The 7th International Conference on Economics and Social Sciences
Exploring Global Perspectives:
The Future of Economics and Social Sciences
June 13-14, 2024
Bucharest University of Economic Studies, Romania

Approach of Determining Process Maturity in Information Security Management Systems

Michael Matthias NAUMANN[1*], Fabian PITZ[2],
Georg Sven LAMPE[3], Stelian Mircea OLARU[4]

DOI: 10.24818/ICESS/2024/023

Abstract

The need in companies to be compliant with their business processes and to identify and minimise possible risks is an essential task today. Thus, the consideration of the process maturity for management systems of companies is an important approach to see immediately the status of processes as well as implemented requirements. By leveraging maturity levels, numbers and metrics provide a quick look at the overall condition and can be used to derive both measures and compliance with requirements. When looking at an information security management system (ISMS), there is a lack of a general process view and evaluation based on it, and thus also a holistic view beyond the detailed requirements and hard facts. The intention of the paper is to look at the status of existing, industry-specific maturity approaches for information security management systems and to analyse the possibilities for adaptation. Furthermore, based on the evaluation, a maturity model for the ISMS will be proposed to ensure key figures for the companies over time regarding the minimum requirements and certification conformity. A mapping to standards such as CMMI for the classification of the maturity level and the consideration of similar solutions and implementations will be considered. The paper is intended to show the possibility to use a concept to enable the calculation of a percentage maturity level for the representation of the information security level in the company and to make the resulting risks in information security visible. The results of this research show that the proposed approach for a unified method will help to report the maturity of information security management system processes in combination with conformity and security risk for the decision makers in companies.

Keywords: process maturity level, information security management system, maturity level assessment.

[1] Bucharest University of Economic Studies, Bucharest, Romania, matthias.naumann@ixactly.com.
* Corresponding author.
[2] Bucharest University of Economic Studies, Bucharest, Romania, fpitz22@gmail.com.
[3] Bucharest University of Economic Studies, Bucharest, Romania, lampe@compliance-docs-group.com.
[4] Bucharest University of Economic Studies, Bucharest, Romania, olaru_stelian@yahoo.com.

JEL Classification: D81, L15, L21, M15, M42, O33.

1. Introduction

In the area of information security and the associated standardised requirements of the international standard ISO/IEC 27001:2022, there are challenges to obtaining a detailed overview of the business processes to control or adapt them due to the several individual requirements. From the point of view of information technology, topics such as business process optimisation and associated cross-disciplinary functions such as project management, documentation, and continuous improvement are considered, but the technical aspects are always in the foreground.

If companies decide to be certified according to ISO/IEC 27001 or must implement this due to customer requirements, then many management system requirements are already covered by the ISMS built up in the process.

Moving from looking at assets such as documents, hardware, software, and premises, as well as general information such as customer data or people's knowledge, and thus protecting information, is the fundamental approach when looking at information security. With this technical approach, the holistic overview of the process-orientated aspects is sometimes lost. This process thinking mentioned above is established in standards such as quality management and IT service management, but within the standard ISO/IEC 27001, which is used as a standard for companies from all industries to assess the conformity of information security, there is no holistic process consideration with maturity levels and the resulting possibility of measuring a continuous improvement process.

In the following methodology and evaluation, a model will be shown to determine maturity levels for the information security management system (ISMS) and thus to map a possibility for the development and control of the management system even above key figures.

2. Problem Statement

There are already many research papers on maturity in business processes and management systems. Based on the classic quality management system, maturity levels within ISO 9001 are considered with the standard ISO 9004 with a definition of management systems to evaluate process improvements (ISO, 2018). Inside other management systems like environmental management systems based on the standard ISO 14001 this will be also relevant and defined as “strategic options for the development” (Negescu Oancea et al., 2019).

However, since this topic is relevant for all management systems, considerations based on the Quality Management Principles QMPs for Performance Evaluation (ISO, 2015) Subject of research and statistical surveys. “Among other things, QMP efficiency scores as a strategy by an organisation with an Integrated Management System” (Ferradaz et al., 2022).

There were also evaluated the maturity levels for integrated management systems, in detail environmental, food safety and quality management systems were

selected to propose a model for the assessment of maturity based on maturity methods (Santos et al., 2021). Since, as explained at the beginning, the problem of a holistic overview of the maturity or achievement of information security requirements for ISO/IEC 27001 is not covered by the standard, research on this topic already exists.

As an approach, the CMMI maturity levels (ISACA, 2023) will be applied on the requirements of Annex A of ISO/IEC 27001 and then a score is determined (Monev, 2020). However, the problem of the missing chapter clauses and thus the overall view of the management system are not considered here.

Other approaches use a self-assessment and external audit to determine a risk score to determine the maturity level in terms of operational excellence. Here, the Shingo model from the field of LEAN management techniques is used (Carvalho et al., 2023).

Based on the implementation status and progress models and approaches several levels and measuring are identified so the Information Security Level in Organisations (Seeba et al., 2022). In general, the possibilities of companies to measure and monitor the fulfilment requirements were also examined (Naumann et al., 2023) and evaluated.

These investigations all deal with the core topic of continuous improvement and the possibilities of management by the company – e.g. with a better overview by means of maturity levels, and thus the treatment of risks in information security. So that “the understanding and awareness of risk officers directly impacts risk and performance outcomes, and hence the “duty of care and proof” of vulnerabilities and exposures within the organisation" (Lampe, 2023).

But there remains the gap of an approach for mapping of maturity levels to the concrete ISO/IEC 270901 which will be evaluated within this paper.

3. Research Questions / Aims of the Research

Within the assessment of the level of information security in companies, there are various problems that have made it difficult to use maturity models in this area so far. On the one hand, these maturity models are usually process-based considerations that cannot be precisely measured, but can only be classified in general, while the information security reviews are based on technical controls and corporate values.

Another challenge in the measurability and applicability of maturity levels to areas of information security is the consideration of continuous improvement and efficiency, some of which are only partially required to be measured in ISO/IEC 27001. There are already approaches from the automotive industry and other industry standards that implement the necessity of considering process maturity and he information security that also supports this.

The hypothesis is that with the proposed approach companies can identify risk and nonconformities and are able to add the maturity as another level of security and performance measurement.

4. Research Methods

This paper investigates the mapping of existing approaches for information security and next analyses the structure of the ISO 27001 to identify the requirements and groups of controls and clauses which can be measured. The next steps then will be the determination of the risks and non-conformity results together with a mapping of standards maturity levels. Finally, the calculation of the maturity level with example evaluations must be defined and shall show how it could work for a company.

Figure 1. Steps to determine the maturity model approach

Source: authors own research.

Based on the proposed maturity model, an approach is developed for ISO/IEC 27001 that can represent the fulfilment of the requirements and, thus, the risk value of information security with a few figures in the form of maturity levels. In addition to covering the minimum requirements from Annex A of the ISO2701: Standards and an overall view should also be considered with the clauses from the management section. The interpretation of the degree of maturity in the context of nonconformities and risks is an important consideration to map the relevance to information security and the resulting effects. Existing procedures will be considered and analysed to see whether they can be adapted for ISO/IEC 27001. It is suggested as an example of how companies can use the approach to identify it within the regular reviews.

5. Findings

5.1 Process Maturity Assessment

The CMMI Maturity Levels of the CMMI Institute have established themselves as a standardised basis for maturity assessment. These were originally developed for software development and are now used in companies to increase process maturity, improve the quality of their products and services, reduce costs, and increase customer satisfaction. From the point of view of continuous improvement, these are divided into 5 maturity levels (ISACA, 2023):

- Maturity Level 0: Incomplete - Ad hoc and unknown.
- Maturity Level 1: Initial - Unpredictable and reactive.
- Maturity Level 2: Managed - Managed on the project level.
- Maturity Level 3: Defined - Proactive, rather than reactive.
- Maturity Level 4: Quantitatively Managed - Measured and controlled.
- Maturity Level 5: Optimising - Stable and flexible.

CMMI also enables organisations to review the processes with assessments and audits and certify them according to the CMMI level standard. These assessments are often conducted by internal or external auditors.

However, the crucial point here is that companies that must be certified and evaluated according to the ISO/IEC 27001 information security standard do not automatically receive this described added value of a process-side maturity assessment.

5.2 VDA TISAX (Trusted Information Security Assessment Exchange)

It continues to exist in the automotive industry with the VDA-ISA (Information security, 2024) of the TISAX (Trusted Information Security Assessment Exchange) mappings on maturity levels in relation to information security, but almost exclusively on requirements that are only related to the ISO/IEC 27001 Appendix A or the ISO27002 Best Practices (ISO, 2023) reference.

However, when considering the maturity levels, the view of conformity to the requirements of the ISO/IEC 27001 standard must also be considered, which is largely the basis here, but is only partially taken into account due to other requirements in the automotive industry, such as prototype protection. Among other things, the management system part of ISO/IEC 27001 with its clauses is not fully covered.

5.3 ISO/IEC 27001:2022

Within the ISO 27001, standardised minimum requirements for information security are defined and required for the certification of companies. The fulfilment of controls, which are documented in the so-called Annex A, in addition to the management system part, defines minimum organisational and technical requirements. Since the sole approach to determining the implementation status of the minimum requirements from the Annex Controls of ISO/IEC 27001 alone is not sufficient, an overall overview of the entire standard, including the Annex, is necessary.

Among other things, in a review of information security by means of an audit, the absence of implemented tasks or of missing defined processes in the clauses is the main deviation, as it poses a high risk to the functioning of the management system. Therefore, a mapping of maturity classes should ideally also include the implementation of the requirements from the management part of the ISO/IEC 27001 standard. With this approach, however, a stricter assessment or reduction of the maturity level in the absence of implementation of requirements must be defined when considering maturity levels. ISO 27001 is a management system standard that is divided into 2 separate parts. The first part is the management system part mentioned above, which consists of chapters 4-10 like the other management system standards. The second part is Annex A with 93 security controls, of which the company excludes or excludes the relevant ones in the so-called Statement of Applicability (SoA).

The question here is what would happen if controls were not applied and how this would affect the confidentiality, integrity, and accessibility of the information as the main objectives for information security. In practice, there is not that much room for excluding many controls from Annex A. Mostly, they are defined as minimum requirements.

5.4 Requirements

The chapter clauses are mandatory and form the basis of the management system. Here, non-compliance would result in a serious/major deviation within a certification audit. If a company is seeking ISO/IEC 27001 certification, these must be complied with, otherwise, the certificate will not be issued or withdrawn during the term. In the case of Annex A Control, noncompliance with these requirements leads to minor deviations in terms of conformity and thus the maintenance of the certificate. To be able to carry out an assessment of the degree of fulfilment of the requirements, the individual requirements must be defined in detail.

5.5 Approach to Maturity Assessment

With the help of the defined documented process documentation and the verifications, the next step is to carry out the process maturity with the help of the fulfilment of the requirements and a mapping on an existing maturity model.

As a reference to such a maturity model for information security, the procedure already mentioned at TISAX of the VDA-ISA is used here (Information security | VDA, 2022) as a basis, whereby this still has to be extended to the requirements from the clauses of the management part. In the TISAX approach, the defined requirements, which were largely based on the Annex A Controls of ISO/IEC 27001 and the best practices in ISO 27002, are mapped to the CMMI maturity model. In addition to assessing the requirements regarding conformity, this enables an assessment of process maturity.

5.6 Definition of Maturity Level

As mentioned, is the difference here, that additionally the conformity regarding the ISO/IEC 27001 standard requirements for the clauses and the Annex A controls will be verified and the resulting Risk for the information security be mapped. The aim is to determine a level of maturity that not only represents the implementation of a certain process maturity, but also represents the risks to the protection goals of availability, confidentiality, and integrity of information security in the company. At the same time, the reference for assessing conformity and thus the view from an audit according to ISO/IEC 27001 will be considered.

However, since the Clauses, as a mandatory requirement, would lead to a major deviation during a certification, the assessment by means of a maturity level must be stricter in the case of non-compliance than in the absence of requirements for Annex A controls.

5.7 Target Maturity Level

As suggested in the CMMI standard, the minimum target maturity level to be achieved here is Level 3. Values below this led to improvements and the need for adjustment. Maturity levels above the minimum level of 3 lead to a less measurable assessment and are therefore secondary to the fulfilment of a minimum level for information security, as this would then only be reflected in an increase in efficiency.

As already defined in the TISAX VDA-ISA standard, a maturity level of 0-1 would be the main deviant and thus associated with major or critical risks for information security, a maturity level of 2 would mean secondary deviation, and a maturity level of 3 or higher would mean compliant or without risks.

To obtain or maintain certification of an ISMS, e.g. according to ISO/IEC 27001, the maturity level of 2 with secondary deviations to be corrected would then be sufficient.

Table 1. Mapping of maturity levels to ISO 27001 clauses and controls

Mat Level	Status	IS-Risk	Conformity		Definition
			Clause	Control	
0	Incomplete	high	NC	MiNC	No process for the requirements exists.
1	Initial	medium	NC	MiNC	The process exists but it is not insufficiently documented, no evidence exists or there are significant gaps, and no regular tasks are planned and performed.
2	Managed	medium/ low	MiNC	MiNC	A process with objectives is defined. Documentation and process implementation evidence is available, but there are gaps at tasks.
3	Defined	-	conform	conform	All the requirements are fulfilled. Regular tasks are documented and performed as required. A standard process has been defined and applied. Evidence exists.
4	Quantitatively Managed	-	conform	conform	A defined process exists and the effectiveness of it is monitored and measured.
5	Optimi-zing	-	conform	conform	A quantitatively managed process with continual improvement is implemented and followed.

Note: Legend:MiNC =Minor Non-Conformity, NC=Non-Conformity, IS=Information Security.

Source: Authors, CMMI (ISACA, 2023), VDA-Isa 6.0 (“Information security | VDA, 2022) .

5.8 Determination of the Degree of Maturity

The goal for companies would therefore also be to strive for a maturity level of 3 for ISO/IEC 27001 audits, at which conformity would be given and no risks would arise due to the lack of requirements for the ISO/IEC 27001 standard.

5.9 Calculation of the Overall Maturity Score

Since Annex A of ISO/IEC 27001 consists of 93 controls, and the management system part with the clauses consists of 7 chapters and 23 subchapters, the simple average value from the total number of 117 requirements can be formed as a first approach to calculating an overall maturity score.

However, if the management part is to be given a higher weighting, then a calculation must be made, e.g. with a double weighting. In the approach presented here, however, the simple calculation is considered. Analogous to the procedure for TISAX, the overall maturity level is limited to a value of 3. All higher values are reduced to this value with 3.0, analogous to the procedure from the VA-ISA (Information security | VDA, 2022). Furthermore, a traffic light system for color coding is possible to display different threshold values based on the degree of non-conformity, the risk in relation to the determined maturity level.

Table 2. Example of a maturity level assessment

ISO/IEC 27001:2022 Clauses / Controls	No. of Clauses/ Controls	Target Maturity	Assessed Maturity Level
4 Context of the org. (4.1-4.4)	4	3	3
5 Leadership (5.1-5.3)	3	3	3
6 Planning (6.1-6.2)	2	3	2
7 Support (7.1-7.5)	5	3	3
8 Operation (8.1-8.3)	3	3	3
9 Performance evaluation (9.1-9.3)	3	3	3
10 Improvement (10.1-10.2)	2	3	3
A.5 Org. controls (A.5.1-A.5.37)	37	3	2
A.6 People controls (A.6.1-A.6.8)	8	3	3
A.7 Phys. controls (A.7.1-A.7.14)	14	3	2
A.8 Techn. controls (A.8.1-A.8.34)	34	3	3
Overall Maturity Score	115	3.0	2,98

Source: Authors, ISO/IEC 27001:2022 (ISO, 2022).

5.10 Regular Assessments

There are several options for regularly checking the degree of ripeness, which are listed below.

Self-assessment / gap analysis: In some industries or for some standards, such as TISAX with the VDA-ISA, a self-assessment before audits is already mandatory.

If a maturity model approach is also introduced for an ISO/IEC 27001 ISMS, then this self-assessment should be used as part of the reviews. This form of self-assessment can be carried out at any time to demonstrate the fulfilment of the fact requirements as well as the process maturity.

Internal and external audits: As part of the regular audits, it is easy to map findings or observations for improvements to the respective requirements of the clauses or controls and to determine a trend in the development of the ISMS maturity level.

6. Conclusions

In this paper, we were able to show that with the help of the proposed maturity model for the requirements of ISO/IEC 27001:2022, it is possible to assess and read the state of compliance, as well as possible risks for information security based on maturity levels.

This enables decision-makers in companies and those responsible for information security to identify changes to the overall system briefly and to counteract trends.

In contrast to other approaches, this approach also includes the management part of ISO/IEC 27001 with its clauses, which makes it possible to assess certifiability in the first place. With the approach described, it is possible to identify targeted improvements or deterioration in individual areas or for the entire ISMS and thus to point out risks and weaknesses in information security to management.

In detail, further evaluations and investigations would then also offer opportunities to consider the evaluations of the clauses with a higher weight compared to the controls from the Annex, as this is where the greatest possibilities for interpretation are possible when classifying the maturity levels. It is also necessary to consider which risks can be represented with which financial and organisational effects under consideration of the degree of maturity or a security score.

However, this proposed approach is only to be regarded as an approach that requires, among other things, the before-mentioned provisions and the practical use in companies with the evaluation of a changed efficiency in the determination of the state of information security and the continuous improvement process.

Bibliography

[1] Carvalho, M., Sá, J.C., Marques, P.A., Santos, G., Pereira, A.M. (2023). Development of a conceptual model integrating management systems and the Shingo Model towards operational excellence. Total Qual. Manag. Bus. Excell. 34, 397-420.

[2] Ferradaz, C., Domingues, P., Sampaio, P., Arezes, P.M. (2022). The Role of the Quality Principles on the Integration of Multiple Management Systems, in: Occupational and Environmental Safety and Health III. Springer, Cham, 603-611.

[3] Information security | VDA [WWW Document] (2022). Inf. Secur. VDA. URL https://www.vda.de/en/topics/digitization/data/information-security (accessed 2.4.23).

[4] Information security [WWW Document] (2024). URL https://www.vda.de/en/topics/digitization/data/information-security (accessed 2.29.24).

[5] ISACA (2023). CMMI Institute – CMMI Levels of Capability and Performance [WWW Document]. URL https://cmmiinstitute.com/learning/appraisals/levels.

[6] ISO (Ed.), (2023). ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection - Information security controls.

[7] ISO (Ed.) (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements.

[8] ISO (Ed.) (2018). ISO 9004:2018 Quality management – Quality of an organization – Guidance to achieve sustained success.

[9] ISO (Ed.) (2015). Quality management principles.

[10] Lampe, G.S. (2023). Critical Success Factors for Integrating a Circular Iinteraction Model for Security Processes in Digital Transformation. Ecoforum Journal, 12(2).

[11] Monev, V. (2020). Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002, in: 2020 International Conference on Information Technologies (InfoTech). Presented at the 2020 International Conference on Information Technologies (InfoTech), 1-5.

[12] Naumann, M.M., Olaru, S.M., Lampe, G.S., Pitz, F. (2023). Measuring and Idicating the Level of Information Scurity – an analysis of current approaches. Ecoforum Journal, 12(2).

[13] Santos, Â.R.S., Melo, R.M. de, Clemente, T.R.N., Santos, S.M. (2021). Integrated management system: methodology for maturity assessment in food industries. Benchmarking Int. J. 29, 1757-1780.

[14] Seeba, M., Mäses, S., Matulevičius, R. (2022). Method for Evaluating Information Security Level in Organisations, in: Research Challenges in Information Science. Presented at the International Conference on Research Challenges in Information Science, Springer, Cham, 644-652.

[15] Negescu Oancea, M.D., Burlacu, S., Buzoianu, O.A.C., Mitrita, M., Diaconu, A. (2019). Strategic Options for the Development of Ecoturism in the Dornelor County. The USV Annals of Economics and Public Administration, 19(1 (29)), 21-28.