# **HRDA Vital Importance:** Innovative Management of Organisational, Operational, and Technological Risk

**Programme Overview**

The programme focuses on risk management (although the more accurate term is "Hazard Management") and follows the specialised NIST methodology in conjunction with the asset-based methodology proposed by ISO 27005 and ISO 31000 standards.

The methodology addressed in this training programme is the one most widely adopted internationally for risk assessments in this category (scope and purpose), and it is fully accepted by the European Union Agency for Network and Information Security (ENISA).

This methodology has advantages over older methodologies as it: (a) it establishes solid foundations for the complex issue of risk identification, and (b) it addresses risk management holistically by incorporating parameters during its application to reduce the subjectivity inherent in every assessment.

**Learning Objectives**

After completing the programme participants will be able to:

**At the Knowledge Level**

- Describe the risk management cycle and its structural characteristics.
- Formulate and describe the pillars of the institutional framework.
- Correlate the pillars with the controls of Annex A.
- Formulate, describe, and classify their resources (assets) and the risks (through threats and vulnerabilities) of their resources.
- Categorise the organisation's resources according to the level of hazard.
- Differentiate when a threat and risk assessment is required and when it is carried out (related to the organisation's operations and its information security).
- Enumerate and describe the steps of the methodology.
- Identify the strategies and tools for risk assessment.
- Correlate the risks with protection measures (countermeasures) based on evaluative data.

**At the Skills Level**

- Document the risks faced by the organisation concerning its organisation, operations, and information security.
- Independently execute the stages (steps) of the Risk Analysis Methodology.
- Calculate the probability and impact of threats on the organisation's resources.
- Explain (to senior management) the likelihood of a risk occurring and its impact.
- Select strategies and appropriate tools for risk assessment.
- Organise and implement risk mitigation plans (countermeasures).

**At the Attitude Level**

- Counter risks through risk mitigation measures.
- Justify, both in terms of timing and methodology, the need for re-evaluating risks.
- Collaborate within the organisation for the methodological handling of threats.
- Encourage colleagues and senior management to implement risk analysis.
- Participate in identifying the appropriate risk mitigation measures.

**Training Outline**

**Introduction to Concepts and Classification of Risks**

• Conceptual Analysis (introduction) from the perspective of risk management.

• What risks lurk in organisational, operational, and technological matters?

• The risk management cycle and its structural characteristics.

**The Importance of the 93 Control Points of Annex A (Control Point, i.e., control)**

• Relevant terminology.

• The 4 thematic categories (organisation and operation – human resources – technology) related to risks and threats.

• A brief presentation of the content of each category. Are these categories sources of risk? Participatory Dialogue.

• Case study for each category.

**Methodological Risk Analysis**

- The flowchart of the Risk Assessment. Analysis and interpretation of the steps in the flowchart
- Discussion.

**Practical Application of Risk Analysis Methodology**

- Practical exercise for participants in Groups.

**Risk Mitigation Strategies and Tools**

- Strategies:
  - Avoidance
  - Transfer to a third-party
  - Reduction of probability or impact
  - Acceptance

- Case Studies on Strategies from International Experience

**Practical Application of Risk Methodology**

- Practical application of Risk Assessment Tools between 'Groups' of non-homogeneous organisations

**Identification and Selection of Protection Measures (Countermeasures)**

- Risk Mitigation by reducing probability.
- Mitigation of risk level by reducing impact.
- Practical application
- Case Study

**Risk Management**

- Developing a risk management plan.
- Case studies on determining the risk level.
- Risk level reduction plans.
- Business Continuity and its importance

**Next Steps** – Plan for the In-house Training/Advisory Session

**Training Style**

The programme is interactive in nature and participants will be actively involved, using their own experiences and challenges to reinforce and adapt the new knowledge and skills to their own reality, as well as examples, case studies, tools and simulations.

The trainer during the in-class part of the training will initiate the multifactorial approach in Risk Assessment and the participants will be involved in actual examples either in their laptops (if available) or in paper form. They will be asked to choose their own components in splitting the two factors of risk (likelihood and impact), as well as tables in those components that have quantitative characteristics. These examples will be used as basis in the In-House training that is the sequence of the in-class training.

The training sessions will combine elements of PowerPoint presentations, open discussions, case studies, audio/visual material and experiential exercises.

**In-house Training/Advisory Session**

Upon completing the 14-hour in-class training programme, participants will engage in a tailored 4-hour in-house session offering focused guidance, advice, and training to address the specific needs and challenges of both the participants and their organisation.

The in-house part of the training has a dual strategic goal that is vital for the participating businesses/organisations: an educational-consulting goal, as well as the goal of producing results for each participating entity.

The achievement of this result is accomplished through the creation of a "Management Support Tool" that is fully tailored to the needs of the entity, through an extensive and rational analysis of the hazards faced by resources and the management scenarios of organisational, operational, and technological risks that these resources face at the present time (and which the trained human resources of the entity will be able to update periodically or whenever required—as detailed in Section 2 of the foundational part).

This tool will facilitate decision-making. It is noted that the Management Support Tool will be fully developed by the end of the in-house training by the executive(s) involved, under the coaching guidance of the trainer/consultant. The development of this tool by the participating executives will not only contribute to

the development of their skills but also foster a sense of "Ownership," which will lead to lasting attitudes that are not dulled by time. In this direction, the foundational part will be fully utilised, with the broad individualised approach that will be applied, as outlined in the syllabus of the foundational part.

During the **in-house** part, the executives participating in the programme will have the opportunity to use their findings from the classroom session, to address their own specific organisational requirements.

**Participant Profile**

Where possible it is recommended that organisations participate with three (3) persons to maximise learning impact and transfer of knowledge to the workplace. An example could be, one person with organisational responsibilities, one with operational responsibilities and one with regards to Technological.

The following are required: a) good knowledge of the processes implemented within the business/organisation, and b) basic skills in handling spreadsheets (Excel or similar). Knowledge of mathematics, probability theory, or statistics is not required, as the mathematical functions that will be used will be explained. Moreover, the mathematical formulas for practical applications will be predefined.

**The programme is ideal for:**

- CEOs, CFOs, COOs, and CROs (Chief Risk Officers)
- Chief Technology Officer (CTOs) and , Information Security Officer (CIOs) interested in leveraging technology for risk management
- Directors and heads of risk management departments
- Senior managers responsible for strategic planning and decision-making
- Heads and Managers of Risk, Compliance and Internal Audit
- Health and Safety Officers
- Decision makers

**Duration**

The duration of the programme is 18 hours as follows:

- The total duration of the in-class training is 14 hours.
    - The 14-hour programme is split over two sessions of 7 hours
    - Dates: 24/06/2026 & 25/06/2026

- The total duration of the In-house Training/Advisory session is 4 hours. This session will be scheduled by mutual agreement between: 26/06/2026 – 26/10/2026.

**The Trainer**

**Kyriakos Dimitriou**

Kyriakos Dimitriou graduated the Physic-Mathematical School of the University of Patras - GR. He is accredited trainer for lifelong learning activities by the Greek Ministry of Labour and the Ministry of Education and thus he may deliver Adults' training all over EU.

Demetris has more than 30 years of field experience in areas such as Project management, Business related consulting, Risk Assessment, Case management, GDPR compliance, Evaluation and Assessment of projects or programmes, Capacity building, Market research, Curricula development, Training needs analysis, Transfer of innovation, Quality assurance, custom-made ISO Standards' Compliance development and especially the ISO 27001 Information Security Management and the ISO 22301 Business Continuity Management Standards, Consultancy Mentoring and Coaching. He has been project manager in more than 20 EU projects participating in more than 70 of those under European Initiatives such as Adapt, Leonardo da Vinci, Socrates, Youth, LLL, Grundtvig, EuropAid, Budget line, Erasmus plus, Horizon 2020, etc. Through these EU projects he has worked almost all over Europe and 3rd Countries like Ukraine and Uzbekistan as Short-Term expert.

In the fields of GDPR Compliance, ISO 27001 and ISO 22301 Certification he has supported more than 150 companies and organisations in Cyprus and Greece to achieve their goals, serving also some of these entities as Data Protection Officer (DPO).