Vulnerability assessment — one step further towards a better safety

Stefan G. KOVACS,INCDPM ”Alexandru Darabont”, Bucharest, Romania

Eugenie POSDĂRĂSCU, Hyperion University, Bucharest, Romania

Vulnerability assessment has many things in common with risk assessment. Assessments are typically performed according to the following steps:

1. Cataloguing assets and capabilities (resources) in a system.
2. Assigning quantifiable value (or at least rank order) and importance to those resources
3. Identifying the vulnerabilities or potential threats to each resource
4. Mitigating or eliminating the most serious vulnerabilities for the most valuable resources.

The paper is based on research done by INCDPM inside the iNTeg-Risk FP7 project and presents a methodology for vulnerability assessment as a preliminary step towards a comprehensive integrated assessment vulnerability- safety-occupational risk. The methodology was developed on the IT concept of vulnerability evaluation together with the US referential regarding vulnerability assessment of critical infrastructures.

The presented method was tested in 50 SME s from the construction industry and manufacturing in order to serve as the basis for an integrated approach- including also quality and environment protection. The main results are also shown in the paper.

Keywords: vulnerability assessment, risk

Introduction

Vulnerability is not a new or modern concept. Before risks and hazards, vulnerability was used to define the exposure of an individual or of a facility to a potential aggression. An individual could be exposed to illnesses, a house to natural disasters, and a facility to malevolence.

So, vulnerability could be divided into:

- individual vulnerability which could be:
    1. physical-takes into account the genetic aspects and also the acquired work consequences like stressed.
    2. social-takes into account the position of the individual on the social ladder, his life goals and expectations, his relationship with colleagues and supervisors.
    3. economic vulnerability-if the individual is exposed he would try a strategy in order to find the necessary money. This strategy could be based on own work (to optimize his activity, to work supplementary hours) or could be based on antisocial and malevolent acts (Berkes, 1998).
- vulnerability of facilities-here being included from hand tools (being vulnerable to decay if not maintained properly) to complex process installations. Facilities are vulnerable to natural and malevolent aggression. In between they are also vulnerable to decay or damage occurring from work acts;
- vulnerability of community-communities are an aggregate of individuals and facilities .The individuals could lead to a vulnerability profile for the community if they have common characteristics-for example populations from a certain area are more exposed to specific aggressors than other populations. The facilities could have certain characteristics that could also increase the community vulnerability (for example nuclear facilities, process facilities near the houses, etc.).A community could also be affected by natural disasters like the Katrina (NRS, 2002).

Vulnerabilities could be studied, managed and in the end could be prevented and mitigated towards an ALARP level. All this process should be done on a systemic and scientific basis in order to have an appropriate and clear image of what is in place at this moment, what should be done, etc. A very important aspect is to prevent eliminated vulnerabilities to re-occur. In this respect a continuous control is needed.

Figure 1 shows the main things to do with vulnerabilities.

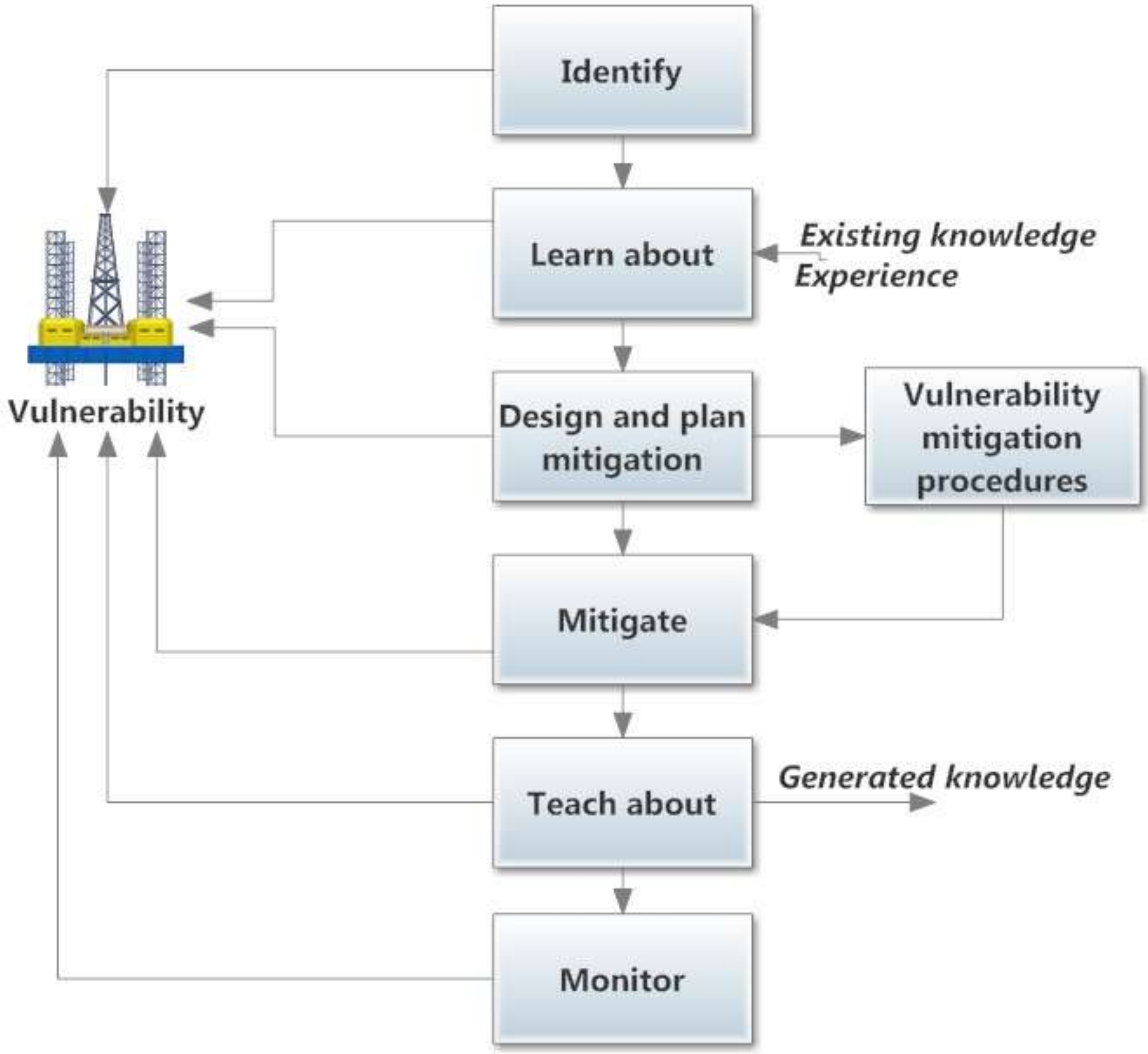

Figure 1 Steps in the treatment of vulnerability

As shown in the figure, vulnerability must initially be identified and we must learn about it. An already identified vulnerability- which is not mitigated- is a very serious problem for every management and a potential major event in happening. A good management would never allow such a vulnerability that is not mitigated below the ALARP level.

A vulnerability management includes the usage of existing knowledge (if we don t know nothing about the vulnerability we could not mitigate it) and also the generation of new knowledge in order to improve the mitigation process.

The paper shows some research based aspects regarding the usage of vulnerability and its derived concepts- like vulnerability assessment and vulnerability management in occupational risk management. Most of these aspects were developed during the preparation for the course Vulnerability Analysis and Return on Prevention Analysis developed inside the iNTegRisk project.

Vulnerability assessment — the first step towards an optimal management

A vulnerability analysis or assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. Examples of systems for which vulnerability assessments are performed could be found in every economic domain- they include, but are not limited to, nuclear power plants, information technology systems, energy supply systems, water supply systems, transportation systems, and communication systems.

Why analyse vulnerabilities and not risks? Vulnerability analysis and research could be a preliminary phase of risk analysis. It involves lesser costs and also could be done more quickly and with lesser resources. As risk is more general notion vulnerabilities could be specifically targeted. Usually, the elimination of vulnerability leads to the elimination of the linked risks. If a building is, for example, no more vulnerable to earthquakes then the risk of falling down is eliminated as the risk of being caught under the rubble. The notion of vulnerability, by itself supposes that some actions should be taken in order to eliminate or mitigate the vulnerability.

Vulnerability assessment has many things in common with risk assessment. Assessments are typically performed according to the following steps:

1. Distributing assets and capabilities (resources) in a system.

2. Assigning quantifiable value (or at least rank order) and importance to those resources
3. Identifying the vulnerabilities or potential threats to each resource
4. Mitigating or eliminating the most serious vulnerabilities for the most valuable resources

Vulnerability assessment is an important subset of the risk assessment process (see figure). It can be more prescriptive than risk assessment. Vulnerability assessment involves looking at the system elements and layout and their failure modes based on a given set of threats or .“attacks...” The vulnerability assessment answers the basic question, “what can go wrong should the system be exposed to threats and hazards of concern?” Line managers and technical staff at individual facilities or service provider organizations can perform a vulnerability assessment. Although risk is often calculated using the likelihood-cost equation, risk assessment ends with the judgment of stakeholders at the executive level of government and private companies. The determination of risk starts with the results of the vulnerability assessment and adds consideration of the likelihood of threats coupled with the economic, political and social consequences of the system failure. The end of the risk assessment process is a decision concerning whether or not to take action based on the acceptability of risks identified.

The mitigation phase should involve:

1. **Collection** – The company collects vulnerability reports in two ways: monitoring public sources of vulnerability information and processing reports sent directly to the company. After receiving reports, they perform an initial surface analysis to eliminate duplicates and false alarms, and then catalog the reports in a database.
2. **Analysis** - Once the vulnerabilities are catalogued, the company determines general severity, considering factors such as the number of affected systems, impact, and attack scenarios. Based on severity and other attributes, they select vulnerabilities for further analysis. The analysis includes background research, runtime and static analyses, reproduction in own test facilities, and consultation with vendors and other experts.
3. **Coordination** - When handling direct reports, the company works privately with suppliers and clients to address vulnerabilities before widespread public disclosure.
4. **Disclosure** - After coordinating with all the stakeholders, the company take steps to notify critical audiences and the public about the vulnerabilities. To the best of their ability, they produce accurate, objective technical information focused on solutions and mitigation techniques. Targeting a technical audience (administrators and others who are responsible for securing systems), they provide sufficient information to make an informed decision about risk (Downing, 2001).

The vulnerability assessment tool — methodology

The vulnerability assessment methodology has the following objectives:

1. Understand the facility/organization’s mission and mission-supporting systems and functions
2. Identify mission-threatening vulnerabilities of critical facility systems
3. Understand system design and operation in order to determine failure modes and likelihoods
4. If possible, identify consequences of system failures in terms of down time, effects on people, and any cascading effects on other systems and organizations.(While failure cost analysis is not an explicit part of a vulnerability assessment, such information may flow from return on prevention (ROP) analysis.) (Turner, 2003)
5. Recommend facility improvements to reduce vulnerability

The methodology is based upon the Improved Vulnerability Assessment Framework (IVAF) which was developed and improved as a response to the Presidential Decision Directive 63.

The **Improved Vulnerability Assessment Framework (IVAF)** that was developed here would act through a three-step process and will enable an economic entity:

- to define its Minimum Essential Infrastructure (MEI),
- identify and locate interdependencies and vulnerabilities of MEI;
- provide the basis for developing mitigation and management plans.

The IVAF has been designed with inherent scalability so that it is applicable to all levels of economic structure.

IVAF is based on a holistic approach taking into account the existing experience, mainly at the national level.

Main objectives of IVAF are presented next:

- The IVAF must apply to enterprise vulnerabilities in both physical and cyber dimensions.
- The IVAF must be scalable, capable of being applied by all the enterprise, irrespective of their employee number.
- The IVAF must be open and flexible, allowing the user to give emphasis to those areas of the IVAF of greatest importance to its specific enterprise.
- The IVAF should incorporate a delivery mechanism that is readily acceptable to both National Authorities and the business world, and not one that would require new government regulation or structures. (The IVAF can be implemented by an

auditor, both within the context of business risk assessment, and the growing accountancy requirement to assess risks and adequacy of controls over enterprise.)

- The IVAF must be flexible enough to draw from other sources of expertise for updated analytical information.
- The IVAF process must be repeatable over time. Today's IVAF outcomes must be valid in tomorrow's investment climate.
- The methodology primarily consists of three major steps, as shown in Figure 2. Each step consists of a series of activities, which are outlined in the following paragraphs. Using these assessment steps, the assessment team will compile a list of vulnerabilities for the organization to evaluate and determine appropriate next steps. Next steps include determining the order in which vulnerabilities should be addressed, the resources required, and the level of investment necessary to meet the management's objectives.

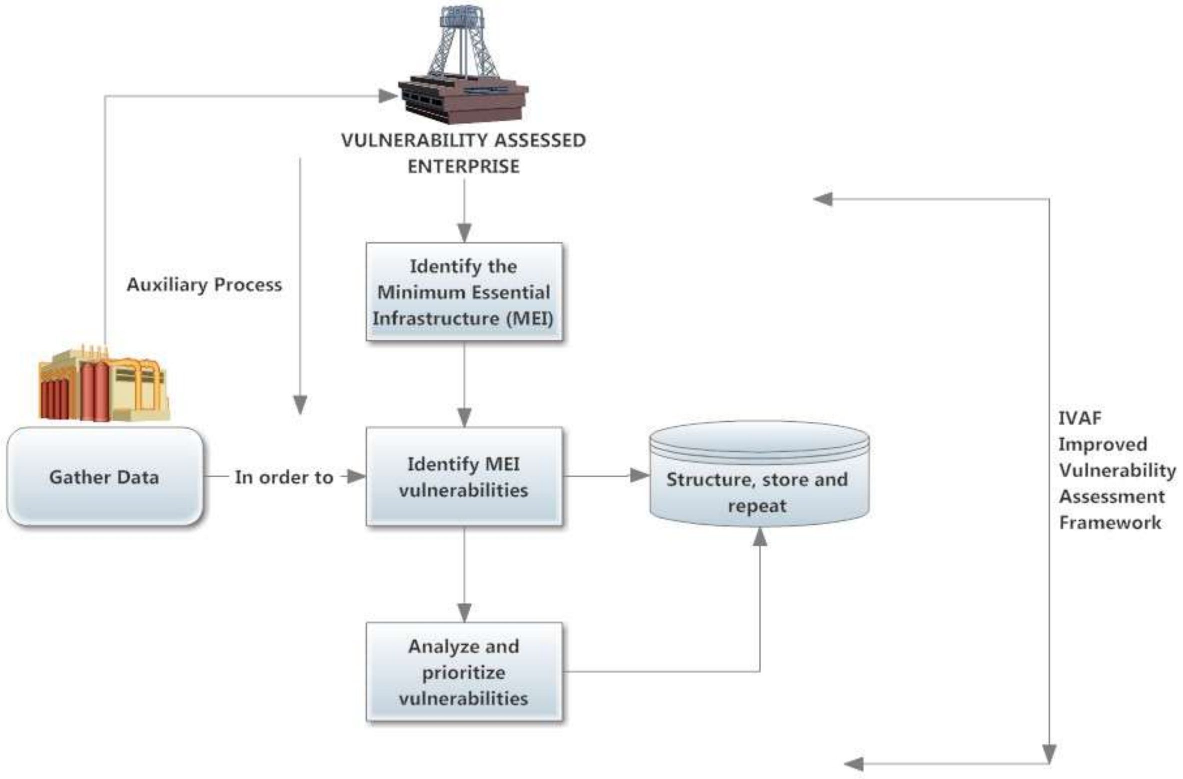
VULNERABILITY ASSESSED ENTERPRISE
Auxiliary Process
Identify the Minimum Essential Infrastructure (MEI)
Gather Data
In order to
Identify MEI vulnerabilities
Structure, store and repeat
Analyze and prioritize vulnerabilities
IVAF
Improved
Vulnerability
Assessment
Framework

Figure 2 IVAF main phases

In Phase 1 the assessment team will define the Minimum Essential Infrastructure for the enterprise. The focus is on the specific infrastructure components that support ***Mission Essential Processes (MEP)*** that is absolutely fundamental to achieving an enterprise's main activities. Once the MEI is identified, the vulnerabilities that potentially affect it are the most important starting points for vulnerability mitigation and minimization plans. In Phase 2 the IVAF evaluation will review actions, devices, procedures, techniques and other measures that potentially place the organization's MEI resources at risk. The outcome will be the identification and reporting of flaws or omissions in controls (e.g. vulnerabilities) that may affect the integrity, confidentiality, accountability, and/or the availability of resources those are essential to achieving the organizations core mission(s).

In Phase 3 the team will define and analyse the vulnerabilities identified in IVAF Phase 2 and MEI external dependencies from IVAF Phase 1, thereby enabling at least a first order of prioritization for purposes of remediation or minimization. Each step of the IVAF will be outlined in the following format:

- Objectives
- Critical Success Factors
- Expected Outcomes
- Activities

The Figure 3 shows the two components of MEI, the tactical and the strategic one.

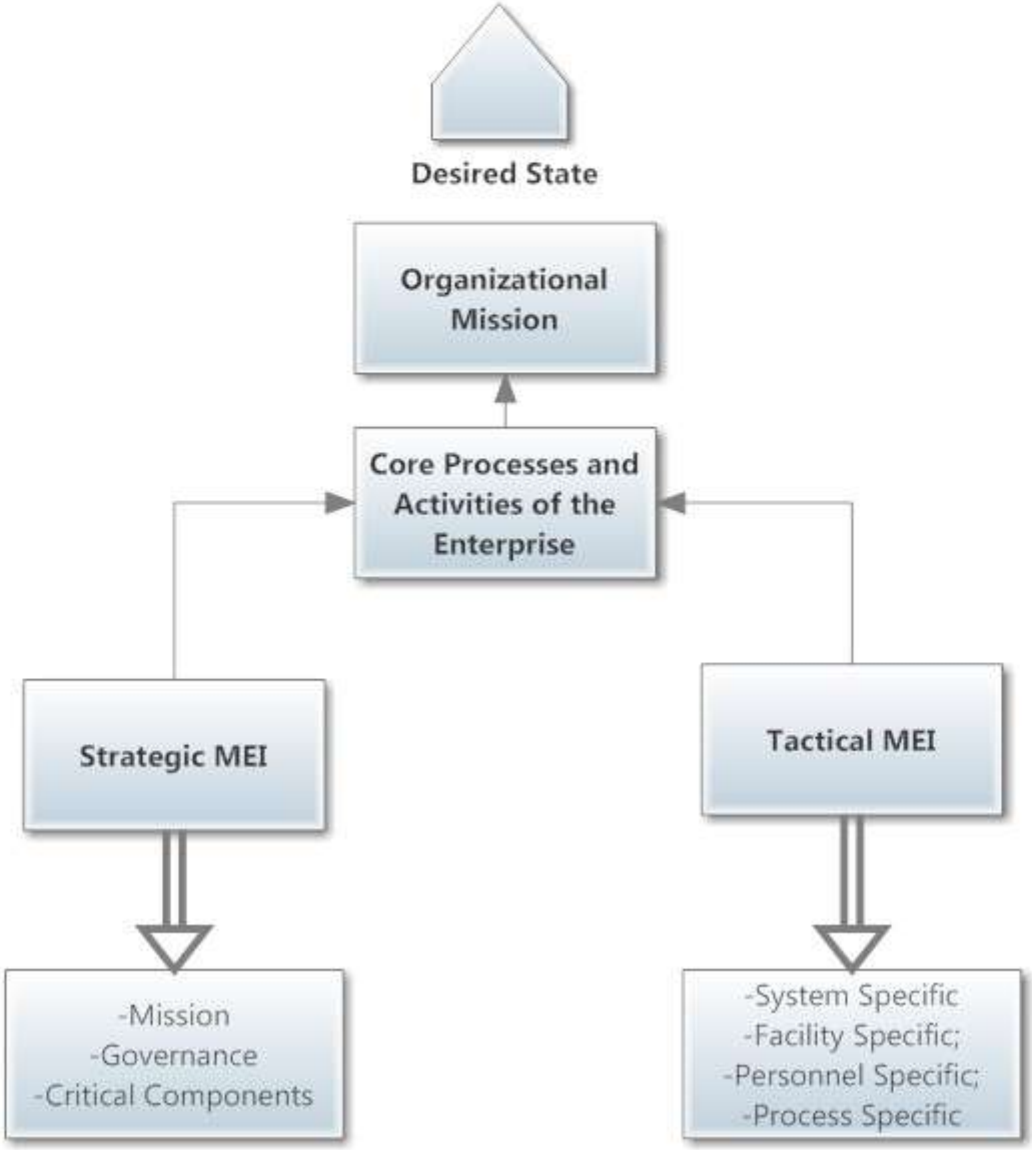

Figure 3 MEI components

In most cases the MEI is intended to be the absolute core component of what is referred to as ***mission critical elements (MCE).***

Essential MEI resource elements include the following:

People - Staff, management, and executives necessary to plan, organize, acquire, deliver, support, and monitor mission related services, information systems, and facilities. This includes groups and individuals external to the organization involved in the fulfilment of the organization's mission. Security management personnel should also be included.

Technology- All hardware and software, connectivity, countermeasures and/or safeguards that are utilized in support of the core process.

Applications- All application systems, internal and external, utilized in support of the core process.

Data -All data (electronic and hard copy) and information required to support the core process. This includes numbers, characters, images or other method of recording, in a form which can be assessed by a human or (especially) input into a computer, stored and processed there, or transmitted on some digital/communication's channel.

Facilities- All facilities required to support the core processes, including the resources to house and support information technology resources, and the other resource elements defined above.

There are primarily nine activities necessary to complete the phase 1.

1.1 Identify the core mission(s) of the organization

1.2 Identify the threat environment

1.3 Identify the core processes and activities supporting the core mission(s)

1.4 Analyse the value of each core process, categorizing them as *Code Red*, *Code Amber*, and *Code Green*

1.5 Identify organizational structure and customers as well as roles and responsibilities

1.6 Identify facilities

1.7 Map architecture and systems

1.8 Link physical, organizational and architecture components to core processes valued "*Code Red*"

1.9 Identify external resources upon which the enterprise MEI is dependent

The three codes had the following significations:

- *Code Red*: Prevent the enterprise from fulfilling its mission. From the perspective of an attacker, this would constitute a "Kill."
- *Code Amber*: Significantly debilitate or interfere with the ability of the enterprise to fulfil its mission, or economic security functions or provide continuity of core services.
- *Code Green*: No appreciable impact on enterprise missions.

The enterprise must review the processes categorized or valued at the Amber or Green level against a variable of time. If the process escalates to next higher value over time, the enterprise should consider whether the process should be included in the MEI.

Considered areas of control for vulnerability analysis are:

- ***Entity-Wide Security*** - Planning and management that provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's physical and cyber security controls.
- ***Access Controls*** - Procedures and controls that limit or detect access to MEI Resource Elements (People, Technology, Applications, Data and/or Facilities) thereby protecting these resources against loss of Integrity, Confidentiality Accountability and/or Availability.
- ***Segregation of Duties - Policies***, procedures, and an organizational structure established so that one individual cannot control key aspects of physical and/or computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to MEI Resource Elements.
- ***Continuity of Service and Operations*** - Controls to ensure that, when unexpected events occur, departmental/agency MEI services and operations, including computer operations, continue without interruption or are promptly resumed and critical and sensitive data are protected through adequate contingency and business recovery plans and exercises.
- ***Change Control & Life Cycle Management*** - Procedures and controls that prevent unauthorized programs or modifications to an existing program from being implemented.

In reviewing the areas of control against the MEI resource elements, if vulnerabilities are

identified, it would mean controls are not in place to ensure the following:

- Integrity - The accuracy, completeness and reliable transmission and reception of information and its validity in accordance with business values and expectations; the adequacy and reliability of processes assuring personnel selection, access and safety; and the adequacy and reliability of processes assuring authorized access to and the safety of physical facilities.
- Confidentiality - The protection of sensitive information from unauthorized disclosure and sensitive facilities from physical, technical or electronic penetration or exploitation.
- Availability - The ability to have access to MEI Resource Elements when required by the mission and core supporting process(s), both now and in the future. It also concerns the safeguarding of those resources and associated capabilities.
- Accountability - The explicit assignment of responsibilities for ownership and/or oversight of the process, system, as well as inputs and outputs. Accountability may be assigned at various levels within the organization to include executives, managers, staff, system, information or facilities owners, providers, and users of MEI Resource Elements. These assignments are reviewed for effectiveness and appropriateness in the areas of control shown before. In the management of vulnerabilities, accountability is imperative and as an area of compromise is highlighted in IVAF Phase 3 (Adger, 2000).

The activities that comprise Phase 2 are essentially the data gathering and analyses necessary to evaluate each of the six areas of control. Each area of control has an assessment questionnaire designed to gather information pertinent to that area of control.

Risk assessments should consider data sensitivity and the need for integrity and the range of risks that an entity's MEI resource elements may be subject to, including those risks posed by authorized internal and external users, as well as unauthorized outsiders who may try to "break into" the cyber systems (Rapoza, 2011) . Such analyses should also draw on reviews of system and network configurations and observations and testing of existing security controls for cyber systems, as well as reviews and testing of controls for the other resource elements.

The next figure (Figure 4) summarizes the activities that are included in Phase 3.

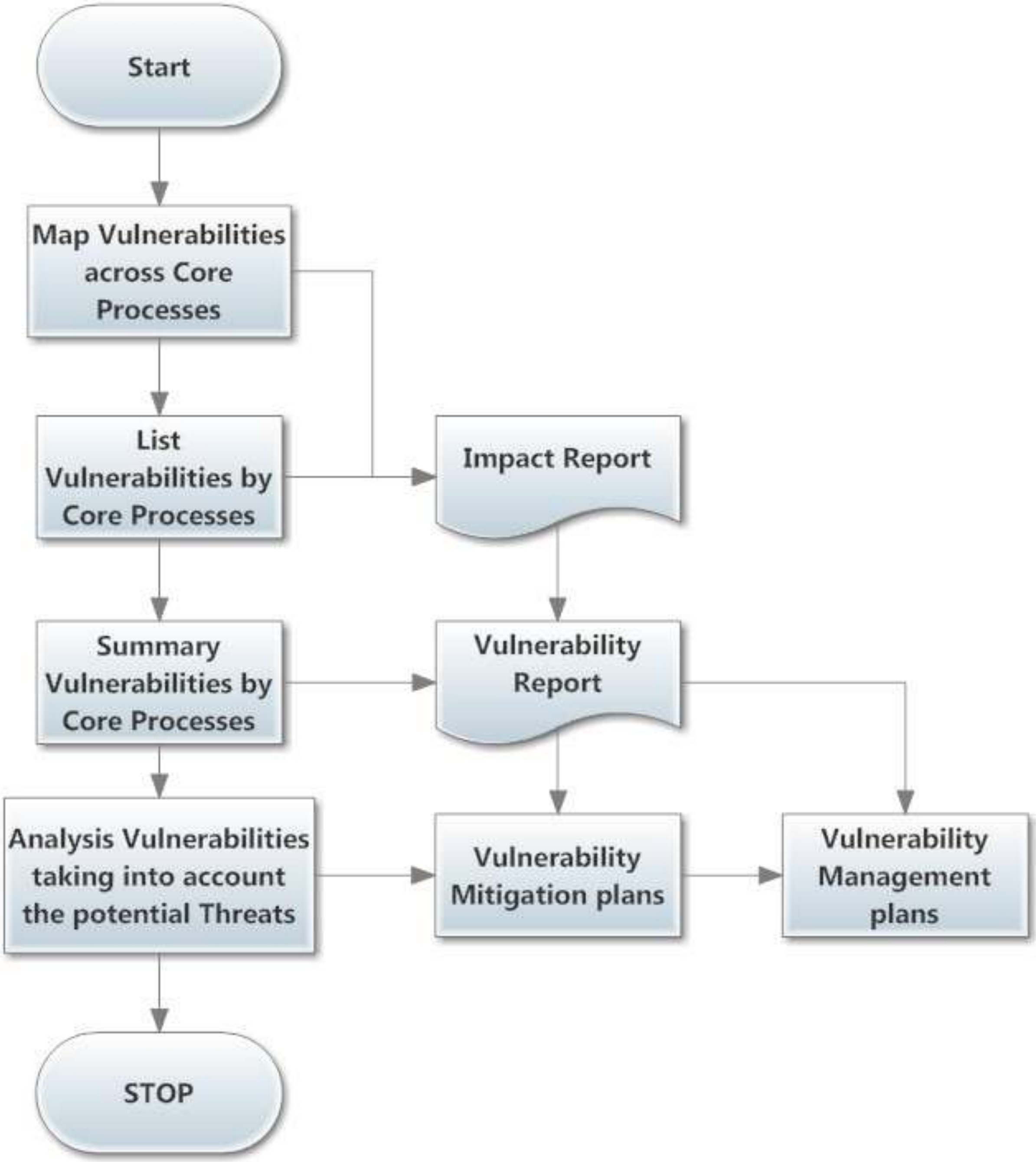
Start
Map Vulnerabilities across Core Processes
List Vulnerabilities by Core Processes
Impact Report
Summary Vulnerabilities by Core Processes
Vulnerability Report
Analysis Vulnerabilities taking into account the potential Threats
Vulnerability Mitigation plans
Vulnerability Management plans
STOP

Figure 4 Activities specific to Phase 3

A Code Red is assigned if:

- a vulnerability is caused by a lack of accountability i.e. if ownership of the process, system or inputs/outputs is not clearly or appropriately defined; or
- a vulnerability is exploited and controls are not in place to warn those accountable.

A checklist example is given in the following table based on (CERCT, 2013)

Table 1- Example checklist

No.	Control Objectives	Control Technique	Compliance Procedures
	Maintain a positive information control environment.	Does Management create a framework and an awareness program fostering a positive control environment throughout the entire organization by addressing aspects such as: integrity, ethical values and competence of the people; management philosophy and operating style;	Review related policies and procedures. Review Senior Management roles and responsibilities. Review objectives and long/short range plans.
2	Periodically assess risks	Are independent risk assessments performed and documented on a regular basis?	Review risk assessment policies.
2.1.		Is a security plan documented and approved? Has independent advice and comment been solicited on the plan before its implementation?	Review the most recent high-level risk assessment.
2.2.		Does the risk assessment consider data sensitivity and integrity and the range of risks to the entity's systems and data?	Review the objectivity of personnel who performed and reviewed the assessment.
3	Proactive Audit Involvement	Does Information Technology management seek audit involvement in a proactive manner before finalizing information technology service solutions?	Interview IT Senior Management.
4	Management ensures that corrective actions are effectively implemented	Does top management initiate prompt action to correct deficiencies?	Review documentation related to corrective actions.

A detailed vulnerability checklist would take into account three component elements: risk, probability and readiness to act (Floke, 2003).

Issues to consider for probability include, but are not limited to:

1. Known risk
2. Historical data
3. Manufacturer/vendor statistics

Issues to consider for risk include, but are not limited to:

1. Threat to life and/or health (SANS, 2013)
2. Disruption of services
3. Damage/failure possibilities
4. Loss of community trust
5. Financial impact
6. Legal issues

Issues to consider for readiness include, but are not limited to:

The next template shows how these elements would be integrated into the assessment of vulnerability.

Table 2-Assessment template

No	Vulnerability assessment for:	Probability					Risk					Readiness					Total
		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	

Core model

For the core model of the vulnerability assessment method described above we have used Structural Equation Modelling (SEM) in order to develop an optimal model. The general diagram used in model is shown in Figure 5.

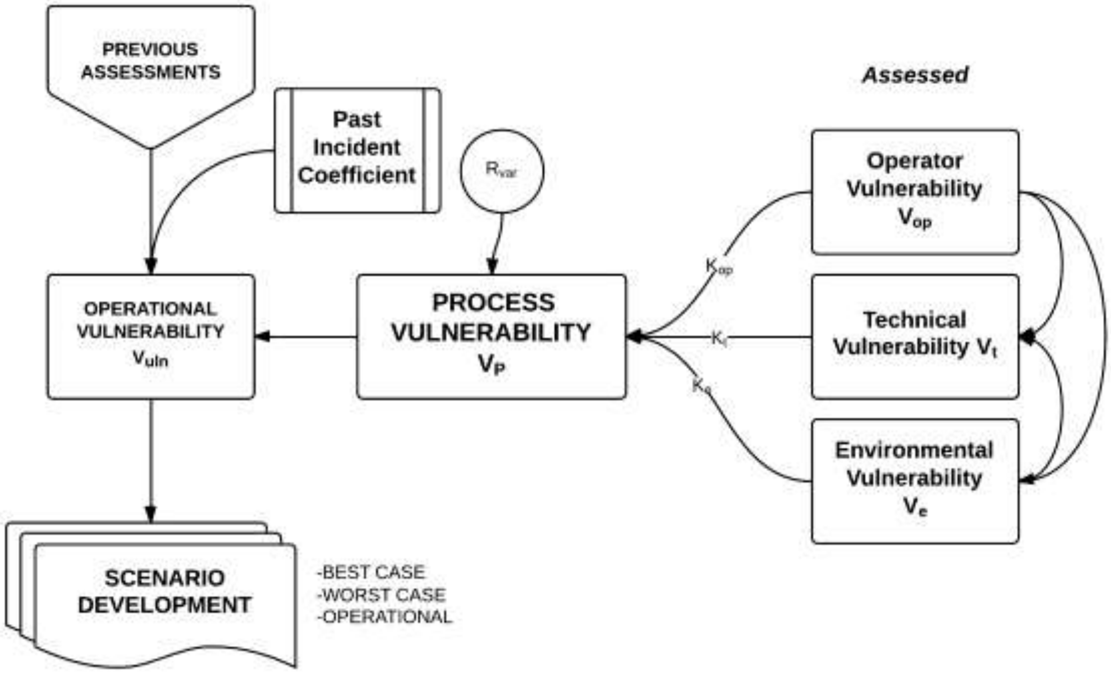
PREVIOUS ASSESSMENTS
Past Incident Coefficient
R_{var}
Assessed
Operator Vulnerability V_{op}
Technical Vulnerability V_t
Environmental Vulnerability V_e
K_{op}
K_t
K_e
OPERATIONAL VULNERABILITY V_{uln}
PROCESS VULNERABILITY V_P
SCENARIO DEVELOPMENT
-BEST CASE
-WORST CASE
-OPERATIONAL

Figure 5 General diagram used in modelling

V_{uln}= (V_p * Pik)/10 (1) (Kovacs, 2008) where

V_{uln} =Operational Vulnerability, V_p =Process Vulnerability and Pik=Past Incident Coefficient which is 0 if there are no reported past incidents, 1.5 if there were near misses, loss incidents or minor incidents and 2 if there were reported accidents before.

V_p= (K_{op}*V_{op}+K_t*V_t+K_e*V_e)/log (R_{var}) (2) where

K_{op}=weight coefficient for the importance of operator vulnerability, K_t =weight coefficient for the importance of technical vulnerability, Ke=weight coefficient for the importance of environmental vulnerability,

K_{op}+K_t+K_e=1 (3)

V_{op},V_t and V_e are the assessed vulnerabilities for the human operator, the technical components of the system and the working environment. Each vulnerability is assessed on a 0...5 Likert scale where 5 is the value for maximum vulnerability. R_{var} =residual variance.

Conclusions

The paper presents a start-up point for vulnerability analysis and management. Vulnerability analysis could be a solution for the understanding of the roots of loss, incidents and accidents that are occurring day by day in enterprises across Europe, SME or big societies. To be vulnerable- is a big risk for every enterprise on a competitive market. Even if not attacked directly a vulnerable enterprise could compete more difficult on this market than a non-vulnerable one.

Connecting vulnerability and risk analysis could give to the management a global image on causes and effects of unexpected events that could disturb the normal enterprise activity (WEF, 2002).

The link between risk and vulnerability assessment is given in Figure 6.

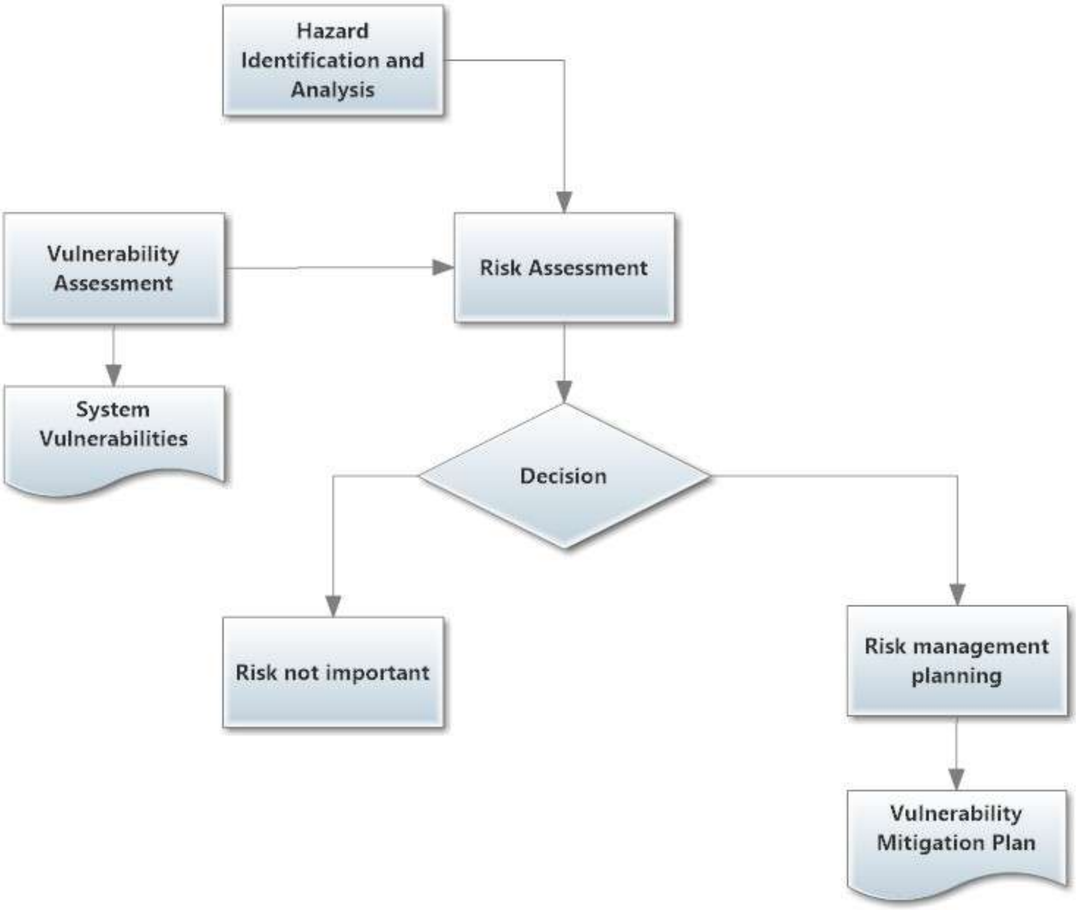

Figure 6- Vulnerability and risk assessments

As it could be seen from the figure, vulnerability assessment could be considered a predecessor of risk assessment, giving opportunities of simplifying the risk assessment (Berg, 2000).

One of the testing results- showing the confidence in the vulnerability assessment method- developed inside the research- is presented in the next table.

Table 3- Degree of confidence in the vulnerability assessment method

Type of industry	Degree of confidence in the developed method after implementation			Observations
	Low	Medium	High	
Construction	10%	40%	50%	The units from the construction industry asked the Labour Inspection to implement this method for risk assessment on the spot.
Manufacturing	15%	55%	30%	Manufacturing industry pilots asked for an integrated approach, including also risk analysis

In order to have a better feedback, after the implementation of the method, the pilots were asked to underline the most important characteristics- and appreciate them on a 0…5 scale with 0 as not significant and 5 as excellent. The next table includes the results.

Table 4- Assessment of the main characteristics for the method

Assessment method	Underlined characteristics	Assessed as	Observations
Vulnerability	Global view upon threats at the enterprise level	0 - 0%	Vulnerability assessment extends the assessment view, including also aspects let outside risk assessment.
		1 - 0%	
		2 - 5%	
		3 - 10%	
		4 - 40%	
		5 - 45%	
	Systemic	0 - 0%	It starts from the beginning with a systemic approach.
		1 - 5%	
		2 - 5%	
		3 - 10%	
		4 - 40%	
		5 - 40%	
	Structural	0 - 0%	New modules could be added. The existing modules could be processed independently.
		1 - 0%	
		2 - 0%	
		3 - 10%	
		4 - 40%	
		5 – 50 %	
	Easiness in usage	0 - 0%	The method was considered the most facile to use.
		1 - 0%	
		2 - 0%	
		3 - 5%	
		4 - 25%	
		5 - 70%	

References

Adger, N., Kelly, M. & Bentham, G. (2000) New Indicators of Vulnerability and Adaptive Capacity (Tyndall Centre for Climate Change Research,Norwich, CT).

Berg, Al. "Part 2: Audits, Assessments & Test (Oh My)". Information Security Magazine August 2000

Berkes, F. & Folk, C. (1998)Linking Social and Ecological Systems(Cambridge Univ. Press, Cambridge, U.K.)

CERT/CC Product Vulnerability Reporting Form v1.0 .

Downing, T. E., Butterfield, R., Cohen, S., Huq, S., Moss, R., Rahman, A.,Sokaona, Y. & Stephen, L. (2001) Climate Change Vulnerability (OxfordEnvironmental Change Institute, Oxford)

Folke, C., Carpenter, S., Elmqvist, T., Gunderson, L., Holling, C., Walker,B., Bengtsson, J., Berkes, F., Colding, J., Danell, K., et al. (2002) Scientific Background Paper Prepared for the Environmental Advisory Council to the Swedish Government (International Council for Science Series for Sustainable Development), No. 3, www.resalliance.orgev.

Kovacs Șt (2008),Complex, expert based multi-role assessment system for SME s, in Safety,Reliability and Risk Analysis:Theory,Methods and Applications, Martorell et all ,Taylor &Francisc Group,London,ISBN 978-0-415-48513-5

National Research Council (2002) Assessment of Proposed Partnerships to Implement a National Landslide Hazards Mitigation Strategy. Interim Report (Natl. Acad. Press, Washington, DC).

Rapoza, Jim. (2011) "Security Core: Best Practices". November 13,00. eWeek.

http://www.zdnet.com/enterprise/stories/main/0,10228,2652346-1,00.html

SANS GIAC Security Essentials Training Manual

Turner, B. L.; Kasperson, R. E.; Matson, P. A.; McCarthy, J. J.; Corell, R. W.; Christensen, L.; Eckley, N.; Kasperson, J. X.; Luers, A.; Martello, M. L.; Polsky, C.; Pulsipher, A.; Schiller, A. (5 June 2003). "Science and Technology for Sustainable Development Special Feature: A framework for vulnerability analysis in sustainability science". *Proceedings of the National Academy of Sciences* 100 (14): 8074–8079.

World Economic Forum (2002) 2002 Environmental Sustainability Index (Global Leaders of Tomorrow Environment Task Force, Geneva)