ISSN 2320 - 2602
Volume 8 No.10 October 2019
International Journal of Advances in Computer Science and Technology
Available Online at http://www.warse.org/IJACST/static/pdf/file/ijacst018102019.pdf
https://doi.org/10.30534/ijacst/2019/018102019

# Information Security Risk Plans within Enterprise Architecture Framework

**Fekry Fouad**
King Abdul Aziz University
ffouad@kau.edu.sa

## ABSTRACT

Among the tremendous progress in information technology and modern communication networks, , the Global Economic Risk Report for Humanity 2018 was presented at the World Economic Forum in Davos. It follows from the report that the importance of information security risks is increasing both due to an increase in the number of implemented attacks, and taking into account their destructive potential.
One of the most common information security risk management techniques in the world is CRAMM, COBIT for Risk, FRAP, Octave and Microsoft. Along with certain advantages, they also have their limitations. In particular, the listed foreign methods can be effectively used by commercial companies, while government organizations should be guided by the nationwide provisions when assessing and managing information security risks. At the same time, this paper could be used by national executive authorities as additional material. Evolution is fraught with many threats and risks that are linked to all different information systems, and may lead to these risks.

**Key words:** CRAMM, COBIT for Risk, FRAP, Octave, Enterprise Architecture for Risk Management.

## 1. INTRODUCTION

Information Security Risks in Modern Societies is, the number of attacks on organizations has doubled. Attacks leading to extraordinary damage are becoming common place. The financial damage from attacks is increasing and some of the biggest losses are associated with attacks by ransomware viruses **[1]**. A striking example of this is the attack by the ransomware viruses WannaCry and NotPetya, which affected more than 300 thousand computers in 150 countries and resulted in financial losses of more than $ 300 million.

Another trend is an increase in the number of attacks on critical infrastructure and strategic industrial facilities, which can lead to the failure of attackers to support systems that support human life and global technological disasters.

Thus, information security risks are among the three most probable risks (together with the risks of natural disasters and extreme weather conditions) and the list of six most critical risks with regard to possible damage (together with the risks of using weapons of mass destruction, natural disasters, weather anomalies and shortages drinking water). Therefore, information security risk management is one of the priority areas for the development of organizations around the world and is absolutely necessary for their further functioning.

The following table 1 illustrates the most common threats and risks, their potential drivers and the ways in which they may occur

| Threat-Source | Motivation | Threat Actions |
|---|---|---|
| Hacker, cracker | Challenge<br>Ego<br>Rebellion | • Hacking<br>• Social engineering<br>• System intrusion, break-ins<br>• Unauthorized system access |
| Computer criminal | Destruction of information<br>Illegal information disclosure<br>Monetary gain<br>Unauthorized data alteration | • Computer crime (e.g., cyber stalking)<br>• Fraudulent act (e.g., replay, impersonation, interception)<br>• Information bribery<br>• Spoofing<br>• System intrusion |
| Terrorist | Blackmail<br>Destruction<br>Exploitation<br>Revenge | • Bomb/Terrorism<br>• Information warfare<br>• System attack (e.g., distributed denial of service)<br>• System penetration<br>• System tampering |
| Industrial espionage (companies, foreign governments, other government interests) | Competitive advantage<br>Economic espionage | • Economic exploitation<br>• Information theft<br>• Intrusion on personal privacy<br>• Social engineering<br>• System penetration<br>• Unauthorized system access (access to classified, proprietary, and/or technology-related information) |
| Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees) | Curiosity<br>Ego<br>Intelligence<br>Monetary gain<br>Revenge<br>Unintentional errors and omissions (e.g., data entry error, programming error) | • Assault on an employee<br>• Blackmail<br>• Browsing of proprietary information<br>• Computer abuse<br>• Fraud and theft<br>• Information bribery<br>• Input of falsified, corrupted data<br>• Interception<br>• Malicious code (e.g., virus, logic bomb, Trojan horse)<br>• Sale of personal information<br>• System bugs<br>• System intrusion<br>• System sabotage<br>• Unauthorized system access |

**Figure 1:** most common threats and risks

## 2. GOALS AND APPROACHES TO INFORMATION SECURITY RISK MANAGEMENT

The goal of any organization is to achieve certain indicators that characterize the results of its activities. For example, for commercial companies this is profit-making, growth of capitalization, market share or turnover, and for government organizations - the provision of public services to the population and solving management problems. In any case, regardless of the purpose of the organization, the achievement of this goal may be prevented by the implementation of information security risks. Moreover, each organization in its own way assesses the risks and the possibility of investing in their reduction [2].

Thus, the goal of managing information security risks is to maintain them at an acceptable level for the organization. To solve this problem, organizations create integrated information security systems (ISS) [3].

When creating such systems, the question arises of the choice of means of protection that ensure the reduction of information security risks identified during the analysis without excessive costs for the implementation and support of these tools. An information security risk analysis allows you to determine the necessary and sufficient set of information protection tools, as well as organizational measures aimed at reducing information security risks, and to develop an organization's NIB architecture that is most effective for its specific activities and aimed at reducing its information security risks.

All risks, including information security risks, are characterized by two parameters: potential damage to the organization and probability of implementation. Using a combination of these two characteristics for risk analysis allows you to compare risks with different levels of damage and likelihood, leading them to a common expression that is understandable to those who make decisions about minimizing risks in the organization. Moreover, the risk management process consists of the following logical steps, the composition and content of which depends on the risk assessment and risk management methodology used:

Determining an acceptable level of risk for an organization (risk appetite) is the criterion used in deciding whether to accept a risk or to process it. Based on this criterion, it is determined which risks identified in the future will be unconditionally accepted and excluded from further consideration, and which are subjected to further analysis and included in the risk response plan. [5]

Identification, analysis and assessment of risks. To make a decision regarding risks, they must be uniquely identified and evaluated in terms of damage from the realization of the risk and the likelihood of its implementation. When assessing damage, the degree of risk exposure on the organization's IT assets and the business processes they support are determined. In assessing the probability, an analysis is made of the probability of the risk occurring. The assessment of these parameters can be based on the identification and analysis of vulnerabilities inherent in IT assets that can be affected by risk, and threats that can be realized through the exploitation of these vulnerabilities. Also, depending on the risk assessment methodology used, an attacker model, information about the organization's business processes and other factors related to risk realization can be used as initial data for their assessment, such as political, economic, market or social situation in the environment of the organization. When assessing risks, a qualitative, quantitative or mixed approach to their assessment can be used. The advantage of a qualitative approach is its simplicity, minimizing the time and labor involved in conducting a risk assessment, and the limitations are the lack of visibility and the difficulty of using the results of a risk analysis for economic justification and evaluating the feasibility of investing in a risk response **[4]**. The advantage of the quantitative approach is the accuracy of risk assessment, the visibility of the results and the ability to compare the value of risk expressed in money with the amount of investment needed to respond to this risk, the disadvantages are complexity, high complexity and length of execution. market or social situation in the environment of the organization. When assessing risks, a qualitative, quantitative or mixed approach to their assessment can be used. The advantage of a qualitative approach is its simplicity, minimizing the time and labor involved in conducting a risk assessment, and the limitations are the lack of visibility and the difficulty of using the results of a risk analysis for economic justification and evaluating the feasibility of investing in a risk response. The advantage of the quantitative approach is the accuracy of risk assessment, the visibility of the results and the ability to compare the value of risk expressed in money with the amount of investment needed to respond to this risk, the disadvantages are complexity, high complexity and length of execution. market or social situation in the environment of the organization. When assessing risks, a qualitative, quantitative or mixed approach to their assessment can be used. The advantage of a qualitative approach is its simplicity, minimizing the time and labor involved in conducting a risk assessment, and the limitations are the lack of

visibility and the difficulty of using the results of a risk analysis for economic justification and evaluating the feasibility of investing in a risk response. The advantage of the quantitative approach is the accuracy of risk assessment, the visibility of the results and the ability to compare the value of risk expressed in money with the amount of investment needed to respond to this risk, the disadvantages are complexity, high complexity and length of execution. When assessing risks, a qualitative, quantitative or mixed approach to their assessment can be used. The advantage of a qualitative approach is its simplicity, minimizing the time and labor involved in conducting a risk assessment, and the limitations are the lack of visibility and the difficulty of using the results of a risk analysis for economic justification and evaluating the feasibility of investing in a risk response. The advantage of the quantitative approach is the accuracy of risk assessment, the visibility of the results and the ability to compare the value of risk expressed in money with the amount of investment needed to respond to this risk, the disadvantages are complexity, high complexity and length of execution. When assessing risks, a qualitative, quantitative or mixed approach to their assessment can be used. The advantage of a qualitative approach is its simplicity, minimizing the time and labor involved in conducting a risk assessment, and the limitations are the lack of visibility and the difficulty of using the results of a risk analysis for economic justification and evaluating the feasibility of investing in a risk response **[7]**. The advantage of the quantitative approach is the accuracy of risk assessment, the visibility of the results and the ability to compare the value of risk expressed in money with the amount of investment needed to respond to this risk, the disadvantages are complexity, high complexity and length of execution. minimization of the time and labor costs for conducting a risk assessment, with limitations - insufficient visibility and the difficulty of using the results of risk analysis for economic justification and evaluating the feasibility of investments in risk response measures. The advantage of the quantitative approach is the accuracy of risk assessment, the visibility of the results and the ability to compare the value of risk expressed in money with the amount of investment needed to respond to this risk, the disadvantages are complexity, high complexity and length of execution. minimization of the time and labor costs for conducting a risk assessment, with limitations - insufficient visibility and the difficulty of using the results of risk analysis for economic justification and evaluating the feasibility of investments in risk response measures. The advantage of the quantitative approach is the accuracy of risk assessment, the visibility of the results and the ability to compare the value of risk expressed in money with the amount of investment needed to respond to this risk, the disadvantages are complexity, high complexity and length of execution.

Risk ranking. To determine the priority in responding to risks and then developing a response plan, all risks should be ranked. When ranking risks, depending on the methodology used, criteria for determining criticality can be applied, such as damage from the realization of risks, probability of realization, IT assets and business processes affected by risk, public outcry and reputation damage from the realization of risk, **[6]**.

Making decisions on risks and developing a plan for responding to risks. To determine the totality of risk response measures, it is necessary to analyze identified and assessed risks in order to make one of the following decisions regarding each of them:

Risk avoidance;

Risk taking;

Risk transfer;

Risk reduction.

The decision taken for each risk should be recorded in terms of responding to risks. Also, this plan may contain, depending on the methodology used, the following information necessary to respond to risks:

Responsible for the response;

Description of response measures;

Assessment of necessary investments in response measures;

Timing for the implementation of these measures.

Implementation of risk response measures. In order to implement risk response measures, responsible persons organize the implementation of the actions described in the risk response plan at the required time.

Assessment of the effectiveness of measures implemented. To achieve confidence that the measures applied in accordance with the response plan are effective and the risk level is acceptable for the organization, the effectiveness of each implemented risk response measure is assessed, as well as regular identification, analysis and risk assessment of the organization.

Consider the most famous information security risk management techniques: EA and RM CRAMM, COBIT for Risk, FRAP, Octave, Microsoft..

## 3. ENTERPRISE ARCHITECTURE AND RISK MANAGEMENT

EA “Enterprise Architecture” is the head of any digital transformation project , builds on and integrates numerous standards to provide framework designed to speed you through the process of modeling your Enterprise Architecture and Enterprise Risk Management. Architecture and Information Strategy Security**[8].**

In order to prepare for the risks of the present and the future, the concept of the Enterprise architecture is needed for information security that permeating all other enterprise architectures.

Information security as a property of enterprise architecture Modern business faces many challenging challenges that are becoming more relevant in an unstable economic situation. These include:

- increase in income,
- increased reaction rate to changing circumstances,
- cost and cost reduction,
- acceleration of innovation,
- reduced time to market products and services,
- increasing the loyalty of customers and partners,
- increasing competitiveness,
- regulatory compliance.

To solve all these problems, the enterprise architecture is used (Enterprise Architecture), which allows to form a set of principles, approaches and technologies, which, given the current state of the organization, lay the foundation for its subsequent transformation, growth and development. Today, there are many approaches to creating such architectures - TOGAF, Zachman Framework, FEAF, DoDAF and others **[9]**.

But whichever approach was chosen, in modern conditions it is simply impossible to develop without the use of information and information technology, which must not only support any changes in the business, but also anticipate them, prepare for them in advance, and in some cases, contribute to the emergence of new business opportunities. However, business is not always developing in a predictable way. The risks of various nature can disrupt the growth and development of the enterprise and put it on the brink extinction. A significant role in this is played by information and operational risks, associated with data leaks, disabling IT infrastructure elements.

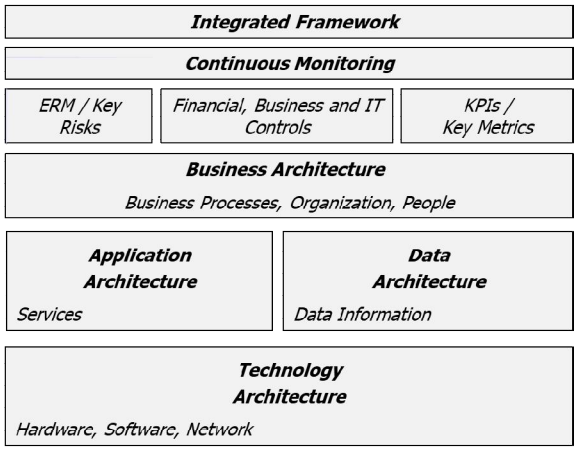


**Figure 2:** Most common threats and risks within the Integrated Approach to EA/RM

- Based on Numerous Standards
  - RM-ODP
  - RUP
  - TOGAF
  - Archimate
  - COSO
- Models the Different Architectural Views
  - Business
  - Information Systems
  - Infrastructure
- Provides Information for Strategic Planning
  - Business Process Realizations
  - Future State Roadmaps
  - Project Portfolio Management
- Integrates with Risk Management
  - Objectives
  - Risks & Opportunities
  - Risk Responses
  - Manual & Automated Controls
  - Transactional and Analytical Data

The CRAMM risk management process consists of the following steps:

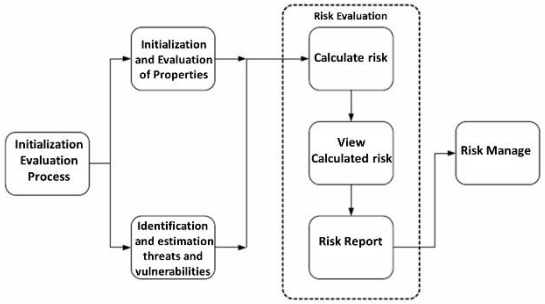


**Figure 3.** CRAMM Process

Initiation At this stage, a series of interviews is conducted with those interested in the information security risk analysis process, including those responsible for the operation, administration, security and use of IT assets for which the risk analysis is performed. As a result, a formalized description of the area for further research is given, its boundaries and the composition of the persons involved in the risk analysis is determined **[10]**.

Identification and Valuation of Assets. The list of IT assets used by the organization in the previously defined research area is determined. According to the CRAMM methodology, IT assets can be one of the following types:

Data;
Software;
Physical assets.

For each asset, its criticality for the organization's activities will be determined and together with representatives of departments that use the IT asset to solve applied problems, the consequences for the organization's activities from violation of its confidentiality, integrity and availability will be evaluated.

Threat and Vulnerability Assessment In addition to assessing the criticality of IT assets, an important part of the CRAMM methodology is assessing the likelihood of threats and vulnerabilities of IT assets. The CRAMM methodology contains tables describing the correspondence between IT asset vulnerabilities and threats that could affect IT assets through these vulnerabilities. There are also tables describing the damage to IT assets if these threats occur. This stage is performed only for the most critical IT assets, for which the introduction of a basic set of information security measures is not enough. Identifying current vulnerabilities and threats is done by interviewing those responsible for administering and operating IT assets **[11]**.

Risk Calculation The calculation of risk is carried out according to the formula: Risk = P (implementation) * Damage. In this case, the probability of risk realization is calculated by the formula: P (implementation) = P (threat) * P (vulnerability). At the stage of calculating risks for each IT asset, the requirements for a set of measures to ensure its information security are determined on a scale from "1" to "7", where a value of "1" corresponds to the minimum necessary set of measures to ensure information security, and a value of "7" - maximum.

Risk Management Based on the results of risk calculation, the CRAMM methodology determines the necessary set of measures to ensure information security. For this, a special catalog is used, including about 4 thousand measures. The set of measures recommended by the CRAMM methodology is compared with measures that have already been taken by the organization. As a result, areas that require additional attention with regard to the application of protective measures and areas with excessive protective measures are identified. This information is used to formulate an action plan to change the composition of protective measures used in the organization - to bring the level of risks to the required level.

From the point of view of practical application, the following advantages of the CRAMM technique can be distinguished:

Repeatedly tested method, according to which considerable experience and professional competencies have been accumulated; CRAMM application results are recognized by international institutions;

The presence of an understandable formalized description of the methodology minimizes the possibility of errors during the implementation of risk analysis and management processes **[13]**.

The availability of automation tools for risk analysis minimizes labor costs and the time taken to carry out risk analysis and management;

The catalogs of threats, vulnerabilities, consequences, information security measures simplify the requirements for special knowledge and competence of direct executors of risk analysis and management activities.

With this CRAMM technique, the following disadvantages are inherent:

High complexity and laboriousness of the collection of source data, requiring the attraction of significant resources within the organization or from the outside;

Large expenditures of resources and time for the implementation of the processes of analysis and risk management of information security;

The involvement of a large number of stakeholders requires significant costs for the organization of joint work, communication within the project team and the coordination of results;

The inability to assess the risks in money makes it difficult to use the results of the risk assessment of information security in the feasibility study of investments necessary for the introduction of means and methods of information protection **[12]**.

CRAMM is widely used in both governmental and commercial organizations around the world, being in fact the standard for information security risk management in the UK. The technique can be successfully applied in large organizations focused on international cooperation and compliance with international management standards, implementing the initial implementation of information security risk management processes to cover the entire organization at once. At the same time, organizations should be able to allocate significant resources and time for applying CRAMM.

## 3. CobIT RISK MANAGEMENT

COBIT for Risk Methodology Overview. The COBIT for Risk methodology was developed by the ISACA (Information Systems Audit and Control Association) in 2013 and is based on best risk management practices (COSO ERM, ISO 31000, ISO \ IEC 27xxx, etc.). The methodology considers the risks of information security in relation to the risks of the core business of the organization, describes the approaches to the implementation of the information security risk management function in the organization and to the processes of a qualitative analysis of information security risks and their management.

When implementing the function and risk management process in an organization, the methodology identifies the following components that affect both information security risks and the process of managing them:

- Organization principles, policies, procedures;
- Processes
- Organizational structure;
- Corporate culture, ethics and rules of conduct;
- Information;
- IT services, IT infrastructure and applications;
- People, their experience and competencies.

In terms of the organization of the information security risk management function, the methodology defines and describes the requirements for the following components:

- Necessary process;
- Information flows;
- Organizational structure;
- People and competencies.

The main element of the analysis and risk management of information security in accordance with the methodology are risk scenarios. Each scenario is "a description of the event, which, if it occurs, can lead to an indefinite (positive or negative) impact on the achievement of the organization's goals". The methodology contains more than 100 risk scenarios covering the following exposure categories:

- Creation and maintenance of IT project portfolios;
- Program / project life cycle management;
- IT investments;
- Expertise and skills of IT staff;
- Operations with staff;
- Information;
- Architecture;
- IT infrastructure Software;
- Inefficient use of IT;
- Selection and management of IT providers;
- Compliance with regulatory requirements;
- Geopolitics;
- Theft of infrastructure elements;
- Malicious software Logical attacks;
- Technogenic impact;
- Environment;
- Natural phenomena;
- Innovation

For each risk scenario, the methodology determines the degree of its belonging to each type of risk:
Strategic risks - risks associated with missed opportunities to use IT to develop and increase the effectiveness of the organization's core business;
Project risks - risks associated with the influence of IT on the creation or development of existing organization processes **[14]**.
Risks of IT management and the provision of IT services are the risks associated with ensuring the availability, stability and provision of IT services to users with the necessary level of quality, problems with which can lead to damage to the core business of the organization.
Each risk scenario contains the following information:
The type of threat source is internal / external.
Type of threat - malicious action, natural phenomenon, mistake, etc.
Description of the event - access to information, destruction, modification, disclosure, theft, etc.
The types of assets (components) of the organization that are affected by the event - people, processes, IT infrastructure, etc.
Event time.
In the case of the implementation of the risk scenario of the organization, damage is caused. Thus, when analyzing information security risks in accordance with the COBIT for Risk methodology, risk scenarios relevant to the organization and risk mitigation measures aimed at reducing the likelihood of these scenarios are identified. For each of the identified risks, an analysis is made of its compliance with the organization's risk appetite, followed by one of the following decisions:
Risk avoidance;
Risk taking;
Risk transfer;
Risk reduction.
Further risk management is carried out by analyzing the residual risk level and deciding on the need to implement additional risk mitigation measures. The methodology contains recommendations for the implementation of risk reduction measures for each of the types of components of the organization.

From the point of view of practical application, the following advantages of the COBIT for Risk methodology can be distinguished:
Communication with the COBIT shared library and the ability to use approaches and "IT controls" (measures to reduce risks) from related areas, allowing to consider information security risks and measures to reduce them in relation to the impact of risks on the organization's business processes;
Repeatedly tested method, according to which considerable experience and professional competencies have been accumulated, and the results of which are recognized by international institutions;
The presence of an understandable formalized description of the methodology allows to minimize

errors in the implementation of the processes of analysis and risk management**[15].**

The catalogs of risk scenarios and "IT controls" simplify the requirements for special knowledge and competence of direct executors of risk analysis and risk management activities;

The possibility of using the methodology in conducting audits allows reducing labor costs and the necessary time for interpreting the results of external and internal audits.

At the same time, the following disadvantages and limitations are inherent in the COBIT for Risk methodology:

The high complexity and complexity of collecting source data requires the involvement of significant resources either within the organization or from the outside **[15]**.

The involvement of a large number of stakeholders requires significant costs for the organization of joint work, the allocation of time for those involved in communication within the project team and the coordination of results with all interested parties;

The inability to assess risk in money makes it difficult to use the results of an information security risk assessment to justify the investments necessary to implement the means and methods of information protection **[18]**..

This method is used both in government and in commercial organizations around the world. The method is most suitable for large technological organizations or organizations with a high degree of dependence of core business on information technology, for those who already use (or plan to use) COBIT standards and methods for managing information technology and have the necessary resources and competencies for this. In this case, it is possible to effectively integrate information security risk management processes and general IT management processes and achieve a synergistic effect that will optimize the costs of implementing information security risk analysis and management processes.

## 4. INFORMATION SECURITY RISK MANAGEMENT

Today, the informatisation of society, coupled with the automation of processes, is developing so rapidly that ignoring the growing risks in the field of information technology is becoming unacceptable. Data center availability is measured in five and six "nines", and failures in the information systems of large companies are becoming global news [19].

As a result, organizations create separate information security and IT risk divisions that identify and manage risks in this area.


**Figure 4:** Risks Governance by EA

Demand generated supply. So, the ISO international organization issued the standard for information security risk management in the organization - ISO 27005: 2008 "Information technology - security techniques - information security risk management". However, besides him, there are other equally useful documents, for example[17].:

- IT Risk Management Framework (The Risk IT Framework) and IT Risk Application Practices (The Risk IT Practitioner Guide) based on ISACA's Cobit standard;
- Ken Jaworski's proprietary information systems risk management methodology.

Let's consider each of them in more detail.

ISO 27005: 2008 defines the risk of information security - the likelihood that a given threat exploits the vulnerabilities of an asset or group of assets and thus harm the organization **[20]**..

In accordance with the standard, the information security risk management process allows you to organize the following:

- risk identification;
- risk assessment in terms of business implications and the likelihood of their occurrence;
- communication and awareness of the likelihood and consequences of risks;
- prioritizing risk management;
- prioritizing actions to reduce the likelihood of risks;
- involving stakeholders in the decision-making process for risk management and informing about the status of the risk management process;

- monitoring the effectiveness of risk treatment;
- regular monitoring and review of risks and the risk management process;
- Identification of information to improve the risk management approach;
- training managers and employees on risks and actions to reduce them.

It is noteworthy that the scheme of the information security risk management process coincides with the scheme of the 31000 standard presented earlier, which once again confirms the same approach to risk management in a series of ISO standards. The standard is theoretical, but will be useful as a basis for further implementation of the risk management system **[21]**..

The IT Risk Management Framework (The Risk IT Framework), based on the ISACA Cobit standard, includes a theoretical framework, instructions for use — a methodology and practical examples.

This document defines the IT risk - this is a business risk, in particular the business risk associated with the use, possession, performance of actions, involvement, influence or adaptation of IT in the organization.

The process model of this environment consists of three domains:

- risk management (Risk Governance);
- risk assessment (Risk Evaluation);
- risk response (Risk Response).

This three-domain model is carefully disassembled in the document. All necessary definitions are given, the role model for the enumerated processes is analyzed, as well as the implementation procedure.

Instructions for use for IT risks (The Risk IT Practitioner Guide) is a logical continuation of the work environment, focused on the practical implementation of a three-domain model in an organization. The document provides the necessary templates, tables and other documents that you can change and use if necessary in your organization's risk management system. It also describes the best practices for implementing IT risk systems.

Ken Javorski's information systems risk management methodology is based on the ISO standard and focuses on the practical aspects of implementing a risk management system, and also contains the necessary templates and methods for calculating the impact of risks on the organization's activities.

Summing up, we can conclude that in the field of information security risk management, there is some progress that allows interested specialists to move from theoretical descriptions to practical actions. Thus, the international standard ISO 27005: 2008 serves as the starting point for a theoretical point, the further practical path from which, despite the individual approach for each organization, can be effectively implemented using at least two methods [22]..

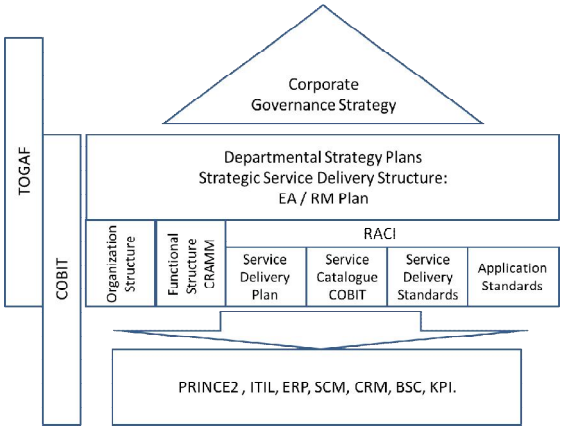


**Figure 5:** Risk Management Plan

## 5. CONCLUSION

The risk management plan as part of corporate governance plan is already showing its effectiveness in those companies in which it is being introduced or has already been implemented. In connection with the crisis state of the world economy at the moment, we can assume the spread in the future of such systems in the public sector. This is possible even today, since there are already standards and other documents on the risk management system that allow you to implement this system efficiently and in a relatively short time. The crucial point is the fact that, in addition to "general" documents, there are industry standards for risk management, in particular IT / IS risk management. However, given the specifics of the economy, many organizations rely more on state support or the so-called administrative resource, not paying enough attention to the corporate governance and risk management system in particular. As a result, in our country there is a growing predisposition to larger bankruptcies than in the USA. But inaction is unlikely to help resolve the problem.

## REFERENCES

1. Gerasimenko V.A., Malyuk A.A. Fundamentals of information security. - M .: Inkombuk, 2017.
2. Hoffman L.J. Modern methods of information protection. / Per. from English - M.: Soviet Radio, 1980.

3. GOST R ISO / IEC 15408-1-2002. Information technology. Security methods and tools. Criteria for assessing the security of information technology. Part 1. Introduction and general model. - M: Gosstandart, 2012.
4. Sidak A.A. Formation of security requirements for network information technologies. - M.: MGUL, 2011.
5. GOST R ISO / IEC 17799-2005. Information technology. Practical rules for managing information security. - M: Standartinform, 2006.
6. GOST R ISO / IEC 27001-2006. Information technology. Security methods and tools. Information Security Management Systems. Requirements.
7. Guide to lifecycle security. - AXENT Technologies 1998.
8. Guidelines for managing security risks. Microsoft Security and Compliance Development Group and Microsoft Security Center of excellence. - URL: http://www.microsoft.com/eng/technet/security/guidance/complianceandpolicies/secrisk/
9. Simonov S. Modern technologies of risk analysis in information systems // PCWEEK. 2015. No. 37.
10. Simonov S. Risk analysis, risk management. // JetInfo No. 1, 1999.
11. Simonov S. Technologies and tools for risk management. // JetInfo No. 2, 2003.
12. The logic behind CRAMM's assessment of measures of risk and determination of appropriate countermeasures. URL: http://www.cramm.com/downloads/techpapers.htm
13. Peltier, Thomas R. Information security risk analysis. Auerbach 2001. ISBN 0-8493-0880-1 https://doi.org/10.1201/b12444
14. Alberts C., Dorofee A. OCTAVE threat profiles. URL: http://www.cert.org/archive/pdf/OCTAVEthreatProfiles.pdf
15. Storms A. Using vulnerability assessment tools to develop an OCTAVE Risk Profile. // SANS Institute. Part of Information security reading room. URL: http://www.sans.org
16. RiskWatch users manual. URL: http://www.riskwatch.com.
17. Alexandrovich G.Ya., Nesterov S.A., Petrenko S.A. Automation of company information risk assessment. // Information security. Confident. 2003, No. 2. P.78-81
18. Taylor L. Risk analysis tools & how they work. URL: http://www.riskwatch.com
19. Winter V.M., Moldovyan A.A., Moldovyan N.A. Computer networks and protection of transmitted information. - St. Petersburg: Publishing House of St. Petersburg State University, 1998.
20. Koneev I.R., Belyaev A.V. Information security of the enterprise. - SPb .: BHV-Petersburg, 2003.
21. Gruntovich M.M. The basics of cryptography with public keys. Tutorial. - Penza: Penza Publishing House. gos. University, 2000.
22. 22. Winter V.M., Moldovyan A.A., Moldovyan N.A. Global network technology security. - 2nd ed. - SPb .: BHV-Petersburg, 2003.