IRSTI 10.19.01; 81.93.29 https://doi.org/10.26577/JAPJ.2021.v100.i4.12

A.N. Ibrahimova

Baku State University, Azerbaijan, Baku
e-mail: aytakinibrahimli@gmail.com

THE FACTOR OF THE RISK AND RISK MANAGEMENT IN INFORMATION SECURITY

Risk is the consequence of events and dangers. To rephrase it, an event that will cause damage and deprivation and this happening can be described via the term of information. The word risk means foreseeable dangers or being under the threat of possible damage. It defines the occurrence of an event that could lead to damage or loss. This term is used for events that are synonymous with danger and are expected to occur, but it is not clear whether they will occur or not. Thus, risk management means managing this uncertain environment. Risk Information Security Management system requires a risk-based approach. Information security policy emerges and is formed based on the results of risk analysis. Therefore, risk management is essential. As well as the systematic use of information contributes to identifying sources and forecasting risks. Information systems analyze the value of assets, threats and shortcomings in risk analysis. Here, the risks are assessed depending on the severity of the potential impact on the confidentiality, integrity and reliability of information systems. Everything that has value for an organization is called information availability. The standards define the availability of information as information that is valuable to the organization and should always be protected.

Key words: risk management, risk processing, risk assessment, risk monitoring, risk reassessment, risk review, Information security risk.

А.Н. Ибрагимова

Баку мемлекеттік университеті, Әзірбайжан, Баку қ.
e-mail: aytakinibrahimli@gmail.com

Ақпараттық қауіпсіздік саласында тәуекел факторы және тәуекелдерді басқару

Тәуекел – бұл оқиғалар мен қауіптердің салдары. Мұны қорытындылай келе, залал мен айырылуды тудыратын оқиға және бұл оқиғаны ақпарат терминімен сипаттауға болады. «Тәуекел» сөзі болжамды қауіпті немесе ықтимал зиян келтіру қаупін білдіреді. Ол зақымға немесе зақымға әкелуі мүмкін оқиғаның басталуын анықтайды. Бұл термин қауіптің синонимі болып табылатын және болуы мүмкін, бірақ олардың пайда болуы немесе болмауы белгісіз оқиғаларға қатысты қолданылады. Осылайша, тәуекелдерді басқару осы белгісіз ортаны басқаруды білдіреді. Тәуекелдердің ақпараттық қауіпсіздігін басқару жүйесі тәуекелдерді бағалауға негізделген тәсілді талап етеді. Ақпараттық қауіпсіздік саясаты тәуекелдерді талдау нәтижелері бойынша қалыптастырылады. Сондықтан тәуекелдерді басқару өте маңызды. Сондай-ақ ақпаратты жүйелі пайдалану көздерді анықтауға және тәуекелдерді болжауға ықпал етеді. Ақпараттық жүйелер активтердің құнын, тәуекелдерді талдаудағы қауіптер мен кемшіліктерді талдайды. Мұнда тәуекелдер ақпараттық жүйелердің құпиялылығына, тұтастығына және сенімділігіне ықтимал әсердің ауырлығына байланысты бағаланады. Ұйым үшін құнды барлық нәрсе ақпараттың қол жетімділігі деп аталады. Стандарттар ақпараттың қол жетімділігін ұйым үшін құнды және әрқашан қорғалуы керек ақпарат ретінде анықтайды.

Түйін сөздер: тәуекелдерді басқару, тәуекелдерді өңдеу, тәуекелдерді бағалау, тәуекелдерді бақылау, тәуекелдерді қайта бағалау, тәуекелдерді талдау, ақпараттық қауіпсіздік тәуекелі.

А.Н. Ибрагимова

Бакинский Государственный Университет, Азербайджан, г. Баку
e-mail: aytakinibrahimli@gmail.com

Фактор риска и управление рисками в информационной безопасности

Риск – это следствие событий и опасностей. Таким образом, событие, которое приводит к ущербу или убыткам, можно описать с помощью информации. Слово «риск» означает вероятную опасность или потенциальный риск причинения вреда. Он определяет наступление

события, которое может привести к травме или ущербу. Этот термин является и может быть синонимом опасности, но применяется к событиям неизвестного происхождения или отсутствия. Таким образом, управление рисками означает управление этой неизвестной средой. Система менеджмента информационной безопасности рисков требует подхода, основанного на оценке рисков. Политика информационной безопасности формируется по результатам анализа рисков. Поэтому управление рисками очень важно. Систематическое использование информации также помогает выявлять источники и прогнозировать риски. Информационные системы анализируют стоимость активов, риски и недостатки при анализе рисков. Здесь риски оцениваются в зависимости от серьезности потенциального воздействия на конфиденциальность, целостность и надежность информационных систем. Все, что ценно для организации, называется доступом к информации. Стандарты определяют доступность информации как информацию, которая ценна для организации и всегда должна быть защищена.

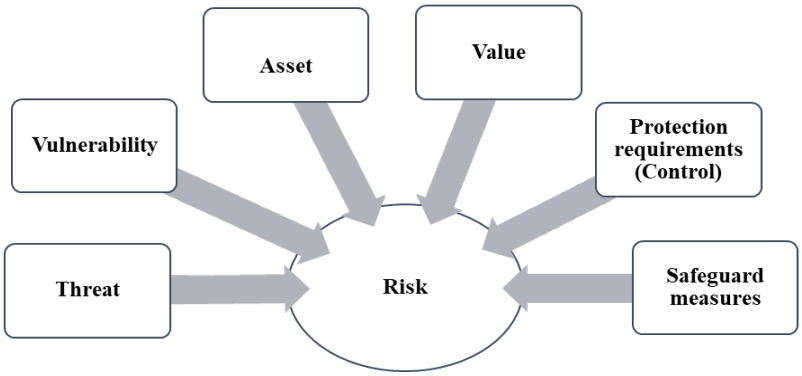
Ключевые слова: управление рисками, обработка рисков, оценка рисков, мониторинг рисков, переоценка рисков, анализ рисков, риск информационной безопасности.

Introduction

Risk management consists of the following steps:

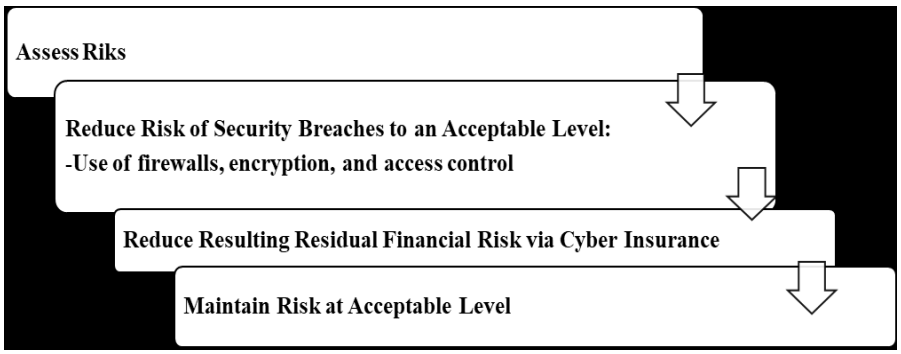
- Risk assessment
- Development of risk action plans
- Selection of related control mechanisms
- Risk monitoring, reassessment, and review (Humphreys E.2008 :249).

The figure shows the cycle of risk components. The means to increase risk are the value of the asset, the vulnerability of the asset, and the threats to the asset. Threats make use of the weakness of asset. Therefore, safeguard measures should be applied to reduce the associated risk. It is significant to measure the impact of the control / protection applied. Thus, the danger can be prevented and the risk reduced.



The source (Farn K.J., Lin S.K. and Fung A.R.W. 2004:507)

Information security management is similar to risk management. The figure below illustrates information security risk management (Lawrence A.Gordon& Martin P.Loeb.2003: 8):



A risk management framework should be established and maintained to assess and manage risks. The risk management framework should cover the general and specific organizational risk levels, the risk management strategies, and the remaining risks. Occurrences that are not expected to have any potential impact on the organizational objectives should be identified, analyzed and evaluated beforehand. Risk management techniques are applied in order to adjust the remaining risks to the acceptable level.

Materials and methods

While analyzing risk problems in information security, the latest doctrinal developments scientists, Eskiyoruk D., Farn K.J., Lin S.K., Fung A.R.W., Humphreys E., Hochstein A.Zarnekow, R.,Brenner W. and others, were used. When writing the study, a set of general and special methods of cognition were used: system and theoretical analysis, comparative legal, historical analytical, structural logical, technical methods etc.

Results and discussion

Risk processing methods. Methods of risk management should be selected in accordance with the aim and mission of each organization. Risk reduction methods can be listed in the form demonstrated below:

-Risk acceptance: the risk is accepted and the work is continuing.

- Avoidance of risk: Eliminates the cause of risk. (for example, not downloading or using a risky part of a program)

- Risk reduction: control reduction by reducing risk factors

- Transfer of risk: in case of realization of the risk, the situation should be transferred to others in search of solutions (for example, insurance) so to cover the damage.

Control Application

Upon finalization of the risk analysis, the existing risks in the system and the controls mechanisms are being identified. However, not every risk may be considered as risk which demands a precautionary measure. Bearing this in mind, from the perspective of organizational expenditure, it is essential to define risks which demand preventive measures to be taken and which of the existing control mechanisms should be applied (Hochstein 2005: 706).

- If a control mechanism that is applied to reduce risks emerged due to the undertaken activity, brings expenditure instead of benefits, then it is considered as a risk;

- In other cases, to overcome risks control mechanisms should be applied.

Control mechanism should be established in a way that it guarantees to overcome or reduce any risk in a range from the biggest to the smallest risks that might cause the damage to the performance of any entity considering the minimization of the financial costs required . The following steps should be undertaken during this period:

1. Risk ranking: Risks should be ranked according to the risk levels defined with the risk analysis. Priority should always be given to high risk levels, and measures to address these risk factors and hazards should be taken in advance.

2. Corresponding control assessment mechanism: Upon ordering the risks, preliminary defined controlled mechanisms should be assessed. Identified control mechanism may not be the most efficient or cost-effective control. A feasibility study will minimize the risk and the most appropriate control should be identified. At this stage, it will be appropriate to conduct a financial-revenue analysis for control mechanisms.

3. Selection of control mechanisms: According to the results of feasibility study and financial-revenue analysis, the most appropriate control mechanisms that will minimize the risk should be selected by management among the control mechanisms identified in the risk analysis. Selected control tools are a combination of technical, managerial, and organizational control mechanisms.

4. Identification of persons in charge of the activity: Persons eligible to apply these control mechanisms must be identified and authorized.

5. Development of a control plan: how the selected control mechanism will be applied, which steps are outlined and how long the control mechanism will be applied. This plan should cover at least the following criteria:

- Risks and risk levels
- Control mechanisms determined as a result of risk analysis
- Advantages
- Selected control mechanisms
- Required resources
- Persons authorized and responsible through the application of control
- Dates set for the application of control (start and end dates)

6. Application of chosen control mechanism: Application of chosen control mechanism should be

according to the developed plan. In case of prolonged application of control mechanisms, meetings can be held at appropriate intervals to assess progress, and the results can be included into reports to senior management. (Hochstein 2005: 706).

7. Additional risk: Applied control mechanisms might not eliminate the existing risk completely.

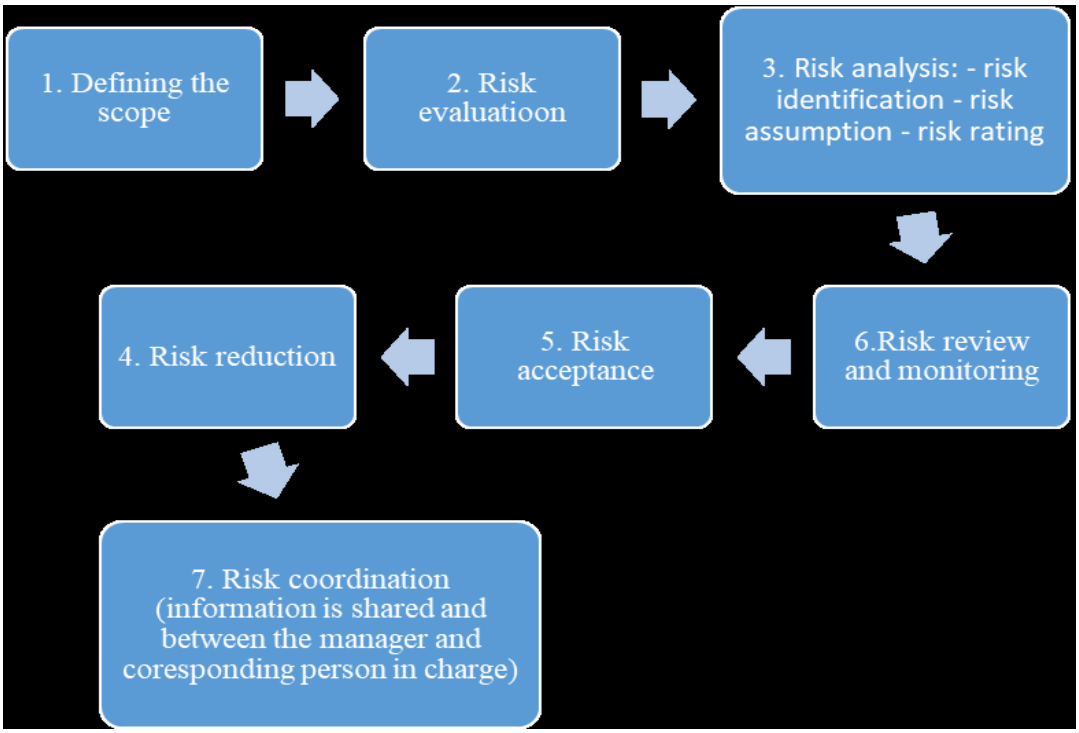
The risk remaining after eliminating the risk is called additional risk (Humphreys 2008: 250). If the current risk level exceeds the acceptable risk level, the risk analysis and risk mitigation should be undertaken again. In case the existing level of risk is below acceptable risk level, the additional risk should be documented, and the fact should be confirmed by the manager.

8. Risk monitoring, reassessment and review: Risk management covers a specific period, and the risk analysis and risk processing periods mentioned in this paper should be applied periodically. As a result, it will be determined to what extent the applied control has achieved its goal. Therefore, information technology and environmental factors are changing rapidly. Moreover, as time passes the organization's work objectives, form of implementation and priority issues may change. All these modifications will lead to changes in assets, in the values of assets, and in threats. The continued application of risk management will ensure that all these changes are taken into account and considered by the manager (Eskiyörük D.2015: 26).

In any enterprise, firstly, risks in the field of operational information are should be identified. Information security departments define the extent to which the current threat poses a risk to the network overall. Afterwards, risk priorities should then be identified, and appropriate action taken against potential risks according to the risk prioritization. This is the only way to minimize risks. The minimized risk according to risk levels can be re-evaluated under changing conditions and controlled with additional measures.

The first step in information security risk management is to determine the scope of risk, followed by the main stages of risk management, risk acceptance, as is emphasized in the relevant articles of the corresponding standard.

The main steps of information security risk management are (ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management):



1. Defining the scope of risk – is the first step in the risk management. The scope of risk management is determined by the needs and expectations of the entity. The following should be taken into consideration while defining the scope of risk:

- Strategy and policy expectations of the entity
- Working hours
- Sustainability of work
- Legal regulation directives
- Contract terms
- Corporate work experience and personal qualities
- Geographical locations

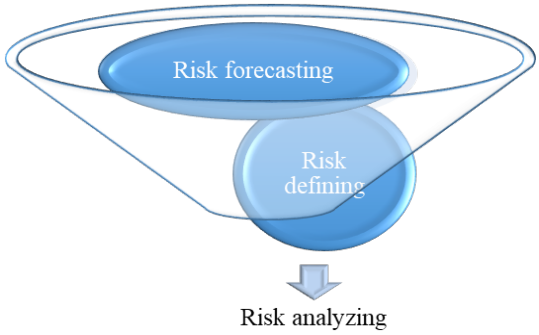
The published standards on this subject (ISO / IEC 27001, ISO / IEC 27005) do not interfere with the defined risk scope of the entity. Institutions may determine this scope according to their needs, but this definition requires that the risk scope document together with the stated reasons of the scope limits to be approved by senior management or a risk management committee appointed by the upper management.

2. Risk assessment: The article 4.2.1 of ISO / IEC 27001 standard requires an institutional risk assessment approach. The choice or definition of an assessment approach should take into account the needs of information security policy and regulatory requirements, as well as the needs of regulatory agencies, and should identify a systematic risk assessment methodology. The chosen risk assessment methodology should ensure that the risk assessments bring comparable and recoverable results (ISO/IEC 27001, 2013).

Risk assessment phases (ISO/IEC 27001, 2018):

- Risk analysis
- Risk determination
- Risk forecasting
- Risk classification

3. Information security risk analysis time frame is the value of information used in the calculation of information security risks, the identification of gaps and threats to information and all preventive measures.



This phase might seem as the most tedious stage. At this phase it is significant to apply a well-chosen or decided risk methodology, to identify the risks connected with the information carriers , and to rank them according to the estimated risks and risk effects.

Defining risks

The risk identification process is a step-by-step procedure: identifying existing data carriers, identifying the owners of these information carriers, ddefining threats on media, identifying gaps to be exploited by these threats and means of influencing the damage caused by the threat.

In the process of risk analysis, the probability of occurrence of the risk is determined. Nowadays, especially in commercial organizations, risk analysis methods based on verbal expressions such as very high, medium, low, and even low, or based on figures such as risk probability 0,1,2,3,4, are widely used. Opting for a mixed model that can use one or both methods may be different for each entity. However, in more limited scientific studies focusing on the likelihood of information security risk analysis suggestion to apply new models using artificial intelligence and other methods was provided, but in practice, which remained largely in academic form, they were insufficient to meet expectations.

4. Risk reduction: risks are identified by reviewing the risks according to the risks ordering identified as a result of the risk assessment. Upon considering the impact and probability of occurrence of a risk beyond the risk assessment period, one of the following decisions can be made according to the risk acceptance criteria:

- Risk reduction is the alleviation risk to an acceptable level by applying additional control mechanisms (risk reduction)
- Risk acceptance: It is the acceptance of risks knowingly and objectively, provided that the institution openly meets its policies and risk acceptance criteria (risk retention) (ISO/IEC 27001, 2013)
- Risk prevention: Risk avoidance is the elimination of risk in whole or in part by eliminating the causes that create the risk.
- Risk transfer: As a result of risk assessment, a decision may be made to insure or transfer part or all of the risk to a third party (risk transfer)

If the risk cannot be completely eliminated as a result of preventive measures to avert the risk, the remaining risk (residual risk) is considered as an additional risk. This residual risk also needs to be controlled.

5. Risk acceptance: ISO / IEC 27001 makes a note on the obligation to determine risk acceptance levels and tolerable risk levels. Institutions must always take into account their needs and expectations, goals, policies and procedures, and criteria such as compliance with domestic and foreign legal obligations when developing their own risk acceptance criteria. In general, it is adequate to live with risk when the damage to the information carrier is less than the cost of the risk mitigation measures.

Based on the value of risk measurement obtained as a result of risk analysis and assessment, institutions can decide what level of risk they will avoid. Moreover, the information must have the authority and obligation to accept and transfer a risk.

1. Risk coordination (distribution of risk information between the manager and a person in charge): is the distribution of risk information between the relevant responsible person and the management. Due to the risk coordination environment, the contribution and opinions of all stakeholders are taken into account, especially in the assessment of risks that will have a significant impact on the institutional base. In this way, all stakeholders can be informed about each phase of the risk management and thus they may contribute.

2. Risk monitoring and review: This is one of the significant phase of the information security risk management. Risk data obtained through risk coordination are reviewed at regular intervals according to the level of risk impact. While these periods vary according to the institution's risk policies and risk strategies, it is recommended in many standard or best programs that all risks to be reviewed at least once or twice a year. ISO / IEC 27001 requires a risk assessment by considering the residual risks over the planned period and the identified acceptable risk levels in a way that also takes into account adjustments that may occur in the tools listed below. The alterations cover the following:

- Structure
- Technological, labour factor, goals and deadlines
- Identified hazards
- Impact of applied control mechanisms
- Modified contractual obligations and alterations in the legal and regulatory environment
- External events such as modifications of the social environment

As stated in the standard, changes in the structure, form of conducting work, goals and priorities, innovations in technology, modification in applying and timing, changes in legal regulation and external interventions brought by legislators may require adjustments in risk assessment or cost of information carriers, including hazards and gaps. In such a situation, the duration of the risk management should be considered and, if required, the necessary updates should be made to ensure more efficient operation of the risk management.

The standard approach to "plan", "implement", "monitoring", "take actions", which is implied by international standards or management systems, also applies here. This phase forms the last two stages of the process. An organization is obliged to perform the following points in the field of information risk management:

- Formation of Information Risk Management Group or Committee
- Determining the value of ICT assets
- Identification of threats to the confidentiality, integrity, and application of each of these assets
- Analysing risks to each or all assets according to an acceptable risk management model
- Analysing the ways of risk management regarding each actual risk to information (accept risk, such as transfer or reduce risk);
- Continuation of the risk management activities by periodically repeating the specified period (California Counties "Best practices" Information Security Program 2010: 31-34)

However, here is one essential point to consider in this process is the choice of risk model. It would be more relevant to write down a mathematical equation of risk before embarking on risk models.

$$\text{Risk} = (\text{the ratio of threat to information}) \times \times (\text{value of information})$$

of the risk and will help the risk analysis team establish a sequence. One of the best ways to choose a model is to formulate risk models that characterize the risk that may arise for each piece of information and measure them by digitizing them. Some of these models involve detailed mathematical and statistical analysis required to draw accurate conclusions. When choosing a model, special attention should be paid to the selection of the model that best suits the needs of the enterprise or department. One of the most commonly used risk models is expressed with this equation.

$$\textbf{Risk}= \frac{hazard}{countre\ measures} \times \frac{vulnerability}{preventive\ measures} \times \times \frac{caused\ damage}{drawn\ conculsions} \times \frac{value}{applied\ efforts}$$

Expressions of variables in the equation are explained as follows:

- Threat is a method aimed to attack.
- Countermeasures are steps taken to prevent the threat of attacks.
- Preventive measures are a step taken to prevent the threat posed by attacks.
- Damage refers to the damage that occurs as a result of an attack.
- The result is positive values after an attack.
- Value is the merit given to those at risk
- This effort is all the work done to preserve value.

Management reveals how risk is managed and what approach is required. Financial analysis is performed for each approach. There are three main approaches to risk management. These are “risk acceptance”, “risk transfer” and “risk reduction”. (California Counties “Best practices” Information Security Program 2010: 35)

1. Acceptance of risk

Basically, there are two situations that make it obligatory for an entity to accept an impending risk:

- Firstly, the risk cost is low and at an acceptable level by the enterprise.
- Secondly, the cost of transferring or reducing the risk is costly than risk itself.

In both cases, the entity can accept the risk. If the cost of accepting the risk is greater than the risk reduction or transfer, the entity should not accept the risk. In this case, the other two options should be considered.

2. Risk transfer

Transfer of risk means that the risk in any area is shared by a third party or firm. This type of activity is mainly carried out by insurance companies. The identified risk is borne by the insurance company in exchange for an appropriate amount depending on the terms of the agreement and the circumstances in which the risk arises.

In such a situation, there may not be a third party to whom the risk will be transferred or the third parties who acknowledge the risk may not want to accept this identified risk. In this case, there will be options to accept the risk or mitigate the risk.

3. Risk mitigation

If the risk transfer does not take place at a high level, efforts should be undertaken to reduce the risk completely or partially. The mitigation period mainly covers the conditions for identifying and investigating threats and implementing effective measures in case of hazards

Reducing risk is sometimes the rapidest and cheapest way. Free security measures provided by information systems, automatic updating mechanisms, free elimination of detected errors should be evaluated from this perspective. The cost of risk reduction varies depending on what the risk is. A building with sensitive information systems should be strengthened and protected from natural disasters in case it can be easily exposed to natural disasters. The costs incurred for this purpose will increase the cost of risk reduction.

In this regard, the use of countermeasures is an effective tool in reducing risk. Taking preventive measures significantly reduces the amount of risk measured.

Planning

Planning is satisfaction of the enterprise needs by an enterprise or organization itself. It will also cover the risk measured as a result of the risk assessment and the preventive measures to be taken financially. The “basic security approach” means that the need can only be met by identifying security risk levels and taking minimal protection measures without a thorough risk analysis. This approach is also supported by the ISO / IEC 13335 technical report . However, there is no consensus on what the minimum safeguards will be. In this regard, it is more relevant for enterprises and organizations to conduct a detailed risk analysis in parallel with planning security measures for the results that will emerge after the analysis

The planning phase also includes the process of documenting the actions that occur. Drafting plans and other required papers for documentation also increases the application rate.

Application

Security measures are implemented in parallel with the prepared security plan / plans. All employees of the enterprise are responsible for the implementation of the plan, and the security agencies and higher executive bodies are responsible for its implementation. Topics to be covered in the application:

- Security management
- Application of smart work
- Data processing

- Communication networks
- System development (can be classified)

The classified topics cover different risks and areas of application. Trends formed by the structure of the enterprise may alter the security approaches to be applied in this regard.

International standards for information security measures and programs are based on the BS7799 (Code of Practice for Information Security Management) standard in the United Kingdom. In Turkey, it came into force under the title "TS ISO / IEC 17799 Information Technology – Application Principle for Information Security Management".

There are different concepts connected with the risk: additional risk, risk acceptance, risk analysis, risk assessment, risk rating, risk management, risk processing, etc.

Let's take a brief look at these concepts (ISO/IEC GUIDE 73:2009. Risk management–Vocabulary):

-Additional risk- risk is a risk which is left after completion of work

- Risk acceptance is the decision to undertake any risk.

- Risk analysis- is the systematic use of information to identify sources and predict risk.

- Risk assessment is the whole process that involves risk analysis and risk rating.

-Risk rating- is the process of comparing the probable risk with the given risk criteria in order to determine the significance of the risk.

- Risk management is an activity carried out by any organization to control and manage risk. Once the risk management framework has been established, the existing risks should be identified and plans for the identified risks should be developed. The implementation and results of the plans should be monitored and evaluated.

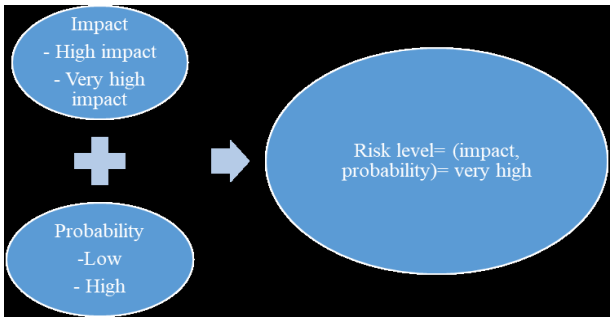
- Risk management is the process of selecting and applying preventive measures to alter risk. Moreover, the processes formed to minimize the existing risks are expressed as a complete process.

Risk basically consists of two components:

• Probability: The probability of occurrence of an unwanted event

• Impact: Damage, repercussions caused by the event of an accident.

Overall, a risk calculation formula can be expressed in a risk level can be expressed as = f (probability, impact). When deciding on the level of risk, decisions are made based on the probability and impact of the risk. As an example, consider the following figure:



Information security risk

Deficiencies of information or information carriers are the result of the misuse conducted by an institution in the face of a threat (ISO/IEC 27005. Information Technology–Security Techniques–Information Security Risk Management. ISO. (2008)) The key features that are important for the protection of information, such as confidentiality, integrity and accessibility, are the known vulnerabilities on the media, or the misuse of this vulnerability, which is likely to harm the organization.

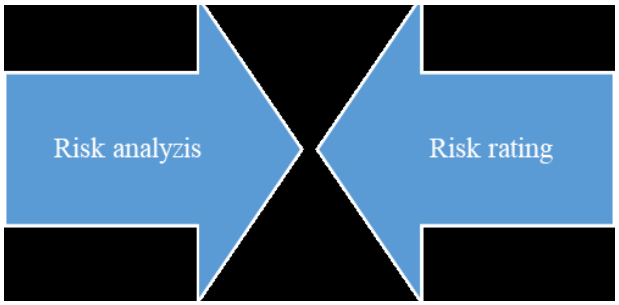
Risk management

The period of identification, control, and minimization or elimination of security risks that may affect information systems at an appropriate cost.

Clearing the identified risks from the damage they have caused to the entity, or managing the risk in a way that will have the least adverse effect. As a result of the risk assessment, the risks can be completely eliminated, and the risk left after the impact of the risk has been reduced to a certain level is an additiona risk (ISO/IEC 27005.Information Technology–Security Techniques–Information Security Risk Management. ISO. (2008)). Risk management must be done to minimize the impact of risk. We can show the duration of risk management in the following stages:

Risk assessment

Covers the entire period, including risk analysis and risk rating. Assessment of threats to information and information processing tools, the impact of hazards on information, the use of information and the likelihood of the occurrence of threats (ISO/IEC 17799:2005). Risk evaluation:



Conclusion

It is the systematic use of information to identify sources and predict risk. Information systems analyze the value of assets, threats and shortcomings in risk analysis. Here, the risks are assessed in relation to the severity of the potential impact on the confidentiality, integrity and reliability of information systems and it includes:

➢ Availability of information: Anything that has value to an organization is called information availability. Standards define the availability of information as information that is valuable to an entity and should always be protected. If this institution is considered as a bank, the information may include the followoings: customer information (general customer services, deposits, credit, credit card, intelligence agencies, contract, etc.) entity related information (programs, licenses, analysis and technical documentation, data, servers, communication networks, internet, etc.).

➢ Risk probability: the probability that a threat will exploit a gap in information, or the probability that a threat will turn into an accident. The value obtained from an accurate gap level measurement with the probability of occurrence of a threat to the availability of information is called the probability of risk. The probability of a risk can be expressed by the formula = f (exact gap, probability of danger). The result is mainly determined by looking at the function parameters. The result received is used to measure an effect of risk. For example, if the threat reflected on an information is highly probable and is protected as information, the level of realization of this risk may be considered low.

➢ Level of impact on the work: It is to determine the severity of the damage caused by the threat to the information as a result of misusing an existent gap in order to cause damage to information security. Decision-makers can determine the criteria and draw the final decision of whether an organization will be affected upon inflicted damage

➢ Risk value is the value obtained using the level of risk and the level of its impact on the work. The value of the risk is measured using the level of exposure to the gaps and hazards reflected in each piece of information obtained from the risk analysis. The formula for this is the following:

Risk value = F (f (Information gaps, probability of danger), level of impact on work)

➢ Risk assessment: is the value of a criteria of comparing the probable risk with the given risk in order to determine the significance of the risk. Risk scores obtained as a result of risk measurement are equated to a certain priority. As a result of risk ranking, it is easier to determine which risk should be considered earlier, which later, or at the same time, and to develop risk management plans, which contributes to the implementation of effective risk management.

Risk management: refers to the process of selecting and applying the necessary measures to change the risk (ISO/IEC 31000. Risk Management-Principles and Guidelines, 2009). A risk at the end of the risk can be classified:

- Lifting up: It can be completely eliminated by taking preventive measures;
- Admission: either all or part of the activity is accepted;
- Transfer: In some cases, it may be decided to reduce or eliminate additional measures, just as a risk transfer decision may be made

For instance, if a risk analysis and assessment reveal that the threat is no longer present, there will be no need for additional controls.

➢ Excessive risk: the additional risk left after finalizing the operation is called an excessive risk (ISO/IEC 31000. Risk Management- Principles and Guidelines, 2009). It is expressed as the risks remaining after the application of security measures. The risk which is still in place after the finalization of risk management when the risk has not been completely eliminated or the undesirable risk due to expenditures cannot be brought to an acceptable level is called an excessive risk. It is given by the formula in the following order:

Excessive risk = Total risk – eliminated risk

➢ Risk termination: It is a termination decision made as a result of working with risk. The decision to terminate the risk can be made in the form of transfer, acceptance or elimination of the risk:

• Risk transfer: is the insurance of information against a risk so to avoid the risk of loss of information

• Risk acceptance: is the decision to undertake a risk. It is defined as an informed decision that assumes the probable outcome of a particular risk.

• Risk elimination: the elimination of the risk reflected in the information as a result of undertaking additional control mechanisms and measures.

References

Amir Aliyev, Gulnaz Rzayeva, Aytakin Ibrahimova, Bahruz Maharramov, ShahinMamadrzali. Information law. Textbook. Baku, 2019, 470 p.

Gulnaz Rzayeva, Aytakin Ibrahimova. Artificial Intelligence, human rights and personal data security. Text-book. Baku: "Nurlar" Publishing House, 2020, 200 p.

Eskiyörük D., Organizational Communication, Cinius Publications, Istanbul, 2015, 207 s.

California Counties "Best practices" Information Security Program, California County Information Services Directors Association, CCISDA Information Security Forum, 2010. 47 P

Farn K.J., Lin S.K. and Fung A.R.W., "A study on information security management system evaluation–assets, threat and vulnerability"., Computer Standards & Interfaces 26(6), 2004. P. 501-513

Humphreys E., Information security management standards: Compliance, governance and risk management",Information Security Technical Report 13(4), 2008., p.247–255

Hochstein A.,Zarnekow R.,Brenner W., ITIL as Common Practice Reference Model for IT Service Management: Formal Assessment and Implications for Practice",The 2005 IEEE International Conference,2005., p.704-710.

ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management

ISO/IEC 27001, 2013

ISO/IEC 27001, 2018

ISO/IEC 17799:2005

ISO/IEC 27005.Information Technology–Security Techniques–Information Security Risk Management. ISO. (2008).

ISO/IEC 31000. Risk Management- Principles and Guidelines, 2009

ISO/IEC GUIDE 73:2009. Risk management–Vocabulary https://www.iso.org/standard/44651.html 11.11.2021

Lawrence A.Gordon& Martin P.Loeb., Economic Aspects Of Information Security.University of Maryland, College Park, 2003,24 p. http://www.umiacs.umd.edu/docs/umiacspresentation.pdf