Miloš Petronijević[1)]
Ana Janković[1)]

1) Visoka tehnička škola Novi Beograd, Zorana Đinđića 152 A
2) Nomobbing, Kragujevac, Nenadovićeva 10

PROTECTION OF DATA IN RISK MANAGEMENT FUNCTION

Abstract: *The principal goal of an organization's risk management process should be to protect the organization and its ability to perform their mission, not just its assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the experts who operate and manage the system, but as an essential management function of the organization.*

Keywords: *Risk, management, analisys, level*

1. INTRODUCTION

The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of a vulnerability. Before beginning the impact analysis, it is necessary to obtain the following necessary information as discussed in Section 3.1.1:

System mission (e.g., the processes performed by the IT system)

System and data criticality (e.g., the system's value or importance to an organization)

System and data sensitivity.

This information can be obtained from existing organizational documentation, such as the mission impact analysis report or asset criticality assessment report. A mission impact analysis (also known as business impact analysis [BIA] for some organizations) prioritizes the impact levels associated with the compromise of an organization's information assets based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets. An asset criticality assessment identifies and prioritizes the sensitive and critical organization information assets (e.g., hardware, software, systems, services, and related technology assets) that support the organization's critical missions.

If this documentation does not exist or such assessments for the organization's IT assets have not been performed, the system and data sensitivity can be determined based on the level of protection required to maintain the system and data's availability, integrity, and confidentiality. Regardless of the method used to determine how sensitive an IT system and its data are, the system and information owners are the ones responsible for determining the impact level for their own system and information. Consequently, in analyzing impact, the appropriate approach is to interview the system and information owner(s).

2.IMPACT OF RISK ANALYSIS IT SYSTEM

Therefore, the adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals: integrity, availability, and confidentiality. The following list provides a brief description of each security goal and the consequence (or impact) of its not being met:

Loss of Integrity. System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.

Loss of Availability. If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.

Loss of Confidentiality. System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

Some tangible impacts can be measured quantitatively in lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other impacts (e.g., loss of public confidence, loss of credibility, damage to an organization's interest) cannot be measured in specific units but can be qualified or described in terms of high, medium, and low impacts. Because of the generic nature of this discussion, this guide designates and describes only the qualitative categories—high, medium, and low impact (see Table1).

Table 1. Magnitude of Impact Definitions

Magnitude of Impact	**Impact Definition**
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

In conducting the impact analysis, consideration should be given to the advantages and disadvantages of quantitative versus qualitative assessments. The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities. The disadvantage of the qualitative analysis is that it does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-benefit analysis of any recommended controls difficult.

The major advantage of a quantitative impact analysis is that it provides a measurement of the impacts' magnitude, which can be used in the cost-benefit analysis of recommended controls. The disadvantage is that, depending on the numerical ranges used to express the measurement, the meaning of the quantitative impact analysis may be unclear, requiring the result to be interpreted in a qualitative manner. Additional factors often must be considered to determine the magnitude of impact. These may include, but are not limited to—

An estimation of the frequency of the threat-source's exercise of the vulnerability over a specified time period (e.g., 1 year)

An approximate cost for each occurrence of the threat-source's exercise of the vulnerability

A weighted factor based on a subjective analysis of the relative impact of a specific threat's exercising a specific vulnerability.

3. RISK DETERMINATION

The purpose of this step is to assess the level of risk to the IT system. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of–

The likelihood of a given threat-source's attempting to exercise a given vulnerability

The magnitude of the impact should a threat-source successfully exercise the vulnerability

The adequacy of planned or existing security controls for reducing or eliminating risk.

3.1 Risk-Level Matrix

The final determination of mission risk is derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact. Table 3.6 below shows how the overall risk ratings might be determined based on inputs from the threat likelihood and threat impact categories. The matrix below is a 3 x 3 matrix of threat likelihood (High, Medium, and Low) and threat impact (High, Medium, and Low). Depending on the site's requirements and the granularity of risk assessment desired, some sites may use a 4 x 4 or a 5 x 5 matrix. The latter can include a Very Low /Very High threat likelihood and a Very Low/Very High threat impact to generate a Very Low/Very High risk level. A "Very High" risk level may require possible system shutdown or stopping of all IT system integration and testing efforts.

The sample matrix in Table 3-6 shows how the overall risk levels of High, Medium, and Low are derived. The determination of these risk levels or ratings may be subjective. The rationale for this justification can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level. For example,

The probability assigned for each threat likelihood level is 1.0 for High, 0.5 for Medium, 0.1 for Low

The value assigned for each impact level is 100 for High, 50 for Medium, and 10 for Low.

Table2. Risk-Level Matrix

Threat Likelihood	**Impact**		
	Low (10)	**Medium** (50)	**High** (100)
High (1.0)	**Low** 10 X 1.0 = 10	**Medium** 50 X 1.0 = 50	**High** 100 X 1.0 = 100
Medium (0.5)	**Low** 10 X 0.5 = 5	**Medium** 50 X 0.5 = 25	**Medium** 100 X 0.5 = 50
Low (0.1)	**Low** 10 X 0.1 = 1	**Low** 50 X 0.1 = 5	**Low** 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

3.2 Description of Risk Level

Table 3-7 describes the risk levels shown in the above matrix. This risk scale, with its ratings of High, Medium, and Low, represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk scale also presents actions that senior management, the mission owners, must take for each risk level.

Table 3. Risk Scale and Necessary Actions

Risk Level	**Risk Description and Necessary Actions**
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.

Output from Step 7–Risk level (High, Medium, Low)

If the level indicated on certain items is so low as to be deemed to be "negligible" or non significant (value is <1 on risk scale of 1 to 100), one may wish to hold these aside in a separate bucket in lieu of forwarding for management action. This will make sure that they are not overlooked when conducting the next periodic risk assessment. It also establishes a complete record of all risks identified in the analysis. These risks may move to a new risk level on a reassessment due to a change in threat likelihood and/or impact and that is why it is critical that their identification not be lost in the exercise.

4. STEP CONTROL RECOMMENDATIONS

During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, are provided. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options (e.g., system compatibility)
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability.

The control recommendations are the results of the risk assessment process and provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.

It should be noted that not all possible recommended controls can be implemented to reduce loss. To determine which ones are required and appropriate for a specific organization, a cost-benefit analysis, as discussed in Section 4.6, should be conducted for the proposed recommended controls, to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. In addition, the operational impact (e.g., effect on system performance) and feasibility (e.g., technical requirements, user acceptance) of introducing the recommended option should be evaluated carefully during the risk mitigation process.

Output from Step 8–Recommendation of control(s) and alternative solutions to mitigate risk

5. RESULTS DOCUMENTATION

Once the risk assessment has been completed (threat-sources and vulnerabilities identified, risks assessed, and recommended controls provided), the results should be documented in an official report or briefing.

A risk assessment report is a management report that helps senior management, the mission owners, make decisions on policy, procedural, budget, and system operational and management changes. Unlike an audit or investigation report, which looks for wrongdoing, a risk assessment report should not be presented in an accusatory manner but as a systematic and analytical approach to assessing risk so that senior management will understand the risks and allocate resources to reduce and correct potential losses. For this reason, some people prefer to address the threat/vulnerability pairs as observations instead of findings in the risk assessment report. Appendix B provides a suggested outline for the risk assessment report.

6. RISK MITIGATION

Risk mitigation, the second process of risk management, involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process.

Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior management and functional and business managers to use the **least-cost approach** and implement the **most appropriate controls** to decrease mission risk to an acceptable level, with **minimal adverse impact** on the organization's resources and mission.

7.1 Risk mitigation options

Risk mitigation is a systematic methodology used by senior management to reduce mission risk. Risk mitigation can be achieved through any of the following risk mitigation options:

Risk Assumption. To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level

Risk Avoidance. To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)

Risk Limitation. To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls)

Risk Planning. To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls

Research and Acknowledgment. To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability

Risk Transference. To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

The goals and mission of an organization should be considered in selecting any of these risk mitigation options. It may not be practical to address all identified risks, so priority should be given to the threat and vulnerability pairs that have the potential to cause significant mission impact or harm. Also, in safeguarding an organization's mission and its IT systems, because of each organization's unique environment and objectives, the option used to mitigate the risk and the methods used to implement controls may vary. The "best of breed" approach is to use appropriate technologies from among the various vendor security products, along with the appropriate risk mitigation option and nontechnical, administrative measures.

In implementing recommended

controls to mitigate risk, an organization should consider technical, management, and operational security controls, or a combination of such controls, to maximize the effectiveness of controls for their IT systems and organization. Security controls, when used appropriately, can prevent, limit, or deter threat-source damage to an organization's mission.

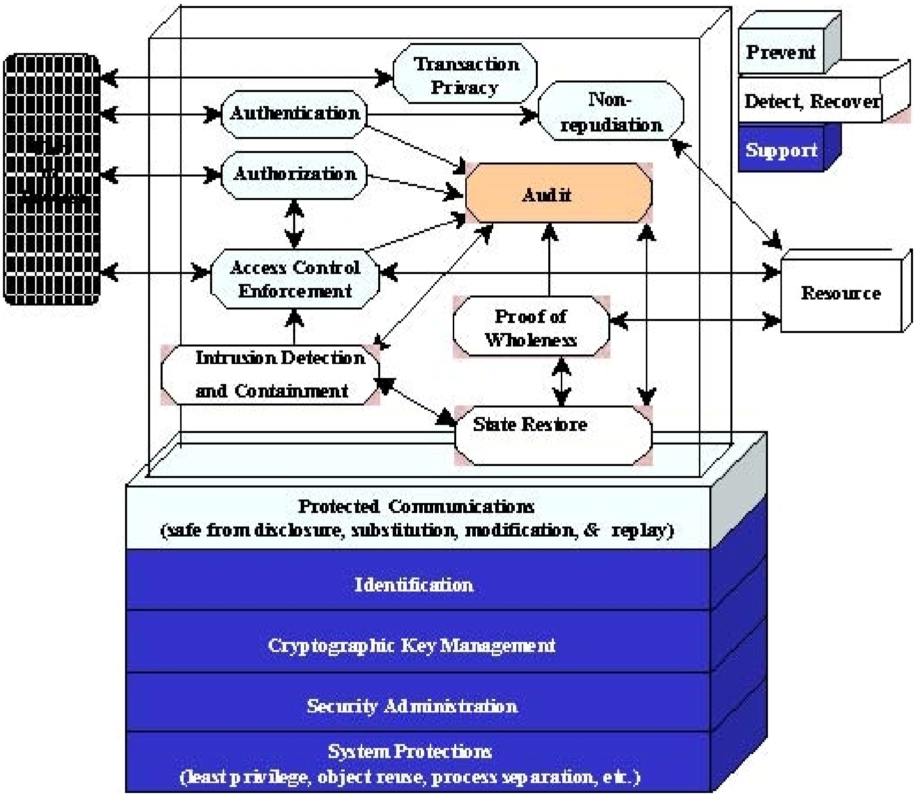
Prevent
Detect, Recover
Support
Transaction Privacy
Authentication
Non-repudiation
Authorization
Audit
Access Control Enforcement
Resource
Proof of Wholeness
Intrusion Detection and Containment
State Restore
Protected Communications (safe from disclosure, substitution, modification, & replay)
Identification
Cryptographic Key Management
Security Administration
System Protections (least privilege, object reuse, process separation, etc.)

Figure1 Technical Security Controls

The control recommendation process will involve choosing among a combination of technical, management, and operational controls for improving the organization's security posture. The trade-offs that an organization will have to consider are illustrated by viewing the decisions involved in enforcing use of complex user passwords to minimize password guessing and cracking. In this case, a technical control requiring add-on security software may be more complex and expensive than a procedural control, but the technical control is likely to be more effective because the enforcement is automated by the system. On the other hand, a procedural control might be implemented simply by means of a memorandum to all concerned individuals and an amendment to the security guidelines for the organization, but ensuring that users consistently follow the memorandum and guideline will be difficult and will require security awareness training and user acceptance.

This section provides a high-level overview of some of the control categories. More detailed guidance about implementing and planning for IT controls can be found in NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems, and NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook.

Technical security controls for risk mitigation can be configured to protect against given types of threats. These controls may range from simple to complex measures and usually involve system architectures; engineering disciplines; and security packages with a mix of hardware, software, and firmware. All of these measures should work together to secure critical and sensitive data, information, and IT system functions. Technical controls can be grouped into the following major categories, according to primary purpose:

Support Supporting controls are generic and underlie most IT security capabilities. These controls must be in place in order to implement other controls.

Prevent. Preventive controls focus on preventing security breaches from occurring in the first place.

Detect and Recover. These controls focus on detecting and recovering from a security breach.

Figure 1 depicts the primary technical controls and the relationships between them.

Supporting controls are, by their very nature, pervasive and interrelated with many other controls. The supporting controls are as follows:

Identification. This control provides the ability to uniquely identify users, processes, and information resources. To implement other security controls (e.g., discretionary access control [DAC], mandatory access control [MAC], accountability), it is essential that both subjects and objects be identifiable.

Cryptographic Key Management. Cryptographic keys must be securely managed when cryptographic functions are implemented in various other controls. Cryptographic key management includes key generation, distribution, storage, and maintenance.

Security Administration. The security features of an IT system must be configured (e.g., enabled or disabled) to meet the needs of a specific installation and to account for changes in the operational environment. System security can be built into operating system security or the application. Commercial off-the-shelf add-on security products are available.

System Protections. Underlying a system's various security functional capabilities is a base of confidence in the technical implementation. This represents the quality of the implementation from the perspective both of the design processes used and of the manner in which the implementation was accomplished. Some examples of system protections are residual information protection (also known as object reuse), least privilege (or "need to know"), process separation, modularity, layering, and minimization of what needs to be trusted.

These controls, which can inhibit attempts to violate security policy, include the following:

Authentication. The authentication control provides the means of verifying the identity of a subject to ensure that a claimed identity is valid. Authentication mechanisms include passwords, personal identification numbers, or PINs, and emerging authentication technology that provides strong authentication (e.g., token, smart card, digital certificate, Kerberos).

Authorization. The authorization control enables specification and subsequent management of the allowed actions for a given system (e.g., the information owner or the database administrator determines who can update a shared file accessed by a group of online users).

Access Control Enforcement. Data integrity and confidentiality are enforced by access controls. When the subject requesting access has been authorized to access particular processes, it is necessary to enforce the defined security policy (e.g., MAC or DAC). These policy-based controls are enforced via access control mechanisms distributed throughout the system (e.g., MAC sensitivity labels; DAC file permission sets, access control lists, roles, user profiles). The effectiveness and the strength of access control depend on the correctness of the access control decisions (e.g., how the security rules are configured) and the strength of access control enforcement (e.g., the design of software or hardware security).

Nonrepudiation. System accountability depends on the ability to ensure that senders cannot deny sending information and that receivers cannot deny receiving it. Nonrepudiation spans both prevention and detection. It has been placed in the prevention category in this guide because the mechanisms implemented prevent the successful repudiation of an action (e.g., the digital certificate that contains the owner's private key is known only to the owner). As a result, this control is typically applied at the point of transmission or reception.

Protected Communications. In a distributed system, the ability to accomplish security objectives is highly dependent on trustworthy communications. The protected communications control ensures the integrity, availability, and confidentiality of sensitive and critical information while it is in transit. Protected communications use data encryption methods (e.g., virtual private network, Internet Protocol Security [IPSEC] Protocol), and deployment of cryptographic technologies (e.g., Data Encryption Standard [DES], Triple DES, RAS, MD4, MD5, secure hash standard, and escrowed encryption algorithms such as Clipper) to minimize network threats such as replay, interception, packet sniffing, wiretapping, or eavesdropping.

Transaction Privacy. Both government and private sector systems are increasingly required to maintain the privacy of individuals. Transaction privacy controls (e.g., Secure Sockets Layer, secure shell) protect against loss of privacy with respect to transactions performed by an individual.

Detection controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums. Recovery controls can be used to restore lost computing resources. They are needed as a complement to the supporting and preventive technical measures, because none of the measures in these other areas is perfect. Detection and recovery controls include—

Audit. The auditing of security-relevant events and the monitoring and tracking of system abnormalities are key elements in the after-the-fact detection of, and recovery from, security breaches.

Intrusion Detection and Containment. It is essential to detect security breaches (e.g., network break-ins, suspicious activities) so that a response can occur in a timely manner. It is also of little use to detect a security breach if no effective response can be initiated. The intrusion detection and containment control provides these two capabilities.

Proof of Wholeness. The proof-of-wholeness control (e.g., system integrity tool) analyzes system integrity and irregularities and identifies exposures and potential threats. This control does not prevent violations of security policy but detects violations and helps determine the type of corrective action needed.

Restore Secure State. This service enables a system to return to a state that is known to be secure, after a security breach occurs.

Virus Detection and Eradication. Virus detection and eradication software installed on servers and user workstations detects, identifies, and removes software viruses to ensure system and data integrity.

Management security controls, in conjunction with technical and operational controls, are implemented to manage and reduce the risk of loss and to protect an organization's mission. Management controls focus on the stipulation of information protection policy, guidelines, and standards, which are carried out through operational procedures to fulfill the organization's goals and missions.

Assign security responsibility to ensure that adequate security is provided for the mission-critical IT systems

Develop and maintain system security plans to document current controls and address planned controls for IT systems in support of the organization's mission

Implement personnel security controls, including separation of duties, least privilege, and user computer access registration and termination

Conduct security awareness and technical training to ensure that end users and system users are aware of the rules of behavior and their responsibilities in protecting the organization's mission.

Detection management controls are as follows:

- Implement personnel security controls, including personnel clearance, background investigations, rotation of duties
- Conduct periodic review of security controls to ensure that the controls are effective
- Perform periodic system audits
- Conduct ongoing risk management to assess and mitigate risk
- Authorize IT systems to address and accept residual risk.

These controls include the following:

- Provide continuity of support and develop, test, and maintain the continuity of operations plan to provide for business resumption and ensure continuity of operations during emergencies or disasters
- Establish an incident response capability to prepare for, recognize, report, and respond to the incident and return the IT system to operational status.

An organization's security standards should establish a set of controls and guidelines to ensure that security procedures governing the use of the organization's IT assets and resources are properly enforced and implemented in accordance with the organization's goals and mission. Management plays a vital role in overseeing policy implementation and in ensuring the establishment of appropriate operational controls.

Control data media access and disposal (e.g., physical access control, degaussing method)

Limit external data distribution (e.g., use of labeling)

Control software viruses

Safeguard computing facility (e.g., security guards, site procedures for visitors, electronic badge system, biometrics access control, management and distribution of locks and keys, barriers and fences)

Secure wiring closets that house hubs and cables

Provide backup capability (e.g., procedures for regular data and system backups, archive logs that save all database changes to be used in various recovery scenarios)

Establish off-site storage procedures and security

Protect laptops, personal computers (PC), workstations .

REFERENCES:

[1] riskrewardlimited.com

[2] en.wikipedia.org/wiki/Risk_management

[3] www.investopedia.com › Dictionary

[4] www.apmg-international.com/APMG-UK/.../MoR_Home.asp

[5] www.theirm.org