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.

1. 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. 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 clients safety and privacy, and numerous legal regulations regarding handling of personal data. We divided risk evaluation criteria in following way:

|  |  |  |
| --- | --- | --- |
| Probability of occurence criteria | Point value | Case |
| Neglible | 0 | An event can occur only in exceptional circumstances (0-25% that will occur once in 5 years, and most likely won’t), it has not occurred so far, it concerns individual cases. |
| Low | 1 | It is unlikely that this event will occur (26-50% that occurs once every 2 years), it applies to a few cases. |
| Medium | 2 | The event is likely to occur in the near future (51-75% that will occur within 2 years), it may occur several times during this period, it applies to some matters |
| High | 3 | The occurrence of the event is very likely (76-100% that will occur at least once a year). It is expected that such an event may occur several times a year. |

* + 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 |
| 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. |
| 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. |
| 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. |

* 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(3)

• 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(3)

• 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(13)

• 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 2,2,3 | 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 2,2,3 | 5%, 2%

Risk acceptance level: 8,75%

Risk status: 10%

• Finance 2,2,3|5%, 3%

Risk acceptance level: 10%

Risk status: 8%

• Social and humanitarian factors 2,2,3| 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