Education & Certification

Program Guide

Updated: July 2025

Overview

This guide provides an overview of the FAIR Institute's professional certification and education program, including course offerings, certification paths, eligibility requirements, continuing education expectations, and supporting policies. It is intended for individuals seeking to validate their expertise in applying the FAIR™ model to cyber and operational risk management.

Table of Contents

Introduction **3**

FAIR Institute Professional Certifications 3

FAIR Institute Course Offerings 3

Certification Prerequisites and Maintenance 5

Appendix A: Relevant Professional Experience **6**

Appendix B: Institutional Qualification Requirements for Formal Education **8**

Appendix C: Certifications Accepted in Lieu of One Year of Professional Experience **9**

Appendix D: Qualifying Activities for Continuing Professional Education (CPE) **10**

Frequently Asked Questions **12**

Introduction

The FAIR Institute Education & Certification Program is designed to build and validate the knowledge, skills, and leadership capabilities needed to apply Factor Analysis of Information Risk (FAIR™)—the global standard for cyber and operational risk quantification. Professionals at all levels can gain a practical, defensible understanding of measuring, managing, and communicating risk in financial terms through a structured learning path that spans foundational concepts to advanced applications.

The program includes role-based training and tiered certifications for Professionals, Leaders, and Executives, each aligned to key responsibilities in a modern cyber risk management function. By combining hands-on learning, real-world scenarios, and rigorous assessment, the FAIR Institute empowers individuals and organizations to make smarter, risk-informed decisions, improve program maturity, and align cybersecurity with business outcomes.

FAIR Institute Professional Certifications

The FAIR Institute offers the following three professional certifications:

- **FAIR Institute Certified Cyber Risk Professional (FAIR-CCRP)**
  This certification signifies deep proficiency in scoping, modeling, and quantifying cyber risk using the FAIR standard. Professionals with this credential are equipped to produce defensible, data-driven risk analyses that support prioritization, investment decisions, and improved communication with business stakeholders.

- **FAIR Institute Certified Cyber Risk Leader (FAIR-CCRL)**
  Designed for professionals who own and operate a cyber risk management program, this certification demonstrates the ability to integrate FAIR into governance, processes, and decision-making. Leaders with this credential can align cyber risk practices with business objectives, drive program maturity, and guide teams in delivering consistent, actionable insights.

- **FAIR Institute Certified Cyber Risk Executive (FAIR-CCRE)**
  Tailored for senior decision-makers, this certification reflects the ability to interpret and leverage FAIR-based analysis to inform strategy, investments, and board-level reporting. Executives with this credential are positioned to champion risk-informed leadership, align cybersecurity with enterprise goals, and foster a culture of accountability and transparency.

FAIR Institute Course Offerings

The following six courses will be developed and offered by the FAIR Institute:

1. **FAIR Foundations** (For: Professionals, Leaders, Executives)
   This 8-hour course is the definitive entry point for learning the FAIR model, the industry standard for quantitative cyber and operational risk analysis. The course introduces core risk concepts, including scenario scoping, frequency and magnitude forecasting, and the application of controls through the FAIR Controls Analytics Model (FAIR-CAM™). Designed for analysts, leaders, and executives, it combines foundational theory with hands-on practice to build the skills needed for accurate, defensible, and business-aligned risk assessments.

2. **Cyber Risk Analysis** (For: Professionals and Leaders)
   This 8-hour hands-on course is designed for analysts who want to apply the FAIR™ model to real-world cyber risk scenarios. Participants learn to scope and quantify cyber risk, measure control effectiveness with FAIR-CAM™, estimate losses using FAIR-MAM™, and assess third-party risk. The course emphasizes practical skills and automation techniques for continuous risk monitoring and effective reporting. By the end, learners are equipped to deliver defensible, data-driven insights that support business and regulatory decisions.

3. **FAIR Mathematics** (For: Professionals)
   This 4-hour course is designed to equip analysts with the technical skills for quantitative risk analysis, focusing on FAIR measurement concepts. Topics include Monte Carlo simulations, Beta PERT and other distribution methods, and mathematical modeling techniques. The course demystifies FAIR calculations and emphasizes that the process is transparent and not a “black box.” Professionals will work with the FAIR Workbook for Learners.

4. **Cyber Risk Communication** (For: Professionals and Leaders)
   This 4-hour course emphasizes the importance of effectively communicating risk assessments and enabling risk decisions by the business. Participants will learn strategies for translating quantitative insights into business impacts and making risk defensible. They will learn how to use risk appetite and risk tolerance to aid in decision making. They will also learn how to define and execute a regular cadence for risk reporting and communications (e.g., monthly operating reviews, quarterly business reviews, on-demand escalation).

5. **Cyber Risk Management** (For: Leaders)
   This 4-hour course covers integrating FAIR with risk management frameworks, technologies, and regulations while aligning with the company’s risk appetite and tolerance. It addresses the integration of cyber and third-party risk management programs. Participants learn about risk visibility, prioritization, and treatment to optimize cyber risk management programs. They will also learn strategies for continuous cyber risk monitoring and management.

6. **Cyber Risk Strategy** (For: Leaders and Executives)
   This 4-hour course prepares executives to align cyber risk management with business objectives strategically. It covers investment decision-making, managing risk appetite with the board, defining risk tolerance, and conducting tabletop exercises for applying cyber risk management strategies. The goal is to empower executives to integrate cyber risk management into broader strategic planning.

Certification Prerequisites and Maintenance

Candidates must meet the following requirements to earn certification.

Education & Experience	To earn certification, a candidate must possess the requisite combination of education and experience, as follows: ➔ A **FAIR Certified Cyber Risk Professional** must take the four designated courses above (approximately 16-24 hours of training), pass a certification exam, and possess three (3) years of relevant experience. ➔ A **FAIR Certified Cyber Risk Leader** must take the four designated courses above (approximately 20 hours of training), pass a certification exam, and possess five (5) years of relevant experience. ➔ A **FAIR Certified Cyber Risk Executive** must take the two designated courses above (approximately 12 hours of training), pass a certification exam, and possess eight (8) years of relevant experience. Relevant experience will be defined as time spent on a job within a specific set of domains. See Appendix A for more information. Having or earning a relevant post-secondary degree (bachelor's or master's) satisfies two years of required experience; having or earning an associate's degree satisfies one year. See Appendix B for more information. The FAIR Institute also accepts specific professional certifications to satisfy one year of required experience. See Appendix C for more information.
Verification Letter	Candidates must obtain and submit an email from a direct supervisor, another sponsor, or a human resources professional at their place of employment; or another FAIR Institute-certified professional attesting to the fulfillment of the education, certification, and professional experience requirements.
Continuing Professional Education	Candidates must acquire and maintain evidence of completing 40 hours of Continuing Professional Education (CPE) every two years. Relevant subjects of study are described in Appendix D.
Biennial Maintenance Fees	The standard course fee includes the certification test and maintenance fees for two years. After this time, candidates must pay the biennial (every two years) certification maintenance fee (not to exceed $300 US). The two-year renewal date shall be set based on the course completion date.
Certification Date	The certification date is the date at which both conditions are met: A. the candidate passed the certification exam; and B. the candidate's education and experience have been verified per the receipt of the referral letter by the FAIR Institute or its designated administrator.

Appendix A: Relevant Professional Experience

Candidates must demonstrate relevant experience in roles related to identifying, assessing, managing, or communicating cyber and operational risk. Experience should reflect meaningful involvement in activities aligned with risk-informed decision-making. Acceptable experience may include, but is not limited to, the following roles and responsibilities:

Cyber and Operational Risk Management

- ➔ Performing qualitative or quantitative risk assessments
- ➔ Scoping or analyzing loss event scenarios
- ➔ Supporting or leading FAIR-based or similar risk analysis methods
- ➔ Defining or managing risk thresholds, risk appetite, or risk reporting programs

Governance, Risk, and Compliance (GRC)

- ➔ Designing or managing compliance and control programs
- ➔ Facilitating risk committee meetings or risk governance processes
- ➔ Mapping controls or risks to regulatory or standards frameworks (e.g., NIST CSF, ISO 27001)

Cybersecurity and Information Security

- ➔ Conducting threat modeling, vulnerability assessments, or incident response planning
- ➔ Managing security operations, controls, or security architecture
- ➔ Leading or supporting cybersecurity initiatives with risk prioritization objectives

Audit and Assurance

- ➔ Performing IT, cyber, or operational risk audits
- ➔ Assessing the effectiveness of security controls or risk mitigation programs
- ➔ Reporting findings and risk exposure to internal or external stakeholders

Business Continuity and Resilience

- ➔ Performing business impact assessments (BIAs)
- ➔ Developing or testing business continuity, disaster recovery, or resilience plans
- ➔ Analyzing operational impacts of cyber threats or disruptions

Data, Analytics, or Risk Reporting

- ➔ Building or maintaining risk dashboards, metrics, or executive reports
- ➔ Supporting decision-making through financial or risk-based modeling
- ➔ Collecting and analyzing empirical or SME-based risk data

Third-Party Risk and Vendor Management

- ➔ Evaluating the security or risk posture of third-party vendors or partners
- ➔ Developing third-party risk tiering and monitoring programs

Financial and Business Management

- ➔ Performing financial forecasting, budgeting, or cost-benefit analysis
- ➔ Supporting capital planning or investment prioritization aligned with risk
- ➔ Leading or advising on business performance management, strategy, or enterprise planning
- ➔ Translating business objectives into operational or technical requirements
- ➔ Managing or advising on programs that align risk management to business value

Leadership or Program Management (for Leader/Executive certifications)

- ➔ Directing cyber risk, security, enterprise risk, or GRC programs
- ➔ Integrating FAIR or other risk methodologies into business planning
- ➔ Communicating risk to executive leadership or board members

Experience may come from formal job titles or hybrid responsibilities within a broader role. To validate relevance, candidates may be asked to provide a résumé, LinkedIn profile, or description of duties.

Appendix B: Institutional Qualification Requirements for Formal Education

Degrees submitted to meet education requirements must be issued by an institution of higher education that is officially recognized or accredited by the appropriate government agency or accrediting body in the country where the institution is based. Accreditation must reflect that the institution is authorized to confer academic degrees at the undergraduate or graduate level.

Examples of recognized accreditation bodies include:

- United States – Institutions accredited by agencies recognized by the U.S. Department of Education or the Council for Higher Education Accreditation (CHEA)
- Canada – Institutions recognized by a provincial or territorial Ministry of Education
- United Kingdom – Institutions with degree-awarding powers recognized by the UK government and listed on the Register of Recognized Bodies
- European Union (and EHEA countries) – Institutions recognized by national education authorities and/or listed in the European Quality Assurance Register for Higher Education (EQAR)
- Australia – Institutions registered with the Tertiary Education Quality and Standards Agency (TEQSA) as authorized higher education providers

The FAIR Institute reserves the right to request documentation or verification of accreditation status if the institution's recognition is unclear.

Appendix C: Certifications Accepted in Lieu of One Year of Professional Experience

The FAIR Institute also accepts the following professional certifications in lieu of one year of experience:

- ➔ International Information Systems Security Certification Consortium (ISC²)
  - ◆ Certified Information Systems Security Professional (CISSP)
  - ◆ Certified Cloud Security Professional (CCSP)
- ➔ Information Systems Audit and Control Association (ISACA)
  - ◆ Certified Information Security Manager (CISM)
  - ◆ Certified in Risk and Information Systems Control (CRISC)
  - ◆ Certified Information Systems Auditor (CISA)
- ➔ Global Information Assurance Certification (GIAC)
  - ◆ GIAC Risk and Information Security Management (GRISC)
  - ◆ GIAC Security Essentials Certification (GSEC)
  - ◆ GIAC Enterprise Vulnerability Assessor (GEVA)
- ➔ Project Management Institute (PMI)
  - ◆ Project Management Professional (PMP)
- ➔ Open Compliance and Ethics Group (OCEG)
  - ◆ Certified GRC Professional (GRCP)
- ➔ BCI (Business Continuity Institute)
  - ◆ CBCI Certification (Certificate of the Business Continuity Institute)
- ➔ National Institute of Standards and Technology (NIST) / NICE Framework Recognized Certifications
  - ◆ NIST Cybersecurity Framework (CSF) training completion from accredited providers

To qualify, the certification candidate must provide evidence of certification. Candidates are not required to maintain current or active status for these certifications; prior attainment is sufficient to meet the experience substitution requirement.

Appendix D: Qualifying Activities for Continuing Professional Education (CPE)

To maintain an active FAIR Institute certification, certified professionals must complete 40 hours of Continuing Professional Education (CPE) every two (2) years. CPE must contribute to the professional's knowledge and capabilities in risk analysis, cybersecurity, governance, controls, compliance, data analytics, or business decision-making aligned with FAIR principles.

Qualifying CPE Activities

The following types of training and learning activities are eligible for CPE credit:

1. Formal Education and Training

- ➔ Courses or workshops offered by accredited universities, colleges, or technical institutes
- ➔ Training from recognized cybersecurity, risk, or governance organizations (e.g., ISACA, ISC², SANS, IIA)
- ➔ FAIR Institute courses, webinars, and conference sessions
- ➔ Vendor-provided training directly related to cybersecurity, risk quantification, or control frameworks

2. Professional Conferences and Events

- ➔ Attendance at industry conferences (e.g., FAIR Conference, RSA Conference, ISACA, NIST events)
- ➔ Participation in panel discussions, workshops, or webinars focused on cyber risk, risk management, or business risk governance

3. Self-Directed Learning

- ➔ Documented self-study of books, white papers, or research reports on cyber risk, quantitative analysis, or related domains (up to 10 CPE hours per cycle)
- ➔ FAIR Institute publications and briefings

4. Instruction and Presentation

- ➔ Preparing and delivering a presentation, workshop, or training session on a FAIR-related or relevant risk management topic
  (CPE credit may be granted for both preparation and delivery time, not to exceed 10 hours per cycle)

5. Authorship and Content Creation

- ➔ Writing and publishing articles, white papers, or blogs on FAIR, risk analysis, cybersecurity governance, or related fields
  (Credit awarded based on content length and relevance, up to 10 hours per cycle)

6. Professional Contributions

- ➔ Active participation in FAIR Institute working groups, committees, or standard development initiatives
- ➔ Mentoring others in risk analysis or FAIR methodology

7. Certifications and Credentialing

- ➔ Earning or renewing a relevant certification (e.g., CISM, CRISC, CISSP, PMP) during the CPE reporting period

CPE activities should be documented with proof of participation (e.g., certificates, transcripts, agendas, publication links) and maintained by the certificant in case of audit.

CPE content must be relevant to the knowledge domains covered by FAIR Institute certifications. The Institute reserves the right to review and approve submitted activities for compliance with CPE policy.

Frequently Asked Questions

1. What's the difference between the FAIR Institute's certification program and the Open Group's Open FAIR certification?

The Open Group's Open FAIR Certification validates foundational knowledge of the FAIR model through a proctored exam. In contrast, the FAIR Institute's certification program evaluates a broader and deeper set of competencies, including applied skill development, professional experience, continuing education, and community engagement. Our program emphasizes practical application and leadership readiness across roles.

2. Why are the requirements for certification more rigorous than Open FAIR's?

The FAIR Institute certifications are role-based and designed to validate both theoretical knowledge and real-world capability. By requiring coursework, demonstrated experience, and ongoing contribution through CPE or community engagement, the program ensures that certified individuals are not only familiar with FAIR concepts but are also prepared to apply them effectively in dynamic, business-critical environments.

Our experience requirements are comparable to the following cybersecurity certifications:

- ➔ Certified Ethical Hacker (CEH): 2 years
- ➔ Certified Information Systems Security Professional (CISSP): 5 years
- ➔ Certified Information Security Manager: 5 years
- ➔ Information Systems Security Management Professional (ISSMP): 7 years

3. Can I earn multiple certifications?

Yes. Candidates can pursue multiple certifications sequentially as long as they meet each requirement. Coursework overlaps between certification levels.

4. Do I need to retake courses to renew my certification?

No. Certification renewal is based on CPE completion and maintenance fees, not on retaking courses unless a significant update to the curriculum has occurred.

5. Can prior learning or external training count toward CPE?

Yes, as long as it meets the relevance and documentation requirements outlined in Appendix D.

6. What can I expect from the certification exam?

The certification exam is designed to assess your ability to apply FAIR principles and standards to real-world cyber and operational risk scenarios. It focuses on practical understanding rather than rote memorization, testing your ability to scope risk scenarios, interpret FAIR model outputs, analyze risk data, and communicate results effectively. The exam is conducted online and consists of a mix of

multiple-choice questions. While not proctored, it is open only to candidates who have completed the required coursework and met the professional experience criteria. The FAIR Institute emphasizes integrity and real-world competency over high-stakes testing, ensuring that certified professionals can apply FAIR in meaningful, defensible ways.

7. How long do I have to complete the certification after taking the required courses?

Candidates are encouraged to complete the certification exam within 6 months of completing the final required course to ensure retention of core concepts. Extensions may be granted upon request.

8. What happens if I fail the exam? Can I retake it?

Yes. Candidates who do not pass the exam on the first attempt may retake it. A waiting period and nominal re-examination fee may apply. Candidates are encouraged to review course materials and/or participate in study sessions before re-attempting.

9. Can I substitute external training for a required course?

Currently, only FAIR Institute-developed courses satisfy the training requirements for certification. This ensures consistency, quality, and alignment with current FAIR standards and practices.

10. Do certifications expire? How do I maintain mine?

Certifications are valid for two years. To maintain active status, certificants must complete 40 CPE hours and pay the biennial maintenance fee. See the “Certification Prerequisites and Maintenance” section for details.

11. Can I use the certification letters (e.g., CCRA, CCRL, CCRE) after my name?

Yes. Once certified, you may use the relevant post-nominal designation as long as your certification remains active (e.g., Jane Smith, CCRA).

12. Will I receive a digital badge or certificate?

Yes. Upon certification, you will receive both a printable certificate and a digital badge that can be added to your LinkedIn profile, résumé, or email signature.