METHODOLOGY AND ALGORITHM OF INFORMATION SECURITY RISK MANAGEMENT FOR LOCAL INFRASTRUCTURE

Bulai Rodica, Ciorbă Dumitru, Poștaru Andrei and Rostislav Călin[1]

Abstract

The complexity of information security does not resume to mere technicality, transferring significant liability to proper management. Risk analysis in information security is a powerful tool that comes in handy for managers in making decisions about the implementation of efficient information management systems, in order to achieve the organization's mission.

As a part of risk management, risk analysis is the systematic implementation of methods, techniques and management practices to assess the context, identify, analyze, evaluate, treat, monitor and communicate the risks for the information security and systems through which they are processed, stored or transmitted.

The ISO/IEC 27005:2011 – Information security risk management, does not specify any particular method for managing the risks associated with information security, but a general approach. It is up to the organization to devise control objectives that would reflect specific approaches to risk management and the degree of assurance required.

There are several models, methodologies and tools amongst which those like CRAMM (United Kingdom, Insight Consulting), Risicare/Mehari (France, Clusif), GSTool (Germany, IT-Grundschutz). The theoretical model of the mentioned methodologies is hard to put in practice without experience required from the members of the risk analysis team. Using the appropriate risk assessment solution, an organization can devise its own security requirements.

1. Introduction

In an *information era*, we cannot and must not ignore the factors that can have a negative influence on the smooth running of daily activities of the society. In each of our daily activities, we operate with information, which has different sensitivity levels depending on the damage its compromising can cause on the individual or organization to which it belongs.

The organizations, no matter of which type, have begun to realize more and more the essential role of information in fulfilling their objectives. The growing tendency of globalization and internationalization of the economy requires a constant exchange of information with other organizations and agencies in order to obtain the necessary managerial knowledge to ensure competitiveness and efficiency.

[1] Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, 7 Studentilor str., Chisinau, MD-2012, Republic of Moldova, Tel:(37322) 509908; E-mail:rodica.bulai@ati.utm.md, dumitru.ciorba@ati.utm.md, andrei.postaru@ati.utm.md, rostislav.calin@ati.utm.md

Certainly, the increasing importance of this resource led to a proportional escalation of potential threat to it, also a favored fact by vulnerabilities presented by the systems through which the information is managed.

In order to establish coherent, efficient and effective information protection measures, the information security management has become an integral part of organizational management, whether it refers to governmental, private and international organizations.

In this regard, the security level to be targeted for information must be in full correspondence with the value of information and the damage that its misuse may cause - disclosure, degradation or lack of availability.

At the same time, security measures must take into account the operational environment vulnerabilities and the threat environment, justifying the application of a measures complex. This demonstrates that the costs of providing protection against threats to information increase with threats and vulnerabilities rise, therefore, it requires a reasoned justification.

2. Information Risks Management

At local level, decisions on information security risks management within organizations, most often, are insufficiently substantiated, sometimes ad hoc, empirical, correction oriented, and therefore inadequate in terms of safety and inefficient in terms of cost. This practice leads to negative effects, including:

- Confidentiality, integrity and availability affecting, if the implemented security systems are not designed to cope with possible threats;

- The allocation of oversized budgets for information security;

- The decrease of employees work performance through the implementation of inefficiently designed security systems, that lead to impaired of information availability, resources and services of information and communication systems within the organization;

- The necessity of taking decision to remedy the effects of an incident affecting information security by implementation of punctual corrective measures, which are more expensive and less effective than if preventive measures had been implemented from the start.

The information security risk analysis represents a powerful tool that managers have in the decision-making process in order to implement efficient information management systems and, ultimately, to fulfill the organization's mission. As part of risk management process, the risk analysis represents the systematic implementation of methods, techniques and management practices for context evaluation, identification, analysis, valuation, treatment, monitoring and communicating risks regarding information security and systems, by which these are processed, stored or transmitted.

To be efficient and effective, the risk analysis of information security must be an integral part of risk management carried out by the organization for its entire range of activities and therefor, objectives. The fluid nature of technological environment requires, however, the need to review the results of the information security risk analysis through regular reruns of this process. Various qualitative and quantitative risk analysis methods have been developed in this direction, the purpose of which is to analyze as accurately as possible the risks the organization's information is exposed to.

Another element that must characterize risk analysis process is that the process must be extended throughout the life cycle of a business, project, product or any other asset that may be affected by the compromising of information managed across the organization. Applying risk analysis at the planning stage of an information management system leads to significant benefits like reduction of development costs, functionality and integration improvement, as well as raising the awareness of possible risks and the countermeasures to be applied for their management.

3. Information security risk management methodology

For this purpose, we intend to recommend a modern methodology of information security risk management, which would positively influence the way managerial decisions are made, whatever the type of organization is. In addition, it has to provide objective arguments for decision making in the identification of internal and external risk factors regarding information managed by the organization, as well as the threat factors trends. The methodology must directly support the efficient and effective use of human, material, financial and information resources of that organization, based on appropriate risk analysis that may have an impact on the security of information handled by the organization.
The proposed methodology is based on the analysis made on the current and well-known standards and methodologies, such as NIST 800-30, ISO / IEC 27005: 2011, AS / NZS ISO 31000: 2009, Mehari, CRAMM, BSI-Standard 100-3 (IT -Grundschutz), as shown in table 1. It contains nine basic steps.

NIST 800-30[1]	**ISO/IEC 27005:2011**[2]	**AS/NZS ISO 31000:2009** [3]	**BSI-Standard 100-3** [4], **IT-Grundschutz** [5]	**MEHARI** [6]	**CRAMM** [7]
National Institute of Standards and Technology, USA	*Information security risk management standard*	*Joint Australian New Zealand International Standard*	*Federal Office for Information Security – BSI), Germany*	*Clusif, France*	*Insight Consulting United Kingdom*
System Characterization	Context establishment	Establishing the context (external, internal, risk criteria)	Preliminary work	Identification of the risk - assets, vulnerabilities, asset damage, threats	Identification and valuation of assets
Threat Identification	Information security risk assessment	Risk assessment	Preparing the threat summary	Impact evaluation	Risk identification and assessment
Vulnerability Identification	*Risk identification* (assets, threats, existing controls, vulnerabilities, consequences)	*Risk identification*	Determination of additional threats	Constraint evaluation	*Threat and vulnerability assessment*
Control Analysis (current and planned)	*Risk analysis* (Qualitative and Quantitative)	*Risk analysis*	Threat assessment	Evaluation of the protection factors – palliative and recovery	*Risk calculation* (Qualitative)
Likelihood Determination	*Risk evaluation*	*Risk evaluation*	Handling risks	Evaluation of the probability - the possible risks are evaluated	Risk Management identification and selection of countermeasures
Impact Analysis (Integrity, Availability, Confidentiality)	Information security risk treatment	Risk treatment (Preparing and implementing risk treatment plans)	Consolidation of the security concept	Impact evaluation, not considering the countermeasures taken	
Risk Determination	Information security risk acceptance	Monitoring and review	Feedback to the security process	Impact evaluation after countermeasures	
Control Recommendations	Information security risk communication and consultation	Recording the risk management process		Identification of the global risks for the organization	
Results Documentation	Information security risk monitoring and review			Taking the decisions to accept the risk or not	

Table 1. Comparison of processes of Information security risk assessment

3.1 Getting the support of the administration

The success of the risk management and analysis depends greatly on the level of involvement and support of top management. Namely, the top management is responsible for initiating the process,

activities coordination and ensuring the reporting in sufficient time. Although its involvement may not be direct, the support of management is essential. Specific tasks of the top management in the process of risk analysis can be:

- Selection and appointment of the team, including the team leader;
- Delegation of authority and responsibility for this task;
- Review and support of the obtained results;
- The final decision making regarding the implementation of certain security measures.

The team leader should be involved in selecting the team members and draw up the plan to perform the necessary activities and to ensure that they will be made in due time. He will also coordinate the preparation of reports for the top management. The number of team members can vary, depending on the size of the organization, however it is advisable to have not less than three, or at least one representative of each subdivision that actively use information resources. The team members must be carefully selected, ensuring their competence in the business processes that take place within the subdivisions they belong to and the way these processes depend on information technologies.

3.2 Description of the organization's information infrastructure

At this stage, information resources and their interdependence are identified (e.g. what system, what data does it manage, what technologies are used, where it is located and whom is it managed by). The limits of the system are determined and a description of the hierarchical information infrastructure of the organization is made in order to easier identify the possible vulnerabilities and define the level of protection provided by the existing control measures.

Information resources are considered here to be:

1. *Information* – information stored electronically and on paper: system and process procedures, work instructions, regulations, system documentation, design documentation, contracts and agreements, financial and accounting documents, personnel files etc.;
2. *Hardware* – server equipment, network equipment, workstations, printers, mobile/media devices, physical security equipment;
3. *Software* – *t*he organization's subsystems and applications, database servers, application servers, portals and Web services;
4. *Personnel* – internal staff and third parties personnel involved in the contractual relationship;
5. *Location and facilities* – premises infrastructure, fixed assets, services and facilities;
6. *Organizational* – contracts / projects in progress, enterprise reputation and image, web site.

Resources are classified in terms of information:

P = Public; *R = Restricted (internal use);* *C = Confidential*

It also suggested to group the resources (e.g.: workstation, printer, documentation) and to record the information on the person responsible for each identified resource.

The owner is not necessarily the resource user, e.g.: the resource "workstation", which is a single heading in the classification of resources, designating all workstations that are exposed to the same type of threats and vulnerabilities, can stand for all the workstations in a department, or on the same floor or a location. In this case, the owner can be the head of the department, the IT manager etc. and not users.

The risks owner is established for each category of resources. It can be the organization administrator or a person nominated by him (subdivision chief, manager or coordinator). The result of this phase may be a list (or multiple lists, for each category separately) with all information resources identified within the organization.

3.3 Information resources classification

It is needed to determine the priorities for their protection. Resource classification criteria are established taking into account the criticality level, the impact of resource unavailability, the cost of resource fail, confidentiality, integrity and availability fail, etc. The classification of resources should take into account the interdependencies between them. The number of resources in each category is arbitrary, but it is preferable to limit the number of critical resources to avoid confusion. The result of this phase is the classification of priority information resources in terms of their level of criticality.

- *Critical resources* – resource owning organization or subdivision cannot continue working without that resource.

- *Essential resources* – resource owning organization or subdivision can continue working, but for a specified period of time (hours or days), so the resource has necessarily to be restored.

- *Normal resources* – resource owning organization or subdivision may continue working for a long time, however, some people will be partially affected, being forced to find alternative.

A method for the identification and ranking of critical resources by team members is presented in Table 2.

RESOURCE LIST									
No.	Resource type	Resource category	Resource code	Resource	Classification	Owner	Location	Value	Description

Table 2: Resource list

3.4 Threats and vulnerability identification

The purpose of this step is to determine potential sources of threats and vulnerabilities for the analyzed IT infrastructure. Based on History of system attack, Data from intelligence agencies, mass media etc., the threats to an organization's information security can be identified and have different dimensions:

- **Of human nature:** *deliberate actions* (e.g.: unauthorized access to data and system, DOS/DDOS, traffic interception/modification, malicious code/software, data or equipment theft or destruction, social engineering, etc.) and accidents – operating errors.

- **Of technical nature -** power outage, equipment failure, etc.

- **Environment -** natural disasters or other external conditions (e.g.: contamination, electromagnetic interference).

Vulnerability identification sources can be: Previous risk assessment documentation of the IT system assessed, The IT system's audit reports, system anomaly reports, security review reports, and system test and evaluation reports, Vulnerability lists or database, Incident Advisory Capability bulletins, Vendor advisories, Commercial computer incident/emergency response teams and post lists, Information Assurance Vulnerability Alerts, System software security analyses, Automated vulnerability scanning tool, Security test and evaluation, Penetration testing.

The threats and vulnerabilities should be identified separately for each resource and included in the list of threats and vulnerabilities, Table 3. This list will be reviewed annually or after some unforeseen security incidents. Existing means of protection implemented by the company are also considered.

List of threats and vulnerabilities		Means of protection
Vulnerabilities	Threats	
INFORMATION		
HARDWARE		
SOFTWARE		
PERSONNEL		
LOCATION and FACILITIES		
ORGANIZATIONAL		

Table 3: Threats and vulnerabilities list

3.5 Determining the impact and probability of risk information

At this stage the probability of a security incident is analyzed, which depends on threats, vulnerabilities and existing security measures set out in the previous step.

The impact and probability of each threat and vulnerability is quantified as follows.

Probability value:

1 = *low* - the occurrence of an incident within three years is unlikely;

2 = *medium* - the effects can occur within two or three years;

3 = *high* - likelihood of one or more incidents a year.

For risks associated with the location of the organization (terrorism, social unrest, natural disasters) incidents in the area of the locality are taken into account.

The impact value is determined, at least in the first iteration, based on the same considerations as in the case of establishing the resource value [8].

Impact value:

1 = *normal* - the impact on the confidentiality, integrity and availability of the normal resources is insignificant for the organization, no additional protection measures are required (e.g.: data about company structure);

2 = *essential* - the impact on the confidentiality, integrity and availability of critical media may damage the organization (e.g.: commercial data, data about orders etc.);

3 = *critical* - the impact on the confidentiality, integrity and availability of critical resources can cause great or even catastrophic damage for the organization (e.g.: the confidential documents of the organization).

3.6 Information risk assessment

This step consists of two approaches: qualitative and quantitative. The approaches are different in the metrics they use.

Qualitative risk assessment is based on the analysis of various scenarios that explore the impact of various potential and possible security incidents through a number of interconnected elements: threats, vulnerabilities and resources. Thus, the risk can be determined as: $R=R_{esource\_value}*V_{ulnerability}*T_{hreat}$.

It is also necessary to take into account several important assumptions for qualitative estimation of information risks, namely:

1. Each asset has its value and every asset is vulnerable or not;

2. If a system is vulnerable, there is at least a threat that can be achieved (threats and vulnerabilities depend on each other);

3. A threat has a certain probability of being achieved, depending on certain circumstances;

4. A threat has consequences that depend on the circumstances.

Based on the above assumptions, the risk can be calculated using the following formula:

$R=P_{robability}*I_{mpact}$, table 4.

Information risk	Probability	1	2	3
Impact (consequence)	1	1	2	3
	2	2	4	6
	3	3	6	9

Table 4: Information risk assessment

The risk hierarchy will be used to identify risk-handling options:

1-3: Minor: Maintain the existing security means
4-6: Significant: Planned corrective actions
7-9: Major: Priority corrective actions

Table 5: Information risk hierarchy

Risks that are considered insignificant have to be removed from the list. Risks should be explicitly identified in relation to one or more resources.

The quantitative approach uses two basic elements, namely the probability that a certain event will occur and the loss associated with this event.

It is recommended that losses to be estimated for a period of one year, so the following can determined:

- Estimated Annual Losses summed by categories of threats: (*EAL_a*$_i$),
- Estimated Annual Losses summed by categories of resources: (*EAL_r*$_j$), and
- Total Estimated Annual Losses Estimate for resource/threat pairs: *EAL*.

In both cases the calculation of total losses, by category of threats or categories of resources, the result should be identical. Thus, we can generate a threats/resources matrix that will contain the corresponding EALs for each resource, and respectively, each threat, and the global EAL:

	Resource r_1	**Resource r_2**	**…**	**Resource r_n**	**EAL_a$_i$**
Threat a_1	V_1xE_1	V_2xE_1	…	V_nxE_1	EAL_a_1
Threat A_2	V_1xE_2	V_2xE_2	…	V_nxE_2	EAL_a_2
…	…	…	…	…	…
Threat a_m	V_1xE_m	V_2xE_m	…	V_nxE_m	EAL_a_m
EAL_r$_j$	EAL_r_1	EAL_r_2	…	EAL_r_n	**∑ EAL**

Table 6: Threats/resources matrix

In this matrix, V_j is the value of the r_j resource, and E_i - the frequency of the a_i threat occurrence during a year.

Measures that can reduce vulnerability to the most expensive threat are identified. It is always envisaged that some measures can be applied for several categories of threats or for several categories of resources. The following objectives must be taken into account when selecting the protective measures:

- Return On Investment must be as high as possible: *ROI* = *r_c*EAL_a–C_c*, where *C_c* = annual cost for using the measure c, *r_c* = the effectiveness index for the measure c and *EAL_a* = Estimated Annual Losses for threat a.
- Minimizing of *EAL* (Estimated Annual Losses) [9].

3.7 Drawing up of information risk treatment recommendations

This phase aims at reducing the level of risk within the organization. For the risks placed in *Major* and *Significant* categories there are identified control means, helping to reduce, redirect or eliminate these risks. In this context, it is recommended to:

- Identify and document every solution that can be implemented. The solutions can be technical, manual or procedural. At this phase, it may be obvious that there is a single solution. In this case, it is necessary to argument why other solutions are impossible to accept;

- Justify each proposed solution. The obvious argument is problem solving, but it could happen that a certain solution can solve several problems simultaneously, fact that must be necessarily mentioned;

- Make a costs/benefits analysis for each proposed solution, including direct costs, staff training costs and future operational costs. In case of necessity, competent specialists within the organization can be consulted;

- Propose an implementation plan for the identified solution. The plan must take into account the priority of the resource and the impact the analyzed risk can have.

It is advisable to identify more solutions for removing the same risk, in this case the priority being given to solutions that enable the removal of a group of risks for a resource or group of resources.

After applying the selected measures, the new values of probability and impact are estimated, and the amount of residual risk is calculated. The owner of risk will approve the residual risk, Table 6. This table is filled in for each resource separately in accordance with the classification of resources and threats and vulnerabilities list.

No.	RISK ASSESSMENT AND SELECTION OF SECURITY MEASURES								
	RESOURCE TYPE: _____								
	Resource code: _____		Resource: _____						
	Vulnerabilities	Threats	Probability (Before the control mechanism)	Impact (Before the control mechanism)	Risk	Reduction/control mechanism	Probability (After the control mechanism)	Impact (After the control mechanism)	Residual risk

Table 7: Risk list

It is recommended to select control measures by Annex A of ISO / IEC 27001: 2013 and develop the risk treatment plan in accordance with the form of risk treatment plan, Table 7. This table is filled in for each type of resource separately, in accordance with the risk list.

No.	RISK TREATMENT PLAN								
	RESOURCE TYPE: _____								
	Vulnerabilities	Threats	Reduction/control mechanism	Objectives	Security measure	Responsible	Date	Resources needed	Achievement

Table 8: Risk treatment plan

The forms that are completed and coordinated with officers involved are included in a final report and addressed to the top management for the final decisions.

3.8 Results Documentation

After completing risk analysis (threats and vulnerabilities are identified, the risks are analyzed, and control means are recommended) it is required to make an official report or some brief instructions.

The report for the top management should contain:

- General information about the team involved (team leader, team members) and the analysis period;
- General comments on the information infrastructure, business processes that are supported by IT processes;
- The list of information resources in descending order of priorities (from the highest to the lowest);
- Informational risks;
- List of risks associated to information resources and means of protection;
- Risk treatment plan, etc.

The final report has to be discussed at the team meeting for the final consultations among team members and the necessary changes can be made. The last version, signed by all team members, is sent to the top management.

Finally, the success of a risk analysis depends on the involvement of the top management. The role of management, in addition to initiating the process, create the team and delegate responsibilities, is to analyze and support the results and proposals made during the risk analysis. The team leader should regularly inform the senior management about the progress and success of completing the risk treatment plan. This way a greater degree of involvement of top management and financial support for the implementation of the suggested solutions will be ensured. The final verdict on the solution to be implemented for each of the identified risks belongs obviously to the top management, but that should not be done without consulting the team. The implemented solution is going to be, most probably, not the most efficient, but it should be the best in terms of cost/benefit.

3.9 Information risk monitoring

This last phase target is to check that:

- risk responses are implemented according to the plan and produce the expected effect;
- symptoms for known risks can be detected;
- new threats and vulnerabilities are tracked, the appearance of identified risks and the detection of previously unidentified risks, but acting on the organization's activities;
- risk response plans and their performance assessment can be executed;
- risk management procedures are followed;
- residual risk for known risks can be determined;
- proposed contingency plans can be implemented;
- new alternative responses can be found;
- the required corrective and re-planning actions can be carried out.

For risk monitoring, it is necessary carefully to measure technical performance for symptoms, regularly rerun qualitative and/or quantitative risk analysis and document any response to risk so that it can be easily used. It is also very important to inform those involved in symptoms and new risks identification about all the changes caused by responses to those risks and resumption of risk management activities: identification, analysis, and response plans preparation.

4. Conclusion

By Government Decision nr. 811 from 11.29.15 (Official Monitor nr.306-310 art.905) was adopted The National Program for Cyber Security of Moldova Republic for 2016-2020, which is oriented towards the implementation of four key components, namely:

1) Introduction of minimum mandatory requirements of cyber security and cyber security national standards for the processing, storage, transmission, storing and secure data access;

2) Certification and authorization of specialists and information systems according to the approved standards;

3) *Cyber security periodical conducting audit of information systems and electronic communications networks* within public authorities and other entities possessing information systems of vital importance to society;

4) Introduction of prescriptions and penalties for non-compliance the minimum-security requirements and national standards in the field.

In February the current year, the Government of Moldova adopted the mandatory minimum requirements of cyber- security.

In the context of the above, we consider that management and risk analysis is required to be approached not as a project activity (finite time) but as an ongoing process. The proposed practical method can be a good start for this process, for the organizations of Moldova Republic, where the information risks are addressed more intuitive on operational level, further activities being necessary for monitoring the implementation of the solutions selected and the developments taking place after.

The existence of a strategic planning that would be based on an analysis of identified risks to the information managed by the organization, will increase the safety culture in organizations in the country, both within the state and the private ones, regarding specific cyber threats and vulnerabilities, which can negatively impact the vehicle information and therefore, on the interests of the organization.

5. References

[1] Guide for Conducting Risk Assessments. National Institute of Standards and Technology. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[2] ISO/IEC 27005:2011. Информационная технология - Методы и средства обеспечения безопасности – Менеджмент риска информационной безопасности. https://exebit.files.wordpress.com/2013/11/iso-27005-2011-ru-v1.pdf

[3] Joint Australian New Zealand International Standard AS/NZS ISO 31000:2009. Risk management – Principles and guidelines. http://www.risknz.org.nz/files/2714/0868/4677/31000.pdf

[4] BSI-Standard 100-3 Risik analysis based in IT-Grundschutz https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_1003_e_pdf.pdf?__blob=publicationFile

[5] BSI-Standard 100-2 IT-Grundschutz Methodology https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_1002_e_pdf.pdf?__blob=publicationFile

[6] Mehari. Privire genrala. http://meharipedia.org/wp-content/uploads/2016/12/CLUSIF-2010-Privire-generala-MEHARI.pdf

[7] www.cramm.com

[8] The Security Risk Management Guide, Microsoft Solutions for Security and Compliance and Microsoft Security Center of Excellence, http://trygstad.rice.iit.edu:8000/Books/TheSecurityRiskManagementGuide-Microsoft.pdf

[9] BULAI RODICA, Estimarea cantitativă şi calitativă a riscurilor informaționale, Conferința internațională *Securitatea Informațională 2013*, ASEM, Chişinău, 2013, http://security.ase.md/materials/publications/pdf/SI2013_conference_book.pdf