MEASURING AND INDICATING THE LEVEL OF INFORMATION SECURITY – AN ANALYSIS OF CURRENT APPROACHES

Michael Matthias NAUMANN
The Bucharest University of Economic Studies, 010374, Romania
matthias.naumann@ixactly.com
Stelian Mircea OLARU
The Bucharest University of Economic Studies, 010374, Romania
olaru_stelian@yahoo.com
Georg Sven LAMPE
The Bucharest University of Economic Studies, 010374, Romania
lampe@compliance-docs-group.com
Fabian PITZ
The Bucharest University of Economic Studies, 010374, Romania
fpitz22@gmail.com

Abstract
In times of increasing digitalization of processes in companies the topic of information security has become relevant for every industry. For this, a standardization of information security with normative standards such as ISO/IEC 27001:2022 has been established to define requirements and to assess at regular intervals the conformity of the management systems. However, practice shows that companies are fulfilling the requirements only at a minimum level and don't have a real overview of their security level and the impact of existing risks. This paper evaluates how decision makers in companies currently interpret their security level using metrics. Regarding this, the relationship with effectiveness and conformity of their information security measures are shown and analyzed. Furthermore, in this paper a selection of the most common used practices and frameworks for measuring and certifying information security systems has been analyzed. The results of this research show that there is a need for on overall security perspective and include a proposal on how a structured approach should be defined.

Key words: *information security risks;key performance indicators;maturity level;metrics;security management systems.*

JEL Classification: *D81; L15; L21; M15; M42; O33*

I. INTRODUCTION

Research has shown that information security management systems have a direct positive impact on companies' operational performance (Hsu, Wang et al, 2016). In frequent situations however, at the level of the responsible persons there is little overview of effectiveness, efficiency and this is also the case regarding the maturity of management systems.

In this case, a risk management system with implemented measures to handle identified security risks needs to be in place. To monitor these risks and the impact of previously defined corresponding measures, the status of the whole information security management system should be managed using appropriate metrics or key performance indicators (KPI). Nevertheless, research shows that KPIs are usually providing "only partial information to decision makers" (Maté, Trujillo et al, 2017) which leads to the need to accurately determine the right measuring objectives.

Another important challenge is that in addition to "You can't manage what you can't measure" (Wills, 2016) it is also necessary to select the right measurement and the right visualization for the data obtained, for example via a dashboard which "has the capability to show trends and changes over time" (Crémilleux, 2019).

The current issues focus on the fact that, for the most part, no suitable metrics or assessed maturity levels of the overall system are in use within the companies. Furthermore, depending on the size of the organization and its technical systems, monitoring is frequently reduced to being carried out only at the level of technical metrics, e.g., within IT. However, when periodically assessing the compliance with plans and with self-imposed or certifiable standards such as ISO/IEC 27001:2022, metrics are only sporadically used to measure effectiveness or performance.

Decision makers need to see what is the maturity level for the information security management system

and also what resources are required to close gaps resulting from identified risks.

This paper will show the current approaches used by companies and that are defined in standards. The assumption is that the current methodologies and available frameworks and not entirely suitable for companies and need further improvement and research.

II.REVIEW OF THE SCIENTIFIC LITERATURE

Some researchers have already focused on the measurement of information security and processes maturity in companies. Additionally, there are research studies that have examined the background and position in the company of the decision-makers regarding information security awareness.

Furthermore, past research defined the measurement of information security level as having to cover three main directions: Security Management, Human Behavior and Practical Frameworks (Diesch, Pfaffet al, 2018).This means that besides the mapping of information security to the companies' strategic objectives in line with the requirements defined by frameworks or standards, also the importance of individual's behavior in relation with the above must be recognized.

Several research studies have found that appropriate measurement and assessment of maturity, performance, and requirements fulfillment can significantly increase both information security awareness and the engagement of non-technical decision makers in organizations (Rapina, Carolina et al, 2022). To monitor and measure systems, responsible persons also must be able to analyze systems having the right monitoring in place. This is achieved both by decision makers (Diesch, Pfaff et al, 2020) and analysts observing the systems behaviors in operations (Agyepong, Cherdantseva et al, 2023). Besides this, the top management must identify and approve the treatment of cyber security inside risk management process and get security risks ideally be mapped to financial impact and security costs (Olifer, Goranin et al, 2017).

The relation of risk management and performance of organizations leads to a need to consider measuring and monitoring not only as a technical topic (Zaripov, Murakaev et al, 2021) but rather as a "means that the cyber security risks are collected and analyzed at the system level in order to align them with the strategic aims of the company." (Lampe, Olaru et al, 2022).

As in all management systems, information security is measured by means of the continuous improvement approach (Cunha, Dinis-Carvalho et al, 2023) and thus may also lead to business process optimizations (Wangen and Snekkenes, 2014).

Information security requires an efficient definition and collection of KPIs by using measurement models (Hoffmann, Napiórkowski et al, 2020) and further an assessment of the conformity of process to its requirements measured with the maturity level (Proença and Borbinha, 2016).The importance of measuring information security level via suitable monitoring means in order to improve the overview regarding technical, strategic, and financial risks and indicators is also reflected in the literature.

Based on this, an overarching approach to the assessment of the security level needs to be undertaken and analyzed in detail, including metrics and maturity levels.

III.RESEARCH METHODOLOGY

The intention of this paper is to show the current state of the use of metrics, indicators, and maturity assessment models in the context of information security management systems and to propose an improved approach. To achieve this objective, it is necessary to determine the current level of usage and implementation in companies regarding key performance indicators for information security and to analyze possible correlations.

A qualitative approach was used to examine the implementation of key performance indicators in a sample of 20 selected companies that had undergone certification audits in the area of information security.

This study shows the correlations between the use of key performance indicators and the effects on information security. Based on this investigation, a literature analysis will then show which standardized metrics are available for measuring and monitoring management systems related to information security.

Finally, a structured high-level approach to the use of metrics and maturity models is proposed to improve the overview on information security and the organizations' related overall maturity level

IV. RESULTS AND DISCUSSION

It needs to be discussed whether a structured approach that defines a metrics definition and a collection of the most important requirements of the companies, as well as a holistic visualization of information security, will improve the overview for decision makers in companies.

1) Interviews to analyze the AS IS status

In order to gain an overview of the current use of metrics in the context of information security, 20 selected companies were surveyed, operating in different industries.

Participating companies were asked about the use of metrics as well as about conclusions about non-conformities (NCs) in audits due to missing measurements of their management systems.

It was also examined whether there is any assistance in selecting suitable key figures and accomplishing maturity level evaluations, which also offers an objective overview of the entire system.

The information security officers of the companies were interviewed about the number of metrics collected and the frequency of measurements (Table 1).

Table 1. Evaluation of selected companies

Interviewed Company	Industrial Sector	Number of Metrics	Measurement Frequency	Standard For Metrics	Enhanced Reporting Approach	NCs during Audit reg. Monitoring
Company 1	Prof. Services	0	annual	o	n/a	x
Company 2	Power & Utilities	16	monthly	o	o	o
Company 3	Engineering	18	annual	o	o	o
Company 4	Financial Services	50	monthly	x	x	o
Company 5	Media	5	annual	o	o	x
Company 6	IT	6	annual	o	o	x
Company 7	IT	4	annual	o	o	o
Company 8	Power & Utilities	3	annual	o	o	x
Company 9	Financials	18	annual	o	o	x
Company 10	Engineering	6	monthly	o	x	o
Company 11	Engineering	30	monthly	o	x	o
Company 12	Automotive	0	annual	o	n/a	x
Company 13	Automotive	10	quarterly	o	o	o
Company 14	Power & Utilities	5	annual	o	o	o
Company 15	Power & Utilities	10	annual	o	o	o
Company 16	Power & Utilities	5	annual	o	o	x
Company 17	IT	16	annual	x	o	o
Company 18	IT	22	annual	o	x	o
Company 19	Engineering	4	annual	o	o	x
Company 20	Automotive	15	annual	o	x	o
Legend: o – not present, x – present, n/a - not applicable						

Source: Authors, 2023

Furthermore, it was asked which procedures and methods of evaluation are used to determine and visualize the metrics relevant for the company.

In addition to determining the current status in the selected companies, possible correlations between the frequency and complexity of monitoring by means of key figures and the subsequent evaluation with regard to conformity to the standards are also to be determined.

For this purpose, the non-conformities that arose due to the lack of monitoring or the lack of an overview of the overall system by means of metrics in certification audits were examined.

Only directly assignable nonconformities were counted among these nonconformities. The audited standards at the time of data collection were ISO/IEC 27001:2017, German IT Security Catalogue and VDA-ISA 5.1. The following correlations have been evaluated in detail:

a) Number of measured metrics

The number of key figures collected also reflects the maturity and conformity of the management system in the audited companies (Table 2). The more metrics respondents use and measure, the better the overview they have on the overall system and thus the fewer non-conformities are identified during audits. Participants who state that they have not currently collected any key figures, also fail to comply with the audited information security standard.

Table 2. Number of measured Metrics

Number of Metrics	Distribution	Occurrence of Nonconformities
0	10%	2 (100%)
1..5	35%	4 (67%)
6..15	20%	1 (20%)
more than 15	35%	1 (14%)

Source: Authors, 2023

b) Frequency of measurement

The research shows that the majority (75%) of the companies surveyed only conduct an annual review of key metrics (Table 3). Thus, only a quarter of respondents conduct a more frequent, monthly or quarterly, collection and analysis of metrics. This overall reduced frequency of measurement if likely a consequence of the effort associated with periodical data gathering, measurement and analysis, often leading to only annual monitoring activities covering a small range of key metrics

Table 3. Frequency of Measurement

Frequency	Distribution	Occurrence of Nonconformities
Monthly	20%	0 (0%)
Quarterly	5%	0 (0%)
Annual	75%	8 (53%)

Source: Authors, 2023

However, it can also be seen that a reduced frequency of measurement also increases the risk of audit nonconformities, given that all such nonconformities among the research participants were recorded by companies with only annual surveys, while those participants that engage in more frequent measurement processes, have not recorded any nonconformities.

c) Reporting of measures

The research also shows a strong correlation between the method used for reporting the KPIs and the resulting related organizational performance: participants with only manual recording and reporting of their KPIs, e.g., with Excel, recorded a deviation from the requirements of the ISO 27001 standard in 46% of the cases in the selected study, while those that use specific tools to support the reporting process did not record any nonconformities (Table 4).

Table 4. Reporting of Measures

Kind of Metrics Reporting	Distribution	Occurrence of Nonconformities
None	10%	2 (100%)
Manually	65%	6 (46%)
Tool Support	25%	0 (0%)

Source: Authors, 2023

To conclude with, 40% of the participants surveyed completed their audit with non-conformities related to lack of monitoring and measurement of their ISMS.

The questions that are further addressed by our research are:

- How can the quality of metrics and their reporting be improved?
- Can a structured approach and framework support in getting an efficient overview and more security?

2) Standard Approaches for Measuring and Monitoring Information Security

Key metrics are used to determine the degree to which predefined requirements have been met, allowing for a snapshot quantitative assessment of a widely-complex process.

Within ISO/IEC 27001:2022, key performance indicators are used to track the achievement of information security objectives and thus the objectives of confidentiality, availability, and integrity of information. This is achieved with the involvement of management in periodical management reviews that include reports on analysis of actual KPI results versus objectives and imply decisions on corrective measures in order to support the achievement of objectives.

To obtain an overall view of the ISMS, it is also necessary to determine the maturity of the individual processes measured.

Process maturity provides information on whether all requirements are generally defined, implemented, measured, and improved. Another aspect concerns having a systematic approach to defining measures to deal with risks or issues identified via various findings, e.g., from audits: if such measures are not fully implemented or measured, their associated risks are not adequately mitigated thus exposing the organization to financial uncertainties and expenses.

In such situations, key figures can measure the degree of implementation and target achievement of the measures. For this purpose, the effectiveness and efficiency of measures needs to be measured.

Adjustments based on the results of these measurements are made in a continuous improvement process (CIP). The employees responsible for the processes collect the key metrics, which must have been coordinated with the company objectives.

Two complementary views are relevant for key figures definition:

- *Strategic figures*. The company's management is responsible for strategic key figures. These key performance indicators are derived from the corporate vision and strategic goals, e.g., compliance and sales.
- *Operational figures*. The key performance indicators are derived from the strategic goals, e.g., the availability of IT systems, and operational management is responsible for them.

Furthermore, there are various tools that enable the recording of events, logs, and activities, such as SIEM, an IDS or IPS to identify malicious activities.

With these technical metrics, measurement of the availability of processes and systems is possible, but key performance indicators are still required for monitoring the achievement of corporate goals and measuring performance and efficiency within information security.

A distinction is made between metrics and key performance indicators (KPIs) considering the form in which target values are defined and an indication of the development towards achieving them

Recommendations for the definition of such indicators are proposed, for example, within ISO/IEC 27004:2016. Furthermore, an approach for determining these indicators relies on using software project management. In almost all information security standards, the review and measurement of requirements is necessary.

For implementation in information security, different maturity models currently exist in practice for companies, depending on the industry, which specify in greater or lesser detail the current security level according to certain controls.

These maturity models are a systematic approach for evaluating the implementation quality of the individual specifications. Direct measurement with key figures is required to monitor the achievement of individual management system objectives.

The following section examines a selection of widely used standards for information security regarding their requirements for the collection and measurement of key performance indicators and a maturity level:

- ISO/IEC 27001:2022 is the standard for information security management systems requirements, ISO/IEC 27004:2016 defines the related standard for monitoring, measurement, analysis, and evaluation.
- VDA-ISA – Information Security Industry Standard of the German Association of the Automotive Industry assessed with TISAX - Trusted Information Security Assessment Exchange.
- COBIT - Control Objectives for Information and Related Technology, ISACA.

(1) ISO/IEC 27001:2022 - Statement of Applicability (SoA)

ISO/IEC 27001:2022 requires a list of all controls from Annex A of the standard with details of the implementation status. In Chapter 6.1.3, a so-called statement of applicability with justifications for inclusion and exclusion is required as part of the risk analysis (ISO, 2022).

In practice, however, there is no mandatory concrete requirement for an overall assessment of the maturity of the ISMS.

In ISO/IEC 27004:2016, as Part of ISO/IEC 27000 Standard Family, entitled "Information security management - Monitoring, measurement, analysis and evaluation", as an informative standard of the ISO/IEC 27000 family, the benefits "increased accountability, improved information security performance and ISMS processes and evidence of meeting requirements, support decision-making" (ISO, 2016) are mentioned.

With a definition of 35 example KPIs for the single controls of ISO/IEC 27001:2022, ISO/IEC 27004:2016 defines the following categories:

- Performance metrics to measure planned results "such as head counts, milestone accomplishments, or the degree to which information security controls have been implemented"(ISO, 2016).
- Metrics to measure effectiveness, for achieving corporate information security objectives.

In this context, ISO/IEC 27004:2016 emphasizes the definition of key performance indicators by adhering to the following questions, using a defined procedure according to ISO/IEC/IEEE 15939:2017 (ISO, 2017):

1. What must be monitored and measured?
2. Definition of methods for monitoring, measurement, analysis, and evaluation
3. When the monitoring and measuring shall be performed?
4. Who shall monitor and measure?
5. When the results from monitoring and measurement shall be analyzed and evaluated?
6. Who shall analyze and evaluate these results?

After determining these points, the following attributes are defined for the collection of KPIs according to ISO/IEC 27004:2016 (ISO, 2016):

- ID, Information need, Measure, Formula/scoring, Target, Implementation evidence, Frequency, Responsible parties, Data source, Reporting format.

Together with the specification of example KPIs for almost all requirements of the main standard and a specification for the determination of metrics, ISO/IEC 2004:2016 is suitable as a reference for companies that want to be certified according to ISO/IEC 27001:2022. However, there is no requirement that the collection of metrics according to this standard is mandatory for certification. Process maturity is not considered in ISO/IEC 27001:2022, but is required, for example, in standards like ISO 9001:2015.

(2) COBIT

Another framework for information security is COBIT from ISACA, which primarily supports the control of IT management. Within COBIT, the topic of metrics is defined with the differentiation into the following categories: enterprise goal metrics, IT goal metrics, process goal metrics.

Regarding this, there are recommendations for the selection of metrics (Bakshi, 2016):

- “Normalize metrics to a common attribute parameter.”
- “Is time defined as per year occurrence, transactions per second/minute/hour, average?”
- “Understand the characteristics of a good metric.”
- “Avoid comparisons against other similar enterprises.”
- “Minimize cost-related comparisons.”
- “Focus on work activities and outcomes.”
- “Keep metrics to a manageable quantity.”

The difference from ISO/IEC 27004:2016 is that COBIT considers all IT processes.

Furthermore, COBIT makes it possible to use a maturity model to describe all activities. For this purpose, the maturity level is determined for 231 practices, 40 objectives and 5 domains (ISACA, 2019).

Using Business Score Cards (BSC), it is also possible to consider performance and strategic alignment of objectives - not only from a technical perspective. COBIT 2019 defines 4 IT BSCs here with prioritized goals and linked KPIs.

COBIT is not a standard for the certification of information security systems but a best practice standard for IT governance and compliance in large enterprises.

(3) VDA-ISA/TISAX

VDA-ISA is an industry standard for auditing information security in the automotive industry, in which both maturity levels and metrics are assessed. The automotive supplier industry is tested for conformity to information security requirements of the VDA-ISA questionnaire using a so-called Trusted Information Security Assessment (TISAX) assessment.

In the current standard VDA-ISA 5.1 (VDA, 2022) there are a total of 39 examples of KPIs including criteria, which, however, are not mandatory to implement. Within the VDA-ISA controls, there are only rough guidelines for measuring and monitoring via metrics. However, there is a greater focus here on the maturity level for measuring the conformity of the processes. Based on CMMI maturity levels, a definition of the maturity level for all individual requirements is collected.

Due to the defined target maturity level of level 3 in VDA-ISA, which requires a fully implemented process including all requirements, it is not mandatory to measure the performance and quality of the process using metrics. This is only done from Maturity Level 4.

In general, the approach used makes it possible to take an immediate look at the implementation of all

requirements of the individual processes, but there are no concrete specifications for the exact classification and interpretation of concrete facts and the associated maturity level.

3) Summary

The selected standards for information security only partially provide guidelines for the collection of metrics and do not consider the overall picture of a management system, including process maturity and the company's view of strategic goals and costs. COBIT offers many more opportunities from an IT management perspective, but this framework is not a certification standard, so most companies focus on meeting the requirements of ISO/IEC 27001:2022 and the associated external impact with achieved certificates. This means that the problem of a holistic overview of the level of information security is still relevant (Table 5).

Table 5. Reporting of Measures

Standard	Metrics Criteria	Metrics Examples	Maturity Level	Map Company Objectives Metrics
ISO/IEC 27001:2022	x	x (ISO27004)	o	-
COBIT	x	x	CMMI based	BSCs
VDA-ISA/TISAX	x	x	CMMI based	o
Legend: o – not present, x – present				

Source: Authors, 2023

As a result of the evaluation of the current status and the already existing specifications in standards, the following topics are proposed as steps to a holistic monitoring and measurement of performance, quality and process maturity as well as an incipient consideration of strategic goals and strategic factors:

- Identification of critical business processes, assets with subsequent risk analysis,
- Definition and collection of metrics using standards and examples e.g., ISO/IEC 27004:2016 for as many defined processes and requirements as possible,
- Determination of a maturity model to assess maturity levels of the overall processes,
- Mapping of security costs such as e.g., needed budget, financial risks, savings to the metrics,
- Survey of the metrics with at least quarterly frequency,
- Visualization of the metrics in management meetings, implementation of a security score,
- Adjustment of criteria and measurements in the context of continuous improvement.

A more detailed approach should be part of further research.

V. CONCLUSION

Currently, there are frameworks and standards which set-up processes for a detailed KPI monitoring as well as maturity assessment.

As the leading standard for information security, ISO/IEC 27001:2022 does not currently take a holistic view of the processes and maturity assessment on information security. Furthermore, there are no mandatory requirements for determining metrics, despite the optional ISO/IEC 27004:2016.

Therefore, it is also shown from the sample survey among the selected companies that existing certification standards, due to their implicit generic applicability, allow a lot of room for measurements and monitoring of the management systems regarding information security. This leads to minimalistic implementations and increased occurrence of nonconformities.

In this paper, we were able to conclude that a definition of individual steps based on an analysis of the processes and a concept for meeting requirements and goals for information security can be improved by metrics. A structured approach should be chosen to present the status in a quantitatively correct way on the one hand and to present strategic goals on the other.

This would give companies and their decision-makers faster opportunities to implement and justify risk treatments or investments for information security.

Further research is necessary to achieve an even deeper integration of the visualization of maturity levels, performance, and costs, and to make visualization approaches easier for decision-makers.

VI. REFERENCES

1. Agyepong, E., Cherdantseva, Y., Reinecke, P., Burnap, P., (2023)*A systematic method for measuring the performance of a cyber security operations centre analyst*,Computers & Security, 124, 102959,https://doi.org/10.1016/j.cose.2022.102959.
2. Bakshi, S., (2016)*Performance Measurement Metrics for IT Governance*, ISACA Journal, 6, https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/performance-measurement-metrics-for-it-governance.

3. Crémilleux, D., (2019)Visualization for information system security monitoring. *Cryptography and Security [cs.CR]*, (PhDthesis),CentraleSupélec, NNT: 2019CSUP0013, tel-02872028, https://theses.hal.science/tel-02872028/document.
4. Cunha, F., Dinis-Carvalho, J., Sousa, R.M.,(2023)*Performance measurement systems in continuous improvement environments: obstacles to their effectiveness*, Sustainability, 15(1), 867, https://doi.org/10.3390/su15010867.
5. Diesch, R., Pfaff, M., Krcmar, H., (2018)P*rerequisite to measure information security - A state of the art literature review*,In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018), SCITEPRESS – Science and Technology Publications, Lda, pp. 207-215 https://doi.org/10.5220/0006545602070215.
6. Diesch, R., Pfaff, M., Krcmar, H., (2020)*A comprehensive model of information security factors for decision-makers*. Computers & Security, 92, 101747, https://doi.org/10.1016/j.cose.2020.101747.
7. Hoffmann, R., Napiórkowski, J., Protasowicki, T., Stanik, J., (2020)*Measurement models of information security based on the principles and practices for risk-based approach*,Procedia Manufacturing, 44(2019), 647–654. https://doi.org/10.1016/j.promfg.2020.02.244.
8. Hsu, C., Wang, T., Lu, A., (2016)*The impact of ISO 27001 certification on firm performance*, In: Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS), IEEE Computer Society, USA, pp. 4842–4848. https://doi.org/10.1109/HICSS.2016.600.
9. ISACA, (2019)*COBIT - Control Objectives for Information Technologies, An ISACA® Framework*, https://www.isaca.org/resources/cobit, accessed January 8, 2023.
10. ISO, (2022)*ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, ISO/IEC, Switzerland.
11. ISO, (2017)*ISO/IEC/IEEE 15939:2017 Systems and software engineering — Measurement process*, ISO/IEC, Switzerland.
12. ISO, (2016)*ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*, ISO/IEC, Switzerland.
13. Lampe, S. G., Olaru, M., Fogoroș, T., Massner, S., (2022)*Critical success factor for integration of cyber security in context of managed services*,In: Pamfilie, R., Dinu, V., Vasiliu, C., Pleșea, D., Tăchiciu L., (Eds), 2022. 8th BASIQ International Conference on New Trends in Sustainable Business and Consumption, Graz, Austria, 25-27 May 2022, ASE, Bucharest, pp.741-748,https://doi.org/10.24818/BASIQ/2022/08/098.
14. Maté, A., Trujillo, J., Mylopoulos, J., (2017)*Specification and derivation of key performance indicators for business analytics: A semantic approach*,Data & Knowledge Engineering, 108, pp.30–49, https://doi.org/10.1016/j.datak.2016.12.004.
15. Zaripov, R. N.,Murakaev, I.M.,Ryapukhin, A.V., (2021)*Development of the organization's key performance indicators system in order to improve the effectiveness of its human capital and risk management*. TEM Journal,10(1), pp.298–302. https://doi.org/10.18421/TEM101-37.
16. Olifer, D., Goranin, N., Kaceniauskas, A., Cenys, A. (2017)*Controls-based approach for evaluation of information security standards implementation costs*,Technological and Economic Development of Economy, 23(1), 196–219, https://doi.org/10.3846/20294913.2017.1280558.
17. Proença, D., Borbinha, J., (2016)*Maturity models for information systems - A state of the art*,Procedia Computer Science,Conference on ENTERprise Information Systems / International Conference on Project MANagement / Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist 2016, October 5-7, 2016,100(2), 1042–1049. https://doi.org/10.1016/j.procs.2016.09.279.
18. Rapina, R., Carolina, Y., Joni, Anggraeni, S., (2022)*User involvement in information system quality*,International Journal of Innovative Technologies in Social Science,4(36),https://doi.org/10.31435/rsglobal_ijitss/30122022/7892.
19. VDA, (2022)*VDA ISA Catalogue version 5.1*, https://www.vda.de/en/news/publications/publication/vda-isa-catalogue-version-5.1.
20. Wangen, G.B., Snekkenes, E., (2014)*A Comparison between Business Process Management and Information Security Management*,2014 Federated Conference on Computer Science and Information Systems,FedCSIS 2014, Warsaw, Poland,October 2014, pp. 901–910, https://doi.org/10.15439/2014F77.
21. Wills, B., (2016)*Measuringwhat matters – KPI development*,In Purposely profitable: embedding sustainability into the DNA of food processing and other businesses, Ed. 1, Wiley-Blackwell,pp. 51–68. https://doi.org/10.1002/9781118977958.ch5.