Pol J Aviat Med Bioeng Psychol 2019; 25(1): 19-28
DOI: 10.13174/pjambp.07.12.2020.02

ORIGINAL ARTICLE

THE MODEL OF RISK MANAGEMENT IN THE FIELD OF AVIATION MEDICINE IN THE ASPECT OF THE ACTIVITIES OF THE MILITARY INSTITUTE OF AVIATION MEDICINE

Mirosław DEREŃ
Department of Flight Simulator Innovations, Military Institute of Aviation Medicine, Warsaw, Poland

Source of support: Own sources

Author's address: M. Dereń, Military Institute of Aviation Medicine, Krasińskiego 54/56 Street, 01-755 Warsaw, Poland, e-mail: mderen@wiml.waw.pl

Abstract: The Military Institute of Aviation Medicine (the Institute) is subject to complex legal conditions resulting from the actions of legislative and executive bodies of the state and their subordinate organs. These conditions, customers and other stakeholders have an impact on the context of the organization. The integrated management system of the Institute, which is compliant with ISO 9001:2015 [10], ISO 27001:2017 [8] and AQAP 2120:2016 [3] standards, systematizes individual scopes of activities so that the requirements of all parties concerned are met. The article presents the risk management model on the basis of which the risk management methodology of the Institute was developed.

Keywords: services, quality management, procedures, risks, opportunities

Figures: 7 • **Tables:** 6 • **References:** 12 • **Full-text PDF:** http://www.pjambp.com • **Copyright** © 2020 Polish Aviation Medicine Society, ul. Krasińskiego 54/56, 01-755 Warsaw, license WIML • **Indexation:** Index Copernicus, Polish Ministry of Science and Higher Education

INTRODUCTION

Managing an organization requires setting its strategic objectives and defining external and internal parameters that contribute to the proper process management and the ability to achieve the intended results.

The complex external and internal conditions of the Military Institute of Aviation Medicine [1,2,4] and the requirements of its customers necessitate a high quality of management. Therefore, the pillar of the management structure at Institute is the ISO 9001:2015 standard. Its structure and requirements enable the construction and maintenance of simple or complex integrated management systems incorporating also other standards. To meet the expectations of parties concerned, the management of Institute has introduced and maintained an integrated management system based on ISO 9001;2015, AQAP 2110:2016 and ISO 27001:2017 standards.

In accordance with the requirements of ISO 9001:2015 standard, the Institute:

- demonstrates the ability to continuously provide services in accordance with the requirements of the customer and the law,
- strives for customer satisfaction through effective use of a quality management system and its continuous improvement,
- plans activities related to risks and opportunities.

The AQAP 2110:2016 standard is based on the requirements of ISO 9001:2015, expanded with specific NATO requirements. The declaration of application of this standard is an offer of the Institute that takes into account, among other things, the risks associated with the provision of the service (product).

ISO 27001:2017 specifies requirements ensuring the confidentiality, integrity and availability of information and requirements for the management of identified risks and opportunities.

The ISO 9001:2015 and ISO 27001:17 standards set out the requirement that risks and opportunities must be included when developing a management system. An opportunity, according to ISO 9001:2015, leads to taking risk in order to seize this opportunity. Therefore, an opportunity can be managed through the risk it entails.

Risk management is now an integral part of managing any business [6,12].

According to ISO 31000:2009 [9], risk is defined as the effect of uncertainty on objectives. According to the PWN Dictionary of Polish Language [11], risk is:

- a possibility that something might go wrong; also: an undertaking the outcome of which is uncertain,
- to dare to face such a danger.

Risk management consists in identifying, correctly classifying and then dealing with it in the most beneficial and safe manner.

Risk management covers two areas of activity of an organization. The first is the strategic risk, taken by the management most often in the

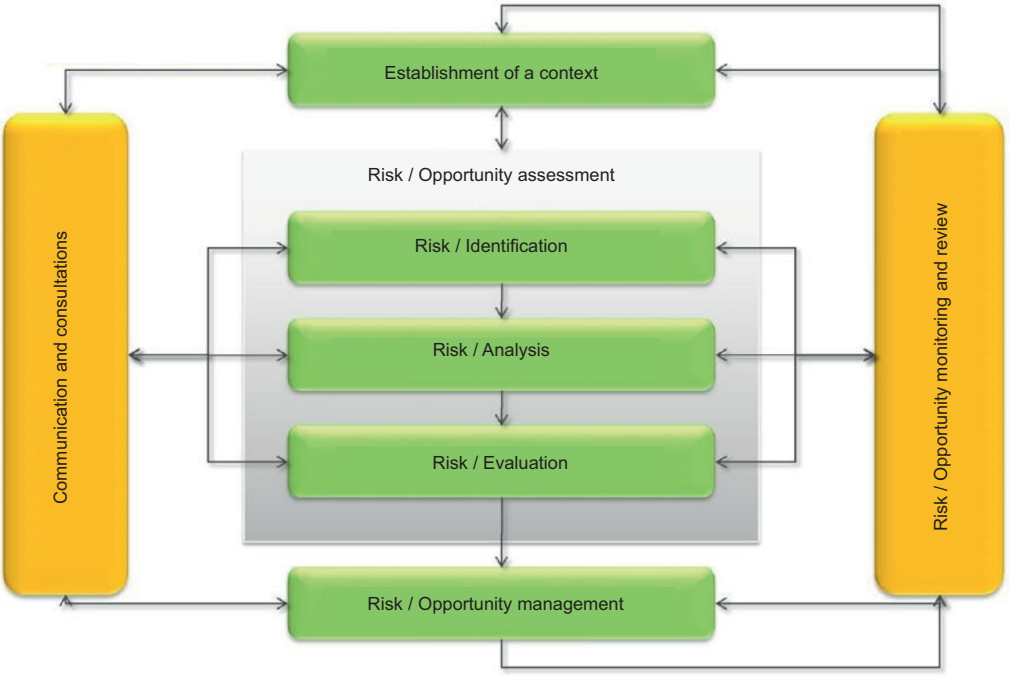

Fig. 1. Diagram of risk and opportunity management.

environment-organization relation. The second area is operational risk, resulting from the process of manufacturing a product (material product or service) [7].

PURPOSE OF THE STUDY

The aim of this study is to present the risk management methodology applied in the Military Institute of Aviation Medicine, which employs a model based on selected risk analysis methods taking into account the recommendations and requirements of ISO 9001:2015, AQAP 2110:2016, ISO 27001:2017 standards, as well as the requirements and expectations of all parties concerned.

RISK MANAGEMENT METHODOLOGY

The methodology systematizes the management of the identified risks related to the implementation of statutory tasks, such as planning the activity of Institute, and systematizes the management of the identified risks in business processes related to the conclusion and performance of contracts signed for the provision of services. The methodology takes into account the requirements of the ISO 9001:2015, AQAP 2110:2016 and ISO 27001:2017 standards as well as the requirements of the Minister of National Defense on planning and settlement of activities in the Ministry of National Defense [5]. The methodology in the field of risk management:

- takes into account requirements resulting from the context of the organization and business requirements,
- meets the requirements of the "Management Control Regulations",
- takes into account the risks associated with information assets,
- systematizes the development of the "Product Quality Plan".

The presented methodology contains a list of basic concepts, general rules of risk management, description of risk components, tables presenting the indexes of threat levels, effects, security and vulnerability, as well as adopted probability indexes. The methodology indicates the sources of input data and describes the methods of calculating the level of risk and the adopted criteria for its acceptance. The necessity to use the context of the Institute in the cyclical process of identification of risks and opportunities was pointed out. The general diagram of risk or opportunity management is shown in fig. 1.

Risk components

The methodology takes into consideration:

- assets / processes / tasks / objectives,
- value (significance) of assets / processes / tasks / objectives,
- location / form of assets,
- potential threats,
- probability of occurrence of these threats,
- vulnerability of assets / processes / tasks / objectives to threats,
- impact of threats on the security of assets / processes / tasks / objectives,
- effectiveness of the applied security measures.

The diagram of the structure of risk components is shown in fig. 2.

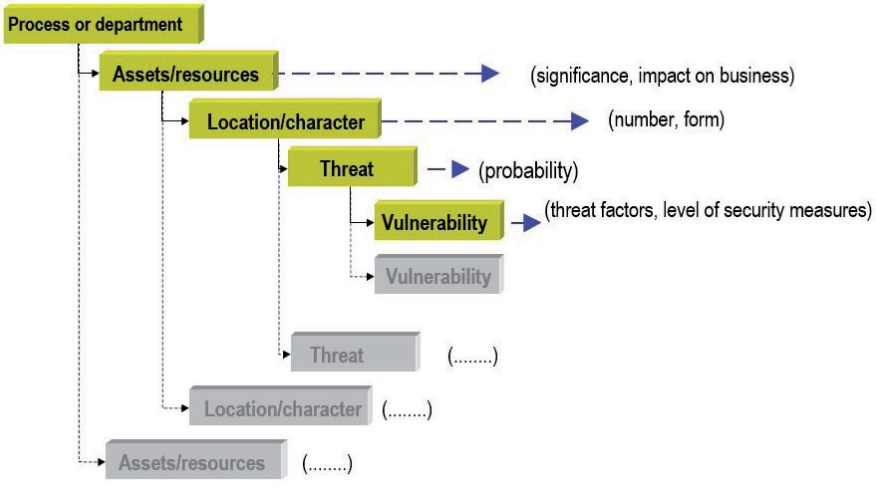

Fig. 2. Diagram of the structure of risk components.

The course of the risk management process

In the process of planning current activities, the result of an analysis of the organization's context (here: Institute) should be taken into account. This planning should consider the risks included in the risk register referred to in the requirements of the Minister of National Defense on planning and settlement of activities in the Ministry of National Defense [5]. As a result of the context analysis, apart from risks, opportunities may be pointed out.

The risk management should be started by carrying out an inventory of assets, processes or objectives in the organizational units within the system and determining their value for the Institute (as an organization), as well as identifying associated threats. Then the relevant characteristics of a given risk should be distinguished, such as the area concerned, the probability of occurrence, the impact of the effects of the event.

Due to the different required purposes of risk analysis and the expected transparency of the analysis results, it is necessary to distinguish three aspects of the risk analysis used at the Institute for:

1) planning of the Institute's activities for the period of the task implementation or for the upcoming planning year,
2) ensuring continuity of information (availability, integrity, confidentiality),
3) performancing of a separate agreement concluded in accordance with the requirements of AQAP 2110:2016.

The risk analysis concerns the assets held, processes carried out at Institute and the assessment of their effect (impact) on its functioning. The effect index values listed in tab. 1 show the power with which neglected assets or a disturbances in functioning of a process may cause disturbances in the functioning of the entire organization.

It is a good practice to identify real threats - i.e. those that can and do occur in the organization (specific breakdowns, power failures, unauthorized transmission of information, theft), and not only those that are easy to name (terrorist attack, fuel dumping by aircraft during emergency landing, especially if there is no airport).

The number of threats identified may be large, which may reflect the reliability of the conducted analysis. However, the identification process should be optimized in terms of the possibility of obtaining up-to-date results on the most relevant threats. If the analysis is too extensive - with irrelevant, unlikely elements - it may be already outdated at the time of its completion, or the cost of obtaining it - the time spent on managing the identified risk factors - will be disproportionately high.

Not all threats occur equally often or are equally likely to occur, hence the concept of the probability of occurrence of a threat has been introduced. Equipment failures or lack of power supply are certainly more frequent than fires or hurricanes with wind force uprooting trees.

A five-grade scale should be adopted to assess the probability: high, large, significant, moderate, small. For each level of probability, a value of the probability assessment index has been assigned. These levels are described in tab. 2.

Tab. 1. The effect (impact) of the event on the functioning of the Institute (effect, impact on business).

Score	Value (E)	Description
Critical	5	a loss or breach of the security or elements of an organizational unit or a process results in interruption of the continuity of the Institute's activity a loss or breach of the security of personal data or the process results in high material and non-material losses, identity theft and loss of control over personal data for the data subject
Very high	4	a loss or breach of the security or elements of an organizational unit or a process results in interruption of the continuity of activity of the Institute's organizational unit a loss or breach of the security of personal data or the process may have a negative impact on the rights and freedoms of data subjects, e.g. as a result of loss of control over personal data, material or non-material loss
Serious	3	a loss or breach of the security or elements of an organizational unit or a process may have a negative impact on the continuity of the Institute's activity a loss or breach of the security of personal data or the process may have a negative impact on the rights and freedoms of data subjects, e.g. as a result of loss of control over personal data, non-material loss
Significant	2	a loss or breach of the security or elements of an organizational unit or a process causes difficulties in the normal functioning of the Institute a loss or breach of the security of personal data or the process has a major impact on the rights and freedoms of data subjects, e.g. as a result non-material loss
Small	1	a loss or breach of the security or elements of an organizational unit or a process has a limited impact on the functioning of the Institute a loss or violation of the security of personal data or the process has a limited impact on the rights and freedoms of data subjects

where "Critical" means the greatest impact and "Small" – the smallest impact.

Tab. 2. The assessment of the probability of occurrence of a threat.

Score	Indicator (P)	Description	
High	5	occurs frequently (e.g. once a month) or regularly with a fixed frequency, or is very likely to occur	>90%
Large	4	occurs relatively frequently (e.g. once a quarter) or regularly with a fixed frequency, or is likely to occur	76-90%
Significant	3	occurred in the last year, occurs irregularly, or there is a real probability of occurrence	41-75%
Moderate	2	has occurred a single time in the last year or is unlikely to occur	10-40%
Small	1	has not occurred even once in the last year and is unlikely to occur	<10%

where "High" is associated with the highest probability and "Small" with the lowest.

Tab. 3. The assessment of the impact of the specific characteristics of the assets on the degree of vulnerability taking into account confidentiality, or integrity, or availability.

Score	Index (Vc, Vi, Va)	Description
Significant	1	assets with certain characteristics are or will be in an environment conducive to the occurrence of the event for an indefinite period
Negligible	0	the characteristics of the asset and its environment are not conducive to the occurrence of the event

Tab. 4. Level of security measures.

Score	Value (S)	Description
High	15	the existing security measure protects effectively against known threats
Significant	10	there are partial security measures that protect only selected areas but are fully effective
Moderate	5	has not occurred a single time in the last year, but there is a real probability of occurrence
Negligible	1	has not occurred even once in the last year and is unlikely to occur

where "High" means the highest value (the highest level of security) and can reach the value of "∞". However, at this stage of effectiveness of security measures a value of "15" is assumed. The "Negligible" level means the lowest value (the lowest level of security measures).

Another group of factors affecting the level of risk are vulnerabilities, i.e. weaknesses in our assets or processes - features and properties of the asset or process that may be exploited by the threat, which may increase the probability of occurrence of an event in specific circumstances.

For example: We protect paper from burning because it is not resistant to fire. Paper is vulnerable to burning.

The information written on paper is at risk of being destroyed, because paper is flammable when the temperature exceeds approximately 250 degrees Celsius. It can be assumed that information written on paper is threatened by high temperatures.

The steel hull of a ship is protected against seawater which accelerates the process of corrosion, because the steel it is made of is not resistant to corrosion. The steel hull of a ship is vulnerable to leakage.

This ship is in danger of sinking because of its steel hull, which is vulnerable to leakage due to corrosion accelerated by seawater.

It can be assumed that it is threatened by seawater accelerating the process of corrosion of the steel hull.

A specific group of assets consists of information assets characterized by vulnerabilities (V) to which apply the following assessment criteria:

1) confidentiality - protection against unauthorized access (Vc),
2) integrity - protection against breaching of information (Vi),
3) availability (Va).

The methodology uses the same scale of impact assessment for the abovementioned vulnerabilities (tab. 3). The vulnerabilities classified as "Significant" increase the value of the probability index (see Formula No. 3).

The impact of the threat on confidentiality, integrity and availability (information security) should be assessed and the level of effectiveness of the implemented security measures should be determined. These are the elements completing

the analysis. The scale of assessment of security levels is specified in tab. 4.

Determination of risk level and residual risk

The risk of an asset (also: process, task, objective) is the basis for assessing the real loss of security of this asset against other assets in a situation where no security measures are yet in place. The list of assets should be arranged according to the associated risk level index values. This list is the basis for determining the methods of risk management and which security features should be selected in order to protect the riskiest assets.

The following calculation method is generally accepted for obtaining mutually comparable indexes of the level of risk of assets. Formula No. 1 is to be filled in with the numerical values from tables 1 to 4, assigned to each item respectively.

$$R = P * E \quad (1)$$

where:

R – risk of an asset / process / task / objective

P – probability of occurrence of the threat (index value)

E – effect (impact) of the occurrence of the threat

$$P = P * (1 + V) \quad (2)$$

where:

V– vulnerability of the asset process, task, objective

$$V = V_c + V_i + V_a \quad (3)$$

where:

Vc, Vi, Va – vulnerability of an information asset, respectively to: confidentiality, integrity, availability.

After the selection and implementation of security measures, the risk assessment should be carried out again, but already considering the levels of security provided by the implemented measures. For each asset, after taking into account the security measures, the residual risk must be calculated.

The residual risk is, as a rule, calculated using the following Formula No. 4:

$$Rs = R / S \quad (4)$$

where:

Rs – residual risk of an asset / process / task

R – risk of an asset / process / task

S – effectiveness of the applied security measures.

Based on the obtained residual risks of the assets, the level of "acceptable risk" should be determined and set as a fixed value of risk below which the risks of assets are considered acceptable.

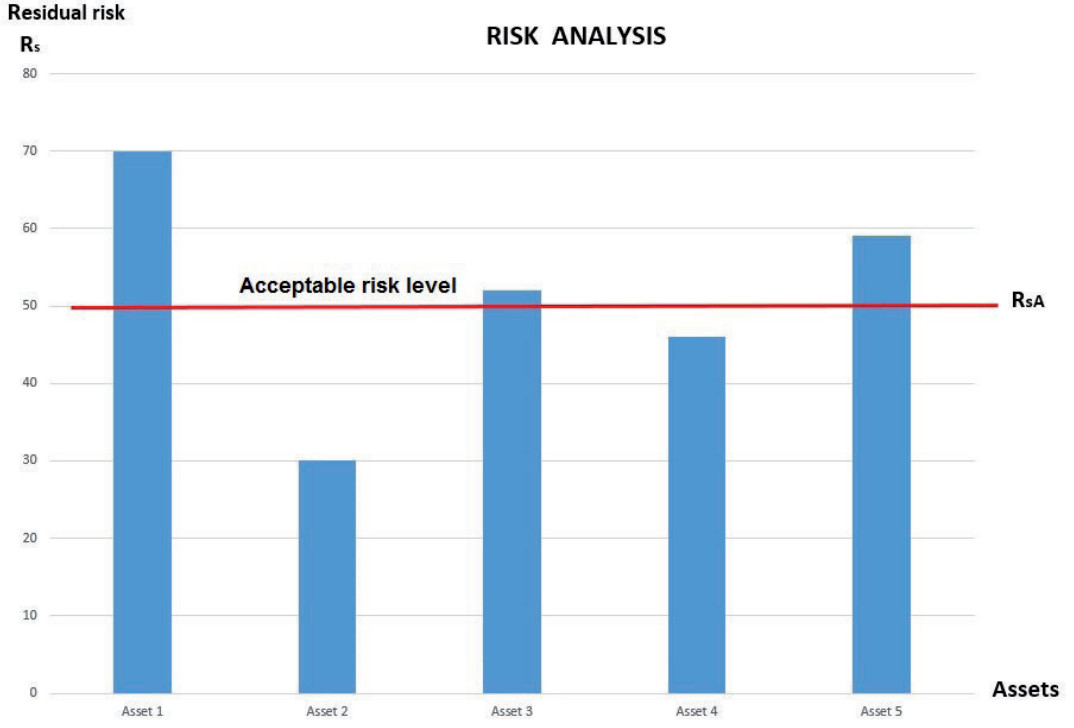

Fig. 3. The result of a risk assessment with a defined level of acceptable residual risk (RsA).

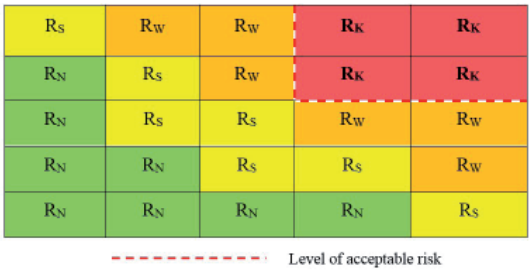

Fig. 4. A risk matrix (R), where: RN - minor risk, RS - moderate risk, RW - major risk, RK - critical risk.

Criteria for the acceptance of risk and the level of acceptable risk

An essential element of the risk assessment process is the definition of "risk assessment criteria", i.e. the approach adopted for dividing risks into acceptable and non-acceptable. The risk acceptance criterion should be to seek to equalize the levels of risk for all assets, in line with the principle that the strength of the security system is indicated by its weakest (riskiest) element. The highest limit value for acceptable residual risk (RsA) should be determined. The assets with risks below the value determined by cutting off the "risk chimneys" have such a risk level that the Institute's management is now ready to accept them .

The level of the acceptable residual risk (RsA) is a specific risk value. In the diagram, an example of which is shown in fig. 3, the level of acceptable risk is marked by a horizontal line running throughout RsA value. The level of acceptable risk should be determined during each risk analysis.

The result of a risk analysis can be presented as a risk quantification matrix, also called the risk matrix (fig. 4) with a dashed line indicating the level of acceptable risk.

The result of the risk analysis can also be presented in a tabular layout (fig. 5) in which, apart from presenting the current value of the level of acceptable risk (RsA), the forecasted result of the level of acceptable risk resulting from the implementation of planned improvement measures can also be determined.

Detailed guidelines for risk analysis, assessment and management

The risk analysis should cover all areas of the Institute's activity that affect the realized processes and be prepared with the participation of the representatives of:

- the main processes,
- the Institute's management,
- Chief Accountant Division,
- Administrative Division (excluding the IT Laboratory),
- IT Laboratory,
- Security Division.

A risk analysis should be carried out:

- when new risks are identified,
- when planning organizational changes,
- in accordance with the adopted plan of activity of the Institute.

The owners of the main processes are responsible for the preparation of partial risk analysis

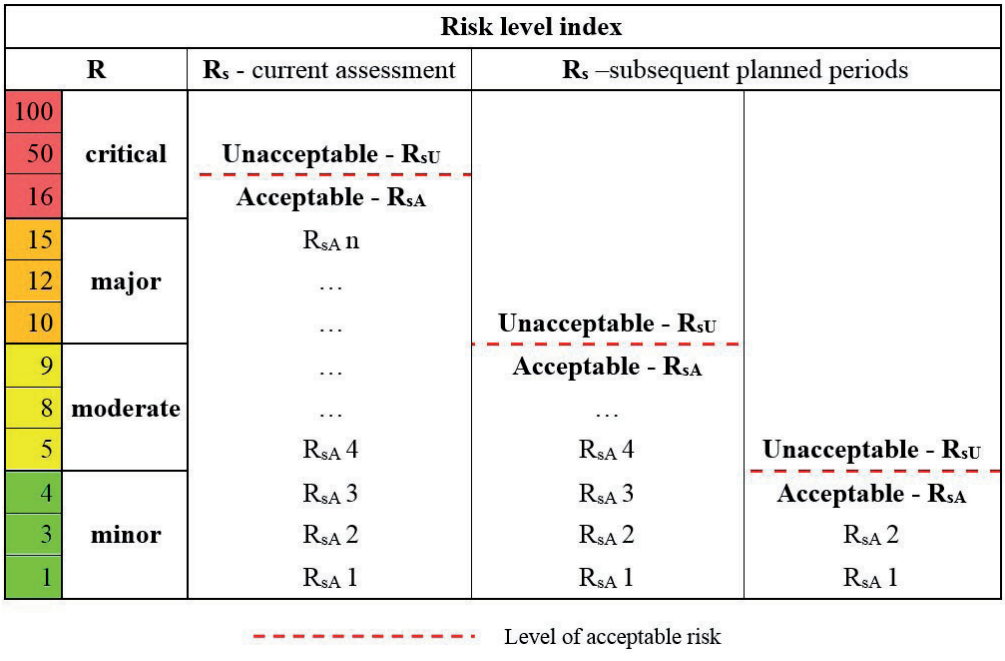

Fig. 5. Limit values of the index grouping risk (R) and residual risk (Rs).

covering assets in their area and submitting them to the Plenipotentiary for the Integrated Management System, who will combine them to obtain a summarized result of the analysis for the Institute's area covered by the system.

For risk analysis one should use a spreadsheet available on the Institute intranet site - a document in the form of an electronic file.

The result of the assessment process should be prepared in the form of a list of the Institute's assets that are most at risk. It allows the Management to decide for which assets additional security measures (technical or organizational) should be implemented first.

The Management should define a risk management plan for risks with values exceeding the adopted acceptable level (RsA). This plan may also include the allocation of resources (including financial ones) to secure the assets that are most at risk and, consequently, reduce the level of residual risk of these assets.

A graphical presentation of the level of acceptable risk should be made in the form of a chart for the assets that are most at risk (fig. 3).

Determining the level of acceptable risk completes the risk assessment stage.

The risk management plan should be prepared in accordance with the form available on the Institute intranet site in the form of an electronic file.

Risk management principles according to AQAP 2110:2016

In accordance with the requirements of the AQAP 2110:2016 standard, contracts for the provision of services by the Institute should take into account the risk associated with the process, as well as the specific features of the product or service, and should also define the principles of risk management associated with the performance of the contract concluded. The AQAP 2110:2016 standard can be applied in case of special requirements of contracts performed for the Minister of National Defense.

In the presented methodology for this type of contracts a method of qualitative risk analysis was adopted. In order to determine the level of risk of factors influencing the performance of contracts, a commonly used risk matrix was used (fig. 6), where:

Level of risk = Probability * Impact on contract performance

Tab. 5. Impact on contract performance.

Score	Value	Description
Critical	4	a loss of a process component or violation of its security results in an interruption of realization of the contract;
Major	3	a loss of a process component or violation of its security may have a negative impact on the date of completion of the contract;
Significant	2	a loss of a process component or violation of its security causes difficulties in the normal course of contract performance;
Normal	1	a loss of a process component or violation of its security has a limited impact on contract performance;

where "Critical" means the greatest impact and "Normal" – the smallest impact.

Probability \ Impact	Normal	Significant	Major	Critical
High	M 5	H 10	H 15	H 20
Large	M 4	M 8	H 12	H 16
Significant	L 3	M 6	M 9	H 12
Moderate	L 2	M 4	M 6	M 8
Small	L 1	L 2	L 3	M 4

Level of acceptable risk

Fig. 6. The risk matrix for the following values adopted in this methodology: values of probability indexes (table 2) and values of threat impact indexes (table 6). The level of risk: Low ("L"); Medium ("M"); High ("H").

Tab. 6. Risks related to the performance of a contract.

Assets/Processes	Symbol	Threat	Probability	Threat impact	Risk
Internet (LAN network)	LAN	broken line	1	1	1
Simulators	Sim	theft	5	1	5
Barofunction test	Bar	upper respiratory tract infection	3	2	6
Technical personnel	Te	absence	3	2	6
…	?	…	…	…	…
Simulators	Sim	break down	3	5	15

In order to assess the probability, the values of the indexes described in table 2 are to be used.

In order to assess the impact on contract performance (effects of the materialization of risks), the criteria in table 5 are to be adopted.

The following general principle has been adopted for the selection of the strategy for the assessed risks of contract performance:

- **high level of risk (10÷20)** – the most effective threat reduction plans should be applied (they may be costly and complex). The possibility of avoiding the threat, i.e. making the given risk factor impossible to occur, should be considered. For example, it's possible to apply withdrawal at the start of the project which also should be considered as a strategy. The decision to withdraw may be preceded by a project feasibility study carried out to assess the chance of providing a product (service) that meets the assumed requirements.
- for **medium-level risks (4÷9)**, less complex (less costly) but perhaps less effective plans for the implementation of mitigating security measures, i.e. reducing the probability or effects of materialization of the risk, may be applied. For **high and medium levels** of risk, a strategy of transfer may also be used. Most often, the transfer of risk consists in taking out insurance against an event or assigning the effects of risk to a counterparty (or a subcontractor),
- for **low-level risks (1÷3)** the acceptance of risks is usually applied. If the threats occur, we accept their effects. Acceptance is divided into active (we have a financial reserve) and passive (no reserves).

Example of a risk assessment in a contract for the provision of a service

Table 6 presents examples of assets and processes, identifies threats, values of indexes of probability of events, and calculates risk values for each asset and process.

The risk matrix has been filled with asset and process symbols put in the fields of the matrix according to the calculated values (fig. 7).

The above example of a risk matrix shows the risk identified by the symbol "Sim" in the high-risk area, above the line indicating the level of acceptable risk ("Risk acceptance line"). It would therefore be advisable, in accordance with the accept-

High	M Sim (5)	H 10	H Sim (15)	H 20
Large	M 4	M 8	H 12	H 16
Significant	L 3	M Te, Bar (6)	M 9	H 12
Medium	L 2	M 4	M 6	M 8
Small	L LAN (1)	L 2	L 3	M 4
Probability / Impact	Normal	Significant	Major	Critical

Level of acceptable risk

Fig. 7. Risk matrix - example.

ed principles, e.g. to prepare a second, alternative simulator for use. For the assets marked with "Te" and the "Bar" process, preventive measures (reducing the probability of occurrence or the effect of a threat) should be applied. For the asset with "LAN" symbol, the associated risk could be accepted.

CONCLUSIONS

Management in each area is a complex, continuous process supported by the knowledge, innate abilities and acquired skills of the manager. An important component of the management process is risk management. The proposed approach to the identification and assessment of risks in the various areas of activity of the Military Institute of Aviation Medicine is the result of optimization which is based on two criteria: the criterion of the risk factors required by the standards and the transparency of the methods used for all parties

The risk management methodology presented above is a tool that supports making decisions that are strategic for the Institute, operational decisions concerning the implementation of current tasks, as well as the development of the content of contracts concluded for the provision of services.

AUTHORS' DECLARATION:

Study Design: Mirosław Dereń. **Data Collection:** Mirosław Dereń. **Manuscript Preparation:** Mirosław Dereń. The Author declares that there is no conflict of interest.

REFERENCES

1. Act of 17 November 2006 on the system of conformity assessment of products intended for the needs of national defense and security. (Journal of Laws of 2018, item 114, consolidated text).
2. Act of 28 April 2011 on the information system in healthcare. (Journal of Laws of 2017, item 1845, consolidated text).
3. AQAP 2110:2016, NATO Quality Assurance Requirements for Design, Development and Production, NATO - AQAP 2110:2016, Polish version: CCJ - WAT Edition D version 1.
4. Decision No. 126/MON of 16 August 2019 on the assurance of quality of military equipment and services concerning military equipment. (Official Journal of the Ministry of National Defense of 2019, item159).
5. Decision No. 218/MON of 6 June 2014 on planning and settlement of activities in the Ministry of National Defense (Official Journal of the Ministry of National Defense of 2014, item 179).
6. Gołaś H. Model doskonalenia przedsiębiorstwa przez zarządzanie ryzykiem zgodnie z ISO 9001:2015, Probl. Jakości 2016; 1(10):11-16.
7. Łagowski E, Świderski A. and Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego (Warszawa) Aplikacje dla procesów w organizacji. Wojskowa Akademia Techniczna, 2016.
8. PKN, ISO 27001:2017, Information technology - Security techniques - Information security management systems - Requirements, PN-EN ISO/IEC 27001:2017-06 - Polish version.
9. PKN, ISO 31000:2018-08, Risk management - Guidelines, PN-ISO 31000:2018-08 - English version.
10. PKN, ISO 9001:2015, Quality management systems - Requirements, PN-EN ISO 9001:2015-10 - Polish version.
11. PWN Dictionary of Polish Language – ryzyko; Retrieved 29 March 2019 from https://sjp.pwn.pl/sjp/ryzyko;2518509.html.
12. Tworek P, Cziura P. Wybrane Problemy Zarządzania Ryzykiem w Działalności Przedsiębiorstw Społecznych, Zesz. Nauk. Politechniki Częstochowskiej. Zarządzanie 2017; 25(1):95-108.

Cite this article as: Dereń M. The Model Of Risk Management In The Field Of Aviation Medicine In The Aspect Of The Activities Of The Military Institute Of Aviation Medicine. Pol J Aviat Med Bioeng Psychol 2019; 25(1): 19-28. DOI: 10.13174/pjambp.07.12.2020.02