Datadock

C-Risk

Training catalogue 2021

Factor Analysis of Information Risk & Cyber Risk Quantification

C-Risk

SUMMARY

Phone :
+33 (0)1 84 202 101

Website :
www.c-risk.com

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

Introduction to financial quantification of cyber risk with the FAIR TM (Factor Analysis of Information Risk) standard and method

CRQ – 01

½ day

595€ / person

Training description

To understand the basic principles of cyber risk quantification using the FAIR standard and methodology and get insights on how it could apply to an organization.

The course "Introduction to Financial Quantification of Cyber Risk with FAIR" covers the basic principles of cyber risk quantification in financial terms. It introduces the FAIR taxonomy and analysis methodology, presents the limits of current qualitative approaches and how FAIR can complement them to support risk treatment decision making and improve governance cyber security strategy.

The audience gets an overview of the main use cases and insights on the possible next steps their organization should take to adopt cyber risk quantification.

Audience

- All management functions (Finance, Audit, LoB, IT, HR, …)
- Risk Managers
- CISO and members of the Operation Security team

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

- Overview of risk and risk management definitions. Risk management objectives and limits of current qualitative risk analysis approaches.
- Overview of how the FAIR standard helps quantify cyber risk to support better decision making in cyber security strategy

At the end of the 4-hour training, participants will be able to understand the objectives of risk management, the limit of current qualitative approaches and the benefit of quantifying cyber risk in financial terms. Uses cases will provide insights on the possible next steps their organization should take to adopt cyber risk quantification.

Duration

½ day – 4 hours

Phone :
+33 (0)1 84 202 101

Website :
www.c-risk.com

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

Content

- Risk and risk management overview
  - Qualitative & Quantitative Analysis as per ISO and EBIOS
  - Cognitive biases and decision process: reducing uncertainty
  - The need for a formal model and method

- The FAIR™ standard overview
  - Ontology – study of the model and each variable and their inter-relation
  - FAIR Analysis method – 4 steps

- Use case and sample deliverables
  - High level review of a risk scenario quantification
  - Practical use cases and sample deliverables
  - Overview of main steps to consider to start adopting cyber risk quantification

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 simulation tool FAIR-U and the RiskLens SaaS platform.

Trainers

- Senior Digital Business consultants specialized in IT Security
- OpenFAIR Standard and methodology certified
- RiskLens certified

Attendance monitoring

- Training attendance form
- Satisfaction survey – training objectives, quality of training content and trainers
- Course Completion Certificate

Phone :
+33 (0)1 84 202 101

Website :
www.c-risk.com

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

Financial quantification of cyber risk with the FAIR ™ *(Factor Analysis of Information Risk)* standard and method

CRQ - 02

2 days

1850€ / person

Training description

To learn how to quantify cyber risk in financial terms using the FAIR standard and methodology.

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 the limits of qualitative methods based on nominal and ordinal scales, the cognitive biases that negatively influence Subject Matter Expert judgment and the benefits of using ratio scales. 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 PearsonVUE exam cost is not included in the course cost and some additional self-study may be required before attempting the certification.

Audience

- Risk Managers
- CISO and members of the Operation Security team
- Auditors
- Generally, anyone on the 1st, 2nd and 3rd line of defense 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.

Duration

2 days – 14 hours

Objectives

- Understand the limits of current qualitative risk analysis
- Understand decision process and decision support methods
- Understand how the FAIR standard helps quantify cyber risk to support better decision making in cyber security strategy
- Practice quantification in financial terms through a field-based use case
- Review of sample Multiple Choice Questions to prepare the OpenFAIR Certification

Phone :
+33 (0)1 84 202 101

Website :
www.c-risk.com

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

At the end of the 2 days training, participants will be able to

- scope risk scenarios,
- collect and estimate data
- iterate and interpret MonteCarlo simulation results
- Present in the context of the use case they're wanting to inform

Attendees will therefore be equipped with the fundamentals to initiate a cyber risk quantification program and improve cyber security budget justification and prioritization.

Content

- 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.
  - Study of 25 questions typical of the 80 questions that students will have to respond to obtain the OpenFAIR certification

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

Phone :
+33 (0)1 84 202 101

Website :
www.c-risk.com

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

Trainers

- Senior Digital Business consultants specialised in IT Security
- OpenFAIR Standard and methodology certified
- RiskLens certified

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 :
+33 (0)1 84 202 101

Website :
www.c-risk.com

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

Training course

Terms & Conditions

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.

Billing

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.

Phone :
+33 (0)1 84 202 101

Website :
www.c-risk.com

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

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.

Intellectual 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, 2021 and subject to change without notice.

Phone :
+33 (0)1 84 202 101

Website :
www.c-risk.com

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