C-Risk

2020 Training Courses

Description and Prices

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

C-Risk

SOMMAIRE

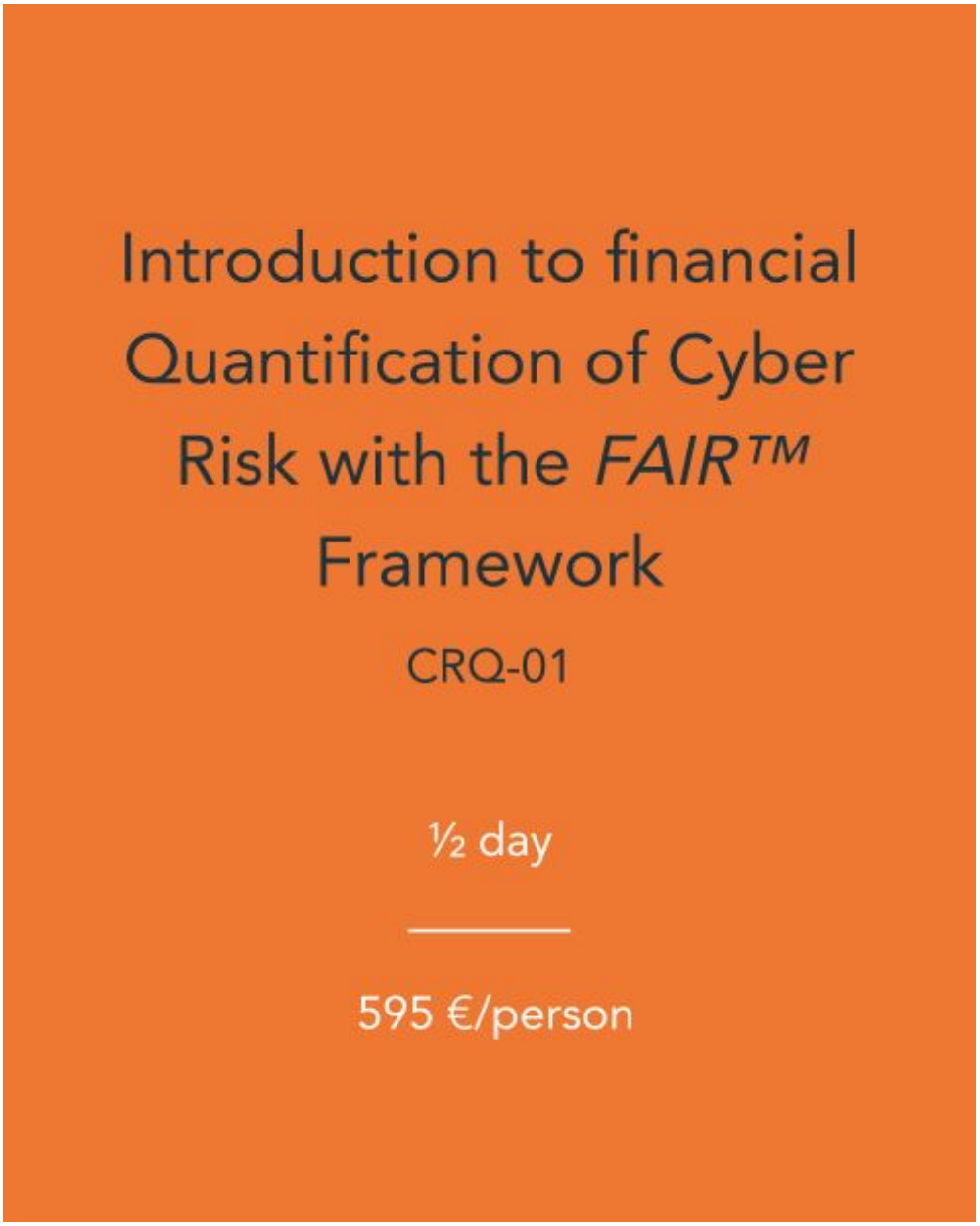
INTRODUCTION TO FINANCIAL QUANTIFICATION OF CYBER RISK WITH FAIR™ CRQ - 01

FINANCIAL QUANTIFICATION OF CYBER RISK WITH FAIR™ CRQ - 02

Phone number:
+33 (0)1 84 20 70 05

Website:
www.c-risk.com

Address:
Wojo - Cœur Défense - Tour A -
110 Esplanade du Gl de Gaulle
92931 Paris La Défense



Phone number:
+33 (0)1 84 20 70 05

Website:
www.c-risk.com

Address:
Wojo - Cœur Défense - Tour A -
110 Esplanade du Gl de Gaulle
92931 Paris La Défense

Training description

"Introduction to Financial Quantification of Cyber Risk with FAIR" covers the basic principles of cyber risk quantification in financial terms. It presents the FAIR taxonomy and analysis methodology. The course teaches attendees the limits of current qualitative approaches, how FAIR can complement them and how to measure cyber risk in a defendable manner to improve IT security decisions.

This course also provides guidance on the next steps an organization should take to begin the adoption of cyber risk quantification.

Audience

- IT Security Professionals.
- Risk Professionals.
- Anybody with an interest in improving their ability to understand, model and measure cyber risk.

Prerequisites

You don't need to be an expert in risk management or an information security engineer to follow this course.

A basic understanding of risk management, cyber risk and Information security concepts will be a benefit.

You should be curious, have an open mind and be ready to model risk in business terms.

Objectives

Understand the FAIR model and ontology

Understand the FAIR risk quantification methodology

High level review of a use case: Ransomware Risk quantification.

Phone number:
+33 (0)1 84 20 70 05

Website:
www.c-risk.com

Address:
Wojo - Cœur Défense - Tour A -
110 Esplanade du Gl de Gaulle
92931 Paris La Défense

Content

- Risk management
  - ISO 31000 and ISO 27005, NIST and EBIOS
  - Qualitative & Quantitative Analysis as per ISO (and optionally EBIOS

- The FAIR™ Framework
  - Ontology – study of the model, each variable and their inter-relationships
  - FAIR Analysis methodology – 4 steps
    - Scoping a Risk Scenario
    - Collecting & estimating data
      - Introduction to estimating data ranges & calibration
    - Statistical Simulation of the risk scenario
      - Introduction to Monte-Carlo simulation
    - Interpretation & presentation of results

- Use case "*Ransomware* "
  - Example of a non-targeted ransomware scenario (similar to "*NotPetya*" in June 2017) in a company providing engineering consulting services.
    - Review of the 4 steps of the method and discussion of the results

Duration

1/2 days – 14 hours

Technical tools and training materials

• Training materials in English (and French if requested) – theory and methodology, use case and practice examples

• Dedicated training room with video-projector and internet access for live training at our facilities

• Dedicated virtual classroom for online live training

Phone number:
+33 (0)1 84 20 70 05

Website:
www.c-risk.com

Address:
Wojo - Cœur Défense - Tour A -
110 Esplanade du Gl de Gaulle
92931 Paris La Défense

Trainers

Our trainers are OpenFAIR certified and have extensive operational experience using the FAIR model to quantify risk. They are also active members of the FAIR Institute with access to a global network of more than 8.000 members. They will be happy to answer any of your questions during the course and share their experience using FAIR.

Attendance monitoring

Training attendance form

Satisfaction survey – training objectives achievement, quality of training content and trainers

Course Completion Certificate

Phone number:
+33 (0)1 84 20 70 05

Website:
www.c-risk.com

Address:
Wojo - Cœur Défense - Tour A -
110 Esplanade du Gl de Gaulle
92931 Paris La Défense

Financial quantification of cyber risk with the *FAIR™* Framework

CRQ-02

2 days

1850 €/person

Phone number:
+33 (0)1 84 20 70 05

Website:
www.c-risk.com

Address:
Wojo - Cœur Défense - Tour A -
110 Esplanade du Gl de Gaulle
92931 Paris La Défense

Training description

The course "Financial Quantification of Cyber Risk with FAIR" prepares trainees to quantify risk in financial terms by providing a detailed understanding of the FAIR taxonomy and analysis methodology. The course teaches attendees how to scope risk scenarios, model them in FAIR, estimate the data required to perform financial quantification and interpret the results.

This course prepares attendees for the OpenFAIR Certification™ examination. The exam is not included in the cost and some additional self-study may be required before attempting the certification.

Audience

- IT Security Professionals.
- Risk Professionals.
- Anybody with an interest in improving their ability to understand, model and measure cyber risk.

Prerequisites

You don't need to be an expert in risk management or an information security engineer to follow this course.

A basic understanding of risk management, cyber risk and Information security concepts will be a benefit.

You should be curious, have an open mind and be ready to model risk in terms of controls and business impact.

Objectives

Understand the limits of current qualitative risk analysis

Understand a decision process and decision support methodologies

Understand the FAIR model and how to build risk scenarios

Understand the FAIR risk quantification methodology

Understand how to interpret the output of financial quantification and use this information to improve your risk analysis and decision making.

Deep Dive on a real-world use case: Risk quantification as a decision support tool in defining the cyber security strategy to reduce the risk of Ransomware.

Contenu

- Risk management
  - ISO 31000 & ISO 27005, NIST and EBIOS
  - Qualitative & Quantitative Analysis as per ISO (and optionally EBIOS)
  - Cognitive biases
  - Decision process: reducing uncertainty
  - The need for a formal model and method
  - Statistics and probabilities in risk quantification

- The FAIR™ Framework
  - Ontology – study of the model, each variable and their inter-relationships
  - FAIR Analysis methodology – 4 steps
    - Scoping a Risk Scenario
    - Collecting & estimating data
      - Introduction to estimating data ranges & calibration
    - Statistical Simulation of the risk scenario
      - Introduction to Monte-Carlo simulation
    - Interpretation & presentation of results

- Use case "*Ransomware* "
  - Example of a non-targeted ransomware scenario (similar to "*NotPetya*" in June 2017) in a company providing engineering consulting services.
    - Review of the 4 steps of the method and discussion of the results

- Review of a sample Multiple Choice Questionnaire in preparation for the OpenFAIR Certification exam.

Duration

2 days – 14 hours

Phone number:
+33 (0)1 84 20 70 05

Website:
www.c-risk.com

Address:
Wojo - Cœur Défense - Tour A -
110 Esplanade du Gl de Gaulle
92931 Paris La Défense

Technical tools and training materials

- Training materials in English (and French if requested) – theory and methodology, use case and practice examples
- Dedicated training room with video-projector and internet access for live training at our facilities
- Dedicated virtual classroom for online live training
- Online access to the FAIR-U risk quantification tool

Trainers

Our trainers are OpenFAIR certified and have extensive operational experience using the FAIR model to quantify risk. They are also active members of the FAIR Institute with access to a global network of more than 8.000 members. They will be happy to answer any of your questions during the course and share their experience using FAIR.

Attendance monitoring and evaluation test

Training attendance form

Satisfaction survey – training objectives achievement, quality of training content and trainers

Multiple Choice Questionnaire to assess level of preparation for the OpenFAIR Certification exam.

Course Completion Certificate

Phone number:
+33 (0)1 84 20 70 05

Website:
www.c-risk.com

Address:
Wojo - Cœur Défense - Tour A -
110 Esplanade du Gl de Gaulle
92931 Paris La Défense

Training course
Terms & Conditions

Phone number:
+33 (0)1 84 20 70 05

Website:
www.c-risk.com

Address:
Wojo - Cœur Défense - Tour A -
110 Esplanade du Gl de Gaulle
92931 Paris La Défense

Purpose and general provisions

C-Risk is a training organization specialized in quantifying cyber risk with the FAIR ™ Framework. C-risk designs, develops and provides inter-company and intra-company training, across Europe, and as either on premise or online courses.

The following definitions apply in these conditions:

- Customer: any natural or legal person who registers or orders training from C-Risk.
- Trainee: the individual participating in training.
- Inter-company training: training courses listed in the C-Risk catalogue which bring together trainees from different organisations.
- 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 training.

Registration

Registration for a course only becomes effective after receipt by C-Risk of a purchase order.

C-Risk will send by email, two weeks before the start of the training, a notice summarizing the practical details: date, location, times and access, to the contacts indicated in the registration documents. C-Risk cannot be held responsible for the non-receipt of the invitation whomever the recipient(s) may be at the client,

especially in the absence of the trainee(s). At the end of the training, an individual training certificate will be sent by post.

Billling

All prices are in euros and excluding taxes. When applicable VAT must be added at the applicable rate.

For intra-company training taking place in the premises provided by the client company, the training prices do not include the trainers' travel and accommodation costs.

For inter-company training, training prices do not include any accommodation or catering costs for the trainees.

Participation fees include: participation in training, course materials and coffee breaks.

The invoice is established on booking of the training course upon receipt of a purchase order.

Any default in payment (in whole or in part) by the client on the due date, unless a delay was requested by the client and formally granted by C-Risk, will automatically result, without any reminder being necessary and as soon as the day following the settlement date appearing on the invoice, the application of late payment penalties set at three times the legal interest rate. C-Risk may also demand the payment of the lump sum indemnity for recovery costs, in the amount of forty (40) euros, as well as, if applicable, the payment of additional compensation, upon justification.

Cancellation, absence or interruption of training

Any module started is due in full and will be invoiced to the Customer by C-Risk.

In case of absence, interruption or cancellation, C-Risk invoicing will distinguish the price corresponding to the days actually attended by the Trainee and the amounts due for the absence or interruption of training. As a reminder, the sums owed by the Customer in this respect cannot be charged by the Customer on its obligation to participate in continuing professional training or be the subject of a request for support by an OPCA (not applicable to customers outside of France). In this case, the Client agrees to settle the sums which remain payable by him directly to C-Risk.

On the other hand, in the event of cancellation of the training by the Client, C-Risk reserves the right to invoice the Client for cancellation fees calculated as follows:

- if the cancellation occurs more than 15 working days before the start of the training: no cancellation fees.
- if the cancellation occurs between 15 and 7 working days before the start of the training: the cancellation fees are equal to 50% of the pre-paid price of the training.
- if the cancellation occurs less than 7 working days before the start of the training: the cancellation fees are equal to 100% of the pre-paid price of the training.

However, when a participant cannot attend a training session for which he is registered, he can be replaced by an employee from the same company.

The name and contact details of this new participant must be confirmed in writing to C-Risk. In the absence of the trainee for a case of force majeure commonly accepted by the courts, exceptionally and after validation of the force majeure character of the situation, C-Risk accepts that the client can, within 12 months at the latest according to his absence, choose a future date for the same training.

C-Risk reserves the right to cancel or postpone training without compensation, if the number of participants is not sufficient or in case of force majeure. The client can then choose another date in the training calendar. C-Risk cannot be held liable for costs or damages resulting from the cancellation of an internship or from a postponement to a later date.

Support by an OPCA (not applicable to customers outside of France)

If the client wishes to request support from the OPCA organisation of which they depend, they must:

- make a request for support within the required time and ensure the completion of this request;
- to indicate this explicitly at the time of registration.

If the acceptance of OPCA financial support has not arrived at C-Risk at the latest one week before the start of the training, the request for subrogation cannot be taken into account by C-Risk. The customer will then have the possibility:

- either cancel or postpone the registration,

- or to produce, before the training, a proper order form by which he undertakes to pay the cost of the training to C-Risk.

Intellectuel property

Each course includes the provision of documentation for the internal use of the client. Any reproduction, modification or disclosure to third parties of all or part of the training materials or documents, in any form whatsoever, is prohibited without the prior written consent of 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 1, 2020 and subject to change without notice.

Phone number:
+33 (0)1 84 20 70 05

Website:
www.c-risk.com

Address:
Wojo - Cœur Défense - Tour A -
110 Esplanade du Gl de Gaulle
92931 Paris La Défense