Advances in Science and Technology Research Journal

Advances in Science and Technology Research Journal 2024, 18(2), 317–332
https://doi.org/10.12913/22998624/185162
ISSN 2299-8624, License CC-BY 4.0

Received: 2024.01.25
Accepted: 2024.02.21
Published: 2024.03.15

Modifications of the Formal Risk Analysis and Assessment for the Information System Security

Imed El Fray[1*], Artur Wiliński[2]

[1] Faculty of Computer Sciences and Information Technology, West Pomeranian University of Technology, Al. Piastów 17, Szczecin, Poland

[2] Faculty of Applied Informatics and Mathematics, Warsaw University of Life Sciences, Nowoursynowska 159, Warsaw, Poland

* Corresponding author's e-mail: artur_wilinski@sggw.edu.pl

ABSTRACT

In the article, a modification of formal model of risk analysis (FoMRA) was proposed. The modified FoMRA1 method takes into account the guidelines of ISO/IEC 27001 and ISO/IEC 27005 standards. The applied modification and abstraction by resources and security controls (also called countermeasures) significantly shortened the time of risk weight calculation in comparison with the MEHARI method. An attempt was also made to further reduce the time of risk analysis using agents collecting information and data from various network nodes, from operating systems and devices, and additional agents containing information on reports on security procedures, security services, security management and organizational activities related to the information systems (maintenance, insurance, outsourcing contracts, etc.) and transfer it to the local FoMRA1 database. The obtained results indicate that the proposed method together with agents installed in various nodes enable a quick reaction to the system threats and prevention of their impacts (quasi-real-time security monitoring system).

Keywords: security monitoring, risk analysis, risk assessment, formal model, information system, MEHARI methods, security monitoring

INTRODUCTION

An analysis of the current state of knowledge shows that much work has been published in the area of risk management information systems [1-3]. For several years, ISO/IEC has also been working intensively on the risk management process (analysis, assessment, management, risk monitoring and communication) [4-6]. Simultaneously, with the development of new standards, various initiatives from governmental institutions and non-profit organizations have emerged, resulting in new methods of risk analysis and/or risk management [7-9]. Most of these standards and methods have the same goal: to actively identify every source of risk, threats and vulnerabilities of the Information System (IS) in an organization and their impact on resources and to propose appropriate security controls [10-12]. Commonly used standards and risk analysis methods are bottom-up methods [19, 20, 30]. These are methods that only allow for an "a posteriori" approach to Information Systems (IS) security [13-15]. These methods usually focus on well-defined steps and actions to be taken in order to achieve the best security level for the IS [16-18]. The added value of these methods and standards is based on the fact that they contain the basis knowledge about the risk and the security requirements [32-34]. The disadvantage of these methods is that they are:

- time-consuming, e.g, require the knowledge and skills from an auditor of linking resources with vulnerabilities, threats, etc.; the input data are based on audit results – checklists and all these links are made by the auditor step by step,

- rigorous, have closed sets of vulnerabilities, threats and risks, sets of ready-made security or configuration settings - therefore do not allow changes, adaptations, extensions, etc. and
- final results generated by those methods, the templates and documents in the output are generally informal, most often expressed in natural language.

All these disadvantages lead to the lack of automation at the level of reasoning, evolution, monitoring or information evidence related to the information security risk management process. The "a priori" approach to IS security according to the author, e.g., at the project level, seems to be much better for a significant improvement of the organization security and acceleration of the risk analysis and assessment process [22, 23]. In various fields of science, and especially in information technologies, formal modelling is an important tool for studying the properties of complex structures, systems or algorithms [24, 25]. Often, only formal models exist that enable, for example, automatic or semi-automatic simulations or verification of the properties of very complex systems [49,50]. The goal of this work is to find a method of risk analysis and assessment, after appropriate modification and optimization, that can be the answer to the problems that most risk analysis and assessment methods have to face, i.e.:

- the fact that it is not rigorous, which means that it has an open knowledge base on threats, vulnerabilities and risks, that it is flexible, which means that it can be configured, developed and adapted to the variety of the requirements of standards and legal acts in Poland.
- limiting the time of risk analysis and in combination with security information and event management (SIEM) solution tool, it is possible to react to various threats to information systems in quasi-real time.

MODIFICATION AND OPTIMIZATION OF THE RISK ANALYSIS METHOD (FOMRA)

Like all computational systems, risk analysis systems are constantly modified or improved and these changes can be divided into two groups. The first group consists of various calculation optimizations, including conceptual changes to the algorithms used, or their optimization, or even the practical application of different methods developed for the solution of any calculation task. The other is to increase the functionality of the system by additional options or completely new possibilities. This article presents such a modification and functional improvement of formalism (FoMRA) published previously in [35, 36].

Automatic risk scenario process

The proposed modification of FoMRA in this section introduces a new functionality to the system, important from the point of view of conducting tests and simulation studies. Risk analysis simulation models should be developed and tested using risk knowledge bases applicable to the methods used in practice. These databases are fixed and static [11, 13, 17], i.e. they cannot be modified. From the point of view of testing and creating research simulation models about the properties of risk analysis calculation methods, this is not a comfortable situation because we are dealing only with a specific, finite and relatively small sets of data. In order to become independent from these knowledge bases and to be able to conduct simulations describing other variants of systems, a method has been developed which allows for automatic generation of risk scenarios. Therefore, the additional modifications of FoMRA1 method, which enable such automatic generation of scenarios will be proposed. First of all, the method is extended by parameters expressing the vulnerability environment and sources of threats. Secondly, the number of arrays determining the risk weight has been reduced. The introduced changes are also aimed at making it possible to reduce the model based on abstraction at the level of resources, scenarios and security controls. The following two sets of objects that characterize the information system have been added to the FoMRA1 method:

$$O = \{o_i : i = 1,\ldots,n_o\} \tag{1}$$

is a set of internal and external factors affecting resource vulnerability,

$$P = \{p_i : i = 1,\ldots,n_p\} \tag{2}$$

is a set of threat actors (sources of threat).

In addition, any subset of O factors we will call the environment of the resource. For further consideration, it is necessary to modify the vulnerability of the information system as follows (see Eqation 11).

Definition 1. Vulnerability of an information system should be any function of the type:

$$vul: A \times 2^{\wedge o} \rightarrow 2^{\wedge V} \quad (3)$$

The modification presented in definition 1 indicates that this time the vulnerability of a given resource to threats also depends on its environment (any subset of the set factors).

Therefore, the definition 2, which defines the general risks of the system, must also be modified. The threat will additionally depend on its sources, i.e. the so-called actors – users of the system:

Definition 2. A general threat to the Information System should be any function of the type:

$$thr: \overline{A \times V \times 2^P} \rightarrow 2^T \quad (4)$$

where the set $thr: \overline{A \times V \times 2^P}$ is a set of all three forms (a, v, X) from the Cartesian product $A \times V \times 2^P$ meeting the following condition:

$$(a,v,Y) \in \Leftrightarrow \exists_{X \subseteq V} \exists_{K \subseteq O} (v \in X \wedge v \in vul(a,K)) \quad (5)$$

As can be seen from the above definition, the arguments of functions are three, where the first coordinate is the resource, the second is the vulnerability of this resource, and the third set are the threat factors. The values of the above function determine the threats to the resources from the set A depending on the vulnerability of the resources from the set V (and thus indirectly through the environment) and the threat factors T.

In accordance with the above modifications, it is also necessary to change the definition of the risk scenario, formulated in the definition 3:

Definition 3. The general risk scenario of the information system will be referred to as a set of all the different four, where the third and fourth component is not an empty set, defined by the following relationship:

$$SI_{(z)} = \left\{ \begin{matrix} \left(a, vul(a,K), thr(a,v,Y)\right) : a \in A \wedge K \subseteq O \wedge \exists_{Y \subseteq V} \exists_{Y \subseteq P} (a,v,Y) \\ \in A \times V \times 2^P \end{matrix} \right\} \quad (6)$$

Note that according to the above modifications, in the new model, the scenario depends on four parameters: resource, vulnerability, environment and threat factors.

The second modification of the FoMRA method consists in removing "recovery controls" from the formal model and algorithm, and thus from the calculations. It should be noted that the set of security controls (i.e. insurance of tangible and intangible resources, outsourcing, etc.) assigned has been transferred to „corrective controls". This was done because during the comparative studies of the risk assessment methods, MEHARI and CRAMM with the FoMRA already published in [31,36,48] the inclusion of security controls in the „recovery controls" in the process of risk estimation generates weight differences between those methods. Such approaches makes this method partially reactive (the security controls are planned as a reaction to possible risks, once they have occurred "post-factum risk").

Considering that most methods, including CRAMM, OCTAVE, etc., are dedicated to active risk analysis (the security controls are planned as a response to possible risks before they occur), the new modified structure of the arrays (remove the "recovery controls" array from the FoMRA model, etc.) determining the risk weight values W^s for each scenario is presented below:

$$M_{pot} = \bigcup_{s\,:\,\exists_{dp \in DP}(s,dp) \in \overline{DP}} \{M_{pot}^{s,t}\} \quad (7)$$

$$M_{imp} = \bigcup_{s\,:\,\exists_{di \in DI}(s,di) \in \overline{DI}} \{M_{imp}^{s,a}\} \quad (8)$$

$$M = \bigcup_{s \in S} \{M^s\} \quad (9)$$

where:

$DP = \{ dp_s : s = 1, ..., n_{DP} \}$ – is a set of security controls reducing a potentiality. This set is assigned to deterrent and preventive controls [17, 21, 47],

$DI = \{ di_t : s = 1, ..., n_{DI} \}$ – is a set of security controls reducing an impact.This set is assigned to protective, corrective controls [17, 21, 47].

The above modification of the FoMRA method, called FoMRA1, has been tested on the appropriateness of removing "recovery controls" from the formal model and algorithm and its impact on the results of risk estimation. Table 1 with 12 scenarios assigned to 7 main groups of risk scenarios and 2 rosettes showing the results of FoMRA and FoMRA1 risk analysis are presented below. The results obtained for all scenarios presented in column 1 (Vs_FoMRA) assume the lack of implementation of security controls assigned to "recovery controls" by organizations and assumes their full implementation as shown in column 2. The same approach was applied to columns 3 and 4 (Vs_FoMRA1) but this set of security controls, as described above, was attached to the set of security controls assigned to "corrective controls". Algorithms, formulae and arrays for calculating weight values for potential and impact actions and risks are presented in [35,36].

As can be seen from Table 1 (Vs_FoMRA - column 2) and Figure 1 – (grey field) where the set of all security controls (i.e. insurance of tangible and intangible resources, etc.) for "recovery controls" are implemented, the risk value is acceptable for most scenarios. In some scenarios there are no security controls provided for "recovery controls" since for example in Poland it is impossible to insure oneself against some deliberate threats (e.g. undertaken by maintenance staff or disloyal employees). Results (column 2 and Figure 1 – grey field) confirm that

FoMRA is a partially reactive method, which may present a misleading picture of the actual risk in the organization [26,29]. The FoMRA method is not an isolated case because both MEHARI [17] and ISRM [27,28] methods are also partially reactive. Contrary to that, the assignment of the set of protections from "recovery controls" from FoMRA to the "corrective controls" in new FoMRA1 as indicated in Table 1 (Vs_FoMRA1 – column 4) and Figure 2 – (grey field) generated minimal changes for some scenarios. This is the effect of changes in the algorithm in FoMRA1 used to calculate "corrective controls" where the security controls transferred (i.e. insurance of tangible and intangible resources, etc.) are part of the security controls supporting an existing security controls (i.e. disaster recovery site or plan, system and data backups, high availability, etc.) in "corrective controls". Some results (reduced risk weight for some scenarios) in column 4 and Figure 2 are the result of lack of sufficient security controls (i.e. data backups, breakdown of

Table 1. Risk estimation values by FoMRA and FoMRA1

Scenarios		Vs_FoMRA Risk Value	Vs FoMRA Risk Value	Vs_FoMRA1 Risk Value	Vs_FOMRA1 Risk Value
01- Unavailability of the resources (Hardware)		3	2	3	3
01-1	Network equipment unavailable due to a breakdown	3	2	3	2
01-2	Multi-user equipment unavailable due to a breakdown (local server, printer, peripheral system, etc.)	3	2	3	3
01-3	Breakdown of an important auxiliary equipment: (air-conditioning, etc) leading to unavailability of (host) system	3	2	3	3
04 - Unavailability of resources (software)		3	2	3	3
04-1	Computing system configurations erased or polluted by a non-operational staff member	3	2	2	2
04-1	User configurations erased by a virus	3	2	3	3
06 - Data alteration		3	2	3	3
06-1	Accidental data alteration during an emergency maintenance operation	3	2	3	3
07 – Data disclosure		3	2	3	2
07-1	Deliberate erroneous data input by a staff member usurping an authorized user‘s identity	3	2	2	2
07-2	Manipulation of data files by an unauthorized third party usurping an authorized user‘s authority	3	2	3	2
09 - Data distortion		3	3	3	3
09-1	Repeated copy of application data files, by an unauthorized third party connecting from outside to an open port for network remote maintenance	3	3	2	2
09-2	Repeated copy of application data files, by unauthorized third party connecting from outside to an open port for network remote maintenance	3	3	2	2
09-3	Access to system storage and copy of application data files, by a maintenance staff	3	3	3	3
09-4	Access to storage area networks and copy of application data files, initiated from a non-authorized server	3	3	3	3
10 - Loss of data files or documents		2	2	2	2
10-1	Massive erasure of archive data files by operational personnel	2	2	2	2
11 - Disaster affecting data		2	2	2	2
11-1	Massive destruction or pollution of business data files and backups, due to a deliberate logical operation by a system admin or operator	2	2	2	2

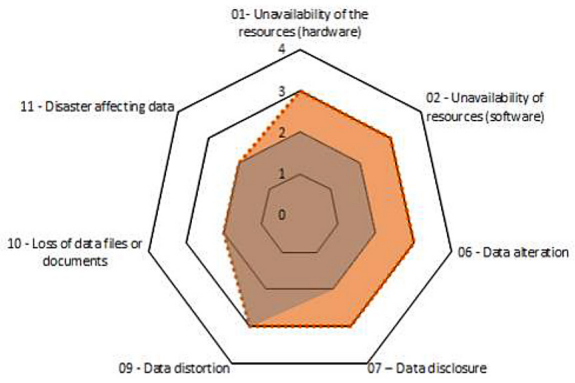

Figure 1. Risk estimation results for FoMRA

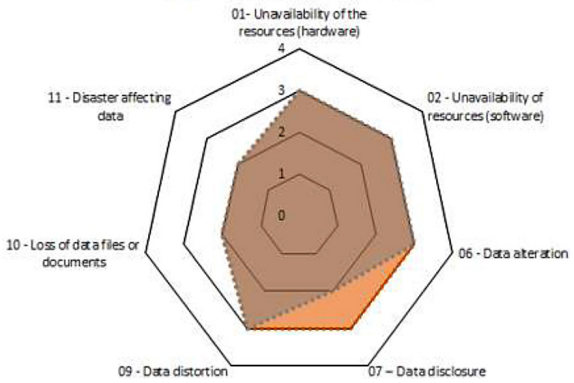

Figure 2. Risk estimation results for FoMRA1

the network equipment). The reduced risk weight for the exemplary scenario of 07-2 is the result of partial activation of the transferred security control (insurance of intangible resources) from "recovery controls". Weighted CMs,j [37-39] for "corrective controls" = Min (CMs, di2=insurance of intangible resources; CMs, di2=data backups) = 4. As can be seen from Table 1 (Vs_FoMRA – column 4) such a state is not a common phenomenon as in the case of FoMRA where the security controls assigned to "recovery control" can have a large impact on the final risk weight. Thanks to the modifications described above and the results obtained in Table 1 it can be assumed that FoMRA1 is an active method such as CRAMM or OCTAVE. Since 2015, FoMRA1 has been continuously and efficiently applied in audits of several enterprises and organizations in Poland of different activity profiles (GUS - Statistics Poland, Bank PKO S.A - Unicredit, Systemics Poland Co. Ltd., The 4 Investment Group Co. Ltd.). In 2016, for the certification process to comply with ISO/IEC 27001 requirements, an additional risk treatment and Statement of Applicability module was developed to enable full risk management of the Certum – Poland, the global registry services information system. Figure 3 below shows the risk treatment module and the effect of the introduced changes on the final risk management module (Fig. 4).

Risk treatment is very important, it will enable to implement the security controls (measures) to reduce the gravity of the selected scenarios. FoMRA1 use an algorithm according to four ways (Retain, Avoid, Share, Modify) suggested by ISO 27001 to treat unacceptable risks. In this module (Fig. 3) the auditor, using the "drag and drop" function, can again raise these questions about the security measures (e.g. 08F02 = 2) for which a negative answer (no implemented security) was originally given (during the audit). If an organization wants to implement these security controls for a given service (e.g. 08F02 = 4), the built-in algorithm will recalculate the final values for all

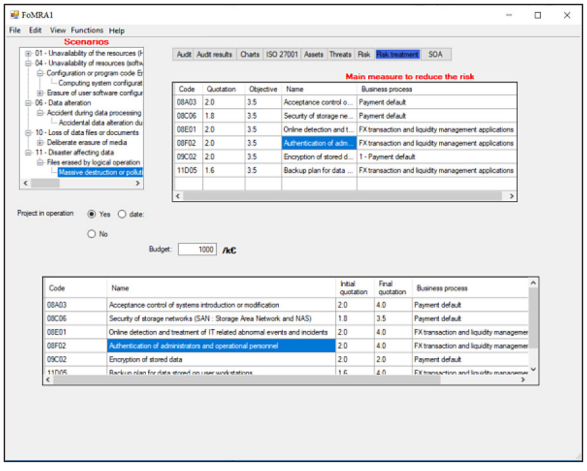

Figure 3. Risk treatment module

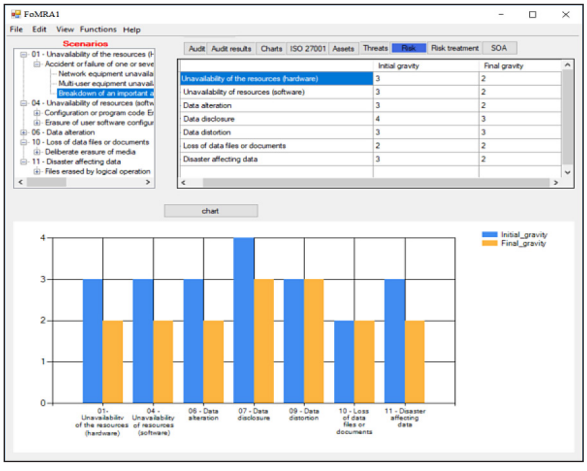

Figure 4. Risk management module

measures (the module assumes that these security controls are implemented and the answer to "yes" is changed for one or more questions) and then indirectly recalculates the final risk (Fig 4). The module can also calculate the costs of the implemented security controls. The results obtained by FoMRA1 method are repeatable and satisfactory and have been accepted by the certification body "TUV Nord" for the information system in Poland of global registry services in compliance with the requirements of ISO/IEC 27001-2016. FoMRA1 enables automatic generation of statement of applicability and effectiveness of the implemented security control documents.

Final summary, FoMRA1 complies with the fundamental requirements of active methods and the ISO standard: ISO/IEC 27005:2018 – Security techniques – Information security risk management.

Reduction of the risk analysis model

One of the popular methods of improving the efficiency of calculations carried out in the computational system or its formal model is to introduce appropriate abstractions in the model. Such reductions are made by applying certain equivalence relationships in the model, which combine many elements of the system into one representative set that can replace all its elements in the calculations. This is a popular technique in many formal modelling applications, which sometimes makes it possible to significantly reduce the size of constructed and tested models, even infinite models, and thus makes it possible to perform effective calculations.

The bi-argument relation defined on the Cartesian product A×A (which is its subset: (δ⊆A×A) for a given set A) we term as an equivalence relationship if it meets the following three properties:

- maneuverability, and therefore the condition is fulfilled when each element of the set is in relation to each other, formally:

$$\forall_{x\in A} x\delta x \tag{10}$$

- symmetricality, i.e. the relation between the elements of the set in one direction enforces the relation in the other direction:

$$\forall_{x,y\in A}(x\delta y \Rightarrow y\delta x) \tag{11}$$

- transitivity, i.e. it is fulfilled:

$$\forall_{x,y,z\in A}(x\delta y \wedge y\delta z \Rightarrow y\delta x) \tag{12}$$

In the following considerations, relations defined by the equality will be used. Reductions of the model, and thus calculations, seem to be a simple task. Even a well-defined formulation of a condition for a given relation can be very complicated and requires from the defining person a perfect knowledge of the system/model. However, even a very good and accurate definition of the relation, which provides a substantial reduction, is not a sufficient condition to achieve the intended goal, i.e., to reduce the number of calculations. Another problem is to indicate a suitably fast method, algorithm of checking whether the data of the state/object of the model are really in relation with each other. It may happen that acceleration of calculations for a well-chosen relation will not be possible to be achieved. The reason may be too much computational complexity of the algorithm of testing the fulfilment of relations between two objects of the model or that it has to make too many comparisons between successive pairs of objects. In the proposed next modification of the model (FOMRA1), the resources and security controls have been abstracted.

Abstraction by the resources

The first reduction by abstraction that can be implemented in the formal model risk analysis under consideration is abstraction by the system resources. Let us consider a set of resources A. Resources were assigned to vulnerabilities and threats.

Definition 4. We will say that two resources are in a similar relationship if and only if the same vulnerabilities and threats correspond to them. If we denote the similarities of resources by σ, then formally we can write this condition as follows:

$$\forall_{x,y\in A}\,[x\sigma y \Leftrightarrow (vul(x) = vul(y) \wedge \forall_{v\in vul(x)}(thr(x,v) = thr(y,v))] \tag{13}$$

The above relation is defined in terms of equality, so it is an equivalence relation. The reasons for the first two conditions for the equivalence relationship are the following dependencies:

$$\forall_{x,y\in A}\left(vul(x) = vul(x) \wedge \forall_{v\in vul(x)}(thr(x,v) = thr(x,v))\right) \tag{14}$$

$$\forall_{x,y\in A}\,[\left(vul(x) = vul(y) \wedge \forall_{v\in vul(x)}(thr(x,v) = thr(y,v))\right) \Rightarrow \left(vul(y) =$$

$$= vul(x) \wedge \forall_{v \in vul(y)} \left(thr(y, v) = thr(x, v) \right) \right) \quad (15)$$

The third condition, i.e. the pass-by, also applies.

The algorithm calculating the risk weight with abstraction by resources consists in checking whether the resources calculated consecutively have the same parameters (vulnerabilities and threats). Calculations are performed in linear time, because they depend on checking the appropriate conditions in the data structure. This reduction justifies the following modification of the risk weighting algorithm. When creating a calculation graph, i.e. when adding another resource, the condition defining the relationship of σ with already calculated resources is checked first. If this is fulfilled for one of them, the values already counted for this case are taken into account during the final phase of risk weight calculation.

Abstraction by security controls

It often happens in the system that the same security controls reducing the potentiality and impact should be taken for different risk scenarios. It is therefore possible at the right time not to recalculate the parameters for the calculation graph. Such a relationship is a theoretical justification for this case and is defined below.

Definition 5. Let ξ be the relation defined on the set $\overline{DP} \cup \overline{DI}$ ($\xi \subseteq \overline{\mathrm{DP}} \cup \overline{\mathrm{DI}} \times \overline{\mathrm{DP}} \cup \overline{\mathrm{DI}}$ as follows:

$$\forall_{(s_1,d_1),(s_2,d_2) \in \overline{DP} \cup \overline{DI}} \; [(s_1, d_1)\xi(s_2, d_2) \Leftrightarrow d_1 = d_2] \quad (16)$$

The above relation is also defined in terms of equality, i.e., it is a relation of equivalence. When performing the algorithm calculating the risk weight, it is checked in constant time that the relevant pairs consisting of the scenario and the security controls reducing the potentiality or impact have the same activity (effect). This reduction justifies the following modification of the risk weighting algorithm. When creating a calculation graph and when considering the next pair consisting of scenario and action, the condition defining the relation x with already calculated pairs of this type is checked first. If it is fulfilled for one of them, the values already counted for this case are taken into account in the final phase of the risk weight calculation.

Situations fulfilling this condition are more common than in the previous case, and one can count on a greater acceleration of the calculations. As before, the discussed optimization is one of several proposed above and as a component of the full process of risk weight calculation optimization it plays an important role.

EXPERIMENTAL RESULTS

In order to verify the correct operation of the FoMRA1 model after modification and abstraction, experimental studies were carried out. Results were obtained on the basis of a specially written for this purpose program.

The results show different possibilities of carrying out time calculations when determining the risk weighting for 100 scenarios within one business process (mortgage applications) of a large organization in Poland (Bank PKO SA – Unicredit) and independently for 10 business processes analyzed simultaneously (mortgage applications, payment default, sales and marketing, intersales, FX transaction and liquidity management applications, etc.) with the same number of scenarios which justifies the possibility of generalizing the results. The results are presented sequentially using the FoMRA1 and MEHARI methods (the only publicly available knowledge base of the Mehari method, which was programmed in the same environment as FoMRA1). The choice of MEHARI as a reference method is dictated by its compliance with ISO/IEC 27005 guidelines and can be additionally programmed for comparison purposes. The results presented in Figures 5–10 are related only to the calculation time of the risk weighting for 100 scenarios, with answers given to all questions. As can be seen from Figures 5–7 for one business process, better results of calculations were obtained for abstraction by security controls (Fig. 5). This result is related to the repeatability of security controls for a larger number of scenarios. The introduction of abstraction by security controls means that those security controls that appears as elements of various scenarios are included in the calculation only once. Calculation results are transferred (value from the stored cache) to the next calculation sequences without the need to perform recalculations for the same security controls.

In the case of abstraction by resources (Fig. 6), we obtained a longer calculation time than in the case of abstraction by security controls. Such result could have been expected, as the similarity of resources with the same risks and vulnerabilities

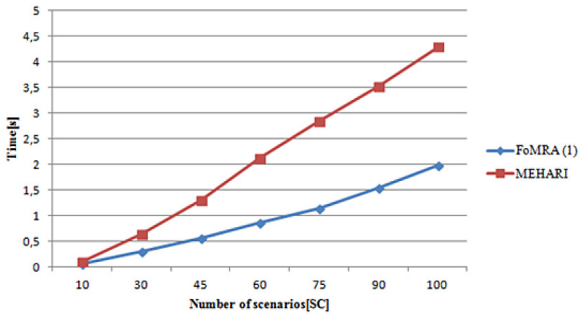

Figure 5. Time dependence of risk weight calculations for modified FOMRA1 and MEHARI with reference to the number of scenarios

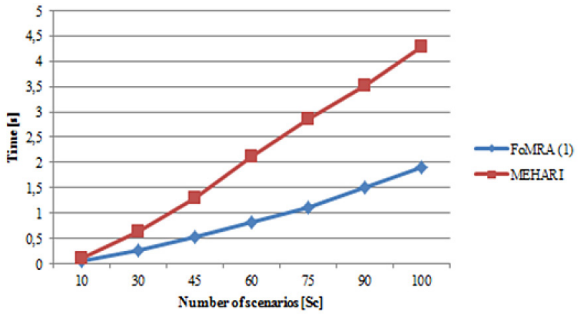

Figure 6. Time dependence of risk weight calculations after modification and abstraction by the resources for FOMRA1 and MEHARI with reference to the number of scenario

within a single business process is very small. Visible changes in calculations could only be expected if there were several dozen business processes under consideration (respondents), where the actual similarity relations between resources can be repeated more often than in the case of one business process. The above thesis is confirmed in Figure 9. Taking into account the percentage difference in time between Figure 6 (55.75%) and Figure 9 (57%), a reduction in calculation time proportional to the number of business processes studied between MEHARI and FoMRA1 can be seen. An analogous situation occurs in the case of abstraction by security controls, Figure 7 (66%) and Figure 10 (79%), show a significant reduction in calculation time between MEHARI and FoMRA1. As described in [48], optimistically it can take up to several days to perform one analysis for one business process in a large organization. This depends on various factors: identification and classification of resources, threats and vulnerabilities, allocation of ownership of resources to the personnel of the organization, association of resources with threats, vulnerabilities, to generate audit questionnaires and to conduct audits.

Most of the available methods are automated (Mehari, Octave, IT-Grundschutz, CRAMM, etc. are supported by commercial software), but require the intervention of an auditor in each of the above-mentioned activities. The process of calculating and assessing the risk after entering the answers from audit questionnaires into the system depends on the abundance of the knowledge base of a given method (e.g. the number of scenarios assigned to a given resource, security, etc.). From the available literature [37,38,40] it can be concluded that the methods are largely similar to each other, which allows to assume that the calculation time of risk weighting for the other methods (CRAMM, OCTAVE, IT-Grundschutz) is similar to the MEHARI method.

In the case of using FoMRA1, thanks to associating all risk parameters, auditor intervention is limited. The auditor should only introduce two values to the model (resource and risk) – the other actions are done automatically, until the audit

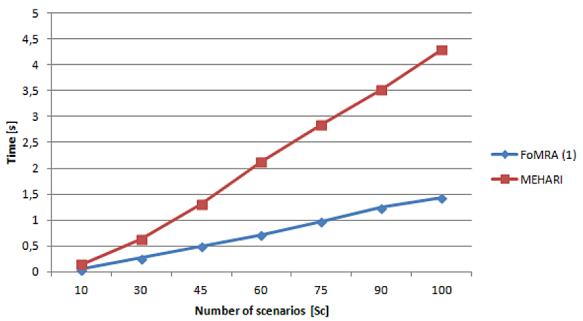

Figure 7. Time dependence of risk weight calculations after modification and abstraction by security controls for FOMRA1 and MEHARI with reference to the number of scenario

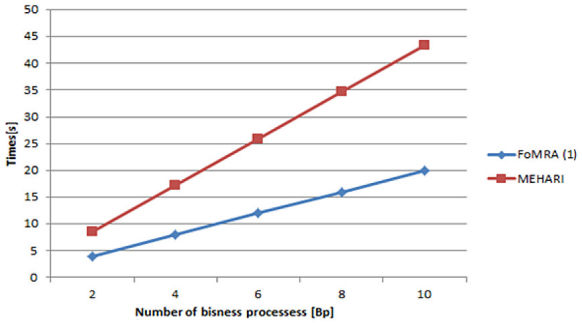

Figure 8. Time dependence of risk weight calculations for modified FOMRA1 and MEHARI with reference to the number of business process

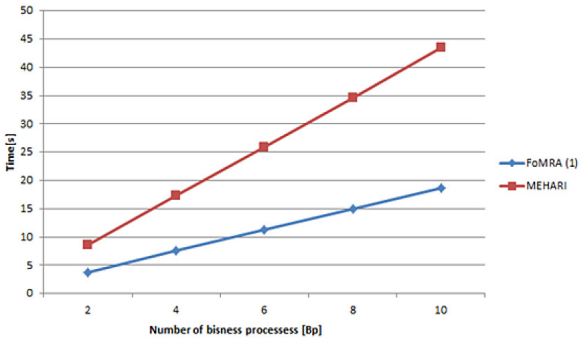

Figure 9. Time dependence of risk weight calculations after modification and abstraction by the resources for FOMRA1 and MEHARI with reference to the number of business process

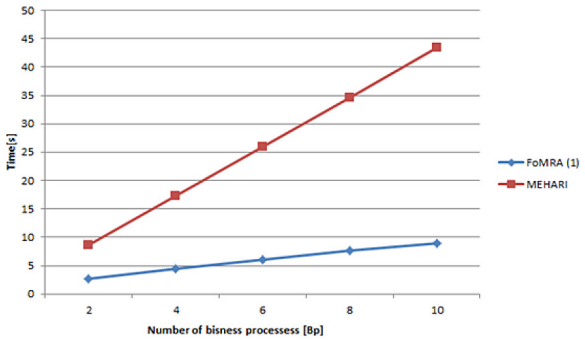

Figure 10. Time dependence of risk weight calculations after modification and abstraction by security controls for FOMRA1 and MEHARI with reference to the number of business process

questionnaires are generated. As shown, using FoMRA1 shortens the time of risk analysis execution. A further problem, that needs solving is shortening the time necessary for completing the answer form provided for staff.

In this case, an attempt was made, to adjust FoMRA1 for the network with agents collecting data from various network nodes, operating systems, hardware and from other agents (in the form of micro service), containing information about completed security procedures, management and organization activities, resulting from implementation of security policy for the system (service, outsourcing, insurance agreements etc.). Figure 11 shows a schematic of the infrastructure model, that is collecting data from the ASSECO Poland company systems. Risk analysis system is made up of three main components:

1) System monitoring module;
2) SIEM module, which is responsible for collecting and processing data, preliminary analysis and contains mechanism that notifies system administrators about malfunctions;
3) Risk analysis – FoMRA1.

There were services launched that are subjected to monitoring in the defined model: OpenLDAP (used as a mechanism of authentication in the role of a domain controller for other services or as a centralized authentication system that

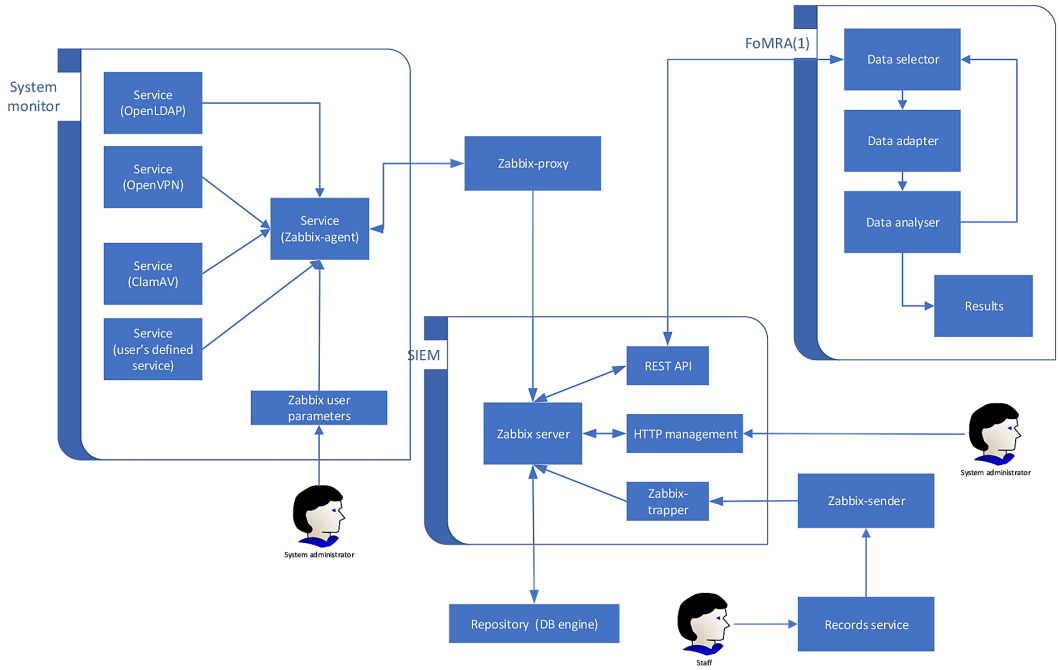

Figure 11. Diagram of the quasi-real time risk analysis infrastructure model

serves as a replacement for /etc/passwd), OpenVPN (user authentication using keys, certificates or username and password in the point to point connections), ClamAV (antivirus tool set).

Original services that are responsible for connecting with existing AC management system (for example LG, Hitachi), SSH service, Fail2ban as a framework that works as a security controls against brute-force attacks (scanning security logs and automatically updating firewall rules) and other services that are critical to system security are listed in Table 2.

Zabbix-agent [39-41] is responsible for monitoring parameters of the launched services. Configuration of the services is also protected by auditing services and tools that are responsible for monitoring the integrity of files and their permissions – AIDE [42-44], which assumes the role of IDS. Communication with SIEM system takes place using Zabbix-agent. Zabbix-agent has been extended using shell scripts, that are being launched on demand at defined time intervals (using Zabbix server). To monitor services defined by the administrator, integration with systemd has been provided (systemd unit), to ensure that service basic parameters can be read (start/stop, enabled/disabled) – parameter type: e.g., „Zabbix agent."

Zabbix-agent is responsible for monitoring parameters of IT systems:

- Servers – available disk space, memory usage, system load.
- Workstations – antivirus status, installed security updates status.
- Network devices – response time, current load of the device, etc.

Zabbix-agent is also responsible for responding to these events in the shortest possible time. Communication between Zabbix server (SIEM) and the system that is being currently monitored takes place using Zabbix-proxy, which allows to combine multiple network segments and systems that are currently operational in these networks (network devices, hosts and services). SIEM mechanism is implemented using launched Zabbix server. Zabbix server contains: REST API [45], HTTP management, Zabbix trapper [46]. REST API allows integration between Zabbix and existing systems that are currently operational in the organization. HTTP Management is a part of Zabbix and allows its configuration. It provides a convenient way of managing systems that are being monitored and managing applications (schematics that are defining the range of the monitored parameters). Zabbix trapper allows to send data about events using the autonomous processing agents by the Zabbix server. In the built model it is being given the handlers role allowing receiving data from the defined agents, which in this case allows convenient integration with the existing agent system. Data collected via the passive check mechanism (Simple check, Zabbix agent and data collected by the Zabbix trapper mechanism) is playing the test role – simplified collection of the elements that are describing real system features that are being monitored. Later they can be assigned to questions in the form. A list of the elements (for which time measures were taken) is shown in the Table 2. An example agent system is the Records Service (Fig. 12) which allows interaction between the user and the system that provides the information containing reports from completed security procedures, security services, and management actions related to the IS.

The logic of the registration system agent uses the system library which allows to use defined handlers (trappers). In the case of parameter extraction (for example getting a specific answer related to the information about reports from completed security procedures), a value is sent by API (or the Zabbix-sender) to the Zabbix server, where it is assigned to the questions in the forms. Data, which is collected and maintained by the Zabbix system, is stored in the external, relational database where it is subjected to analysis (trend, history). Modules that are used for risk analysis (Table 3) contain the Data selector, which provides communication with the Zabbix server using shared API.

Table 2. Examples of selected criteria assigned to risk scenarios

Criterion	Type	Reading frequency [s]	Service
net.tcp.service[ldap]	Simple check	60/45/30	OpenLDAP
net.udp.listen[1194]	Zabbix agent	60/45/30	OpenVPN
systemd.unit.is-active[firewalld.service]	Zabbix agent	60/45/30	Firewalld
proc.num[clamd]	Zabbix agent	60/45/30	ClamAV
systemd.unit.is-active[rsyslog.service]	Zabbix agent	60/45/30	Rsyslog

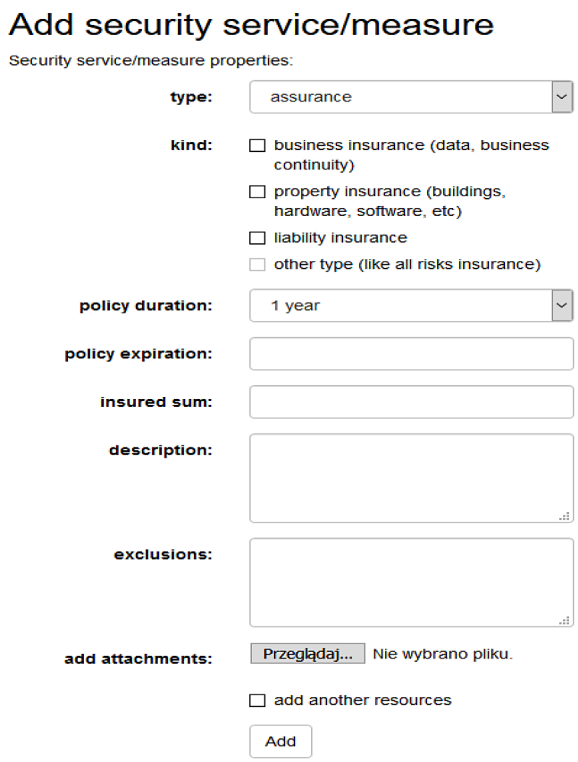

Figure 12. An example of user interface used to define security insurance status

Parameter values required to complete analysis (itemd, clock, value, ns) are serialized and forwarded to the module responsible for creating criteria (Data adapter). Below is an example of collected data from the Zabbix server using the API:

{'itemid': '28409', 'clock': '1531523669', 'value': '1', 'ns': '854693995'}

At this stage, analysis module uses defined schematics that are prepared by the auditor who uses criteria choice (Table 4) and correlates them with questions included in the FoMRA1 scenarios.

The process of risk analysis takes place in a loop in a quasi-real time. Therefore, monitored parameters are updated frequently by the Zabbix server at defined time intervals, which could directly affect the analysis. Results are presented in various forms (diagrams, descriptions, times) that are presented in real time by the result presenting module. Analysis results are shown below (for the random actions of stopping and restarting services, done periodically depending on the defined parameter sampling times using Table 2): Table 5 shows a correlation between execution of real action and time when this action was noticed by the SIEM mechanism. For example: OpenLDAP service launched on the serv-001 server has been shut down at 01:01:00 and this event has been registered by SIEM at 01:01:17, therefore time to react by the risk analysis system equals 17 seconds (this is the time that has passed since the event of shut down of the service, to the parameter value update by SIEM system).

Results of an event taking place and SIEM update of the event are shown in Table 6 (for four servers with five services installed). As shown in Table 6, there are four servers that provide exactly the same services. The time, between an event and SIEM update, has been analysed for every service. As shown, time for the event detection for most services (start-stop) is close to zero.

Based on these data, a statement can be made, that decentralization of the servers has a significant impact on event detection in quasi-real time. Considering additional results, from completed procedures, reports and security policies and correlating them with system events, we can obtain complete information about valid or invalid operations of the IS.

Figures (13-15) show that we can see the risk factor changing depending on event and procedure completions. As shown on the first rosette (Fig. 13), risk level is acceptable after the implementation of the procedures and starting the services.

Table 3. Example source code of a function that retrieves criteria values from the serv-001

```
    zapi = ZabbixAPI(url='http://localhost:2080/', user='Admin', password='zabbix')
df = pd.read_csv("audyt.csv")
host = 'service-001'
for i in range(len(df)):
 zabbix_key = df['zabbix_key'].values[i]
 if zabbix_key and (zabbix_key == 'yes' or zabbix_key == 'no'):
 df['zabbix_lastvalue'].values[i] = zabbix_key
 else:
 if zabbix_key:
 zabbix_values = get_key_values(zapi, host, zabbix_key)
 df['zabbix_lastvalue'].values[i] = zabbix_values.get('lastvalue')
 print(zabbix_values.get('itemid'))
df.to_csv('out.csv', encoding='utf-8', index=False)
```

Table 4. A set of criteria used in the automatic risk analysis process

#system (monitoring service) net.udp.listen[1194] net.tcp.service[ldap] net.tcp.service[ssh] agent.ping proc.num[clamd] proc.num[fail2ban-server] systemd.unit.is-active[auditd.service] systemd.unit.is-active[firewalld.service] systemd.unit.is-active[rsyslogd.service] systemd.unit.is-active[storage-management.service] systemd.unit.is-active[cryptsetup.service] systemd.unit.is-active[ac.service]	#Organization (trapper) anomaly.detection.procedures service.procedures storage.procedures backups.procedures incident.response.procedures administrative.law.and.politics.procedures recovery.procedures malware.procedures equipment.maintenance.contract.procedures insurance.procedures
#integration (trapper) application.status.aide application.status.ac application.status.backup application.status.storage-management application.status.auditd application.status.rsnapshot	

Table 5. Reaction time to the status service changes (on/off service)

The actual action performed (on/off -services)					SIEM value reading			
	Service	Data	Timestamp	Stop/Start	0 – Stop 1 – Start	Data	Timestamp	Reaction time
Serv-001	OpenLDAP:	07/28/18	01:01:00	Stop	0	2018-07-28	01:01:17	00:00:17
	OpenLDA:	07/28/18	01:02:45	Start	1	2018-07-28	01:03:17	00:00:32
	OpenVPN:	07/28/18	01:05:47	Stop	0	2018-07-28	01:06:22	00:00:35
	OpenVPN:	07/28/18	01:06:30	Start	1	2018-07-28	01:07:52	00:01:22
	ClamAV:	07/28/18	01:07:21	Stop	0	2018-07-28	01:08:20	00:00:59
	ClamAV:	07/28/18	01:09:14	Start	1	2018-07-28	01:09:50	00:00:36
	firewalld:	07/28/18	01:10:23	Stop	0	2018-07-28	01:10:43	00:00:20
	firewalld:	07/28/18	01:12:02	Start	1	2018-07-28	01:12:13	00:00:11

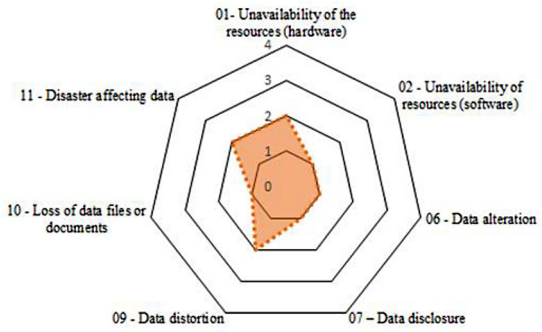

Figure 13. Risk assessment weight with implemented and including 5 started services

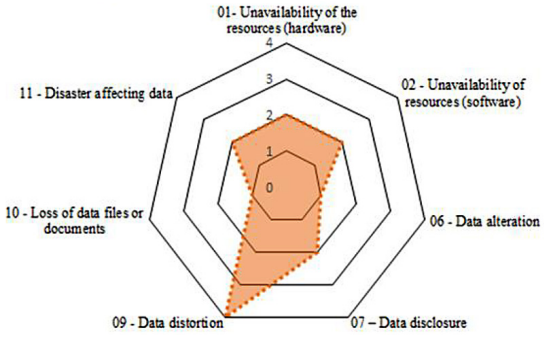

Figure 14. Risk assessment weight with implemented procedures and 5 stopped services

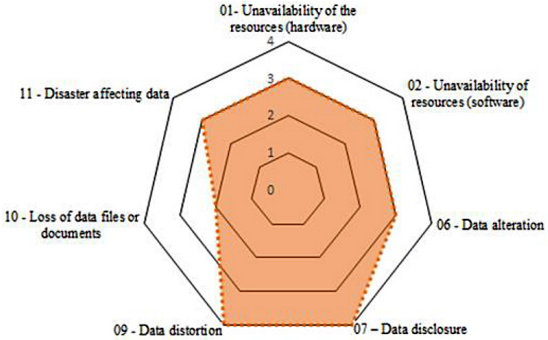

Figure 15. Risk assessment weight with 5 started services and without procedures

Table 6. Reaction time to the status service changes (on/off service) in dispersed architecture

SVR 01								
Monitor reading in real time				The real time system event				
0 - stop 1 - start	Data	Time	Ns	Service	data	Time	start/ stop	Time difference
0	23.10.2018	00:01:17	0.376786094	slapd:	10/23/18	00:01:01	stop	00:00:16
1	23.10.2018	00:02:17	0.753597012	slapd:	10/23/18	00:02:03	start	00:00:14
0	23.10.2018	00:03:22	0.378834303	openvpn@server:	10/23/18	00:03:05	stop	00:00:17
1	23.10.2018	00:04:22	0.504978168	openvpn@server:	10/23/18	00:04:06	start	00:00:16
0	23.10.2018	00:05:20	0.902057511	clamd:	10/23/18	00:05:07	stop	00:00:13
1	23.10.2018	00:06:20	0.335244672	clamd:	10/23/18	00:06:07	start	00:00:13
0	23.10.2018	00:07:13	0.705973697	firewalld:	10/23/18	00:07:08	stop	00:00:05
1	23.10.2018	00:08:13	0.132257813	firewalld:	10/23/18	00:08:08	start	00:00:05
0	23.10.2018	00:09:15	0.532597249	rsyslog:	10/23/18	00:09:08	stop	00:00:07
1	23.10.2018	00:10:15	0.929308531	rsyslog:	10/23/18	00:10:08	start	00:00:07
SVR 02								
Monitor reading in real time				The real time system event				
0 – stop 1 - start	Data	Time	Ns	Service	data	Time	start/ stop	Time difference
0	23.10.2018	00:01:28	0.471125	slapd:	10/23/18	00:01:01	stop	00:00:27
1	23.10.2018	00:02:28	0.887063048	slapd:	10/23/18	00:02:03	start	00:00:25
0	23.10.2018	00:03:26	0.007033749	openvpn@server:	10/23/18	00:03:05	stop	00:00:21
1	23.10.2018	00:04:26	0.52978571	openvpn@server:	10/23/18	00:04:06	start	00:00:20
0	23.10.2018	00:05:27	0.969126884	clamd:	10/23/18	00:05:08	stop	00:00:19
1	23.10.2018	00:06:27	0.424735015	clamd:	10/23/18	00:06:08	start	00:00:19
0	23.10.2018	00:07:14	0.7300522	firewalld:	10/23/18	00:07:08	stop	00:00:06
1	23.10.2018	00:08:14	0.13149157	firewalld:	10/23/18	00:08:09	start	00:00:05
0	23.10.2018	00:09:15	0.531309126	rsyslog:	10/23/18	00:09:09	stop	00:00:06
1	23.10.2018	00:10:15	0.930057567	rsyslog:	10/23/18	00:10:09	start	00:00:06
SVR 03								
Monitor reading in real time				The real time system event				
0 – stop 1 - start	Data	Time	Ns	Service	Data	Time	start/ stop	Time difference
0	23.10.2018	00:01:24	0.451179133	slapd:	10/23/18	00:01:01	stop	00:00:23
1	23.10.2018	00:02:24	0.847699727	slapd:	10/23/18	00:02:03	start	00:00:21
0	23.10.2018	00:03:22	0.379944833	openvpn@server:	10/23/18	00:03:05	stop	00:00:17
1	23.10.2018	00:04:22	0.506155911	openvpn@server:	10/23/18	00:04:05	start	00:00:17
0	23.10.2018	00:05:23	0.948696302	clamd:	10/23/18	00:05:07	stop	00:00:16
1	23.10.2018	00:06:23	0.40846815	clamd:	10/23/18	00:06:07	start	00:00:16
0	23.10.2018	00:07:20	0.765989308	firewalld:	10/23/18	00:07:08	stop	00:00:12
1	23.10.2018	00:08:20	0.171053139	firewalld:	10/23/18	00:08:08	start	00:00:12
0	23.10.2018	00:09:21	0.578181011	rsyslog:	10/23/18	00:09:08	stop	00:00:13
1	23.10.2018	00:10:21	0.965743759	rsyslog:	10/23/18	00:10:08	start	00:00:13
SVR 04								
Monitor reading in real time				The real time system event				
0 – stop 1 - start	Data	Time	Ns	Service	Data	Time	start/ stop	Time difference
0	23.10.2018	00:01:02	0.094734848	slapd:	10/23/18	00:01:01	stop	00:00:01
1	23.10.2018	00:02:32	0.886024345	slapd:	10/23/18	00:02:03	start	00:00:29
0	23.10.2018	00:03:30	0.056353826	openvpn@server:	10/23/18	00:03:05	stop	00:00:25
1	23.10.2018	00:04:30	0.57513603	openvpn@server:	10/23/18	00:04:05	start	00:00:25
0	23.10.2018	00:05:31	0.993219933	clamd:	10/23/18	00:05:07	stop	00:00:24
1	23.10.2018	00:06:31	0.430883448	clamd:	10/23/18	00:06:07	start	00:00:24
0	23.10.2018	00:07:08	0.691340145	firewalld:	10/23/18	00:07:08	stop	00:00:00
1	23.10.2018	00:08:38	0.289562079	firewalld:	10/23/18	00:08:08	start	00:00:04
0	23.10.2018	00:09:09	0.488830697	rsyslog:	10/23/18	00:09:08	stop	00:00:01
1	23.10.2018	00:10:09	0.887307452	rsyslog:	10/23/18	00:10:08	start	00:00:01

The second rosette (Fig. 14) represents the risk level, which is critical for one scenario when the services are stopped. The third rosette (Fig. 15) represents the level of risk for most scenarios, when all procedures are not implemented and all services are started. Example of the shown architecture (Fig. 11) and the obtained results (Table 5 and Table 6 and Figs. (13-15)), which are only a part of the system information (12 risk scenarios and 5 services) tells us that the idea of speeding up risk analysis process is right. When configuring such working agents, the FoMRA1 method could serve as an IS security monitoring method, providing information in a very short time about all risks for the IS security. The obtained results both, qualitatively and quantitatively are identical as in the case of FoMRA1 version, without automatic downloading of data to the questionnaire. In this way, the response time to the emerging threat is much shorter (the average time of collecting answers to the questionnaire entered in manual mode takes several hours).

CONCLUSIONS

The proposed modifications of the formal risk analysis method and assessment clearly show that it is possible to implement new features to FoMRA, which are important from the auditor's point of view, and allow automation of the risk analysis and assessment process. This solution is unique today, as none of the current methods together with the supporting tools are characterized by automation of the processes, limiting themselves only to manual control.

As a result of modification and abstraction by resources and security controls, the calculation time was significantly shortened. Introduced modifications and abstraction are a good starting point for monitoring the security status of the IS (shortening the calculation time by one second is very important for the security of the IS). Additionally, by using properly configured agents, the modified FoMRA1 gives the auditors information about any security threats to the organization's information system in quasi-real time.

A further study will focus on comparing as many methods as possible for speed of risk assessment and estimation. This will include monitoring a larger number of risk scenarios and most importantly, the automated risk treatment using deep agent learning.

REFERENCES

1. Jones A., Ashenden D. Risk Management for Computer Security: Protecting Your Network & Information assets. Elsevier, Oxford, UK, 2005. https://www.amazon.com/Risk-Management-Computer-Security-Information/dp/0750677953.
2. Bandyopadhyay K., Mykytyn P., Mykytyn K. A framework for integrated risk management in information technology. Management Decision 1999, 37(5), 437–445. https://doi.org/ 10.1108/00251749910274216.
3. Spears J. L., Barki H. User participation in information systems security risk management. MIS Quarterly 2010, 34(3), 503-522. https://doi.org/10.2307/25750689.
4. Lathrop J., Ezell B. A systems approach to risk analysis validation for risk management. Safety Science 2017, 99, 187–195. https://doi.org/10.1016/j.ssci.2017.04.006.
5. Sepczuk M, Kotulski Z. A new risk-based authentication management model oriented on user's experience. Computers & Security 2018, 73, 17-33. https://doi.org/10.1016/j.cose.2017.10.002.
6. Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization, Genève, Suisse. https://www.iso.org/standard/69379.html. (Accessed: 25.01.2023).
7. Information technology - Security techniques - Code of practice for information security controls. International Organization for Standardization, Genève, Suisse. https://www.iso.org/standard/69379.html. (Accessed: 27.01.2023).
8. Information technology - Security techniques - Information security risk management. International Organization for Standardization, Genève, Suisse. https://www.iso.org/standard/73906.html. (Accessed: 28.01.2023).
9. Risk management – Guidelines. International Organization for Standardization, Genève, Suisse. https://www.iso.org/standard/65694.html. (Accessed: 28.01.2023).
10. Stoneburner G., Goguen A., Feringa A. NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology, Gaithersburg, US. 2002. https://doi.org/10.6028/nist.sp.
11. Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-2: IT-Grundschutz Methodology, Bonn, Deutsche 2008.
12. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile.

13. A Risk Management Standard. Federation of European Risk Management in Dynamic Open Systems, London, UK 2003. https://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-english-version.pdf.
14. CCTA Risk Analysis and Management Method. Central Computing and Telecommunications Agency, UK 1987. https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html.
15. COBRA: Consultative, Objective and Bi-functional Risk Analysis. Disaster Recovery Planning Group, UK 1991.
16. Méthodologie d'Analyse des Risques Informatique et d'Optimation par Niveau. France. 1998. https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_marion.html.
17. Expression des Besoins et Identification des Objectifs de Securite, France 2004. https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_ebios.html.
18. MEthode Harmonisée d'Analyse du Risque Informatique. CLUSIF, France 2022. https://clusif.fr/services/management-des-risques/les-versions-de-mehari/mehari-standard/.
19. Alberts C. J., Dorofee A. J. OCTAVE Method Implementation Guide Version 2.0. Carnegie Mellon University, Pittsburgh, Pennsylvania, US, 2001.
20. https://insights.sei.cmu.edu/documents/18/2001_012_001_51572.pdf.
21. MSAT: Microsoft Security Assessment Tool. US, 2008. http://technet. Microsoft.com/en-us/security/cc18512.aspx.
22. Humphreys E. Information security management standards: Compliance, governance and risk management. Information Security Technical Rep. 2008, 13(4), 247–255. https://doi.org/10.1016/j.istr.2008.10.010.
23. Parker D.B. Computer Security Management. Reston Publishing Company Inc., Reston VA. US, 1981. https://books.google.pl/books/about/Computer_ Security_Management.html?id=a1MkAQAAIAAJ&redir_esc=y.
24. Baskerville R. Information Systems Security Design Methods: Implications for Information Systems Development. Computing Surveys, 1994, 25(4).
25. Hartawan F., Suroso J.S. Information Technology Services Evaluation Based ITIL V3 2011 and COBIT 5 in Center for Data and Information. In: Nguyen N., Tojo S., Nguyen L., Trawiński B. (eds) Intelligent Information and Database Systems 2017. https://doi.org/10.1007/978-3-319-54430-4_5.
26. Sardjono W., Cholik M.I. Information Systems Risk Analysis Using Octave Allegro Method Based at Deutsche Bank. International Conference on Information Management and Technology 2018. https://doi.org/10.1109/ICIMTech.2018.8528108.
27. Suroso J.S., Fakhrozi M.A. Assessment of Information System Risk Management with Octave Allegro at Education Institution. Procedia Computer Science 2018, 135, 202–213. https://doi.org/10.1016/j.procs.2018.08.167.
28. Awad A.I., Shokry M., Khalaf A.A.M., Abd-Ellah M.K. Assessment of potential security risks in advanced metering infrastructure using the OCTAVE Allegro approach, Computers and Electrical Engineering 2023, 108. https://research.uaeu.ac.ae/en/publications/assessment-of-potential-security-risks-in-advanced-metering-infra.
29. Shamala P., Ahmad R., Zolait A., Sedek M. Integrating information quality dimensions into information security risk management (ISRM). Journal of Information Security and Applications 2017. https://doi.org/10.1016/j.jisa.2017.07.004.
30. Baraforta B., Mesquidab A.L., Masb A. Integrating risk management in IT settings from ISO standards and management systems perspectives. Computer Standards & Interfaces 2017, 54, 176-185. https://doi.org/10.1016/j.csi.2016.11.010.
31. Aven T. How the integration of System 1-System 2 thinking and recent risk perspectives can improve risk assessment and management. Reliability Engineering and System Safety 2018, 180, 237-244. https://doi.org/10.1016/j.ress.2018.07.031.
32. Tai V.W., Lai Y-H., Yang T-H. The role of the board and the audit committee in corporate risk management. North American Journal of Economics and Finance 2018. https://doi.org/10.1016/j.najef.2018.11.008.
33. Irsheid A., Murad A., AlNajdawi M., Qusef A., Information security risk management models for cloud hosted systems: A comparative study, Procedia Computer Science 2022, 204, 205-217. https://doi.org/10.1016/j.procs.2022.08.025.
34. Pejaś J., El Fray I., Ruciński A. Authentication protocol for software and hardware components in distributed electronic signature creation system. Electrical Review 2012, 88(10b), 192-197. http://pe.org.pl/articles/2012/10b/51.pdf.
35. Białas A., Lisek K. Integrated, Business-Oriented, Two-Stage Risk Analysis. Proceedings of the International Multiconference on Computer Science and Information Technology 2007, 617–628. https://annals-csis.org/proceedings/2007/pliks/ii_imcsit.pdf.
36. El Fray I. About Some Application of Risk Analysis and Evaluation. Artificial Intelligence and Security in Computing Systems, The Springer International Series in Engineering and Computer Science 2003, 752, 283-292. https://link.springer.com/chapter/10.1007/978-1-4419-9226-0_27.

37. El Fray I., Kurkowski M., Pejaś J., Maćków W. A New mathematical model for analytical risk assessment and prediction In IT systems. Control and Cybernetics 2012, 41(1), 241-268. https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-article-BATC-0009-0045?q=bwmeta1.element.baztech-volume-0324-8569-control_and_cybernetics-2012-vol__41_no_1;11&qt=CHILDREN-STATELESS.
38. El Fray I. A comparative study of risk assessment methods, MEHARI & CRAMM with a new formal model of risk assessment (FoMRA) in information systems. CISIM 2012, LNCS 7564, 428–442. https://link.springer.com/content/pdf/10.1007/978-3-642-33260-9_37.pdf.
39. Ghazouani M., Faris S., Medromi H., Sayouti A. Information Security Risk Assessment — A Practical Approach with a Mathematical Formulation of Risk. International Journal of Computer Applications 2014, 103 (8). https://doi.org/10.5120/18097-9155.
40. European Network and information Security Agency-Total Information Security Management 2008. http://www.enisa.europa.eu/media/press-releases/prs/201cinside-the-matrix-privacy-data-protection-challenges201d/ methods_tools.
41. http//www.zabbix.com.
42. Hernantes J., Gallardo G. and Serrano N. IT Infrastructure-Monitoring Tools. IEEE Software Technology 2015, 88-93. https://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-c7aafda9-c004-4f5f-8eec-1379d471ae94.
43. Petruti C.-M., Ivanciu I.-A., Puiu B.-A., Dobrota V. Automatic Management Solution in Cloud Using NtopNG and Zabbix. IEEE 2018. https://doi.org/10.1109/ROEDUNET.2018.8514142.
44. Taherizadeh S., Jones A.C., Taylor I., Zhao Z., Stankovski V. Monitoring self-adaptive applications within edge computing frameworks: A state-of-the-art review. The Journal of Systems and Software 2018, 136, 19–38. https://doi.org/10.1016/j.jss.2017.10.033.
45. https://www.zabbix.com/zabbix_agent.
46. http://aide.sourceforge.net/.
47. https://www.zabbix.com/documentation/3.4/manual/api.
48. https://www.zabbix.com/documentation/3.4/manual/concepts/sender.
49. Gopal R.D. and Sanders G.L. Preventive and Deterrent Controls. Journal of Management Information Systems for Software Piracy 1997, 13(4), 29-47. https://www.jmis-web.org/keywords/998.
50. https://clusif.fr/publications/mehari-2010 -overview.
51. Pearlson K.E., Saunders C.S., Dennis F. Galletta: Managing and Using Information Systems: A Strategic Approach, Wiley 2024.
52. https://www.wiley.com/en-us/export Product/pdf/9781119688891.