



LEDRA
COLLEGE
NICOSIA

Information Systems Risk Management



Information Systems Risk Management



Organizations depending upon information systems to carry out their missions and business functions are challenged by serious threats that can exploit both known and unknown vulnerabilities in systems. Threats include targeted attacks, operational disruptions due to natural disasters, human and system errors, and structural failures.

This course focuses on the current Information Systems Risk Management processes and relevant best practices. In order for security staff to be effective, it is important that they have a firm understanding of risk management strategies. Such awareness would enable them to properly analyze business threats and the risks they pose, within well-known frameworks, while also being able to take countermeasures against those threats and commensurate with the level of risk they carry.

Course Aims

After the successful completion of this course, learners should be able to:

- Have an understanding of the main concepts of risk management within the context of information security.
- Have an understanding of quantitative and qualitative risk assessment approaches
- Justify the need for information risk management in the context of risk to the business.
- Develop an information risk management strategy
- Apply appropriate risk management, risk assessment and risk treatment measures
- Apply appropriate controls to manage risk commensurate with the level of risk exposure.
- Understand the Risk Management Life Cycle.

Eligible Participants

This course is targeted at all those involved in the areas of information security and assurance, including IT professionals, auditors, managers and system and network administrators

Course Duration

The total duration of this course is forty (40) hours. Upon completion of the course, successful participants will be awarded a certification approved by the HRDA.

Course Indicative Content

NO	INDICATIVE CONTENT	DURATION (HOURS)
1	<p>Concepts of Risk Management IT Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization. The aim is to provide an overview of the risk and security management iterative processes.</p>	4
2	<p>Asset Identification The assets of an organization can be tangible (computers, facilities, supplies) or intangible (reputation, data, intellectual property). Understanding the value of an asset is the first step to understanding what security measures should be put in place and what funds should go towards protecting it. The aim is to identify qualitative and quantitative measurements applied to assets of an organization. It is also presented how assets are identified, categorized, valued and used in the context of a risk management process.</p>	4
3	<p>Developing an Information Risk Management Strategy The process of developing an Information Risk Management strategy includes identifying and assessing risk, reducing it to an acceptable level and implementing the right mechanisms to maintain that level. The aim is to introduce the process and the necessary requirements for developing a risk management strategy. The steps, procedures, factors and elements involved in such a process are defined and analyzed.</p>	4
4	<p>Information Risk Management Although security is big business today, the focus is more on applications, devices, protocols, viruses and hacking. Although these items all must be considered and weighed in risk management process, they should be considered small pieces of the overall security puzzle. The aim is to present relevant risk management terms and processes, such as risk analysis, cost/benefit analysis, risk factors and risk ownership. Risk treatment options and risk handling techniques are also presented and analyzed.</p>	4
5	<p>Layers of Responsibility Each organization is different in its size, security posture requirements, and security budget. One organization may have one individual responsible for IRM or a team that works in a coordinated manner. The overall goal of the team is to ensure the company is protected in the most cost-effective manner. The aim is to introduce the different layers of responsibility in the risk management process as well as to present the different people and roles involved in such a process. Common controls and practices are also presented.</p>	4
6	<p>Threat and Vulnerability Modeling and Analysis A vulnerability is a software, hardware, procedural or human weakness that may provide an attacker an open door to the organization. A threat is any potential danger to information or systems. A risk is the likelihood of a threat agent taking advantage of a vulnerability. An exposure is an instance of being exposed to losses from a threat agent. Applying the right countermeasures, can eliminate the vulnerability and exposure and thus reduce the risk.</p>	4
7	<p>Risk Management Life Cycle It is important to understand that a security program has a life cycle that is always continuing, because it should be constantly evaluated and improved upon. Without setting up a life cycle approach to a security program and the security management that maintains that program, an organization is doomed to treat security as merely another project. The aim is to introduce the various stages of the risk management procedure, from vulnerability and threat identification, to risk treatment options and revisit policies. The iterative nature of the risk management procedure is presented and analysed.</p>	4
8	<p>Information Classification Value should be assigned to different types of data, to enable an organization to gauge the amount of funds and resources that should go towards protecting each type of data; not all data has the same value. After identifying all important information, it should be properly classified; to organize it according to its sensitivity to loss, disclosure or unavailability. The aim is to stretch the importance of recognizing what information is critical to an organisation and assigning value to it.</p>	4
9	<p>Risk Management Frameworks Risk management frameworks are a description of an organizational specific set of functional activities and associated definitions that specify the processes that will be used to manage risks. A good risk management framework should enhance and improve risk management by making it more transparent and understandable to stakeholders, by making its processes more efficient and by allowing for sharing of best practice in the implementation of risk identification, risk assessment and risk treatment.</p>	4
10	<p>Relevant International Standards The purpose of international risk management standards (such as ISO/IEC 27005) is to provide guidelines for information security risk management. They are designed to assist the satisfactory implementation of information security based on a risk management approach. These standards specify a structured, systematic and rigorous process from analysing risks to creating the risk treatment plan.</p>	4

Ταχύρυθμα επιχορηγημένα μαθήματα Αρχής Ανάπτυξης Ανθρώπινου Δυναμικού (ΑΝΑΔ) 2014

Το LEDRA COLLEGE προσφέρει ταχύρυθμα επιχορηγημένα πολυεπιχειρησιακά προγράμματα σε άτομα που επιθυμούν να εμπλουτίσουν τις γνώσεις και τα επαγγελματικά τους προσόντα.

Σημαντικές πληροφορίες & κριτήρια για τα επιχορηγημένα προγράμματα της ΑΝΑΔ

- Τα μαθήματα δικαιούνται να τα παρακολουθήσουν άτομα που εργάζονται στον ιδιωτικό τομέα, σε ημικρατικούς οργανισμούς και σε δημοτικές αρχές. Εξαιρούνται από την επιχορήγηση οι κυβερνητικοί υπάλληλοι.
- Για να δικαιούται ένα άτομο να παρακολουθήσει κάποιο από τα επιχορηγημένα προγράμματα της ΑΝΑΔ, θα πρέπει να καταβάλλει εισφορές στο Ταμείο Κοινωνικών Ασφαλίσεων
- Για κάθε πρόγραμμα υπάρχουν επιπλέον συγκεκριμένα κριτήρια εισδοχής, τα οποία αναγράφονται στον οδηγό κάθε προγράμματος.
- Το ποσοστό της επιχορήγησης διαφέρει ανάλογα με το μέγεθος της επιχείρησης/οργανισμού: Αν η επιχείρηση είναι μικρού μεγέθους (κάτω των 50 ατόμων), η επιχορήγηση ανέρχεται στο 80%, αν η επιχείρηση είναι μεσαίου μεγέθους (κάτω των 250 ατόμων), η επιχορήγηση ανέρχεται στο 70% και αν είναι μεγάλου μεγέθους (άνω των 250 ατόμων), η επιχορήγηση ανέρχεται στο 60%.
- Δεν υπάρχει περιορισμός όσο αφορά τον συνολικό αριθμό των εργοδοτούμενων που μπορεί να στείλει κάθε εταιρεία για κάθε πρόγραμμα.
- Δεν υπάρχει περιορισμός όσο αφορά τον συνολικό αριθμό των προγραμμάτων που μπορεί να παρακολουθήσει κάθε ενδιαφερόμενος.
- Όλα τα μαθήματα ξεκινούν την εβδομάδα 10-16 Φεβρουαρίου 2014



LEDRA
COLLEGE
NICOSIA