THE 10th ANNIVERSARY INTERNATIONAL SCIENTIFIC PROFESSIONAL CONFERENCE
SECURITY AND CRISIS MANAGEMENT – THEORY AND PRACTICE (SeCMan)
- THE 10th ANNIVERSARY INTERNATIONAL FORUM
„SAFETY FOR THE FUTURE 2024" -
27th and 28th September 2024, Belgrade, Republic of Serbia

INFORMATION SECURITY AND BUSINESS CONTINUITY ASSURANCE – PRACTICAL EXPERIENCES

Radoslav Rakovic[1a]
[1] Engineering Academy of Serbia, Kneza Milosa 9, Belgrade, Republic of Serbia,
rrakovici@gmail.com

Received: 25th July 2024
Accepted: 8th August 2024

Review paper

Abstract: *Business continuity assurance is a concept that is oriented towards the adaptability of the organization in order to prepare to respond to disturbances that may occur in the environment, especially extreme disturbances - disasters, which can have a very large impact on the organization's operations, on its ability to deliver products and provide services. The main goal is to mitigate the consequences of these disturbances, to ensure the recovery of the organization and the continuation of its work even after these events. This concept is the subject of particular standards of the ISO/IEC 22300 series. In the implementation of the concept, information security is of particular importance, considering that nowadays the performance of the activities of organizations is closely related to information technologies. Information security is the subject of particular standards from ISO/IEC 27000 series, which are oriented towards preserving the basic properties of information - confidentiality, integrity and availability. This paper presents practical experiences in connecting these standards within the integrated management system in the organization.*

Key words: *Information Security, Business Continuity, Integrated management system, Disaster recovery location*

1. INTRODUCTION

Business Continuity (BC) assurance represents a concept that is oriented towards the adaptability of the organization in order to be prepared to respond to disturbances that may occur in the environment, especially extreme disturbances - disasters, which can have a very large impact on the organization's operations, on its ability to deliver products and provide services. This especially applies to catastrophic disturbances such as earthquakes, fires, floods, war conflicts, terrorist attacks, cyber-attacks etc. In order to ensure the continuity of the business of an organization even after such events, it is necessary to apply a whole series of measures of an organizational and technical nature. In this sense, the ISO 22300 series of standards for business continuity management (BCM) represent a valuable framework.

[a] ORCID: 0000-0002-8067-6582

The essence of these standards is vividly represented by the saying that was chosen as the motto of this paper - organizations must be prepared for reaction in the event of extraordinary events, when an event occurs there is no time for agreements, plans and training, because then it is necessary to react quickly as the consequences would be minimized as much as possible. In the last ten years, we have had at least three very serious disturbances in our immediate environment, major floods in 2014. and 2016. and a period of pandemic, and in recent times we are increasingly facing extreme bed weather situations. All these circumstances lead us to the conclusion that the result we achieve often does not depend on how we work when everything is fine, but how we react when it is not!

In the implementation of the business continuity concept, information security has particular importance, considering that nowadays the performance of the activities of organizations is closely related to information technologies. Information security is the subject of particular standards the ISO/IEC 27000 series, related to Information Security Management Systems (ISMS), oriented towards preserving the basic properties of information - confidentiality, integrity and availability.

After a brief overview of abovementioned ISO standards, in this paper some practical experiences in connecting these standards within the integrated management system (IMS) in the organization are presented.

2. BUSINES CONTINUITY MANAGEMENT STANDARDS

In accordance with the usual practice when it comes to management standards, the family of ISO 22300 standards contains, Figure 1, standard related to vocabulary i.e. terms and definitions ISO 22300:2021 (ISO 2021), standard with BCM system requirements ISO 22301:2019 (ISO 2019), standard with guidelines for implementation of requirements ISO 22313:2020 (ISO 2020) and standards that develop some specific aspects of requirements,

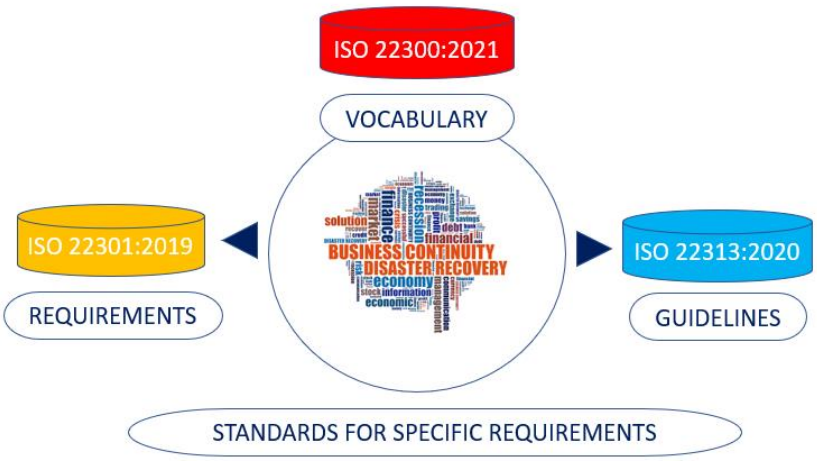

Figure 1: Standards od ISO 22300 series
Source: Author

The standard with terminology ISO 22300 (ISO, 2021) contains 360 terms and definitions. For the purposes of this paper, the three most important ones have been highlighted - business continuity, business continuity management and disaster.

Fundamental term – business continuity – is defined as „capability of an organization to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption“ (definition 3.1.19). It is clear that business continuity assurance cannot be just one activity, given that it is a complex problem that includes a whole series of issues that need to be resolved. That is why it is the subject of a special field known as Business Continuity Management (BCM), which is defined as „process of implementing and maintaining business continuity“, definition 3.1.20. As a matter od fact, it is the overall management process that identifies potential threats to the organization and the impacts on business activities that these threats may cause if they materialize and that creates a framework for the adaptability of the organization with the ability to respond adequately to these threats and to protect the interests of all stakeholders, reputation, brand and activities they create value.

It has already been pointed out that the most critical events are of a catastrophic nature. A disaster is defined as „situation where widespread human, material, economic or environmental losses have occurred that exceeded the ability of the affected organization, communuty, or society to respond and recover using its own resources“, definition 3.1.73. In order to enable organization to recover its activities after such events, it must be prepared in advance i.e. to have prepared certain strategies and operational plans that will be activated when the event occurs.

Standard with business continuity requirements ISO 22301 (ISO 2019) has structure that is standardised at the level of all management standards published by ISO, as per well known Annex SL. This unified structure has 10 chapters, the first three has no requirements (1- Scope, 2-Normative refereences and 3-Terms and definitions) and others seven include requirements (4-Context of the organization, 5-Leadership, 6-Planning, 7-Support, 8-Operations, 9-Evaluation of performances and 10-Improvement).

Chapter 8 represents the segment by which the management standards differ the most, given that this chapter mostly expresses the specifics of the area to which the management system refers. This is also the case in the case of business continuity, where this chapter contains 6 chapters, Figure 2.

In item 8.1 Operational planning and control general frameworks for planning, implementation and management of processes are determined in order to realize the planning settings foreseen in chapter 6, with a special emphasis on the establishment of criteria for processes and storage of documented information.

Item 8.2 Business impact analysis and risk assessment deals with a very important element of BCM - Business Impact Analysis (BIA) and Risk assessment. Business impact analysis represents the „process of analysing the impact over time of a dispruption on the organization“, definition 3.1.24, and the magnitude of that impact is expressed through the level of risk. Within these analyses, the organization must define the Maximum Tolerable Period of Disruption (MTPD) in order to ensure that the recovery time objective (RTO) is shorter i.e. (RTO<MTPD).

Based on results of business impact analysis and risk assessment, in item 8.3 Business continuity strategies and solutions it is intended to identify and select business continuity strategies that consider the options used before, during and after the disruption. Those strategies must consist of one or more solutions (approaches, arrangements, methods, procedures, actions and activities for the implementation of strategies), and the solutions can be applied in one or more strategies.

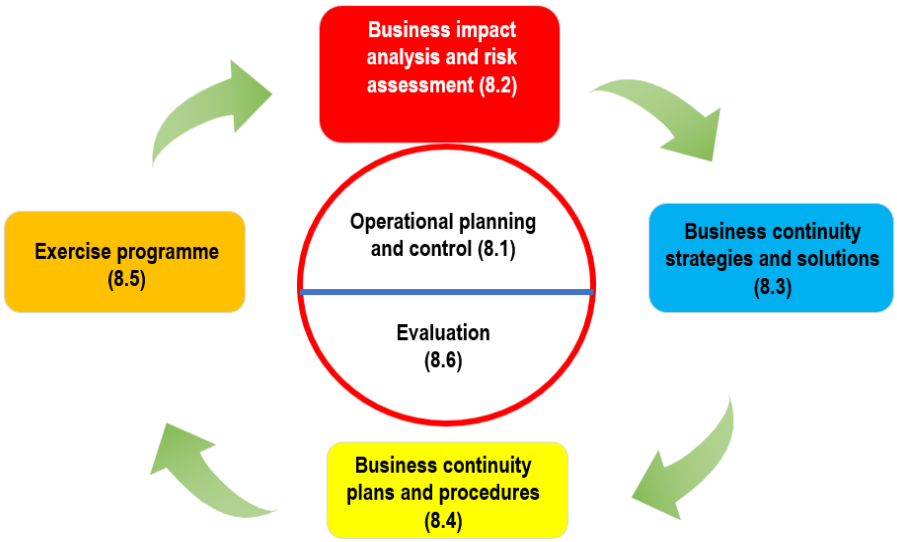

Figure 2: Structure of Chapter 8: Operation, standard ISO 22301
Source: Author

Strategies and solutions defined within item 8.3 are elaborated within item 8.4 into Business continuity plans and procedures. These plans define scenarios that represent „pre-planned storyline that drives an exercise, as well as the stimuli used to achieve exercise project performance objectives“, definition 3.1.234. As in all plans, the procedures for dealing with the occurrence of these scenarios are defined, along with the definition of those who are in charge of it and the means that should be provided for it. The key result is the Business Continuity Plan - BCP, which is defined as “documented information that guides an organization to respond to a disruption and resume, recover and restore the delivery of products and services consistent with its business continuity objectives“, definition 3.1.22.

In order for strategies, solutions, plans and procedures to be successfully implemented, the standard in chapter 8.5 Exercises program establishes the organization's obligation to determine through the training and testing program whether the planned measures and means are adequate and whether all actors know what their task is. After the exercises, the results are analyzed and, if necessary, changes are made in the system.

In item 8.6 Evaluation of documentation it is determined the obligation of the organization to periodically review all documentation related to ensuring business continuity at regular intervals, and necessarily after one of the disruptive events. The essence of this chapter is in the concept known as "lessons learned" in order to improve the system.

The ISO 22313:2020 (ISO 2020) standard elaborates the requirements of the ISO 22301 standard through guidelines on how to implement them. The standard recognizes two global scenarios in which BCM systems are applied - one, when a sudden event occurs, which could not be predicted, and the other, when there is a hint of an unwanted event through a warning that gives us a certain time to better prepare for it. These two scenarios are shown in Figure 3a and 3b respectively (ISO 2020)

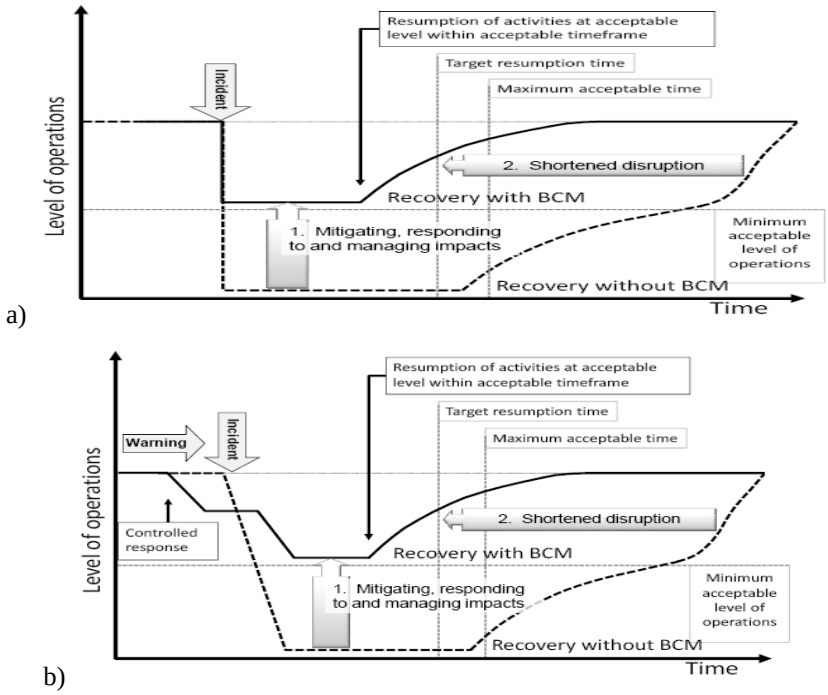

Figure 3: Effectiveness of BCMS – two scenarios
Source: ISO 22313:2020

In both cases there is a certain level of operations, characteristic of regular conditions, and a minimum acceptable level of operations. The dotted line shows the course of events if they did not have BCM systems in place. The differences between these scenarios are in the course of the process in relation to the moment of occurrence of the incident. In the case of a sudden event, Figure 3a, there is a sudden drop in the level of operations, which thanks to the BCM systems we maintain above the minimum acceptable level, and then we gradually move towards recovery and re-establishment of the regular level. In the case of a gradual occurrence of an event preceded by some kind of warning, Figure 3b, the level of operations does not drop suddenly but gradually, the elements of the BCM system react already at the first hints, so through the "controlled response" the level of characteristics is kept at a minimum for a short time level.

The remaining standards from the ISO 22300 series deal with specific aspects of ensuring business continuity. At this point, we will mention the document ISO/TS 22317:2021 (ISO 2021), which presents guidelines for the preparation of business impact analysis. This document does not have the status of an approved standard but is marked as "TS" (Technical Specification) which is part of ISO's practice to publish documents even if full agreement has not been reached to approve it as a standard, in order to enable its practical application in all situations in which organizations find it useful.

3. INFORMATION SECURITY STANDARDS

The rapid development of information technologies marked the end of the 20th and the beginning of the 21st century. Knowing how to work on a computer has become part of elementary literacy, because without it it is practically impossible to function both in professional and private life. There is no doubt that it significantly facilitated work in all

segments of human activity, but the problem of information security is open. Namely, it became clear that possible intentional or unintentional influences on the properties of the information that is transmitted and/or stored can have unforeseeable consequences for the safety of systems, equipment and people. A systematic approach to solving this problem is defined by standards from the ISO/IEC 27000 series, which refers to Information Security Management Systems - ISMS.

The information security management system is based on the business risk approach to which the organization is exposed if information important to its business or market status falls into the hands of those who, for whatever reason, are not "friendly" towards it. The main task in establishing these systems is to implement, monitor, review, maintain and improve system related to information security. Information security refers to the preservation of the following properties of information (ISO 2018) (Rakovic 2017):

Confidentiality, property that information is not made available or disclosed to unauthorized individuals, entities or processes, definition 3.10. Most people think of this property when talking about information security

Integrity, property of accuracy and completeness i.e. there is no any part of information that is changed or deleted by unauthorized person.

Availability, property of being accessible and usable on demand by an authorized entity.

Fundamental information security principles included into standard ISO/IEC 27000 (ISO 2018) are:

- Awareness of the need for information security.
- Assignment of responsibility on information security.
- Incorporation of management committment and the interests of stakeholders.
- Enhancing societal values.
- Risk assessment determining appropriate controls to reach acceptable levels of risks.
- Security incorporated as an essential element of information networs and systems.
- Active prevention and detection of information security incidents.
- Ensuring a comprehensive approach to information security management.
- Continual reassessment of information security and making of modiffications as appropriate.

The standards belonging to the 27000 family are grouped into five levels - vocabulary, requirements, guidelines, sector-specific guidelines and guidelines for information security controls. In practice, three standards are most often used - a standard related to the dictionary of terms, ISO/IEC 27000 (ISO 2018), a standard with requirements for information security ISO/IEC 27001 (ISO 2022a) and a standard that provides practical guidelines for the implementation of standards with requirements ISO/IEC 27002 (ISO 2022b).

The central standard of the family is the ISO/IEC 27001 (ISO 2022a) standard, which contains requirements for an ISMS. What is specific about this standard in relation to other standards with requirements for other management systems is that, apart from the requirements in the basic part of the standard, this standard contains normative Annex A with 93 controls that are oriented towards reducing information security risks. These controls are grouped into four categories – organizational controls (37), people controls (8), physical controls (14) and technological controls (34). The number in parentheses represents the total number of controls in the particular category.

The most important document within ISMS represent Statement of Applicability (SoA). This statement describes how particular information security controls are applied within the organization. This statement is based on risk assessment and risk management processes, regulatory requirements, contractual obligations and business requirements related to information security.

4. ISMS AND BUSINESS CONTINUITY

A special segment of the ISMS standards refers to information security from the aspect of ensuring business continuity. This means that the organization must establish, implement and maintain processes, procedures and controls that will ensure that in the event of emergency situations, especially disasters, the organization can function to a certain level in order to overcome the period until full recovery from the consequences of these events. Two organizational controls a very important:

Control A.5.29: Information security during disruption. As per this control. the organization shall plan how to maintain information security at an appropriate level during disruption.

Control A.5.30: ICT (Information Communication Technologies) readiness for business continuity. As per this control, ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements

One of the most important segments related to ensuring business continuity is the establishment of a Disaster Recovery (DR) location - a backup location where necessary information is stored that enables system recovery in the event of disasters that in some way disable the main location. Establishing a DR location is based on several assumptions:

- That the organization bases its activities on a specific set of information without which the functioning of the organization would be impossible.
- That this set of information may be threatened by a catastrophic event that would affect the location where the information is located and from which the organization performs its activities
- That the restoration of the organization's activities after a catastrophic event requires some minimum set of information that enables the establishment of elementary functions in the first moment.
- That the recovery of the organization from disasters requires a set of information that allows gradual restoration of activities until complete normalization (if it is possible).
- In order for this DR location to play its role, it is necessary to:
- To be spatially far enough from the primary location, beyond the reach of the catastrophic event that caused the problems at the primary location. In general, this means that the backup location should be at least 10 km as the crow flies from the primary location.
- That a carefully selected set of information that enables the establishment of the most important functions of the organization is kept at the DR location.
- That a mechanism is provided that reconciles that information at the DR location with the information at the primary location. This coordination is performed, as a rule, on a daily basis, with the exchange of information at night, when the load on communication networks is the least.

5. CASE STUDY: EP ENTEL

Practical aspects of information security and business continuity are illustrated on the example of the company Energoprojekt Entel plc, Belgrade (ENTEL). It is the company whose activity is design, consulting and engineering in the fields of energy, water, telecommunications and environmental protection. The organization has implemented an integrated management system (IMS) with five management standards - quality, environmental protection, operational, health and safety, information security and energy management, in accordance with the relevant ISO standards (EPE, 2022).

Essentially, in the implementation of all management systems within the IMS, ENTEL operates in three groups of aspects - preparation of design documents, supervision over the execution of works and its own business premises. They are listed below 2 examples related to business continuity, which belong to the first and third aspects, considering that in them the influence of the company is more significant. In the aspect related to the supervision of the execution of the works, the main responsibility rests with the main contractor and its subcontractors, while the role of ENTEL is to monitor it and give suggestions for maintaining the process within the planned framework.

In the first aspect, the preparation of design documents, the responsibility of ENTEL is great, because when creating design solutions, it is necessary to respect international standards, legal regulations in the country where the building of the facility and/or system is planned, the best global practice for that type of facility and/or or system as well as prospective trends in technologies related to the facility and/or system.

Application of information security approach is illustrated on example of High Voltage (HV) Supervisory Control and Data Acquisition (SCADA) system, designed as per requirements of client from the Persian Gulf region. The essence of the SCADA system is to collect information from the technological process (which can be an electrical and energy facility, a facility in the oil and gas system, water supply or sewage system, etc.) and to manage the system based on that information. In this particular case, scope of Terms of Reference was to establish Substation Control Systems (SCSs) in 13 substations for the purposes of local monitoring and control. It was planned to collect all data to SCADA servers in central location to enable remote control of switches (switching on and off). Control of local processes is planned to be done from local SCSs. The system solution is shown in Figure 4 (Rakovic et all 2016)

It was applied information security approach known as the „Defense in depth“ concept (Rakovic et all 2016). This model is implemented in several layers (physical, network perimeter, security of computer, application and equipment). The network is divided into network segments with different access rights (establishing of demilitarized zone - DMZ, separating of IT and ICS network). Physical protection at physical perimeter included access control system (biometric check of identity) and video surveillance (CCTV), covering equipment rooms, corridors and entries. Security system was connected through dedicated infrastructure, independent of SCADA network. Taking into account that any information loss in such a system could have serious consequences, a system's availability of 99.999% („five 9s“) has been proposed. It means that all links and equipment have redundant configuration, two SCADA centers are proposed, one as primary and another as secondary with the role of Disaster Recovery Site, to keep reserve copies of data. Master SCADA servers from both locations receive all information from subatations at the same time and in case of failure of any SCADA centre, another continues to provide full service. Segregation of networks provides better protection of information and localization of any problems within the network.

All unnecessary services (for example HTTP approach to network equipment) are switched off to decrease system vulnerability.

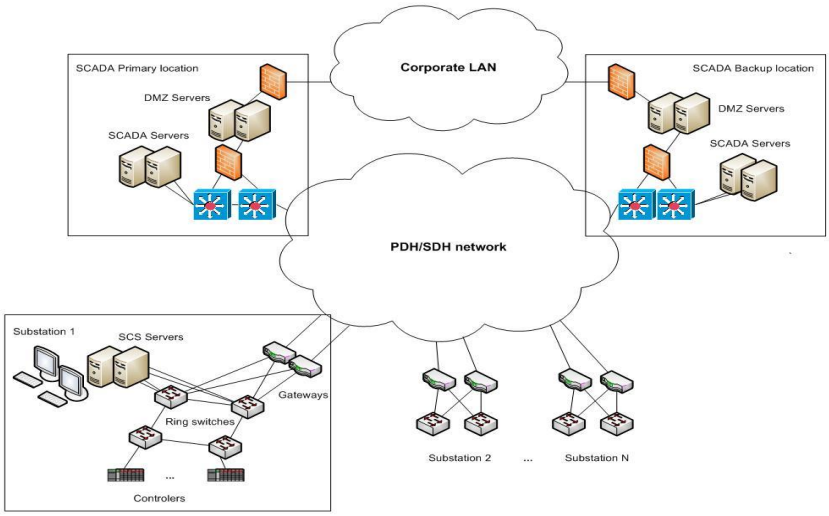

Figure 4: Block diagram of HV SCADA system
Source: Rakovic et all 2016

Protection of operator work stations is provided by installation of anti-virus application. Intrusion Protection System (IPS) is proposed against physical endangering of facilities. Control of network equipment and links is provided by Network Management System (NMS). Approach to applications is enabled using authentication system – each particular user enters its username and password. Authentication is based on role that user has within the system, and all actions are subject of monitoring. Access to data from the corporate network is enabled only via firewall, and only to servers within DMZ, that have copy of data necessary for performing of integrated services. Choice of software, updates and use of antivirus applications are strictly controlled, to avoid any loss of information because of slow down of processes.

In the third aspect, its own business premises, ENTEL established the ISMS supported by the following documents within ENTEL IMS (EPE 2024) - procedure EN-27P-01: Information Security management, procedure EN-27P-02: Personal Data Protection and instructions EN-27I-01: Information security techniques.

A particular segment of the EN-27P-01 procedure is dedicated to business continuity assurance. As part of this procedure, a risk assessment is provided, which represents the elements of the Business Impact Assessment (BIA), and through a particular document - the Business Continuity Plan (BCP), activities and participants are provided for recovery in the event of an emergency situations such as malicious software, failure of key equipment, interruption of communications with the Internet service provider, etc.

In addition, the BCP document defines maximum acceptable levels for each of the key services (e-mail, File Transfer Protocol - FTP, File Server, Document management system -DMS, Correspondence Exchange Management System - CEMS and ENTEL's information system - ENTIS) - Maximum Allowable Downtime (MAD) and Recovery Time Objective (RTO). All activities and technical solutions, including software and equipment, are aimed at ensuring that the target recovery time for all services is less than the maximum acceptable interruption time, i.e. to be RTO < MAD. Additionally, within the BCP ENTEL document, it was foreseen the

establishment of a DR location at a distance of more than 10 km as the crow flies from the Energoprojekt office building, and a selection of key information was made that is stored at that location and regularly updated.

6. CONCLUSION

Business continuity represents very important issue for any organization, especially in situation when business activities are endangered from large number of impacts in complex business environment. At the same time, the rapid breakthrough of information technologies in all aspects of our life caused that we are faced with the problem of information security. Both areas, business continuity and information security are subject of international management standards, series ISO 22300 and ISO/IEC 27000 successively. These standards provide a valuable framework that enables these topics to be approached in a systematic way. After a brief review of the basic elements contained within the relevant standards, the emphasis is placed on their mutual connection, and especially on the role of the Disaster Recovery location. Finally, the mutual intertwining of these standards within the integrated management system is illustrated by a practical example in the case of a particular organization

REFERENCES

EPE (2024) Energoprojekt Entel plc Belgrade IMS documents 2022-2024

ISO (2019) Security and resilience – Business security management systems – Requirements (ISO 22301)

ISO (2020) Security and resilience – Business security management systems – Guidance on the use of ISO 22301 (ISO 22313)

ISO (2021) Security and resilience – Vocabulary (ISO 22300)

ISO/IEC (2018) Information technology - Security techniques - Information security management systems - Overview and vocabulary (ISO 27000)

ISO/IEC (2022a) Information security, cyber security and privacy protection - Information security management systems - Requirements (ISO 27001)

ISO/IEC (2022b) Information security, cyber security and privacy protection - Information security controls (ISO 27002)

ISO/TS (2021) Security and resilience – Business security management systems – Guidelines for business impact analysis (ISO/TS 22317)

Rakovic (2017). Rakovic R. Information Security – Fundamentals and guidelines, Belgrade: Akademska misao (in Serbian)

Rakovic et all (2016). Rakovic R, Mandic Lukic J, Cukic N: „Information Security in Electric Power Utilities' Environment", First South East European Regional CIGRÉ (SEERC) Conference, Portoroz, 6-8 June 2016, paper 1252, pp 1-8