Deliverable 3.1

Cross-matching of organizations with EU standards

European Commission Tempus Project:

544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES

This project has been funded with support from the European Commission.
This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of content

1. Introduction

The purpose of the ECESM Project is to pave the way for the complex process that will turn Montenegro into a cyber secure nation. Along this line, WP2 was conceived to increase the cyber security awareness of Montenegrin citizens at all levels. However, we still need to identify proper instruments to fully secure, protect, and defend the Montenegrin information systems from all types of cyber threats. To this end, it is fundamental to concurrently address two main goals: (i) the development of an advanced ICT infrastructure, and (ii) the formation of an agile, highly skilled professional cyber security workforce. WP3 was designed exactly to trace the path for the improvement of the cyber security knowledge maturity of the governmental, public and private Montenegrin institutions.

ICT related organizations demand a globally competitive, up-to-date cyber security workforce, able to foresee and prevent cyber risks (when possible), and to promptly tackle ongoing cyber attacks. The process of educating a national cyber security workforce consists in three main complementary components: workforce planning, professional development, and identification of core professional competencies.

Workforce planning means to analyse the functional capabilities needed to achieve the current mission, forecast future capabilities, and identify specific knowledge, skills, and abilities for cyber security professionals. Professional development incorporates formal training and education to maintain the technical health of the cyber security workforce. Professionalization of cyber security identifies core occupational competencies, sets objective standards for skills development, accreditation, and job performance of cyber security practitioners, and develops career ladders within the various cyber security disciplines.

All the aforementioned activities need to be performed in accordance with EU recognized best-practices and principles. For this reason, the first step is a careful cross-matching of the current scenario of Montenegrin organizations with respect to EU standards and guidelines for cyber security enforcement. This report summarizes the joint work of staff from the Montenegrin institutions involved in the project and of representatives from the EU partners, to explore the deficiencies of Montenegrin organizations in order to schedule training activities and produce recommendations for implementation of well-defined corrective actions.

Unfortunately, assessing the responsiveness of organizations to cyber threats, and the general cyber security competence of their staff, is a very hard task. This is mainly due to two factors: on the one hand, the general reluctance of most companies to share supposedly confidential information; on the other hand, the likely discrepancy between claims and facts. Nevertheless, based on a detailed analysis of EU standards, to assess the current situation of Montenegrin organizations we decided to organize a survey of the practical countermeasures to cyber risks implemented in Montenegro and of the training of Montenegrin employees. The analysis of EU cyber security standards, together with the expertise of EU partners, was also the stepping stone to identify relevant training topics. Collecting the interest that Montenegrin organizations exhibit with respect to such topics, we argue to gain additional information about their need for specific education in the field. More specifically, we proceeded in the following way:

- We collected EU standards, guidelines and best-practices for cyber security in public and private organizations, discussed them and pinpointed the aspects of cyber security enforcement that emerge as the most important ones.
- We consequently identified a set of cyber security requirements for organizations and their staff to meet EU standards.
- Based on such requirements, we elaborated a cyber security questionnaire and a set of fundamental cyber security training topics.

- We contacted all main Montenegrin public and private organizations to collect their answers to the questionnaire and to measure their interest for all identified training topics.
- Based on the responses received from such organizations, we assessed the needs of Montenegrin institutions and companies compared to EU standards.

Summing up, we were able to analyze existing level of cyber security knowledge (focusing on specialized knowledge related to work position) in Montenegrin governmental, public and private organizations through inquiries for employers within different works and positions, and to cross-match the results with European standards and practices, using the results to define realistic needs and basic structure of the future sustainable framework.

2. EU standards for cyber security in public and private organizations

“Standards play a key role in improving cyber defense and cyber security across different geographical regions and communities. Standardizing processes and procedures is also essential to achieve effective cooperation in cross-border and cross-community environments”[1].

The main purpose of this section is to provide an overview of the referential standards for cyber security in EU public and private organizations. However, it is fundamental to understand that standards are not the solutions. Standards provide a series of guideline that could support the organizations to structure, to measure and to improve their level of preparedness and response. For this reason, it is of primary importance to understand how to translate standards into operational instructions. Based on the identified standards and guidelines, we will therefore point out a set of cyber security requirements for organizations and their staff, and consequently delineate a list of relevant cyber security training topics.

2.1. EU standards, guidelines and best-practices

The European Union has not yet adopted specific standards for cyber security, but it has recognized their importance, as certified by the emergence of several standard development organizations over the last ten years. Cyber security related laws and standards vary significantly in different EU countries: UK, Germany and Estonia are examples of countries with strong cyber security legal frameworks, but not all countries are as much careful when it comes to providing clear rules, guidelines and best-practices. For this reason, the work performed by bodies such as the Cybersecurity Coordination Group (CSCG), the EU Network and Information Security Agency (ENISA), the European Telecommunications Standards Institute (ETSI) and the CEN-CENELEC (European Committe for Standardisation and members of the National Electrotechnical Committees of European Countries) is extremely important.

[1] “Best Practices in Computer Network Defense: Incident Detection and Response”, M.E. Hathaway (Ed.), Steve Purser, ENISA, pag. 97, IOS Press 2014

The standards and recommendations created and used in EU vary widely in their focus, from highly technical interoperability standards to generic organizational standards and strategies. A good general recommendation is to adopt mid-level (*i.e.*, not purely technical and not purely strategic/organisational) standards, such as the IT Baseline Protection Manual (IT-Grundschutz) used by the German BSI[2] (Federal Office for Information Security). A similar approach is also used, for instance, by the main Estonian practical cyber security standardization framework, called ISKE.

In this following, we will provide a list of standard development organizations and a series of standards that companies could take in consideration to improve their cyber security.

2.1.1. BSI

BSI standards are publicly available both in German, English and Swedish. Several EU countries have developed their own modifications of BSI standards, like Estonian ISKE.

Citing from the BSI web page: "The BSI Standards contain recommendations by the Federal Office for Information Security (BSI) on methods, processes, procedures, approaches and measures relating to information security. For this the BSI addresses issues that are of fundamental importance for information security in public authorities and companies and for which appropriate, practical, national or international approaches have been established.

On the one hand, BSI Standards are used to provide technical support to users of information technology. Public agencies and companies can use the BSI recommendations and adapt them to their own needs. This facilitates the secure use of information technology as trusted methods, processes or procedures are used. Manufacturers of information technology or service providers can also dispose of the BSI recommendations to make their products more secure.

On the other hand, BSI Standards are also used to depict proven approaches to co-operation. BSI Standards can be quoted, and this will contribute to establishing uniform specialist terms."

The BSI standards are organized upon three main layers[3]:

1. BSI Standard 100-1 defines the general requirements for an ISMS. It is completely compatible with ISO Standard 27001 and moreover takes the recommendations in ISO Standards of the ISO 2700x family into consideration.
2. BSI-Standard 100-2: IT-Grundschutz Methodology progressively describes (step by step) how information security management can be set up and operated in practice.
3. BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz contain standard security safeguards required in the organisational, personnel, infrastructure and technical areas that are generally appropriate for normal security requirements and to protect typical information domains.

More details can be found in the chapter IT-Grundschutz International[4].

[2] https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html

[3] https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html

2.1.2. International Organization for Standardization

The International Organization for Standardization (ISO), established in 1947, is a non-governmental international body that collaborates with the International Electrotechnical Commission (IEC) 3 and the International Telecommunication Union (ITU) 4 on information and communications technology (ICT) standards 5 . The following are commonly referenced ISO security standards:

ISO/IEC 27001:2005 (Information Security Management System Requirements):

The international standard ISO/IEC 27001:2005 has its roots in the technical content derived from BSI standard BS7799 Part 2:2002. It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) within an organization. It is designed to ensure the selection of adequate and proportionate security controls to protect information assets9. This standard is usually applicable to all types of organizations, including business enterprises, government agencies, and so on. The standard introduces a cyclic model known as the "Plan-Do-Check-Act" (PDCA) model that aims to establish, implement, monitor and improve the effectiveness of an organization's ISMS. The PDCA cycle has these four phases:

a) "Plan" phase – establishing the ISMS

b) "Do" phase – implementing and operating the ISMS

c) "Check" phase – monitoring and reviewing the ISMS

d) "Act" phase – maintaining and improving the ISMS

Often, ISO/IEC 27001:2005 is implemented together with ISO/IEC 27002:2005. ISO/IEC 27001 defines the requirements for ISMS, and uses ISO/IEC 27002 to outline the most suitable information security controls within the ISMS10. ISO/IEC 27002 is a code of practice that provides suggested controls that an organization can adopt to address information security risks. These controls are not mandatory. There is therefore no certification for ISO/IEC 27002, but a company can be certified compliant with ISO/IEC 27001 if the management process follows the ISMS standard. There is a list of accredited certification bodies that can certify an organisation against the ISMS standard, which is maintained on the UK Accreditation Service website

ISO/IEC 27002:2005 (Code of Practice for Information Security Management): (replaced ISO/IEC 17799:2005 in April 2007)

This is an international standard that originated from the BS7799-1, one that was originally laid down by the British Standards Institute (BSI). ISO/IEC 27002:2005 refers to a code of practice for information security management, and is intended as a common basis and practical guideline for developing organizational security standards and effective management practices. This standard contains guidelines and best practices recommendations for these 10 security domains: (a) security policy; (b) organization of information security; (c) asset management; (d) human resources security; (e) physical and environmental security; (f) communications and operations management; (g) access control; (h) information systems acquisition, development and maintenance; (i) information security incident management; (j) business continuity management; and (k) compliance. Among these 10 security domains, a total of 39 control objectives and hundreds of best-practice information security control measures are recommended for organizations to satisfy the control objectives and protect information assets against threats to confidentiality, integrity and availability.

ISO/IEC 15408 (Evaluation Criteria for IT Security):

The international standard ISO/IEC 15408 is commonly known as the “Common Criteria” (CC)12. It consists of three parts: ISO/IEC 15408-1:2005 (introduction and general model), ISO/IEC 15408-2:2005 (security functional requirements) and ISO/IEC 15408-3:2005 (security assurance requirements). This standard helps evaluate, validate, and certify the security assurance of a technology product against a number of factors, such as the security functional requirements specified in the standard. Hardware and software can be evaluated against CC requirements in accredited testing laboratories to certify the exact EAL (Evaluation Assurance Level) the product or system can attain. There are 7 EALs: EAL1 - Functionally tested, EAL2 - Structurally tested, EAL3 - Methodically tested and checked, EAL4 - Methodically designed, tested and reviewed, EAL5 - Semi-formally designed and tested, EAL6 - Semi-formally verified, designed and tested, and EAL7 - Formally verified, designed and tested. A list of accredited laboratories as well as a list of evaluated products can be found on the Common Criteria portal13. The list of products validated in the USA can be found on web-site of the Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS).

ISO/IEC 13335 (IT Security Management):

ISO/IEC 13335 was initially a Technical Report (TR) before becoming a full ISO/IEC standard. It consists of a series of guidelines for technical security control measures:

a) ISO/IEC 13335-1:2004 documents the concepts and models for information and communications technology security management.

b) ISO/IEC TR 13335-3:1998 documents the techniques for the management of IT security. This is under review and may be superseded by ISO/IEC 27005.

c) ISO/IEC TR 13335-4:2000 covers the selection of safeguards (i.e. technical security controls). This is under review and may be superseded by ISO/IEC 27005.

d) ISO/IEC TR 13335-5:2001 covers management guidance on network security. This is also under review, and may be merged into ISO/IEC 18028-1, and ISO/IEC 27033

2.1.3. National Institute of Standards and Technology

Founded in 1901, NIST is a non-regulatory U.S. federal agency within the Department of Commerce. NIST promotes U.S. innovation and develop standards in several fields included information security. The NIST developed a series of standards, some of them are technical standards dealing with particular IT infrastructures. Here below a couple of standards, that have a wider perimeter:

NIST SP 800-39:

Managing Information Security Risk, defines risk management as "the program and supporting processes to manage information security risk to organizational operations (including mission, functions, and reputation), organizational assets, individuals, other organizations, and the Nations". To integrate the risk management process throughout an organization and to address its mission and business concerns, a three-tiered approach is employed. The process is carried out across three tiers with the objective of continuous improvement in the organization's risk-related activities, with effective communication among tiers and stakeholders. Figure 1 illustrates the three-tiered approach to risk management.

NIST SP 800-53, August 2009, – "Security and Privacy Controls for Federal Information Systems and Organizations,":

NIST Special Publication 800-53 is part of the Special Publication 800-series that reports on the Information Technology Laboratory's (ITL) research, guidelines, and outreach efforts in information system security, and on ITL's activity with industry, government, and academic organizations. Specifically, NIST Special Publication 800-53 covers the steps in the Risk Management Framework that address security control selection for federal information systems in accordance with the security requirements in Federal Information Processing Standard (FIPS) 200. This includes selecting an initial set of baseline security controls based on a FIPS 199 worst-case impact analysis, tailoring the baseline security controls, and supplementing the security controls based on an organizational assessment of risk.[3] The security rules cover 17 areas including access control, incident response, business continuity, and disaster recoverability

2.1.4. ISACA

With 95,000 constituents in 160 countries, ISACA (www.isaca.org) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the non-profit, independent ISACA hosts international conferences, publishes the ISACA® Journal, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests. IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in

Risk and Information Systems ControlTM (CRISCTM) designations. ISACA continually updates COBIT®, which helps IT professionals and enterprise leaders fulfil their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

COBIT 5:

A Business Framework for the Governance and Management of Enterprise IT: COBIT 5 is a comprehensive framework of globally accepted principles, practices, analytical tools and models that can help any enterprise effectively address critical business issues related to the governance and management of information and technology.

2.1.5. Information Security Forum

The ISF is the world's leading authority on information risk management. A not-for-profit organisation, we supply authoritative opinion and guidance on all aspects of information security. We deliver practical solutions to overcome the wide-ranging security challenges that impact business information today. ISF Members have unlimited access to a library of reports about information security issues, along with powerful web-based solutions for security assessment, benchmarking and risk management. We also provide Member organisations with the opportunity to connect with other Members, so they can share, discuss and resolve the key information security issues facing their businesses.

The 2014 Standard of Good Practice for Information Security:

Updated annually, the Standard of Good Practice for Information Security (the Standard) is the most comprehensive information security standard in the world, providing more coverage of topics than ISO. It covers the complete spectrum of information security arrangements that need to be made to keep the business risks associated with information systems within acceptable limits, and presents good practice in practical, clear statements.

2.1.6. SANS Institute

The SANS Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. A range of individuals from auditors and network administrators, to chief information security officers are sharing the lessons they learn and are jointly finding solutions to the challenges they face. At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community. SANS is the most trusted and by far the largest source for information security training and security certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - the Internet Storm Center.

Critical Security Controls for Effective Cyber Defense:

Over the years, many security standards and requirements frameworks have been developed in attempts to address risks to enterprise systems and the critical data in them. However, most of these efforts have essentially become exercises in reporting on compliance and have actually diverted security program resources from the constantly evolving attacks that must be addressed. In 2008, this was recognized as a serious problem by the U.S. National Security Agency (NSA), and they began an effort that took an "offense must inform defense" approach to prioritizing a list of the controls that would have the greatest impact in improving risk posture against real-world threats. A consortium of U.S. and international agencies quickly grew, and was joined by experts from private industry and around the globe. Ultimately, recommendations for what became the Critical Security Controls (the Controls) were coordinated through the SANS Institute. In 2013, the stewardship and sustainment of the Controls was transferred to the Council on Cyber Security (the Council), an independent, global non-profit entity committed to a secure and open Internet. The Critical Security Controls focuses first on prioritizing security functions that are effective against the latest Advanced Targeted Threats, with a strong emphasis on "What Works" - security controls where products, processes, architectures and services are in use that have demonstrated real world effectiveness.

The standards above are only a part of the standards developed for the information security. As cited before, the standards are only guideline that an organization could or should choose depending on the business sector in which it operates. There are specific standards for specific sector, for example, standards of the Institute of Electrical and Electronics Engineers and the Payment Card Industry Data Security Standard. Moreover, there are other standards not strictly connected with cyber/information security but useful to manage it inside a company. Some of these standards are ISO 31000 on Risk Management or ISO 22301 on Business Continuity Management.

2.2. Cyber security requirements for organizations and their staff

On the basis of the standards, and considering the evaluation done by all partners of the ECESM consortium, it is fundamental to provide information security basis to the staff of all main Montenegrin organizations. The idea is to create a common layer of knowledge that could help organizations and staff to cooperate together and to share information inside and outside companies.

Our general recommendation is to use German BSI standards for organisations and their staff, starting with the introductory BSI-Standard 100-1[5] and continuing deeper from there. Citing the BSI-Standard 100-2[6]:

"(...) the IT-Grundschutz Catalogues describe how to create and monitor security concepts based on standard security safeguards. Suitable bundles ('modules') of standard security safeguards are available for common processes, applications, and components used in information technology. These modules are classified into five different layers according to their focus:

- **Layer 1** covers all generic information security issues. These include the human resources, data backup concept, and outsourcing modules.

[5] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile

[6] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile

- **Layer 2** covers the technical issues related to building construction. Examples include the modules for buildings, server rooms, and home offices.
- **Layer 3** covers individual IT systems. Examples include the general client, general server, telecommunication system, laptop, and mobile telephone modules.
- **Layer 4** concerns the issues relating to networking IT systems. Examples include the heterogeneous networks, WLAN, VoIP, network management, and system management modules.
- Finally, **Layer 5** deals with the actual applications. Examples include the e-mail, web server, and database modules.

Based on the aforementioned layers, we identify the following requirements for staff of Montenegrin public and private organizations:

- **Information security management system and its main process through the ISO/IEC 27001:2013:** it's important to have a framework the staff can implement to organize the activities. The standards are helpful in providing a good guideline.
- **Cyber security risk management:** it provides the decisional core. The risk management allows staff to prioritize the interventions, the investments on countermeasures depending on vulnerabilities, threats and impacts.
- **Network security:** it provides the knowledge of the activities design to protect the usability, reliability, integrity and safety of the network.
- **Incident handling:** it concerns the activities of response to an attack. "An organized and careful reaction to an incident can mean the difference between complete recovery and total disaster"[7].
- **Network forensics:** it provides the instruments to analyze the events happened in a network. It allows to investigate and obtain information useful to understand the causes of an event.
- **Cyber Security Awareness:** It is essential the commitment of all company's employees and managers. Most of the incidents happens caused by lack of awareness

2.3. Cyber security questionnaire

Based on the latter analysis of Cyber security requirements for organizations and their staff, we designed a cyber security questionnaire to be submitted to representatives of all main Montenegrin public and private companies. The questionnaire, other than being an important self-assessment instruments for these companies, is a powerful instrument for the Consortium to establish the current status of Montenegrin organizations with respect to several aspects related to the prevention of and response to cyber security threats.

The questionnaire is organized around four main pillars:

1. *Governance, leadership and management* – The goal of this part of the questionnaire is to establish whether administrative aspects of cyber security, like budget planning and responsibility assignment, are correctly implemented

[7] http://www.symantec.com/connect/articles/introduction-incident-handling

2. *Identify* – This part of the questionnaire deals with understanding whether organizations assign the correct importance to cyber threats, ant to risk and vulnerabilities assessment
3. *Protect* – This is the part of the questionnaire responsible of assessing the capability of an organization to sufficiently protect its assets from cyber attacks, encompassing both technical solutions and a proper training of its employees
4. *Detect, respond and recover* – Finally, this part of the questionnaire is focused on the implementation of proper instruments to detect cyber security breaches, to promptly respond to cyber attacks and to restore normal and secure system activities

For the sake of readability, the questionnaire is reported in the Appendix, together with the answers collected, that are analysed and discussed in Section 3.

2.4. Relevant cyber security training topics

While the topics for training should adhere to the cyber security standards and guidelines recommended in the previous sections, the aforementioned documents focus mostly on management issues and are meant to be complementary to technological steps and technological education.

Traditional cyber security topics are suitable for most enterprises, but several organizations, due to their large workforce or to the critical assets they handle, would significantly benefit from having at least part of their employees attending basic training in more advanced topics. In particular, we envisage intensive study programs specifically targeted for state agencies, police, prosecutors and courts, banks and financial institutions, and IT and telecommunication companies. Cyber security training should therefore be layered into core studies (that all staff is expected to take) and special studies, that comprehend, for instance, network security, access-control, and IT forensics.

Core studies should cover topics related to:

- Principles and standards for cyber security
- Main strategies and operational aspects of cyber security
- Introduction to network technologies
- Introduction to malware

Special studies should cover both administrative topics and specialized/ technical ones, like:

- Organizational theory and psychology
- Information and cyber security assurance in organisations
- Information systems attacks and defence
- Computer network security
- Data mining and network analysis
- Principles of secure software design
- Network protocol design
- Advanced network technologies

- Cyber defence monitoring solutions
- Simulation of attacks and defense
- Cryptology and cryptography

Unfortunately, completing a thorough training path in the aforementioned topics is well beyond the scope of this project. In order to give a complete overview of the most important topics related to cyber security, the consortium has listed a series of courses that will touch the main areas relevant to understand and develop a valid action plan on cyber security. Along the line delineated before, the topics start from an overview of "what it means cyber security" and the security threats that should be faced until descriptions of first responder and network forensics activities. Another relevant topic is the cyber security awareness for employees that are involved in other business areas.

The topics are listed below with a brief description:

- **Security Threats on the Web:** The course covers the topics of threats an employee is facing on the web and adequate protection measures. The course is oriented and the non-professional ICT user, who uses the web at work.
- **Introduction to Cyber Security at a glance:** The Cisco Networking Academy® Introduction to Cyber security course covers trends in cyber security and career opportunities available in this field. This course introduces students to a variety of networking professionals who discuss the exciting and growing industry of cyber security.
- **Web Security:** The course covers the topics of web security from the providers / developers perspective and it is intended for the ICT professional. It covers the principles of web security and attacks scenarios and countermeasures.
- **Information security Standards:** In the society interconnected characterized by interoperability, global connectivity and communications, organizations requires common approaches for information security. This course aims to provide an overview of the main information security standards internationally adopted and in particular standards of 27000's family. These standards provide a globally recognized framework for information security management system needed to guarantee an effective and efficient control of all the activities related to the information security. The duration of this course is one day.
- **Cyber Security Risks and Resilience:** This course introduces a variety of cybersecurity information and practices, and explain why it is important, and introduce some of the products and processes used to secure data.
- **Introduction to network security:** This course will last one day and will survey main network protocols and architectures. It will then discuss most relevant attack types and vectors. Protection and prevention mechanisms as well as Best Practices will be introduced and discussed.
- **Access Control:** To design a secure information system, it is fundamental to enforce access control mechanisms, able to protect resources against unauthorized viewing, tampering or destruction. This course will provide an overview of the main models, techniques, processes, and policies related to users authentication and access control.
- **First responder intro to Internet:** introduction to network, internet and IP addresses (where to get IP address related data, how actionable it is; internet functions and governance).

- **Introduction to network forensic:** overview of network forensic and file carving with introduction of tools and methodology (Analysis methodologies acquiring of data; flow analysis practical example, etc. etc.).

3. Cross-matching with Montenegrin organizations

3.1. Current scenario of Montenegrin public and private organizations

Report answers to the questionnaire and interest scores collected for the proposed list of training topics (or courses) - ME partners

3.2. Cross-matching Montenegrin organizations with EU standards

Discuss the report of Section 3.1. to compare ME organizations needs with EU standards – ME partners

4. Conclusions

Appendix

GOVERNANCE, LEADERSHIP & MANAGEMENT			
1	**Has your cyber security strategy been approved by the board?**	**Answer**	**Comments and explanations**
1.a	Yes		
1.b	No, but it is being submitted for approaval		
1.c	No		
2	**Did your organization align the cyber security roles to the strategy? (you MUST select 2.c if you selected 1.c)**	**Answer**	**Comments and explanations**
2.a	Yes		
2.b	No, but this is in progress and will be aligned within this year		
2.c	No, it is assumed that existing cyber security roles are sufficient		
3	**Who is in charge for the risk management process?**	**Answer**	**Comments and explanations**
3.a	Chief security Officer		
3.b	Chief Information Security Officer		
3.c	Enterprise Risk Manager		
3.d	Other (specify)		
4	**Are cyber security issues brought to the attention of the CEO?**	**Answer**	**Comments and explanations**
4.a	Weekly		
4.b	Monthly		
4.c	Yearly		
4.d	Only in case of an incident/accident impacting also external stakeholders		
4.e	Never		

5	**What is the (approximate) budget spent by your organization for cyber security?**	**Answer**	**Comments and explanations**
5.a	< 1.000.000 Euro		
5.b	1.000.000 - 5.000.000		
5.c	5.000.000 - 10.000.000		
5.d	> 10.000.000		
5.e	It is not possible to evaluate it because we do not have specific budget headings for cyber security		
5.f	It is difficult to evaluate it because the budget for cyber security is spread in several Departments		
6	**What fraction of your cyber security budget is dedicated to IT solutions?**	**Answer**	**Comments and explanations**
6.a	< 30%		
6.b	30% - 50%		
6.c	50% - 70%		
6.d	> 70%		
6.e	It is not possbile to establish it		
7	**Which of the following actions do you consider most urgent for the Government to enforce cyber security?**	**Answer**	**Comments and explanations**
7.a	Strengthen awareness campaigns for citizens		
7.b	Improve monitoring systems		
7.c	Strengthen collaboration for threat and vulnerability analysis		
7.d	Release of cyber security policies and regulations at National and International level		
7.e	Strengthen collaboration at International level between Judicial Authority to speed up the contrast to cyber crime		

IDENTIFY			
8	**Do you adopt a specific cyber security taxonomy?**	**Answer**	**Comments and explanations**
8.a	Yes, a taxonomy defined by the organization		
8.b	Yes a National Standard Taxonomy (Please specify which one)		
8.c	Yes, an International Standard (Please specify which one)		
8.d	No, we don't adopt any taxonomy		
8.e	Other (specify)		
9	**Are effective risk management practices in place to address cyber security risks?**	**Answer**	**Comments and explanations**
9.a	Yes, these are well documented, and effectiveness is regularly included in management information reporting		
9.b	Yes, these are well documented, but effectiveness is not measured, nor reported or challenged		
9.c	Not specifically, but existing operational risk practices have been deemed appropriate and it is assumed that they are implemented effectively		
9.d	No, it is assumed that existing practices are sufficient		
10	**Do you have a process to identify your organisation's critical functions and processes? If yes, describe it briefly**	**Answer**	**Comments and explanations**
10.a	Yes, and this is annually verified		
10.b	Yes, this activity has been undertaken but it is not considered a routine, repeatable process		
10.c	No		
11	**Are hardware and software vulnerabilities identified, documented and remediated?**	**Answer**	**Comments and explanations**
11.a	Yes, and there is an established process for prioritisation of critical vulnerabilities		
11.b	Yes, but no prioritisation process is implemented		
11.c	No, vulnerabilities are remediated on an ad□hoc basis		

12	What are the parameters to calculate the impact of a cyber attack/incident in your oompany? (Multiple answers possible)	Answer	Comments and explanations
12.a	Service time disruption		
12.b	Direct economic loss		
12.c	Data/information loss		
12.d	Brand image loss		
12.e	Customers loss		
12.f	Recovery time		
12.g	Penalties on commercial agreement		
12.h	Legal costs		
12.i	There is no methodology to estimate the impact		
12.j	Other (Specify)		
13	**Are the above parameters translated into a corresponding economic value?**	**Answer**	**Comments and explanations**
13.a	Yes, always		
13.b	Yes in general, but it is not always possible to estimate it		
13.c	Yes, but only at the incident/attack closure		
13.d	No		
13.e	Other (Specify)		

14	**Which of the following correctly describe your cyber risk management methodology? (Multiple answers possible)**	**Answer**	**Comments and explanations**
14.a	It includes a quantitative methodology		
14.b	It includes a qualitative methodology		
14.c	It includes a methodology integrated with enterprise risk management		
14.d	It is a yearly formal process		
14.e	It is a yearly formal process and it is activated if any parameters change during the year (assets, services, …)		
14.f	It is a process that involves more departments		
14.g	The results of this process are communicated also to the Board of Directors		
14.h	It allows to prioritize the investments for the countermeasures		
14.i	It takes in consideration also the risk transfer to an insurance policy		
14.j	Other (specify)		
15	**Does your organization assume that cyber security countermeasures can impact on any of the following? (Multiple answers possible)**	**Answer**	**Comments and explanations**
15.a	Limitation in sharing results of Research and Development activities		
15.b	Outsourcing of activities to external companies		
15.c	Slow-down of production activities		
15.d	Other (specify)		
16	**Which kind of cyber attacks is your organization more afraid of?**	**Answer**	**Comments and explanations**
16.a	DOS		
16.b	Advanced Persistent Threat		
16.c	Attacks against Industrial Control System		
16.d	Phishing		
16.e	Other (Specify)		

PROTECT			
17	**Do you have a structured education and training cyber security programme for all employees?**	**Answer**	**Comments and explanations**
17.a	Yes, and management information is collected on completion of training		
17.b	Yes, training is made available to all staff, but no management information is collected		
17.c	No, training is ad hoc		
18	**Do you have an advanced structured education and training cyber security programme for the employees specifically involved in cyber security activities?**	**Answer**	**Comments and explanations**
18.a	Yes, and management information is collected on completion of training		
18.b	Yes, training is made available to all staff, but no management information is collected		
18.c	No, training is ad hoc		
19	**Which of the following best-practices related to the use of systems and equipments are your employees explicitly trained to follow? (Multiple answers possible)**		
19.a	Comply with a specific home-working policy		
19.b	Protect data both in transit and at rest		
19.c	Use a strong password and/or change the password periodically		
19.d	Comply with a specific policy for mobile and removable computer media		
19.e	Scan for malware before allowing connections to the systems		
19.f	Other (Specify)		
20	**Is there any specific requirement related to cyber security for SMEs working for your organization?**	**Answer**	**Comments and explanations**
20.a	Yes, ISO 27001 is required		
20.b	Yes, on the basis of the activities to be performed, it shall have specific security certifications		
20.c	No, it is assumed that they implement sufficient solutions		
20.d	They are included in our risk assessment and we support them to apply the proper countermeasures		
20.e	Other (Specify)		

21	Which of the following countermeasures are implemented within your organization to guarantee information security? (More answers possible)	Answer	Comments and explanations
21.a	A set of policies related to the use of digital devices and to data protection		
21.b	Awareness campaigns for employees		
21.c	Standards and certifications (*i.e.*, ISO27001)		
21.d	Disaster recovery plans		
21.e	Cyber threat intelligence analysis center		
21.f	Endpoint protections (*i.e.*, antivirus)		
21.g	Security Operation Center		
21.h	Computer Emergency Response Team		
21.i	Other (Specify)		
22	**For the implemented countermeasures, have you defined clear indicators to determine their effectiveness?**	**Answer**	**Comments and explanations**
22.a	Yes		
22.b	Only for some of them		
22.c	No		
22.d	Other (Specify)		
23	**Which of the following is considered by your organization the main systemic problem related to cyber crime?**	**Answer**	**Comments and explanations**
23.a	Service disruption		
23.b	Loss of trust in digital services and devices		
23.c	Economic losses		
24	**Are effective physical access controls implemented, maintained and monitored across your organisation's facilities?**	**Answer**	**Comments and explanations**
24.a	Yes, and these are reviewed on an regular basis		
24.b	Yes, there are controls in place, but there is no routine review process		
24.c	There are some, but I can not be sure that they are implemented across the organisation		
24.d	No		

25	Are effective remote access controls implemented, maintained and monitored across your organisation's facilities?	Answer	Comments and explanations
25.a	Yes, and these are reviewed on an regular basis		
25.b	Yes, there are controls in place, but there is no routine review process		
25.c	There are some, but I can not be sure that they are implemented across the organisation		
25.d	No		
26	**Are effective privileged user access rights implemented, maintained and monitored across your organisation's facilities?**	**Answer**	**Comments and explanations**
26.a	Yes, and these are reviewed on an regular basis		
26.b	Yes, there are controls in place, but there is no routine review process		
26.c	There are some, but I can not be sure that they are implemented across the organisation		
26.d	No		
27	**Which of the following best describes your data leakage prevention strategy?**	**Answer**	**Comments and explanations**
27.a	All data is encrypted at rest		
27.b	All data considered critical is encrypted at rest		
27.c	No data is encrypted at rest		
28	**Which of the following best describes your data back-up process?**	**Answer**	**Comments and explanations**
28.a	All data is backed up, single format		
28.b	All data is backed up, multiple formats		
28.c	Critical data is backed up, multiple formats		
28.d	Some data is backed up, single format		
28.e	No data is backed up		

	DETECT, RESPOND & RECOVER		
29	**Have you produced and maintained a baseline of network operations and expected data flows?**	**Answer**	**Comments and explanations**
29.a	Yes, and this is annually reviewed and verified		
29.b	Yes, we undertook this process but a review has not taken place		
29.c	No		
30	**Which of the following best describes your network detection and monitoring processes and controls?**	**Answer**	**Comments and explanations**
30.a	All events are analysed (automated and manual) to attribute attacker, methodology and potential impacts to critical functions and processes		
30.b	An automated system highlights anomalies but little analysis is undertaken		
30.c	We analyse network logs in real time, looking for evidence of mounting attacks		
30.d	We have no capability to analyse network anomalies		
31	**Do you perform regular vulnerability scanning?**	**Answer**	**Comments and explanations**
31.a	Yes, we have a rolling programme, agreed at board (or senior executives) level		
31.b	Yes, there is a regular programme in place		
31.c	No, vulnerability scanning is performed on an ad-hoc basis		
32	**Which of the following measures do you implement to protect your networks against internal and external attacks? (Multiple answers possible)**	**Answer**	**Comments and explanations**
32.a	We use firewalls		
32.b	We have a regular programme in place for penetration testing		
32.c	We conduct penetration testing on an ad-hoc basis		
32.d	We monitor user activity, and control access to activity and audit logs		
32.e	Other (Specify)		

33	**How frequently do you undertake vulnerability scanning and penetration testing and ensure that both are effective?**	**Answer**	**Comments and explanations**
33.a	At least weekly		
33.b	At least monthly		
33.c	At least twice a year		
33.d	At least annually		
33.e	On an ad-hoc basis		
33.f	Not at all		
34	**Which of the following actions is contemplated in case of an attack? (Multiple answers possible)**	**Answer**	**Comments and explanations**
34.a	Request of collaboration to CERT/SOC of other private entities		
34.b	Request of support to National CERT		
34.c	Notification to the Law Enforcement Agencies		
34.d	Support in forensic analysis from Law Enforcement Agency		
35	**Are thresholds (aligned to impacts) set for events and incidents to determine the most appropriate response?**	**Answer**	**Comments and explanations**
35.a	Yes and these have been approved by business and supporting IT functions		
35.b	Yes and these have been approved by supporting IT functions		
35.c	No formal thresholds, we respond on an ad□hoc basis		
36	**Do you have a documented and regularly tested response plan (business continuity, disaster recovery and/or cyber incident response)?**	**Answer**	**Comments and explanations**
36.a	We only have a business continuity plan, tested in the last 12 months		
36.b	We only have a disaster recovery and/or cyber incident response plan, tested in the last 12 months		
36.c	Existing business continuity plans are considered sufficient, but these have not been tested against a cyber incident		
36.d	Yes. We have separate cyber incident response, disaster recovery and business continuity plans forming a recovery framework. The effectiveness of this framework has been tested in the last 12 months		
36.e	Yes. We have separate cyber incident response, disaster recovery and business continuity plans forming a recovery framework. These have been tested separately within the last 12 months, and it is assumed that they can work collectively		
36.e	No		

37	**Which of the following options best describes your data breach notification policy?**	**Answer**	**Comments and explanations**
37.a	All critical breaches are to be reported to: law enforcement, customers and regulator		
37.b	Critical breaches are only reported to law enforcement		
37.c	Critical breaches are reported internally only		
37.d	No formal breach notification policy		
38	**Does your response planning explicitly refer to recovery activities, including retuning to normal operations, or to a pre□defined, acceptable level?**	**Answer**	**Comments and explanations**
38.a	Yes, and the timeframe for returning to normal operation/acceptable level is reviewed on an annual basis.		
38.b	Yes, but the timeframe for returning to normal operation/acceptable level has not been reviewed in the last 12 months		
38.c	No		