibility needs or accommodation requests, please contact us to explore available options.

Contact us for any quote request or for further information.