



Deliverable 3.1

Cross-matching of organizations with EU standards



Tempus

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	3
2.EU standards for cyber security in public and private organizations.....	4
2.1.EU standards, guidelines and best-practices.....	4
2.1.1.BSI.....	5
2.1.2.International Organization for Standardization.....	5
2.1.3.National Institute of Standards and Technology.....	7
2.1.4.ISACA.....	9
2.1.5.Information Security Forum.....	9
2.1.6.SANS Institute.....	10
2.2.Cyber security requirements for organizations and their staff.....	11
2.3.Cyber security questionnaire.....	12
2.4.Relevant cyber security training topics.....	13
3.Cross-matching with Montenegrin organizations.....	15
3.1.Current scenario of Montenegrin public and private organizations	15
<i>Governance, leadership and management</i>	16
<i>Identify</i>	16
<i>Protect and respond</i>	16
3.2.Cross-matching Montenegrin organizations with EU standards	17
4.Conclusions.....	18
References	18
Appendix.....	19



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 possible discrepancy between claims and facts. Nevertheless, in this document we provide and discuss the outcomes of a survey of the practical countermeasures to cyber risks implemented in Montenegro and of the training of Montenegrin employees. A detailed analysis of EU standards and best-practices allows us to both identify a concise set of relevant questions, and to assess the current situation of Montenegrin organizations with respect to the rest of the EU. The expertise of EU partners finally permits to identify relevant training topics, that will be further developed in the following Deliverables.

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 guidelines 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 Committee for Standardisation and members of the National Electrotechnical Committees of European Countries) is extremely important.

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 the 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 in either 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 [2]:

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 contains 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 [3].

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) [4] and the International Telecommunication Union (ITU) [5] on information and communications technology (ICT) standards [6]. 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 assets [7]. 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 ISMS [8]. 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 11 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 11 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) [9]. 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 portal [10]. 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.

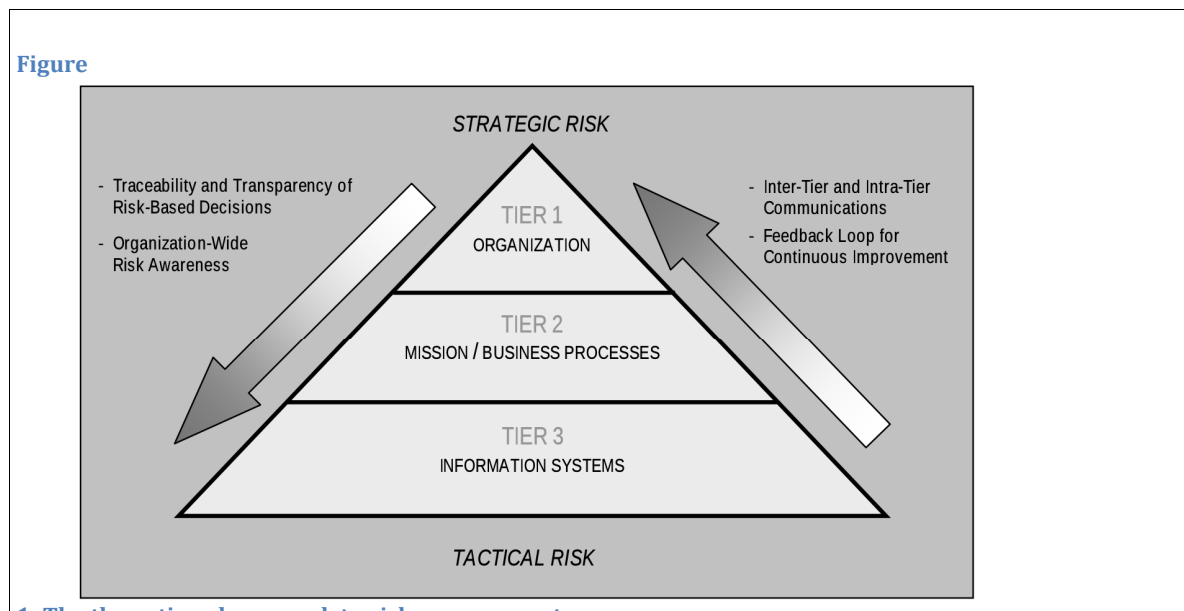
- c) ISO/IEC TR 13335-4:2000 covers the selection of safeguards (i.e. technical security controls). This is under review and may be superseded by ISO/IEC 27005.
- d) ISO/IEC TR 13335-5:2001 covers management guidance on network security. This is also under review, and may be merged into ISO/IEC 18028-1, 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 including 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 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 [11]. 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 [12] 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 Control™ (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, supplying authoritative opinion and guidance on all aspects of information security, and delivering practical solutions to overcome the wide-ranging security challenges that impact business information. 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. ISF also provides 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 information security worldwide. As cited before, the standards are only guidelines 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 [13] and continuing deeper from there. Citing the BSI-Standard 100-2 [14]:

“(...) 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.
- **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” [15].



- **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 three 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.
2. *Identify* – This part of the questionnaire deals with understanding whether organizations assign the correct importance to cyber threats, and to risk and vulnerabilities assessment.
3. *Protect and respond* – This is the part of the questionnaire responsible of assessing the capability of an organization to sufficiently protect its assets from cyber attacks, to promptly respond to cyber attacks, encompassing both technical solutions and a proper training of its employees.

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 towards 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 require 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 the 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.

- **Cyber Security Risks and Resilience:** This course introduces a variety of cybersecurity information and practices, explaining why it is important, and introducing some of the products and processes used to secure data.
- **Introduction to network security:** This course 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:** This course provides an 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:** This course provides an 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

In this section, we report and discuss the results of our survey about the current mechanisms in place in the most important Montenegrin organizations in order to enforce cyber security at all levels.

Additionally, we cross-match the above outcomes with the EU standards delineated in Section 2, with the main purpose of underlining what are the major deficiencies and how they can be solved.

3.1. Current scenario of Montenegrin public and private organizations

The survey we performed involved five of the most important Montenegrin organizations and companies involved with ICT:

- Crnogorski Telekom a.d. [16]: It is the largest telecommunications company in Montenegro, providing a full range of fixed-line, mobile, IPTV, and internet telecommunication services. Merged in May 2009 with T-Mobile Crna Gora d.o.o. and Internet Crna Gora d.o.o., Crnogorski Telekom a.d. provides local, national, and international services, in addition to a wide range of telecommunications services involving leased-line circuits and data networks.
- Telenor Montenegro [17]: It is the first and largest mobile phone operator in Montenegro, currently holding 175 base stations which cover all main roads, the majority of tunnels and all the beaches and winter tourist centers in Montenegro.

Telenor Montenegro's signal covers 98% of the places where Montenegro's inhabitants reside.

- M:tel d.o.o. [18]: It is a major telecommunications company in Montenegro, a 51-49% joint venture between Telekom Srbija and Telekom Srpske. After obtaining its license in May 2007, as of the end of the year M:tel's market share in Montenegro (a market of 992,000 mobile sets at this time) already reached 22.66%.
- Telemach [19]: It is the first cable operator in the market of Montenegro. It was created as BBM 2006, and in January 2015 changed its name to Telemach, following the acquisition of United Group. With this acquisition the company has entered the largest operators in the region - SBB in Serbia and Telemach in Bosnia and Herzegovina and Slovenia and Total TV. Compared to other operators in Montenegro, Telemach provides advanced services based on the latest technologies.
- Wireless Montenegro d.o.o. [20]: Founded in September 2011 as a private-public partnership between the Government of Montenegro and the Austrian company EOSS Innovationsmanagement GmbH (the first company in Montenegro founded as a private-public partnership in this field), it aims at implementing a digital radio system with TETRA standard in the entire territory of Montenegro and to provide free wireless Internet services in all municipalities for the citizens of Montenegro, and to provide additional services to tourists visiting Montenegro.

Representatives from these five companies were asked to respond to a questionnaire, reported in the appendix, that covered many aspects of cyber security management, ranging from policies and budget, to employees training and risk assessment. Detailed answers are also reported in the appendix, while here we present a general discussion of the outcomes, divided into the three main pillars identified in Section 2.3.

Governance, leadership and management

3 out of 5 companies admitted the lack of any specific cyber security taxonomy in place. In most cases, the cyber risk management methodology presents significant flaws: it is often completely disjoint from the overall enterprise risk management, the board of directors are rarely involved in the process, quality assessment is underestimated, and quantitative aspects and insurances are completely neglected. Cyber security issues are regularly reported to the CEO, but not always with sufficient frequency. The budget spent for cyber security, when estimable, is low, even considering the limits imposed by operating in a small country. Interestingly, two of the core activities of this Project, *i.e.*, developing awareness campaigns for citizens and introducing clear policies and regulations, are identified by most companies as the most desirable contributions of the public sector to cyber security enforcement.

Identify

Although several parameters are usually considered in order to estimate the impact of cyber threats, and their economic value is estimated whenever possible, important aspects such as customer and legal loss are ignored by most companies. Additionally, some companies do not recognize the possible impact of cyber security on research and development (and *viceversa*), and on the ability to outsource activities to third parties, while they only foresee a potential slow-down in production. While not all companies are aware of concrete threats such as a DOS attack, and they completely ignore attacks against their industrial control system, they identify service disruption as the main systemic impact of cyber crime.



Protect and respond

2 out of 5 companies have no structured education and training programme for their employees involved in cyber security activities. Additionally, none of the companies seems to have specific requirements concerning the cyber security capabilities of the SME working for them. Luckily, most companies have several countermeasures in place to guarantee information security, although some of them do not implement fundamental solutions such as recurring to a SOC or a CERT, and indicators are in general defined only for specific countermeasures. Requesting the collaboration of the CERT/SOC of other private entities or to the national CERT is contemplated by almost all companies, but notification to and support from law enforcement agencies is sometimes dangerously neglected.

3.2. Cross-matching Montenegrin organizations with EU standards

To cross-match the cyber security related measures implemented by Montenegrin organizations with EU standards, let us compare the scenario highlighted in the previous section with the main requirements identified in Section 2.2.

First, the majority of the companies we contacted do not implement the ISO/IEC 27001:2013 standard for the management of information security and all related processes. Making sure that all (or, at least, all large) companies adhere to this standard is the primary step to adequate Montenegrin organizations to what happens in other EU countries. A framework for staff at all levels is fundamental and the quality of the ISO/IEC 27001:2013 is universally recognized. Cyber security risk management need to be improved in two main directions. On the one hand, all Montenegrin companies must improve the level of coordination of cyber security risk management with the overall enterprise-wide risk management, strengthening the chain of command and allowing for a proper involvement of the CEO and the board. On the other hand, these companies need to prove themselves able to assess their current effort in enforcing cyber security and to dedicate a suitable budget to cyber security risk assessment and response.

Companies need to understand that cyber threats are pervasive and incidents need to be both prevented and countered. They need to better protect their networks, which includes not only protecting their intranets from external attacks, but also establishing precise mechanism to evaluate the risks of collaborating with other companies and sharing common resources. Additionally, SOCs and CERTs are fundamental instruments for incident handling and no enterprise nowadays can operate in ICT without similar solutions in place. Additionally, appropriate network forensics instruments and constant interaction with law enforcement agencies are necessary in order to analyse events and identify their causes, to allow a proper investigation process, find evidences of a crime, persecute responsible individuals, and avoid that similar violations recur in the future.

Finally, all companies need to provide sufficient means for all their employees and managers to be always aware of most recent cyber risks, to be trained to recognize them, and to be ready to counteract. Specific training campaigns with certified instructors need to be scheduled regularly at a national level, in order to guarantee up-to-date competencies for all workers, commensurate to their duties and responsibilities. The main purpose of this Work Package is exactly to pave the way for a similar ambitious but essential process.

4. Conclusions

Collecting the feedbacks of some of the most important Montenegrin companies involved in ICTs was a fundamental step in order to gain the necessary information about their need for specific education in the field of cyber security prevention, defence and response. The cross-match of Montenegrin organizations with EU standards was carried on as follows:

- 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 analyse 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.

References

- [1] “Best Practices in Computer Network Defense: Incident Detection and Response”, M.E. Hathaway (Ed.), Steve Purser, ENISA, pag. 97, IOS Press 2014
- [2] www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html
- [3] www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzInternational/international.html
- [4] www.iec.ch/
- [5] www.itu.int/net/home/index.aspx
- [6] www.iso.org/iso/iso_catalogue/faq_standards_2.htm
- [7] www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103
- [8] www.iso27001security.com/html/27002.html#RelationTo27001
- [9] isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.html



- [10] www.commoncriteriaportal.org/public/consumer/
- [11] "Guide for Assessing the Security Controls in Federal Information Systems, Building Effective Security Assessment Plans", Ross, Ron; Jahnsen, Arnold; Katzke, Stu; Toth, Patricia; Stoneburner, Gary; Rogers, George (2008)
- [12] www.isaca.org/
- [13] www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile
- [14] www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile
- [15] www.symantec.com/connect/articles/introduction-incident-handling
- [16] <https://www.telekom.me/>
- [17] www.telenor.me/
- [18] mtel.me/
- [19] www.telemach.me/
- [20] www.wirelessmontenegro.com/



Appendix



n°	Questions	Companies				
		Telekom a.d.	Telenor a.d.	M-tel d.o.o.	Telemach	Wireless Montenegro d.o.o.
1	Do you adopt a specific cyber security taxonomy?					
1.a	Yes, a Company taxonomy					
1.b	Yes a National Standard Taxonomy (Please specify which one)		x (ISO 27001)			
1.c	Yes, an International Standard (Please specify which one)		x (ISO 27001)		x (ISO 27001)	
1.d	No, we don't adopt any Taxonomy	x		x		x
1.e	Other (specify)					
2	What are the parameters to calculate the impact of a cyber attack/incident in your Company? (More options available)					
2.a	Service Time Disruption		x	x	x	x
2.b	Direct economic loss		x (only in the case of bigger attacks)	x		
2.c	Data/Information loss		x	x	x	x
2.d	Brand Image loss		x	x	x	x
2.e	Customers loss			x		
2.f	Recovery time		x	x	x	
2.g	Penalties on commercial agreement		x	x		
2.h	Legal costs			x		
2.i	There is no a methodology to estimate the impact	x				
2.l	Other (Specify)					
3	Are the parameters translated in economic value?					
3.a	Yes always					
3.b	Yes when it is possible to estimate		x	x	x	x
3.c	Yes only at the incident/attack closure					
3.d	No					
3.e	Other (Specify)					
4	What are the elements included in your cyber risk management methodology? (More options available)					
4.a	Quantitative methodology					
4.b	Quality methodology		x		x	
4.c	Methodology integrated with Enterprise Risk Management		x			x
4.d	It's a yearly formal process		x	x		
4.e	It's a yearly formal process and it is activated if any parameters change during the year (assets, services,...)		x		x	
4.f	It's a process that involves more departments	x	x	x		
4.g	The results of this process are communicated also to the Board of Directors		x			
4.h	It allows to prioritize the investments for the countermeasures		x		x	
4.i	It takes in consideration also the risk transfer to an insurance policy					
4.l	Other (specify)					
5	Who is in charge for the risk management process?					
5.a	Chief security Officer					
5.b	Chief Information Security Officer		x (for risks in the field of information security, related to the threat of availability, services and systems, and the integrity and confidentiality of information)			
5.c	Enterprise Risk Manager	x	x (at company level)	x		
5.d	Other (specify)				x (The responsibility of the company security policy is delegated to the Technical Director)	x
6	Do you have a structured education and training programme for the employees involved in cyber security activities?					
6.a	Yes	x	x	x		
6.b	No				x	x
7	Are Cyber Security Issues brought at the attention of the CEO? (2 options could be chosen in terms of period and crisis)					
7.a	Weekly		x			x
7.b	Monthly	x		x		
7.c	Yearly				x	
7.d	In case of an incident/accident impacting also external stakeholders	x	x	x	x	x
7.e	Never					
8	In your opinion, the impact of cyber security countermeasures can be measured as follows: (More options available)					
8.a	Limitation in sharing results of Research and Development activities		x	x		
8.b	Outsourcing of activities to external companies		x	x		
8.c	Slow-down of production activities		x	x	x	x
8.d	Other (specify)					



9	Which kind of cyber attacks are you more afraid of in your sector?					
9.a	DOS	X		X	X	X
9.b	Advanced Persistent Threat	X	X			
9.c	Attacks against Industrial Control System					
9.d	Phishing	X	X			
9.e	Other (Specify)					
10	Are there any specific cyber security requirements for the SME working for your company?					
10.a	Yes, the ISO 27001 is required					
10.b	Yes, on the basis of the activities to be performed, it shall have specific security certifications					
10.c	No, there is no specific requirements	X		X	X	X
10.d	They are included in our perimeters of risk assessment and we support them to apply the proper countermeasures					
10.e	Other (Specify)		X			
11	What are the counter measures implemented within your Company to guarantee information security? (More options available)					
11.a	A series of policies on the use of digital devices and on Data protection	X	X	X	X	X
11.b	Awareness campaigns for employees	X	X	X		
11.c	Standards and certifications (i.e. ISO27001)		X (Use policies (security directives) in accordance with security standards)	X		
11.d	Public and Private information exchange	X	X	X		
11.e	Disaster recovery plans	X	X	X	X	
11.f	Cyber threat intelligence analysis center					
11.g	Endpoint protections (i.e. antivirus)	X	X	X	X	
11.h	Security Operation Center	X	X			
11.i	Computer Emergency Response Team	X	X			
11.l	Other (Specify)					
12	For the implemented countermeasures, have you defined other indicators to determine their effectiveness?					
12.a	Yes					
12.b	Just for some of them	X	X	X	X	
12.c	No					X
12.d	Other (Specify)					
13	Could you indicate an estimate of the budget spent by your Company for cyber security?					
13.a	< 1.000.000 Euro	X	X	X		
13.b	1.000.000 - 5.000.000					
13.c	5.000.000 - 10.000.000					
13.d	> 10.000.000					
13.e	It's not possible to evaluate it				X	X
13.f	It is difficult because the budget is spread in several Departments					
14	The portion of cyber security budget dedicated to IT solutions is:					
14.a	< 30%	X				
14.b	30% - 50%					
14.c	50% - 70%					
14.d	> 70%					
14.e	It's not possible to evaluate it		X	X	X	X
15	In case of an attack, are these actions potentially contemplated?					
15.a	Request of collaboration to CERT/SOC of other private entities		X (All relevant information are shared within DT Group)	X	X	X
15.b	Request of support to National CERT			X	X	
15.c	Notification to the Law Enforcement Agencies		X (Telecom performs its activity in accordance with Law and Regulations about manners and deadlines for measures of security and integrity protection of e-communication network, and accordingly reports the Agency for Electronic Communications and Postal Services)	X	X	
15.d	Support in forensic analysis from Law Enforcement Agency			X	X	
16	Which of the following would you identify as the main systemic impact related to cyber crime?					
16.a	Service disruption	X	X	X	X	X
16.b	Loss of trust in digital services and devices	X	X			
16.c	Economic losses	X	X (This consequence is directly related to the previous two and depends on them)	X		
17	Which of the following efforts do you expect from the Public Sector to contrast cyber crime? (More options available)					
17.a	Strengthen awareness campaigns for citizens	X		X	X	X
17.b	More monitoring systems					X
17.c	Strengthen collaboration for threat and vulnerability analysis		X	X		
17.d	Release of cyber security policy and regulations at National and International Level	X	X	X		
17.e	Strengthen collaboration at International level between Judicial Authority to speed up the contrast to cyber crime		X	X	X	