A NEW APPROACH FOR IMPLEMENTATION THE EU NIS DIRECTIVE IN ROMANIAN INSTITUTIONS – INFORMATION SECURITY MANAGER TRAINING PROGRAM

A.M. Udriou

National Institute for Research and Development in Information (ROMANIA)

Abstract

As part of the EU Cybersecurity strategy the European Commission proposed the EU Network and Information Security Directive. The NIS (Network Information Security) Directive (see EU 2016/1148) is the first piece of EU-wide cybersecurity legislation. The goal is to enhance cybersecurity across the EU. Romania has some legislation about information security and cybersecurity such as Decision no. 271/2013 for the approval of the Cyber Security Strategy of Romania and the National Action Plan on the Implementation of the National Cyber Security System published at 25 March 2013. In this context, the NIS Directive successfully complements the legislative framework in the field of cyber security.

The Information Security Manager training program represents a part of strategy to implement NIS Directive in Romanian institutions, because it is very important to institutions has a qualified human resource to implement this Directive. In this context, National Institute for Research and Development in Informatics (ICI - Bucharest) develops, through Lifelong Learning Centre, the CISO program focused on specialization in information security.

The Information Security Manager training program addresses people who design, develop and manage the security of organizational information and who have experience in areas such as Information Security Governance, Information Risk Management, Development of the information security program, Information security program management and Incident management.

The competencies obtained after graduating from the training program are:

- Establishment of strategy and management in the field of information security, harmonized with the strategy of the organization,
- Planning, designing, implementing and evaluating the information security management system based on risks and requirements
- Designing the organization’s security measures in accordance with the risk analysis of information security
- Integrate information security requirements at the organization level set out in third-party contracts and activities and so on.

The program consists of 6 training modules, with a duration of about 40 hours, with a weekly distribution, but accessible according to the student's needs. Each module contains a theoretical, interactive module that uses game-based self-learning methods, interactive phrases puzzles, and an application part with problem-solving methods based on scenarios the student needs to solve.

These training modules are:

- Module I – Information security – basic concepts
- Module II – Information security Management system (ISMS. Designing
- Module III – Risk Management
- Module IV – Designing security measures for implementing the ISMS
- Module V - Information security Management system. Implementing
- Module VI - Monitoring, evaluation, improvement of ISMS.

In the future we intend to certify this course at national level and to align with the national occupational standards on information security management system.

Keywords: Information Security Manager Training Program, NIS Directive, Lifelong Learning Center.
1 INTRODUCTION

In the context of the fourth Industrial Revolution, the exponential growth of connectivity and networking, the competencies related to the design and implementation of information security and cyber security at organizational, local or regional level are fundamental.[2]

The changes made by Industry 4.0 are, at the same time, deep and strong for each company. The interconnection of physical, digital and biological systems through cloud computing will produce major changes in all domains. Business governance will change the governance of society, and the intensity and the depth of these changes cause full transformation of production systems, management systems and last, but not least, the development of society. [3]

As much as the society becomes a knowledge society, an interdependent and a "smart" society, information and communication technologies will play an important role in ensuring the success of economic, scientific and even personal projects. The management of cyber security incidents and information security is an area whose relevance to contemporary organizations is steadily increasing with the level of professionalism required. In addition to high-level scientific and engineering skills, the labor market requires skills to understand and manage risks, workload planning, cost-benefit analysis, mixed team interaction, complex tasks. This training programme prepares qualified engineers and innovation specialists to find technical and social solutions as well as scientific research in the field. The program provides the training of highly trained specialists in a very current and important field for research in information technology, as well as for valorization of innovation in the companies involved in the development of high-complex IT products.[3]

2 METHODOLOGY

The "Information Security Manager" training programme is addressed to individuals (individuals) who design, develop and manage the security of organisational information and who have experience in areas such as information security governance; Information risk management; Development of the information security program; Management of the information security program; Incident Management.

The relationship between training modules and acquired competence is described in the following table:

<table>
<thead>
<tr>
<th>Module/Discipline</th>
<th>Acquired competence</th>
</tr>
</thead>
<tbody>
<tr>
<td>M I – Information Security</td>
<td>• Establishment of strategy and management in the field of information security, harmonized with the strategy of the organization</td>
</tr>
<tr>
<td>M II – Information security management system (ISMS)</td>
<td>• Establishment of the information security management framework</td>
</tr>
<tr>
<td></td>
<td>• Establishment of security domain and management of information resources</td>
</tr>
<tr>
<td>M III – Risk management</td>
<td>• Planning the information security management system based on risks and requirements</td>
</tr>
<tr>
<td>M IV – Design security measures</td>
<td>• Designing organizational and human security measures necessary to address information security risks</td>
</tr>
<tr>
<td></td>
<td>• Managing access to resources and information</td>
</tr>
<tr>
<td></td>
<td>• Designing security measures in operational processes</td>
</tr>
<tr>
<td></td>
<td>• Design of IT &amp; C security measures</td>
</tr>
<tr>
<td></td>
<td>• Designing the organization's security measures in accordance with the risk analysis of information security</td>
</tr>
<tr>
<td></td>
<td>• Integrate information security requirements at the organization level set out in third-party contracts and activities</td>
</tr>
<tr>
<td>M V Implement the information security management</td>
<td>• Implementation and follow-up of the action plan in the field</td>
</tr>
<tr>
<td></td>
<td>• Advising the organization's management on the information security management system</td>
</tr>
<tr>
<td></td>
<td>• Managing information security incidents to minimize their impact on business</td>
</tr>
<tr>
<td>M VI – Monitoring, Evaluation, Improvement of ISMS</td>
<td>• Evaluation of the information security management system</td>
</tr>
<tr>
<td></td>
<td>• Applying tools and methods to improve the effectiveness of the information security management system</td>
</tr>
</tbody>
</table>
The curriculum

The program consists of 6 training modules, with a duration of about 40 hours, with a weekly distribution, but accessible according to the student's needs. Each module contains a theoretical, interactive module that uses game-based self-learning methods, interactive phrases puzzles, and an application part with problem-solving methods based on scenarios the student needs to solve.

These training modules are:
- Module I – Information security – basic concepts
- Module II – Information security Management system (ISMS). Designing
- Module III – Risk Management
- Module IV – Designing security measures for implementing the ISMS
- Module V - Information security Management system. Implementing
- Module VI - Monitoring, evaluation, improvement of ISMS

MI – Information Security.

Establishing the strategy and objectives in the field of information security, harmonised with the organisation's strategy

- Information security:
  - A definition in information security management;
  - A trend in information security;
  - A general element of computer architectures;
  - A notion of cybersecurity;
  - A legislation in the field of classified information.

- Strategic management elements:
  - The components of the strategy;
  - A strategic management models and methods;
  - An understanding of the organization and context of the Organization;
  - Understanding the needs and expectations of interested parties;
  - Defining strategic objectives.

- Information Security Strategy:
  - A strategic information security context;
  - An information security governance framework;
  - A definition and provision of resources for the information security management system;
  - Leadership and commitment of leadership.

M2- Information Security Management System (ISMS).

Establishment of the Information Security management framework

- Management systems:
  - Evolution of the concept of management systems;
  - Quality management systems;
  - Relationship between different management systems;
  - ISO standards in the field of information security management systems. Presentation, Evolution. Relationship between standards;
  - EFQM Excellence Model criteria.

- Process Management:
  - The procedural approach and the systemic approach to management;
  - Description of process interlinking;
  - Process performance objectives and indicators;
  - Process analysis;
• Analysis of patterns trends.

• Defining the scope of SMSI:
  o Area and limits of SMSI;
  o Management of information assets;
  o Classification of information.

• Information Security management System:
  o ISO 27001 requirements;
  o Roles, responsibilities and authorities;
  o Organizing information security.

M3 - Risk Management.
Planning of information security management system based on risks and requirements

• Introduction to Risk management:
  o A role of risk management;
  o A context of risk management;
  o A risk management process.

• Legal and contractual information security requirements:
  o A commercial requirement;
  o A legal requirements for information security;
  o Sectoral regulatory requirements.

• Analysis and assessment of information security risks:
  o A risk assessment criteria;
  o A threat, vulnerability, risk;
  o A methodology for analysing and evaluating information security risks.

• Risk Management:
  o A selection of risk-handling options;
  o Identification of security measures for the treatment of risks;
  o A declaration of applicability;
  o A plan to treat the Rscas/compliance.

M4 - Designing security measures for implementing the ISMS.
Designing organisational and human resources security measures necessary to address information security risks.

• Access management to resources and information
• Designing security measures in operational processes
• Design of IT&C security measures
• Designing the organisation's security measures in line with the risk analysis of information security

M5 - Information security Management system. Implementing.
Integration of information security requirements established at the level of the organisation into third-party contracts and activities

• Organizational security and human resources:
  o A security organisation;
  o A security of human resources.

• Management of access to resources and information:
  o An access control
• Security measures in operational processes:
  o An integration of security requirements into operational processes;
  o A change management;
  o a project management;
  o a purchase;
  o a business continuity;
  o A specific process.
• IT&C security measures:
  o Protection of IT systems & C;
  o Recommendations ISO 27002;
  o ISO/IEC 27032 – Cyber Security Guide;
  o ISO/IEC 27033 network security.
• Physical Security:
  o a safe Zone;
  o A security of equipment
• Integration of security requirements into third party contracts and activities:
  o Security requirements in contracts with third parties;
  o Management of outsourced services.

M6 - Monitoring, evaluation, improvement of ISMS.
Implementation and follow-up of the action plan in the field of information security
• Advising the organisation’s management on the Information security management system
• Managing information security incidents to minimize their impact on business
• Defining and pursuing the action plan in the field of information security:
  o Defining the Security action plan;
  o Operational planning and control;
  o A documentation of the information security Management system.
• Incident Management:
  o Management of information security incidents;
  o ISO/IEC 27035
  o Identification, collection and retention of digital evidence; ISO/IEC 27037 standard.

Aspects of continuity management within SMSI
• Evaluation of the information security management system
• Application of tools and methods to improve the effectiveness of the information security management system
• Information security Assessment:
  o Monitoring, measurement, analysis and evaluation – requirements of the ISI/IEC 27001:2013;
  o ISO/IEC 27004 – measurement;
  o An analysis carried out by management.
• Internal Audit:
  o An audit requirements for the information management system
• Management of improvement actions:
  o Continuous improvement of SMSI
Evaluation modalities

1 Initial assessment (if applicable)
- Where appropriate, a grid test and an in-kind sample shall be applied in which the knowledge acquired in formal or informal ways in the field of personal data protection will be tested.
- If this is not the case, the training sessions will be elaborated so as to meet the needs of the participants with different experiences and knowledge, in compliance with the conditions for the competences and skills necessary for access to the program.
- An application form will be completed, part of the participant's dossier, which will contain the information necessary to adapt the training program to the needs and expertise of the participants, without constituting an assessment or selection criterion.

2 Evaluation along the way (may be presented separately for theoretical and practical training, respectively on modules/disciplines/learning sequences)
- Frequency
  - Grid tests and open questions of partial evaluation for each module – to assess the level of knowledge fixation;
- Methods – Tools
  - written tests of the grid test, reflection themes, open questions for theoretical preparation testing;
  - instruction, systematic observation in solving applications on the training platform for the assessment of practical training;
- Appreciation Scale
  - the partial evaluations will be denoted on a scale of 1 to 10 (where 1 is the minimum note and 10 the maximum).

3 Final assessment (to be presented separately on samples – written, oral, practical – if applicable)
- Methods – Tools
  - written test sample of the grid for theoretical preparation testing;
  - The project for the evaluation of practical training (elaboration and presentation);
- Appreciation Scale
  - Final evaluations for theoretical and practical evidence will be noted on a scale of 1 to 10 (Minimum note 6 required to promote theoretical proof and minimum note 7 for the promotion of practical proof).

3 RESULTS

As a result, from our clients, we have a positive feedback through the training program they understanding the importance of information security. Until now, we have two series of students. Each student has a folder with curriculum, electronic content of theoretical course, exercises and subjects for exam.

Two months ago, we started the accreditation of the course at the Ministry of Labor. We developed the accreditation folder that contains the documents necessary for the authorization of the specialized training according to the occupational standard. This folder entered in a complex accreditation process, resulting in the authorization required for national recognition. Thus, we completed the certification process of this training program at national level and to align with the national occupational standards on information security management system.

ACKNOWLEDGEMENTS

This work was supported by a grant on the Ministry of Innovation and Research, UEFISCDI, project number 8SOL/2018 within PNCDIII, project code: PN-III-P2-2.1-SOL-2017-09-0102, project name Information Integrated System for Management of Activities (IISMA).
REFERENCES

