Risk Management & Business Continuity Plan as fundamental activites for an implementation of Information Security Management Systems

Zoran Ćosić, *Statheros ltd., Kaštel Stari, Croatia,* Marija Boban, *University of Split - Faculty of Law, Split, Croatia,* Jasmin Ćosić, *Ministry of Interior,Bihać, B&H*

***Abstract*— This paper addresses to the importance of establishing the information security management systems (ISMS) as a foundation for managing an organization's information security risks. Probability of company's business success depends on the efficient design and implementation of the ISMS that is influenced by actual company needs and objectives, security requirements, employed business processes and organizational overall business risks. Further the authors will give the presentation of the fundamental activities of Business Continuity Plan (BCP) methodology including the main process of operational continuity**

***Keywords* — information security, international standard, risk management, risk analysis, security threats, business continuity, operations continuity, impact analysis**

I. INTRODUCTION

INFORMATION is the lifeblood [1] of business and organisations are increasingly dependent on the use of information systems and networks to process information. Computer 'literacy' is now widespread making systems ever more open to abuse, whether deliberate or accidental. Consequently, businesses are increasingly at risk through use of the very tool introduced to increase efficiency, i.e. information technology (IT). Managers must therefore address these risks where they would affect their systems and the information used on them in terms of:

- confidentiality
- integrity
- availability.

CIA triad (confidentiality, integrity and availability) make the core principles of information security.[2] In the increasingly interconnected business environment, information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities [3]. Information can exist in many forms: it can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected. It is important to stress that information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

ISO 27001 defines Risk Analysis as "systematic use of information for identification of cause and risk evaluation" where under risk is implied "probability that one threat will seize assets vulnerability and cause loss to organization".[4]

Risk analysis is integral part of activity that is a lot wider than Risk Management activity focused on risk control to which organization is oriented.

There are several international standards that point out importance of this kind of activity, which receives strong signals from international banking standards (Basilea 2), as well as growing interest for operation continuity and general security specially coming from recent political situation (activity reliability and campaign against terrorism).

Among this standards the most renowned are: ISO/IEC 27001 and 13335, COBITv4, ITIL and others less noted..[5]

II. ISMS IMPLEMENTATION & SECURITY MANAGEMENT

Modern security management systems now acknowledge that most risks cannot be completely eliminated and that they need to be managed in a cost effective manner. This paper will concentrate on the development of a methodology for the assessment and analysis of threat and vulnerabilities within the context of a security risk management. We will discuss a threat and vulnerability assessment method developed with the needs of mobile computer systems in mind. This method consists of four stages: a) Assessment Scope, b) Scenario Construction & Modelling, c) Threat Agent & Vulnerability Analysis, and d) Stakeholder Evaluation. This method actively involves stakeholders and focuses upon a technical, socio-technical and business aspect of the system.[5]

A. *Information system vulnerability*

In IT sector the goal of risk analysis activity is to perceive and quantify real risks to which Information System is vulnerable to. Risk expresses probability to occur unwanted event to security system with harmful consequence to system. According Business Dictionary threat is defined like: "action or potential occurrence (whether or not malicious) to breach the security of the system by exploiting its known or unknown vulnerabilities" [6]. To each external threat corresponds weak or critical point inside system that is defined as *vulnerability*. During risk definition there is direct correlation between probability to occur harmful event and system vulnerability. Testing system vulnerability i.e. threats and probability to occur harmful events represent center of Risk Analysis activity.

Consequences[7] to system, caused by threat, depend of course on asset value and consequence analysis for each typology of events represent another important aspect of risk analysis process. Risks are analyzed by determining harmful event impact according to potential damage value and probability of harmful event occurrence.

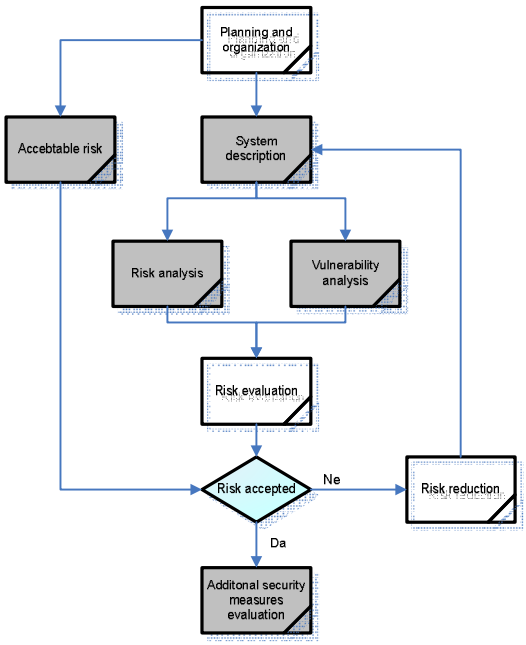

Fig. 1. Process of system vulnerability analysis

A.1 Planning and Organization:

- Selection of adequate risk evaluation method and qualitative and quantitative approach
- Definition system perimeter
- Identification of demands for business, legal and normative security information
- Organizational predisposition and process coordination

A.2 System Description

Perimeter research, drafting of procedures list, asset and countermeasures as well as their evaluation.

A.3 Threat Analysis

Identification of threats to company asset security and active countermeasures.

A.4 Vulnerability Analysis

Identification of innate vulnerability for each and every company asset typology.

III. RISK ANALYSIS METHODOLOGY

A. *Terminology*

Used terminology and term definitions are as follows:

Asset- private information system resources or resources related to them, required for properly organization functioning in order to achieve goals set by company governance.

Endangering- reduction of asset value because of concretization of threat

Countermeasures- procedures or technological mechanisms for risk reduction

Influence- consequence of concretization of asset threat

Threats- events that can cause accident in organization by creating material and immaterial loses (loss of service process continuity, loss to image of organization etc.)

Risk- estimation of exposure level to concretization of asset threat in relation to possibility of harmful event

B. *Methodological approach*

B.1. *Step 1: Asset*

Crucial asset for company activity is represented with information or data that company disposes of. Starting with them we can identify other important asset typologies:

- Services based on specific or essential data
- Informatics programs for data analysis
- Informatics instruments that contain data, applications or services
- Media for data storage
- Auxiliary informatics tools that complete informatics material
- Communication network that allow data interchange
- Structure in which are set informatics and communication resources
- Personnel that uses or controls above mentioned elements

Asset of general character is represented with data or services. In each case, it depends on other asset typologies as informatics tools, communication tools and personnel that uses or controls them. Because of everything that is mentioned, of enormous significance is interaction dependence concept between different asset typologies or measures in which higher rank asset can be endangered by lower rank asset security accident.

Division of asset by rank represents presentation of interaction cause-effect connection and allows calculation of information total risk.

Level of importance can be described as follows:

Level 3:Infrastructure that is necessary for functioning of others levels of importance (electric energy, acclimatization, personnel, objects)

Level 2: Information, data, company responsibility functions

Level 1: Other asset (company identification, image etc.)

Each type of property requires the following:

- Users or informations authenticity
- Privacy
- Integrity
- Availability
- Traceability

The property has to be valuated. That can be realized by using quality and quantity scales.

The use of quality scale speeds up the activity. It is positioning the property value as relative relation against the rest of property. At the end, the result does not show the absolute value of risk in money. It shows risk valuation considering order of relevance[8].

B.2. Step 2: Threats

In this step we define threats that might compromise all types of property. The threats include natural disasters (flood, earthquake) and problems with electric power that can harm passive information systems. We should consider also the threats from man's behavior that can be malicious or accidental damages. All types of threats do not consider all types of property, but there is a certain relation between types.

When we determine what threat can affect the certain property, we also determine the level of sensitivity for each type of property. We use the following parameters:

- **endanger**: what is the result of endangered property (per cent)
- **frequency:** how often we verify the threat (in one year)

TABLE I.

PRESENTANTION OF ENADAGEMENT AND FREQUENCY OF THREAT VERIFICATION

frequency	*Definition*
100	Very often
10	Often
1	Normal
1/10	Rarely

B.3. Step 3: Countermeasures

The risks and influences on companies property must be considered as the property is not protected. Some threats can be eliminated by better process organizing and some require technical solutions, protection and Human resources management. The countermeasures are used for risk analysis in 2 ways:

1) By reducing threats frequency,

These are so called preventive countermeasures.

2) By limiting volume of damage

These are so called corrective countermeasures. They prevent the systems endanger, so the consequences are limited.

B.4. Step 4: The definition of impact on property

If we know the value or importance of property and the level of systems endanger, it is possible to analyze the impact of incidence on system.

It is often that systems value is concentrated on data or services, that it is offering, while threats are pointed to the medias that contain data.

There are 2 types of impact analysis:

a. Cumulative impact

It is analyzed considering the cumulative value of property (own value and related value) and the threats that is exposed to.

b. Reflected impact

It is analyzed considering the estimated value of property considering and the threats considered by the values of the asset that is exposed to.

Both impacts are analyzed for each type of property, for each level and level of importance.

B.5. Step 5: Determination of risk

There are 2 ways to evaluate the risk:

a. Cumulative risk

It is valuated for property considering the cumulative impact, that is connected to threat and its frequency.

Cumulative risk insures the determination of countermeasures that are relateted to protection of working environment (safe copy of data, computer protection).

b. Reflective risk

It is analyzed for each property considering the reflective impact, that is connected with threat an its frequency.

Reflective risk that is calculated for property that has its own value, insures the determination of consequences related to technical incidents, that affect Information security system. This parameter is very important for management decisions in order to accept the certain level of risk.

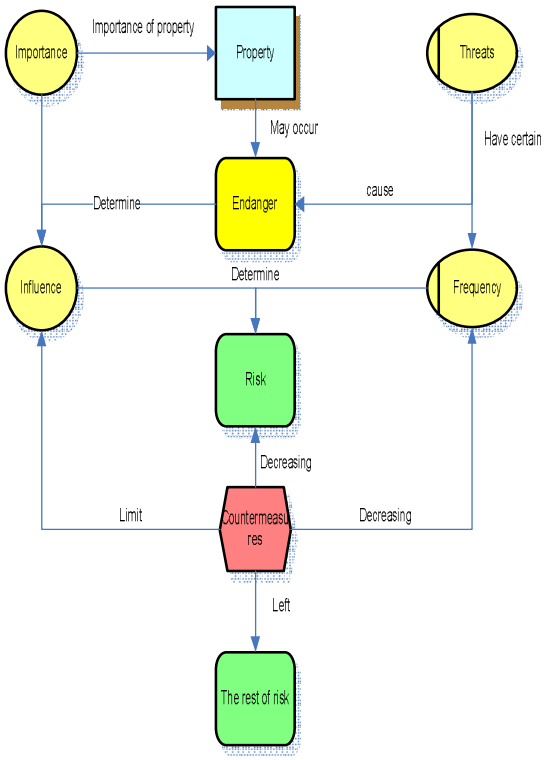

Fig. 2. The risk evaluation methodology

IV. BUSINESS CONTINUITY PLAN REALISATION

A. *Importance of BCP*

Business continuity planning (BCP) [9] is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. In plain language, BCP is working out how to stay in business in the event of disaster. Incidents include local incidents like building fires, regional incidents like earthquakes, or national incidents like pandemic illnesses. BCP may be a part of an organizational learning effort that helps reduce operational risk associated with lax information management controls. Process of BCP may be integrated with improving information security and corporate reputation risk management practices. BCP may be a part of organisational development strategy and operational politics that helps reduce risk associated with lax information management controls. This process may be integrated with improving information security and corporate governance and best risk management practices.

Every organization is at risk from potential disasters that include:

- Natural disasters-floods, earthquakes and fire
- Accidents
- Sabotage
- Power and energy disruptions
- Communications, transportation, safety and service sector failure
- Environmental disasters such as pollution and hazardous materials spills
- Cyber attacks, hacker and social engineering activity.

Creating and maintaining a BCP helps ensure that an organization has the resources and information needed to deal with these emergencies.

A BCP typically includes five sections:

1. BCP Governance
2. Business Impact Analysis (BIA)
3. Plans, measures, and arrangements for business continuity
4. Readiness procedures
5. Quality assurance techniques (exercises, maintenance and auditing)

B. *Methodological approach*

Process by which is managed with operational continuity may be represented in a following way:

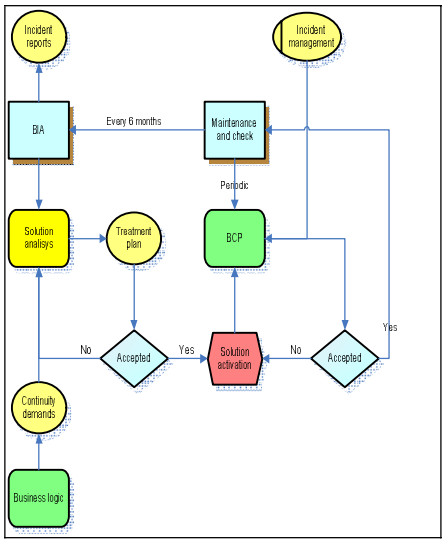

Fig. 3, Process by which is managed operational continuity

Business continuity management[10] is consisted of five macro activity that can be described as follows[1]:

B.1. Incident Impact Analysis on Business Processes (BIA) [11]

First step is consisted of analysis of business processes included in perimeter of information security system with special emphasis and attention on resources that are capable of blocking these processes and on importance of processes in relation to time of interruption.

System analysis has been performed during activities of integrated system implementation.

[1] Composing of this operational procedure is based on documents published on national and international level, and it is referred to continuous functioning since BS 25999-1 Scheme (august 2006)

B.2 Impact Treatment as a Result of Analysis

Based on BIA results analysis, solutions are produced to satisfy business processes operational continuity demands defined by Board of Directors decision and client demands.
Risk treatment plan includes solutions for prevention and risk management, approved by Board of Directors, that are applied based on risk analysis with the goal of company's risk exposure reduction in the period of next 6 months.

B.3 . BCP Drafting

Risk treatment plan is approved and implemented and on base of that should be prepared BCP.
BCP, as reference for business processes management, includes following elements:

- Checklist for beginning and conduct of plan (e.g. who goes where, where are placed dislocated equipment, who has to be reported and for what, evaluation criteria)
- Dislocation and availability of important information (e.g. insurance policies, supplier's lists etc.)
- Roles and responsibility (internal and external)
- Connections with Incident Management
- Necessary resources for operational continuity guarantee
- Procedures for operational continuity guarantee

Plan must be approved by top management.

B.4. Checking, maintenance and periodical testing of BCP

Periodical revision of BCP is done for taking into consideration possible changes in processes, asset and services of company. Minimum period of BCP revision is 6 months.
BCP, if possible, is tested in its all components at least once a year, simulating critical situations.

B.5. Updating BCP Support Plans

Parallel with afore-mentioned activities, it is necessary to valuate possible creation of documents that serve as support for easier implementation of BCP,.

The most important documents of this type are:

✓ ***Incident Management Plan (IMP)***

It guarantees safety of persons included in implementing of activity and is focused on minimizing of loos. It usually includes:

- Activities plans that follow after determining problems inside BIA
- Strategies of internal and external communication
- Area of primary and secondary incident management control and their characteristics (redundant communication)

✓ ***Disaster recovery plan (DRP)***

If incident is connected with natural disaster that disable resumption of operational continuity on master location, set up plan of business activity resumption is implemented

V. CONCLUSION

This paper gives an overview of implementing the efficient design and implementation of the Information security management within fundamental activities of Business Continuity Plan (BCP) methodology including the main process of operational continuity Business Impact Analysis (BIA) and definition of it's main components. Creating of the BCP, is influenced by actual company needs and objectives, security requirements, employed business processes in order to avoid organizational overall business risks. The risk analysis is presented on the actual project of implementing risk evaluation methodology in three phases. The chosen method presents the key of successful implementation of risk analysis as the most important subject of data security in digital economy. Without using of this or any other methods, it is not possible to manage the organization's information security threats, risks and it's vulnerability.

VI. REFERENCES

[1] M.Boban, Z.Ćosić, Information security management systems as Fundamental requirement for business success, MIPRO 2007, Opatija, Croatia
[2] J.Ćosić, A.Medić, Information security, standard and state in B&H Institutions (on croatian), M&S conference, Čakovec, Croatia, 2010
[3] OECD Guidelines for the Security of Information System and Networks,Available at: http://www.oecd.org/dataoecd/16/22/15582260.pdf
[4] ISO/IEC 27001:2005, International Standard
[5] Aligning CoBit, ITIL and ISO 17799 for Bussiness benefit: Management summary, itSMF International, The IT Service Management Forum,2005
[6] S.Vidalis, A. Blyth, Understanding and Developing a Threat Assessment Model, School of Computing, University of Glamorgan, Pontypridd, Wales, UK.October 2002
[7] Business Dictionary, available at: http://www.businessdictionary.com/definition/threat.html
[8] B.L.Turner, Roger.E.Kasperson, A framework for vulnerability analysis in sustainability science, National academy of science 2003
[9] Z.Ćosić, M .Boban, Business continuity plan methodology – challenges of risk management on the way to business success in digital economy, M&S 2009, Čakovec, Croatia
[10] Hecht, Jeffrey A, (2002) "Business Continuity Management," Communications of the Association for Information Systems: Vol. 8, Article 30.
[11] Lorin M.Hitt, D.J.Wu, Xioaoge Zhou, Journal of management Information systems, Summer 2002