Irmina Chmielowska

Kamil Kwiatkowski

Krzysztof Pochrebiennik

Jakub Wrzodek

Przemysław Gradziński

Information Security Management System

Report

Task 4:

Prepare an Information Security Management System for a health insurance company. The company processes a large volume of medical transactions of their clients and must distinguish fake transactions from the genuine ones. Moreover, the company stores an archive of the transactions for the purpose of calculating future insurance rates.

Table of Contents:

1. **Context establishment** **2**
   1. Scope and boundaries…………………………………………………………………2
      1. The organization’s main purpose…………………………………………...….2
      2. The organization's business…………………………………………………….2
      3. The organization’s motto……………………………………………………….2
      4. The organization’s values…………………………………………..…………..2
      5. Structure of the organization…………………………………………………...3
      6. List of the constraints affecting the organization………………………………3
      7. List of the legislative and regulatory references applicable to the organization.3
   2. Basic Criteria………………………………………………………………………….4
      1. Risk evaluation criteria…………………………………………………………4
      2. Impact criteria……………………………………………………………….….5
      3. Risk table……………………………………………………………………….6
      4. Risk assessment criteria…………………………………………………...……6
      5. Risk acceptance criteria………………………………………………...………7
   3. Development of the information security risk…………………………….…………..9
      1. Archiving of important records………………………………………...………9
      2. Establishment of important relations between the parties…………….………10
      3. Definition of decision escalation paths………………………………..………10
      4. Definition of the responsibilities of internal and external parties…………….10
      5. The hierarchy of persons responsible for ISMS………………………………10
2. **Risk assessment 11**
   1. Risk analysis…………………………………………………………………………11
      1. Risk identification……………………………………………………….……11
         1. Identification of assets………………………………………...………11
         2. Identification of threats…………………………………….………….13
         3. Identification of existing controls……………………………..………15
         4. Identification of vulnerabilities………………………………..………15
         5. Identification of consequences……………………………………..…17
      2. Risk estimation…………………………………………………………..……19
   2. Risk evaluation……………………………………………………………….………21
3. **Risk treatment plan** **23**
4. **Risk acceptance statement** **26**
5. **Risk communication** **28**
6. **Risk monitoring and review** **29**
7. **Context establishment**

Information security is important for the business; however, its importance is generally underestimated. Main reason is that the profits of high developed information security management system are not easily palpable – their point rely on preventing loss, of any kind. As figures speak louder than words, resulting business losses should be quantified as a consequence of actual, simulated, and hypothetical security breaches. However, we understand ISMS necessity, especially in insurance industry, therefore we put effort into implementing system in our company.

Following document covers necessary points of Information Security Management System, according to ISO/IEC 27005:2008.

* 1. Scope and boundaries
     1. The organization’s main purpose
* provide health insurance services
* providing around the clock information and help via call center
  + 1. The organization's business:
* developing an algorithm for calculating future insurance rates, based on past transactions archives
* storing and processing a large volume of medical transactions data
* monitoring signed contracts and reacting to risk calculations changes (reinsurance etc.)
* observing market prices in order to ensure competitive offers
* constant growth towards gaining new customers and sustain current ones
* investing in employee competences
  + 1. Organization motto

Better health, better life.

* + 1. Organization’s values:
* attention to details
* respect for privacy
* ability to adapt to changing conditions
* quick response to client’s requests
  + 1. Structure of the organization:
* call center department – receiving calls from clients - x people
* sales department - sustain customers, get new ones – x people
* compensation department – claims settlement – x people
* analytic section – group engineers and economists developing an algorithm and analyzing data in order to create profitable contract data – x people
* system administrators - company’s infrastructure maintenance – x people
* accountancy – keeping pay records, archive company’s turnover data – x people
* financial section – making investment decisions – x people
* legal section – taking care of legal side of business – x people
* public relations and marketing – creating positive company image and brand recognition – x people
* human resources - recruiting new workers – x people
* guards receptionists and cleaning staff – x people
* management of the company – making decisions about the company’s operations based upon reports and analyzes provided from departments - x people
  + 1. List of the constraints affecting the organization
* HR constraint: shortage of skilled computer security employees
* Financial: investment priority of stakeholders is mainly focused on visible income, information security is less important matter
* Technical: Large volume of medical transactions and customer data, moreover company uses Libre Office as main office suite
* Legal: General Data Protection Regulation sets additional restrictions on handling customer data
* Environmental: SARS-CoV-2 spread, managers have to work remotely
  + 1. List of the legislative and regulatory references applicable to the organization

The main legal acts related to information security are:

* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (General Data Protection Regulation )(Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych))
* Consolidated text of the EP and Council Regulation (Skonsolidowany tekst rozporządzenia PE i Rady (UE) 2016/679 z 27 kwietnia 2016 r.)
* Corrigendum to European Parliament and Council regulation (Sprostowanie do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r.)
* Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June

2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem).

* Act of 16 April 1993 on combating unfair competition. (Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji.)
  1. Basic Criteria

As health insurance company we process large volume of medical transactions of our clients and store an archive of the transactions for the purpose of calculating future insurance rates. This directly influences types of criteria we want to adopt, and way we approach them.

* + 1. Risk evaluation criteria

Since we are health insurance company, information safety is crucial for us. Not only because of the company’s prosperity, but also our customers safety and privacy, and numerous legal regulations regarding handling of personal data. Following risk prioritizing rules have been chosen:

* Prioritizing by probability of occurrence
* Prioritizing by criteria of impact, as percentage of annual income
* Additionally, risks with legal consequences cannot be accepte

Which has been gathered in following tables:

|  |  |  |
| --- | --- | --- |
| Probability of occurence criteria | Point value | Case |
| Neglible | 0 | An event can occur only in exceptional circumstances (event that occurs once in 5 years), it concerns individual cases. |
| Low | 1 | It is unlikely that this event will occur (event that occurs once per 2 years), it applies to a few cases. |
| Medium | 2 | The event is likely to occur in the near future (event that occurs once per year), it applies to some matters |
| High | 3 | The occurrence of the event is very likely (event that occurs at least once per year). It is expected that such an event may occur several times a year. |

Table 1. Probability of occurrence criteria.

* + 1. Impact criteria

|  |  |  |
| --- | --- | --- |
| Level of impact | Point value | Case |
| Insignificant | 0 | Negligible effect on the objectives and tasks of the organization, no legal effect; slight financial effect, no impact on employee safety, no impact on the image of the organization.  Less than 0,1% of annual income |
| Low | 1 | Little impact on the achievement of goals and tasks, without legal effects, little financial effect; no impact on employee safety, little impact on the image of the organization.  0,1 – 1% of annual income |
| Medium | 2 | The average impact on the implementation of objectives and tasks, potential threats may lead to the failure to perform basic tasks within a specified scope, moderate legal consequences, average financial effect, no impact on employee safety, medium risk of losing good image.  1 – 5% of annual income |
| High | 3 | Serious impact on the implementation of the task, including a serious threat to the date of its implementation and achievement of the goal; extensive legal consequences; threat to employee safety; high financial losses; loss of a good image of the organization in the environment and in public opinion.  More than 5% of annual income |

Table 2. Level of impact criteria.

* + 1. Risk table

Risk values have been calculated as sum of impact and probability.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Risk | | Impact | | | |
| 0 | 1 | 2 | 3 |
| Probability | 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 3 | 4 | 5 |
| 3 | 3 | 4 | 5 | 6 |

Table 3. Risk values

We consider risk as:

• Low – [0 to 2]

• Medium [3 to 4]

• High [5 to 6]

With the note that risk can’t be accepted at any level, if it has legal consequences.

* + 1. Risk assessment criteria:

• The strategic value of the business information process -> business information process is shaped by future insurance rates, so it is an offer and the opportunity to acquire new customers. Its absence results in a lack of customers.

Impact(2), Probability(2), Risk(4)

• The criticality of the information assets involved -> assessment of the reliability of up-to-date information stored in the company database. Falsification and manipulation of the information could be used to steal goods and collect large amounts of financial money from the company.

Impact(2), Probability(2), Risk(4)

• Legal and regulatory requirements and contractual obligations -> Are the company’s main base, because when they are not strict enough, the potential customer will abuse them by using the company's finances wrongly. When you take into account the criterions on the scale of many customers with potential bad intentions, this can result in the collapse of the company.

Impact(2), Probability(2), Risk(4)

• Operational and business importance of availability, confidentiality and integrity -> build trust with the customer. As an insurance company, health is the key point provide a steady income. Customers will be willing to spend more money by their own will to take out insurance. Otherwise, this will limit the company's revenue to some extent.

Impact(1), Probability(1), Risk(2)

• confidentiality and honesty -> in this case, there are many insurance companies that do not meet these conditions. So the risk margin is remote, however it is good to stand out as a reliable and honest company.

Impact(0), Probability(0), Risk(0)

• Expectations and perceptions of stakeholders and negative consequences for goodwill and reputation ->perception of stakeholders is important, although insurance companies are famous of. If the company is aspiring to reach the richest customers negative reviews will not allow it. However, for most leads, this will not significantly affect.

Impact(0), Probability(1), Risk(1)

Qualitative estimate - scales and attributes eligible to describe the magnitude of potential consequences:

- low; Impact(0), Probability(0), Risk(0)

+medium; ; Impact(1), Probability of occurrence(1), Risk(1-2)

++high;; Impact(2), Probability(2), Risk(3-4)

generally: Impact(7), Probability(8), Risk(15)

• Breaches of information security (e.g. loss of confidentiality, integrity and availability) -> risk of claiming financial compensation by a company client. When security breaches are high, the company is spleened by lawsuits. 5%

• (Reduced quality actions) Impaired operations (internal or third parties) -> Reduced-quality internal activities can bring big losses and put the company at high risk. An example is an error in calculating future insurance rates. Even a small difference can cause the company to collapse. On the other hand, external works of reduced quality, such as marketing, advertising – it will not be as significant and the company will still have a chance to generate profits. 5%

• Loss of business and financial value -> It is worth having these criteria under constant analysis, as it can indicate the reason for the generation of losses by the company and be a good clue to finding mistakes made when managing your business. This will help to minimize the losses generated. 3%

• Disruption of plans and deadlines -> This is noticeable in any larger enterprise and should usually be minimized such distortions, but are inevitable. When paying insurance rates, a margin of several weeks can be adopted so that the company has a constant financial potential, at the expense of a minor reputational downgrade. 2%

• Damage of reputation -> inhibits the growth of future, potential customers and thus limits the possibility of business development. This are important points, however into building the company's reputation. It is difficult to sharply sway the reputation of the company, so this criterion can be considered low risk. 0.5%

• (exception) Breaches of legal, regulatory or contractual requirements -> with high risk and a case of state-owned government shutdown. 15%

impact criteria:

-low; less than 1% of annual income

+medium; 1% to 5% of annual income

++high; more than 5% of the annual

Initial output: 3,1%(5,08%)

* + 1. Risk acceptance criteria

• Business criteria 2,2,4 | 1,1,2|0,1,1|5%, 3%, 2%, 0,5%

Risk acceptance level: 5%

Risk status: 4,725%

• Legal and regulatory aspects 2,2,4|5%, 15%

Risk acceptance level: 30% for infringement of legislation up to 3months

Risk status: 40%

• Operations |5%, 5%, 3%, 2%

Risk acceptance level: 15%

Risk status: 20%

• Technology 2,2,4 | 5%, 2%

Risk acceptance level: 8,75%

Risk status: 10%

• Finance 2,2,4|5%, 3%

Risk acceptance level: 10%

Risk status: 8%

• Social and humanitarian factors 2,2,4| 1,1,2|0,0,0|0,1,1|5%, 2%, 0,5%

Risk acceptance level: 5,62% for infringement of legislation up to 6months

Risk status: 8%

((ΣImpact + ΣRisk)/ ΣProbability) \* impact criteria

**Risk is acceptable if its less or equal level 3 from risk table, and it doesn’t lead to legal consequences.**

* 1. Development of the information security risk

The appropriate information security risk management process should be tailored to the nature of the organization. For the health insurance company should be established assessing the reality of transactions system. To manage risk, must be develop a plan to assess the severity of the hazards and identify potential hazards.

* + 1. Archiving of important records

The specification of records that should be kept is the basis of any risk assessment system. Records should contain relevant information from the point of view of the health insurance company, such as:

* date of recording (date of transaction execution)
* transaction process
* transaction result (if it was found to be false or true)
* parties involved in the transaction
  + 1. Establishment of important relations between the parties

It is extremely important for the proper functioning of the organization to determine the relationship between this organization and the units with which it cooperates under the system being developed. For the health insurance company, it is crucial to establish the relationship between it and private clients as well as entire companies.

* + 1. Definition of decision escalation paths

Inadequately designed decision escalation paths can destroy entire projects by complicating the production and development process. Regardless of the company's sector, decision escalation paths should be:

* easy to read and understand
* uncomplicated (minimizing the number of paths)
* flexible (easy to update)
  + 1. Definition of the responsibilities of internal and external parties

Establishing internal obligations is a requirement for the functioning of each organization. Creating an appropriate hierarchy of responsibility and controlling positions allows ensuring the proper functioning of the organization. Determining the liability of external parties is part of the contract. Therefore, they are obliged to fulfill specific responsibilities.

* + 1. The hierarchy of persons responsible for ISMS

Four important roles make up the Information Security Section. The Information Security Section is in cooperation with the legal department. Main person in the responsible for ISMS hierarchy is the Information Security Officer. He has to coordinate all activities related to the ISMS and communication of information relating to ISMS in the Organization. Information Security Officer appoints three deputies focused on a specific sector of responsibility:

* network and software security
* organizational procedures and updates of ISMS
* physical security and surveillance systems

1. **Risk assessment**

2.1. Risk analysis

2.1.1. Risk identification

2.1.1.1. Identification of assets

* The primary assets

Company’s good reputation:

The company will not break laws in its assumptions and take care of the highest best interests of the customer. Thanks to such attitude, company will be well known of good reputation and appreciated by other customers.

**Relevance of assets: low**

The process of security evaluation of client’s products:

In our insurance company, the target product for us is customer’s payment of the insurance contribution. When a company accepts proper people to manage their budgets, it can guarantee a timely payment of the amount of insurance. Otherwise, the client can be delayed and the company record losses.

**Relevance of assets:**  **medium**

Personnel with new devices and solutions:

It’s important to hire well prepared and professional employees, as they’re the first-level contact with client. To achieve it, you should provide numerous of trainings, that will require to prepare additional company’s budget. There should include also employees of basic work tasks, computer and phone service.

**Relevance of assets: low**

The research process that allows to issue new publications and supports company’s good image:

To achieve client’s trust and authentic image of the company it is very important matter. In order to build trust with the client, the company will cooperate with schools and medical university, financing selected scientific publications. In this way, the company will build its authority, while supporting beginners to develop their learning process. This is more effective solution than investment in advertisements.

**Relevance of assets:**  **low**

The recruitment process enabling the company to grow gradually:

Acquiring new employees is also a development of the company and even necessary for the proper functioning and growth of the company. However, the deficit of the number of employees can be easily replenished.

**Relevance of assets: low**

* The supporting assets

The core personnel:

Core personnel has a lot to provide in the company working in it for many years and thus, has access to a lot of information. Both to confidential information as well as secret information. If such employee would use confidential information in work with another company and consciously betray our company conduct, the consequences would be meaningful harmful.

**Relevance of assets:**  **high**

The contracts executions:

Contracts are currently being executed as a source of recent income for the company and it is in process until will be necessary to finalize them. Otherwise, this can result in a budget hole that will result in less efficiency of the company.

**Relevance of assets: medium**

The gathered database for the past 10 years regarding attacks on client’s devices:

This is an important collection of information that can be reference point for new attacks. This will improve system security against future attacks and guarantee customers the safe use of the company's services.

**Relevance of assets: medium**

The laboratory equipment and software tools:

Very important in building security and software. Their deficit can compromise the reputation of the company.

**Relevance of assets:**  **medium**

The software for automatic analysis of client’s documentation:

It allows for fast information flow provided by the customer and thus, to a smooth response from the company for the submitted customer documentation.

**Relevance of assets: low**

Confidential information zone:

Security of the information on the highest level, without straight access to confidential finance information.

**Risk of assets: medium**

Secret information zone:

The security of the company's information is at the most confidential level. After leaking such information, the company’s bankruptcy is almost sure. We should invest in the best security features, including DNA readers and biometric verification.

**Relevance of assets: high**

The network and the supportive software:

The software that belongs to this office, e-mail clients, encryption and decryption software which are the main keys to the correct operation processes of the company.

**Relevance of assets: high**

The supporting personnel:

Helps in the daily functioning of the company.

**Relevance of assets: low**

2.1.1.2. Identification of threats

• Physical damage:

– Fire: Probability 1, Impact 2 --> Risk 3

– Water damage: Probability 0, Impact 1 --> Risk 1

– Pollution: Probability 0, Impact 1 --> Risk 1

– Major accident: Probability 1, Impact 3 --> Risk 4

– Destruction of equipment or media: Probability 1, Impact 2 --> Risk 3

• Type of threat - natural events:

– Climatic phenomenon: Probability 1, Impact 1 --> Risk 2

– Seismic phenomenon: Probability 1, Impact 1 --> Risk 2

– Meteorological phenomenon: Probability 2, Impact 1 --> Risk 3

• Loss of essential services:

– Failure of air-conditionin: Probability 2, Impact 2 --> Risk 4

– Loss of power supply: Probability 3, Impact 2 --> Risk 5

– Failure of telecommunication equipment: Probability 1, Impact 3--> Risk 4

• Compromise of information:

– Remote spying: Probability 1, Impact 3 --> Risk 4

– Eavesdropping: Probability 1, Impact 3 --> Risk 4

– Theft of media or documents: Probability 2, Impact 3 --> Risk 5

– Theft of equipment: Probability 1, Impact 3 --> Risk 4

– Disclosure: Probability 1, Impact 2 --> Risk 3

– Data from untrustworthy sources: Probability 1, Impact 1 --> Risk 2

– Position detection: Probability 1, Impact 1 --> Risk 2

• Technical failures:

– Equipment failure: Probability 1, Impact 3 --> Risk 4

– Software malfunction: Probability 1, Impact 2 --> Risk 3

– Breach of information system maintainability: Probability 1, Impact 1 --> Risk 2

• Unauthorised actions:

– Unauthorised use of equipment: Probability 1, Impact 2 --> Risk 3

– Fraudulent copying of software: Probability 1, Impact 3 --> Risk 4

– Corruption of data: Probability 1, Impact 2 --> Risk 3

– Illegal processing of data: : Probability 1, Impact 3 --> Risk 4

• Type of threat - Compromise of functions:

– Error in use: Probability 1, Impact 2 --> Risk 3

– Forging of rights: Probability 1, Impact 1 --> Risk 2

– Denial of actions: Probability 1, Impact 2 --> Risk 3

– Breach of personnel availability: Probability 1, Impact 3 --> Risk 4

2.1.1.3. Identification of existing controls

To identify and evaluate state of existing controls, following activities have been carried out:

* Reviewing documents containing information about the controls: risk-related documents, risk treatment plans
* Interviews with the people responsible for information security and the users as to which controls are really implemented
* Comparing implemented physical controls with the list of what controls should be there, and checking for correctness and efficiency.
* Reviewing results of previous internal audits

Existing organizational and legal controls:

* Security awareness trainings for new employees
* Every employee has to sign NDA
* Agreement with security company - if alarm is raised, armed employees have to arrive within 5 minutes

Existing physical controls:

* Alarm system
* Doors and windows have anti-burglar reinforcements

Existing IT controls:

* All data about clients and transactions are securely encrypted
* Emails are sent signed and encrypted
* Regular checking for software updates
* Company is using Kaspersky Internet Security on every computer
* Fake transaction distinguishing algorithms
* Users have limited access rights to company computers
* USB ports are monitored

2.1.1.4. Identification of vulnerabilities

Proactive methods in identification of vulnerabilities:

* Code review and analysis.
* Automated vulnerability scanning tools.
* Penetration tests.
* Security testing and evaluation.

Components in the process of identifying vulnerabilities:

* + Input data contains:

List of known threats during the transaction between the client and the health insurance organization, the list of resources at the disposal of the organization and existing controls establishing the rules for concluding the contract and determining the security of personal data and key information for the operation of health insurance organizations.

* + Action:

Identify vulnerabilities that protect your health insurance company against leaks of valuable data such as customer, employee, and contract details. Appropriate safeguards against system overloading should be performed with DDos attacks.

* + Output data:

A list of vulnerabilities not related to any identified risk for review, problematic from the point of view of securing a place in the security system of health insurance organizations. Points not included in activities of the action section.

Security vulnerabilities can be identified in the following areas:

* Entire insurance organization
* Staff such as specialists, managers etc.
* Physical environment - including the ability to access the center for third parties
* Management procedures and their disadvantages
* Dependence on external sites

Code review and analysis:

Reviewing the source code is the most expensive and the most accurate way to assess vulnerabilities.

Automated vulnerability scanning tools:

It is used to scan hosts, client accounts or the entire network for commonly known sensitive services. It allows you to quickly identify known vulnerabilities. Unfortunately, some of the weaknesses obtained thanks to the scanning process may not correspond to the designed security system of the insurance company.

Penetration tests:

Tests involving intentional attacks against potential vulnerabilities in the health insurance security system. Penetration tools and techniques can give false results unless the vulnerability is successfully exploited.

Security testing and evaluation:

Includes development and execution of the test script along with testing procedures and expectations. The purpose of system security testing is to check the current effectiveness of security checks.

Reactive and other methods in identification of vulnerabilities:

* Interview of potential clients, employees and ordinary unrelated people with the insurance organization.
* Analysis of documents (employment contracts, contracts with third parties as well as documents specifying individual health insurance with clients).
* Use questionnaires to examine (identical to the above) groups of people to obtain information on possible vulnerabilities.
* Physical control using specially appointed personnel.

2.1.1.5. Identification of consequences

List of incident scenarios with their consequences:

• **Physical damage**: fire, water damage, pollution, major accident, destruction of equipment or media;

Consequences: investigation and repair time, financial cost of specific skills to repair the damage, (work)time loss, opportunity loss, health and safety loss, data loss;

We consider the impact as High.

• **Natural events**: climatic phenomenon, seismic phenomenon, meteorological phenomenon;

Consequences: investigation and repair time, financial cost of specific skills to repair the damage, (work)time loss, opportunity loss, health and safety loss, data loss, customers loss;

We consider the impact as Very High.

• **Loss of essential services**: failure of air-condition, loss of power supply, failure of telecommunication equipment;

Consequences: investigation and repair time, financial cost of specific skills to repair the damage, opportunity loss, customers loss;

We consider the impact as Medium.

• **Compromise of information**: remote spying, eavesdropping, theft of media or documents, theft of equipment, disclosure, data from untrustworthy sources, position detection;

Consequences: financial cost of specific skills to repair the damage, (work)time loss, safety loss, data loss, customers loss, confidentiality loss, image reputation and goodwill loss;

We consider the impact as Very High.

• **Technical failures**: equipment failure, software malfunction, breach of information system maintainability;

Consequences: investigation and repair time, financial cost of specific skills to repair the damage, (work)time loss, opportunity loss, customers loss, image reputation and goodwill loss;

We consider the impact as High.

• **Unauthorised actions**: unauthorised use of equipment, fraudulent copying of software, corruption of data, illegal processing of data;

Consequences: financial cost of specific skills to repair the damage, (work)time loss, opportunity loss, data loss, confidentiality loss, customers loss, image reputation and goodwill loss;

We consider the impact as Very High.

• **Compromise of functions**: error in use, forging of rights, denial of actions, breach of personnel availability;

Consequences: investigation and repair time, (work)time loss;

We consider the impact as Low.

2.1.2. Risk estimation

Qualitative risk assessment:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Category | Name | Probability | Impact | Risk score |
| 1.1 | Physical damage | fire | Very low | High | Medium |
| 1.2 | water damage | Implausibility | High | Low |
| 1.3 | pollution | Implausibility | High | Low |
| 1.4 | major accident | Very low | High | High |
| 1.5 | destruction of equipment or media | Very low | high | Medium |

Table.4. List of risks depending on the physical damage with value levels assigned.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Category | Name | Probability | Impact | Risk score |
| 2.1 | Natural events | Climatic phenomenon | Very low | High | Low |
| 2.2 | Seismic phenomenon | Very low | High | Low |
| 2.3 | Meteorological phenomenon | Low | High | Medium |

Table.5. List of risks depending on the natural events with value levels assigned.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Category | Name | Probability | Impact | Risk score |
| 3.1 | Loss of essential services | Failure of air-conditioning | Low | Low | High |
| 3.2 | Loss of power supply | Medium | Low | Very high |
| 3.3 | Failure of telecommunication equipment | Very low | Medium | High |

Table.6. List of risks depending on the loss of essential services with value levels assigned.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Category | Name | Probability | Impact | Risk score |
| 4.1 | Compromise of information | Remote spying | Very low | Medium | High |
| 4.2 | Eavesdropping | Very low | Medium | High |
| 4.3 | Theft of media or documents | Low | Medium | Very high |
| 4.4 | Theft of equipment | Very low | Medium | High |
| 4.5 | Disclosure | Very low | Low | Medium |
| 4.6 | Data from untrustworthy sources | Very low | Very low | Low |
| 4.7 | Position detection | Very low | Very low | Low |

Table.7. List of risks depending on the compromise of information with value levels assigned.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Category | Name | Probability | Impact | Risk score |
| 5.1 | Technical failures | Equipment failure | Very low | Medium | High |
| 5.2 | Software malfunction | Very low | Low | Medium |
| 5.3 | Breach of information system maintainability | Very low | Low | Low |

Table.8. List of risks depending on the technical failures with value levels assigned.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Category | Name | Probability | Impact | Risk score |
| 6.1 | Unauthorised actions | Unauthorised use of equipment | Very low | Low | Medium |
| 6.2 | Fraudulent copying of software | Very low | Medium | High |
| 6.3 | Corruption of data | Very low | Low | Medium |
| 6.4 | Illegal processing of data | Very low | Medium | High |

Table.9. List of risks depending on the unauthorised actions with value levels assigned.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Category | Name | Probability | Impact | Risk score |
| 7.1 | Compromise of functions | Error in use | Very low | Low | Medium |
| 7.2 | Forging of rights | Very low | Very low | Low |
| 7.3 | Denial of actions | Very low | Low | Medium |
| 7.4 | Breach of personnel availability | Very low | Medium | High |

Table.10. List of risks depending on the compromise of functions with value levels assigned.

2.2 Risk evaluation

The following list of risks was prioritized according to the company’s main

values and assets.

Very high risk value:

As the company’s main asset is a secure, private storage of data,

the theft of media or documents is prioritized more than loss of power supply.

Depending on what kind of information is stolen, it can threaten the security of secret information zone, database, or client’s personal data.

1.Theft of media or documents

2. Loss of power supply

High risk value:

3. Failure of telecommunication equipment:

•Network and supported software is marked as an asset of high relevance.

•Unavailability of network makes the work of company impossible.

4. Theft of equipment:

•Equipment itself is marked as important to the company.

•Pen drives, hard discs or laptops and contain sensible company data.

•This threat is connected with the one: “Theft of media or documents”.

5.Remote spying:

•It can violate the security of private company data.

•It may lead to steal of employees, contracts (main assets) etc.

6.Eavesdropping:

•Directly connected with remote spying

7. Fire:

•Threat to employees’ health and life – personnel is one of main assets of company.

•It can damage company’s equipment, documents and infrastructure, which will cause huge delays in contracts execution.

8. Equipment failure:

•May lead to unavailability of company’s processes, data loss.

9. Failure of air condition:

•May lead to the equipment overheating.

•May cause the dissatisfaction of employees and reduction of their work efficiency.

Medium risk value:

10. Software malfunction

•may affect the correctness of business processes

•may cause the sensible data leakage or loss

•may cause unavailability of main company services

11. Unauthorized use of equipment

•may cause the sensible data leakage or loss

•may cause software corruption

12. Corruption of data

•may affect the correctness of business processes

13. Meteorological phenomenon

Disclosure

Denial of action

**Values:**

High:

-Secret information zone

-The network and the supportive software

-The core personnel

Medium:

-The process of security evaluation of client’s products

-The contracts executions

-The gathered database for the past 10 years regarding attacks on client’s devices

-The laboratory equipment and software tools

Low:

-Company’s good reputation

-Personnel with new devices and solutions

-The research process that allows to issue new publications and supports company’s good image

-The recruitment process enabling the company to grow gradually

-The software for automatic analysis of client’s documentation

-Supporting personnel

1. **Risk treatment plan**

All risks from previous point have been enlisted and appropriate treatments have been proposed to reduce them to minimal, residual risks. Possible treatments are:

* Risk reduction (applying appropriate treatment to lower risk level)
* Risk retention (if level is acceptable, not further treatment is required)
* Risk avoidance (avoiding activity and conditions leading to a particular risk)
* Risk transfer (by insurance or by sub-contracting a partner)
* Theft of media or documents (risk level – Very high)

Risk reduction:

* all company computers have to be fully encrypted
* passwords are generated randomly and provided to computers users

Risk avoidance

* if not necessary, employees aren’t allowed to take company computers to their homes

Estimated residual risk level, after applying risk treatment: **High**

* Loss of power supply (risk level – Very high)

Risk reduction:

* annual electrical infrastructure audits made by external company
* repairs of electrical infrastructure can be made only by qualified staff
* all PCs are used only with UPS units
* applying emergency power system for crucial areas

Risk transfer:

* power outage insurance

Estimated residual risk level, after applying risk treatment: **Low**

* Failure of telecommunication equipment (risk level – high)

Network and supported software is marked as an asset of high relevance.

Unavailability of network makes the work of company impossible.

Risk reduction:

* automated cloud backups are done daily
* redundant network connection – at least two different network services providers
* all the risk reduction from “Loss of power supply” point are applied

Risk transfer:

* insurance in case of network downtime

Estimated residual risk level, after applying risk treatment: **Low**

* Theft of equipment (risk level – high)

Equipment itself is marked as important to the company.

Pen drives, hard discs or laptops and contain sensible company data.

This threat is connected with the one: “Theft of media or documents”.

Risk avoidance:

* if not necessary, employees aren’t allowed to take company computers to their homes

Risk transfer:

* equipment theft insurance

Estimated residual risk level, after applying risk treatment: **Medium**

* Remote spying (risk level – high)

It can violate the security of private company data.

It may lead to steal of employees, contracts (main assets) etc.

Risk reduction:

* frequent scans for malicious software
* annual PC security audit
* only IT department authorized employees are allowed to install new software

Risk avoidance:

* if not necessary, employees aren’t allowed to take company computers to their homes

Estimated residual risk level, after applying risk treatment: **Medium**

* Eavesdropping (risk level – high)

Directly connected with remote spying

Risk reduction:

* all points from “Remote spying” section have to be applied
* continuous supervision of all service personnel allowed into the area for repairs/alterations

Estimated residual risk level, after applying risk treatment: **Medium**

* Fire (risk level – high)

Threat to employees’ health and life – personnel is one of main assets of company.

It can damage company’s equipment, documents and infrastructure, which will cause huge delays in contracts execution.

Risk reduction:

* fire plans, evacuation plans, fire extinguishers and first aid kits made widely available, with appropriate training for employees
* fire drill at least once a year to keep employees aware of company safety protocol
* sprinkle system installation
* employees and managers should only smoke in designated areas outside the building
* improving alarm system

Risk transfer:

* fire insurance

Estimated residual risk level, after applying risk treatment: **Low**

* Equipment failure (risk level – high)

May lead to unavailability of company’s processes, data loss.

Risk reduction:

* all points from “Loss of power supply” have to be implemented
* regular software updates

Estimated residual risk level, after applying risk treatment: **Medium**

* Failure of air condition (risk level – high)

May lead to the equipment overheating.

May cause the dissatisfaction of employees and reduction of their work efficiency.

Risk reduction:

* regular air condition system audits by external company

Estimated residual risk level, after applying risk treatment: **Medium**

* Major accident (risk level – high)

Risk reduction:

* available first aid kits, safety training
* all employees are able to get attractive insurance with discount

Estimated residual risk level, after applying risk treatment: **Medium**

* Breach of personnel availability (risk level – high)

Risk reduction:

* HR department actively uses social media to efficiently get new potential employees
* personnel might be allowed to work remotely

Estimated residual risk level, after applying risk treatment: **Medium**

* Software malfunction (risk level – medium)

may affect the correctness of business processes

may cause the sensible data leakage or loss

may cause unavailability of main company services

Risk retention – current risk level is acceptable: **Medium**

* Unauthorized use of equipment (risk level – medium)

may cause the sensible data leakage or loss

may cause software corruption

Since it can result in legal consequences, medium level is unacceptable here.

Risk reduction:

* all company computers have to be fully encrypted
* passwords are generated randomly and provided to computers users

Risk avoidance:

* if not necessary, employees aren’t allowed to take company computers to their homes

Estimated residual risk level, after applying risk treatment: **Low**

* Corruption of data (risk level – medium)

Risk retention – current risk level is acceptable: **Medium**

* Meteorological phenomenon (risk level – medium)

Risk retention – current risk level is acceptable: **Medium**

Risk treatment plan and residual risks are provided for acceptance decision of the organization’s managers.

1. **Risk acceptance statement**

Referring to the risk treatment plan and residual risks, assessment with acceptance decisions have been made and put together in Table 8. If residual risk level exceeded acceptance level, and still risk still have been accepted, justification is provided in last column. Acceptable are risks lower or equal medium, only but only if they will result in legal consequences. Otherwise they are not acceptable and acceptance risk level is changed to low.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Threats | Residual risk  level: | Acceptance risk level | Accepted | Reason for acceptance if residual risk level exceeds acceptance risk level |
| Theft of media or documents | High | Low | Yes | Further risk reducing could be done for example by prohibiting employees work remote, but impact of that exceeds impact of theft, therefore it has been accepted. |
| Loss of power supply | Low | Medium | Yes | N.A. |
| Failure of telecommunication equipment: | Low | Medium | Yes | N.A. |
| Theft of equipment: | Medium | Low | Yes | N.A. |
| Remote spying | Medium | Medium | Yes | N.A. |
| Eavesdropping | Medium | Medium | Yes | N.A. |
| Fire | Low | Medium | Yes | N.A. |
| Equipment failure | Medium | Medium | Yes | N.A. |
| Failure of air condition | Medium | Medium | Yes | N.A. |
| Major accident | Medium | Medium | Yes | N.A. |
| Breach of personnel availability | Medium | Medium | Yes | N.A. |
| Software malfunction | Medium | Medium | Yes | N.A. |
| Unauthorized use of equipment | Low | Low | Yes | N.A. |
| Corruption of data | Medium | Medium | Yes | N.A. |
| Meteorological phenomenon | Medium | Medium | Yes | N.A. |

Table.11. List of risks assessed to residual risk level and acceptance

Summary, list of accepted risks that exceed acceptance level with justification:

1. Theft of media or documents

Further risk reducing could be done for example by prohibiting employees work remote, but impact of that solution exceeds impact of theft, therefore it has been accepted.

1. **Risk communication**

Components in the process of identifying vulnerabilities:

Input data contains:

List of all risk information obtained from risk management activities. For the health insurance company, this list should consist of all information on the course of the transaction, as well as systematic system reports (containing information about network traffic).

Action:

Risk information should be shared between the decision maker and other parties. Which means that the information should be stored in a dedicated database. Stakeholders should be able to access this database.

Output data:

Continuous improvement of the risk management process. Using different risk information to improve the security system.

The scope of risk communication process:

Risk communication is an action aimed at reaching agreement on risk management by sharing information on risk. Effective communication between stakeholders enables more thoughtful and appropriate risk management decisions. An appropriate database to which stakeholders have access will enable an efficient and secure risk communication process. In addition, the database stores all information in an orderly manner which makes it easier to use it later. Stakeholders should understand the grounds on which decisions are made, therefore information exchange is required. Risk perception between parties is different and communication should be a common language between different stakeholders.

Risk communication objectives:

* To improve the risk management process at this health insurance organization.
* To gather risk information in one place - in the database.
* To avoid an information security breach due to a lack of mutual understanding between the organization and stakeholders.
* To support the decision-making process (a large amount of information allows you to make decisions more efficiently).
* To improve awareness of the risks involved, inform stakeholders about them.
* To give stakeholders a sense of responsibility for the risks affecting our organization, including theirs.
* To obtain new knowledge on information security from interested parties.
* To share the full results of the risk assessment and present a risk reduction plan.

1. **Risk monitoring and review**

Risk monitoring and review is necessary to   
ensure the availability of useful, complete and up-to-date risk information in the decision-making process. As the identified risk may change in time, there is a need of

continuous reacting to changes.

Steps taken:

- periodic identification of changes in risks found – every 3 months

Includes reassignment of risk levels based on new information. New risks are also described, if found. If necessary, a new risk management plan is implemented.

- anonymous checks to of the physical security of the company's building. This includes checking if an unauthorized person is able to get inside the building.

In case of a discrepancy between the specified levels of physical hazards and the actual capabilities of a potential attacker, the risks are reevaluated.

-looking for new vulnerabilities and identifying new, previously unknown threats. Reports may come from employees, who will be rewarded by a bug bounty.   
Besides, every six months  
there is a thorough search of new vulnerabilities by the employees of ISMS provider.   
Reported information should be considered during the next periodic identification of risks.

-any legal changes that may affect the company's interests (e.g. regarding the protection of personal data) should be considered separately (regardless of periodic testing) and immediately (special meeting).

After determining their impact on the company, they can lead to changes in existing risk assessment criteria. If they have a significant impact on the interests or values ​​of the company,

periodic identification of changes in risks should be done as soon as possible.

-any changes in the company's values ​​and priorities, etc. should be consulted in order to set new priorities for the company and if it is deemed necessary - reevaluation of risks (or taking into account changes in the next periodic test).