sciendo

Analysis of Relationships between Non-conformities, Process Maturity and Continual Improvement in Information Security Management Systems

Michael Matthias NAUMANN*
Bucharest University of Economic Studies, 010374, Romania
**Corresponding author, matthias.naumann@ixactly.com*

Stelian Mircea OLARU
Bucharest University of Economic Studies, 010374, Romania
olaru_stelian@yahoo.com

Georg Sven LAMPE
Bucharest University of Economic Studies, 010374, Romania
lampe@compliance-docs-group.com

Fabian PITZ
Bucharest University of Economic Studies, 010374, Romania
fpitz22@gmail.com

Abstract. *In the current global context, companies need a defined minimum level of information security to recognize and deal with related threats and risks.*

Due to market, customer or legal requirements, specifications and requirements for information security are implemented uniformly according to standards such as the information security management standard ISO/IEC 27001 or industry-specific standards such as Trusted Information Security Assessment Exchange - TISAX, ISO IEC 27019 Energy Utility Information Security Standard.

The conformity to these standard requirements within the established management system is checked during periodically required audits.

However, there are various reasons for which, even after many years of audits in companies, there are still insufficient process implementations for information security requirements.

The aim of the paper is to analyze the status of conformity and thus also the process maturity in selected samples of companies that have already had information security management systems (ISMS) implemented for several years.

In detail, the reasons for deviations from the minimum requirements with associated risks for the security of information in companies were analyzed, which allow conclusions to be drawn about possible process improvements. The paper also analyzes why, despite established measures and existing expertise, only a limited level of process maturity is achieved on average.

Other possible approaches to the implementation procedure for dealing with non-conformities in information security are also considered.

The results of this research show that there is a need for an adjusted continuous improvement process, which makes risks resulting from insufficient process maturity more visible. Proposals for such improvements are listed.

Keywords: information security management systems, system-audit, non-conformities, process maturity, continuous improvement, information security risks.

DOI: 10.2478/picbe-2024-0043

Introduction

It is essential for companies to regularly review management systems that have been set up and implemented, including information security management systems (ISMS). This assessment of compliance with defined requirements is carried out by determining conformity with certifiable standards.

Industry best practices for information security management have been summarized by the International Organization for Standardization in the ISO 27000 series of standards, out of which the ISO 27001 standard defined the requirements regarding the information security management system (Ionescu et all, 2020).

As in the case of other management systems, the information security management system is based on the Plan-Do-Check-Act (PDCA) principles which describe the continuous improvement process in its main phases.

While within the basic cycle, Planning and Doing are covered by means such as regular reviews and corrections of the organizational framework, scope definition, guidelines, and asset- and risk management, the Check phase evaluates the efficiency and conformity with the requirements as well as the objectives of the organization with regard to information security. In the ACT phase, measures are taken with the goal of correcting and improving.

Over years of reviews by internal 2nd party and external 3rd party audits in companies, it has been noticed that these reviewed information security management systems still produce a number of non-conformity findings even after many years since their establishment.

The type and distribution of unfulfilled requirements, the non-conformities in relation to the information security standards, should be considered here. In ISO 27001, there is no clear specification for an easier classification and estimation of the remaining process adjustments.

This paper is intended to illustrate the relationships between non-conformities, the achieved process maturity and the continuous improvement in the information security management system.

Literature Review

There are already numerous research papers on continuous improvement in management systems and the relationship between non-conformities. It is considered that an organization's information security architecture is influenced by information security policies, risk management, internal and external audits (Lampe et all, 2020).

As already mentioned, the PDCA cycle in information security management systems plays an important role as a fundamental component of a management system for "improved balance between the effectiveness and efficiency" from an organizational and structural perspective (Qusef et al., 2018).

Being compliant via an effective ISMS sets the basis also for the risks for information security to be tracked and under control. Implementing the requirements based on an international standard such as ISO/IEC 27001:2022 will allow for an improved mitigation of standard threats and resulting risks (Stefanova-Stoyanova and Danov, 2022).

The ISO standard also requires measuring the performance of the ISMS by using metrics. An analysis of existing information security metrics was performed and a related structured approach has been recommended (M. M. Naumann et al., 2023)

The verification of compliance to these standards is done via periodical audits, which should “Integrate the audit of management systems into the process of continuous improvement” (Mejias, 2023). When assessing conformity and performing audits, the International Standard for terms and definitions in the field of conformity (ISO17000) is used as a basis (Naden, 2020).

When verifications are carried out, a conformity assessment is performed, which provides the assurance that defined expectations and requirements are met. Conformity to requirements can lead to the achievement of various objectives. The International Organization for Standardization lists "conformity assessment activities to build trust in the circular economy" (ISO, 2023) as an example of how this can be applied in different industries, with the example of achieving sustainability by reducing non-conformities.

The difference between auditing quality management systems and information security systems is the perspective: the former evaluates the conformity of processes for the value chain or the "identification and registration of non-conforming products" (Mandrakov et al., 2020) while the later focuses on non-conformities impacting the protection requirements of company information assets.

Another research proposes a methodology for assessing security for cloud services by using for evaluation different assessment parameters (Ismail & Islam, 2020).

Besides such specific approaches and research the factors leading to being non-compliant within a management system after performing regularly the required audits need to be evaluated more in detail.

There exist already some surveys and research which evaluate deviations and non-conformities as identified for each kind of requirement. But there is still a research gap for evaluation regarding why companies seem to be still having over time the same issues and not have an adequate, functional continuous improvement process.

These specific details as part of the continuous improvement process of their certified management systems will be analyzed and handled with this paper.

Methodology

This paper investigates the evolution of non-conformities over time in companies that already have an implemented information security management system. In particular, the correlation between audit nonconformities and associated information security risks in companies with many years of experience is examined.

To this end, a qualitative approach was used to interview and examine companies regarding the results of audits as part of ISO 27001 certification.

These results show the relationships between the number and type of non-conformities identified during the audits carried out and their development over the years.

In this context, it will also be considered what possibilities exist within the companies to get a better view of the level of their information security level, in addition to existing internal and external audits.

Non-conformities identified during assessments or audits will be tracked and relevant for preparing the recertification of companies with the ISO 27001 standard.

Companies from the IT services, automation/engineering, marketing, automotive, finance and energy sectors were surveyed and analyzed regarding their audit findings and non-conformities discovered over the last 2 audits. The selected sample was used to examine how conformity with the information security requirements of ISO 27001 has developed over time, as depicted in Table 2 below.

Initially, we recorded for how many years the company has had a certified management system, in order to be able to draw conclusions about the continuous improvement process.

Certified years – The number of years the company has been certified and therefore audited regarding information security management.

Audit type - the type of the audit, in order to differentiate if it is either a Repeat Audit (RA) or a Surveillance Audit (SA) between the years of certification. Companies with initial certification audits were not surveyed.

Findings at year before / Findings at current year - the number of audit non-conformities identified in the previous year and the current year, respectively.

Furthermore, the audit type was recorded as part of the evaluation, as the scope of the audit is larger during the 3-year repeat audit which is part of ISO certification than for the more frequent surveillance audits carried out within this timeframe. This schedule is defined in an audit program, usually over 3 years, and follows the ISO 19011 standard (ISO, 2018) For this reason, only companies that had been certified prior to the last year were examined.

Size – determination based on SME Definition by the European Commission as depicted in Table 1 below. All other companies are in the large category.

Table 1: SME Definition of European Commission

Company category	Staff headcount	Turnover	Balance sheet total
Micro	< 10	≤ € 2 m	≤ € 2 m
Small	< 50	≤ € 10 m	≤ € 10 m
Medium-sized	< 250	≤ € 50 m	≤ € 43 m

Source: (European Commission, 2003, 2021).

Table 2. Findings during audits of information security management systems for analyzed companies

Company		Audit		Findings	
ID	Size	Certified years	Audit type	# Findings at year before	# Findings at current year
1	Medium	6	SA	3	2
2	Medium	5	SA	0	2
3	Medium	3	SA	7	6
4	Medium	2	SA	6	2
5	Medium	5	SA	2	4
6	Large	2	SA	7	3
7	Small	2	SA	8	6
8	Large	6	SA	4	5
9	Large	12	SA	2	2
10	Large	6	SA	7	1
11	Medium	4	RA	1	3
12	Medium	5	SA	3	1
13	Medium	1	RA	7	6
14	Small	4	RA	0	2
15	Medium	3	SA	0	15
16	Medium	6	SA	3	0
17	Large	4	RA	4	3
18	Large	5	SA	1	7
19	Medium	2	SA	12	2
20	Small	8	SA	7	2
21	Small	3	SA	6	5
22	Small	4	RA	6	0

Source: Authors' own research.

Results and discussion

Identified non-conformities regarding requirements during the audit of information security management systems (ISMS)

The values from Table 3 below show the distribution of the audit findings by Chapter clauses and Annex control sections of the ISO 27001:2022

Because the ISO 27001 standard was revised in 2022 a mapping of the Annex A controls from the old 2013 version to new 2022 version was performed based on proposed grouping in technical, organizational, resourcing and physical controls using mapping tables (J. Naumann, 2022).

Table 3: Identified non-conformities during the audit of information security management systems (ISMS)

Findings						Findings inside ISO27001							Reasons/root causes of findings					
ID	No. of Findings at current year	Chapter4 Context	Chapter5 Leadership	Chapter6 Planning	Chapter7 Support	Chapter8 Operation	Chapter9 Perform	Chapter10 Improvement	Annex A.5 Org. controls	Annex A.6 People controls	Annex A.7 Physical controls	Annex A.8 Techn. controls	Lack of resources	Lack of employee awareness	Insufficient task management	Organizational changes	Insufficient process definition	Insufficient technical realization
1	2							1		1					x		x	
2	2								1		1			x			x	
3	6				1		2		1		1			x	x		x	
4	2										2			x				
5	4			1					1	1	1				x		x	x
6	3							1	1	1					x		x	
7	6			1	1		1		2		1				x		x	
8	5			1	1		1		1					x	x		x	
9	2								2						x		x	
10	1			1											x			
11	3							1			1				x		x	
12	1							1							x			
13	6								3	2		1				x		
14	2										2			x				
15	15		1	2	2	1	3	1	1	3		1	x		x		x	
16	0																	
17	3								2		1			x			x	
18	7			2		1	2	1				1			x		x	x
19	2			1								1			x			
20	2										1	1		x				x
21	5			1			3		1						x		x	
22	0			1			1		1	1	2				x		x	

Source: Authors' own research.

The distribution of the non-conformities based on the numbers of findings in relation with the standard clauses and annex A controls of ISO 27001:2022 is presented in Table 4.

Table 4: Distribution of audit non-conformities in relation to ISO 27001 requirements

Clause / Control	Number of non-conformities	Share in total number of non-conformities
Chapter4 Context	0	0%
Chapter5 Leadership	0	0%
Chapter6 Planning	11	14%
Chapter7 Support	5	6%
Chapter8 Operation	2	2%
Chapter9 Perform.	13	16%
Chapter10 Improvement	6	7%
Annex A.5 Org. controls	17	21%
Annex A.6 People controls	9	11%
Annex A.7 Physical controls	13	16%
Annex A.8 Techn. controls	5	6%
Total non-conformities	81	100%

Source: Authors' own research.

In this analysis, the largest share of non-conformities is thus in relation with Annex A organization (A.5) and (A.7) physical controls, chapter 9 performance evaluation topics such as internal audits, metrics and KPIs and the Management Review and chapter 6 on planning including risk management. The above-mentioned clauses and controls account for 67% of total non-conformities identified by the sample of companies, as depicted in Figure 1 below.

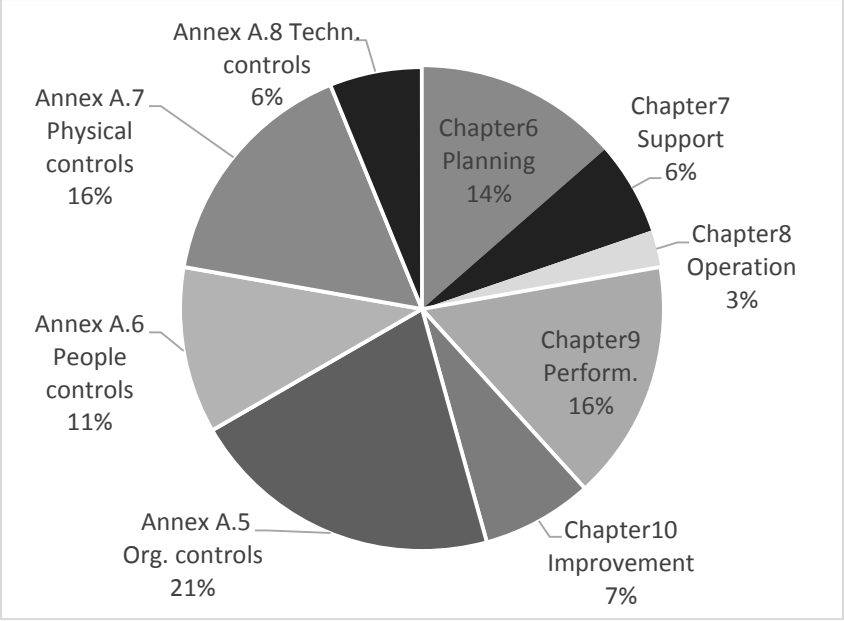

Figure SEQ Figure * ARABIC 1: Distribution of identified non-conformities in relation with ISO 27001 chapters and annexes

Source: Authors' own research.

Trend of non-conformities after several audits

Taking into account that the analysis shown in Picture 2 below is only a snapshot from a statistical perspective, a higher number of samples would likely increase the accuracy of the results. Nevertheless, the analysis in Picture 2 shows that even after several years, a small number of issues and non-conformities related to the information security management systems still remain.

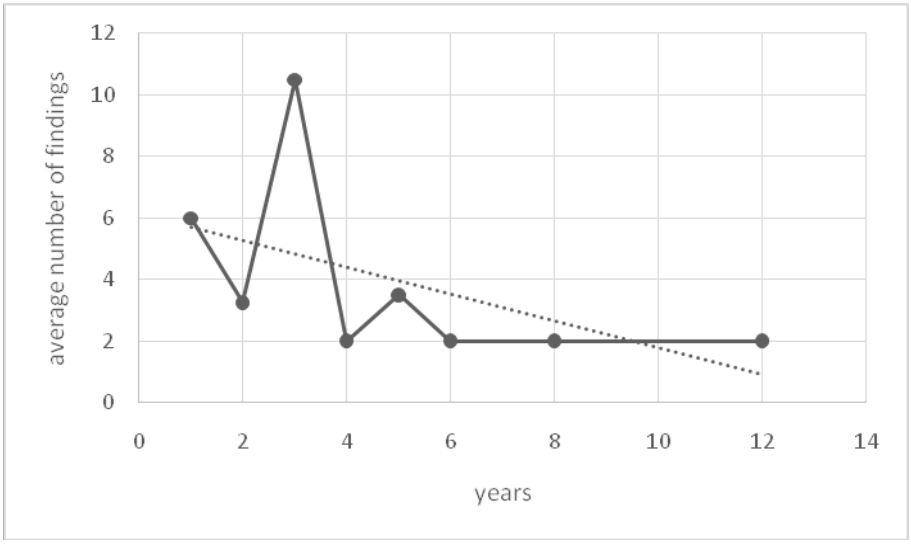

Figure 2. Historical evolution of the average number of findings resulting from information security management system audits

Source: Authors' own research.

The findings for the sample companies that had the longest period of certified information security management systems are related mostly to Annex Organization controls and partially to the Planning clauses.

There were also a few cases of sample companies that represented statistical outliers given that they did not improve over the analyzed period and thus recorded more findings in the current year than in the previous one. This situation can be caused by several reasons, such as a change in audit personnel, which may judge the same topic differently.

Root causes of identified non-conformities regarding requirements during the audit of information security management systems (ISMS)

For the interviewed and analyzed companies the following main reasons for not meeting standard requirements in relation with information security management systems were determined:

Insufficient technical realization.

Incorrect or inadequate technical measures have been taken:

- There are too many administrators or privileged users in the systems.
- Physical security in rooms was not adequately realized.
- The protection of equipment had not been realized in an appropriate manner.
- There were issues with physical security during inspection.

Insufficient process definition.

Processes had not been sufficiently or adequately defined, and some of them were not documented:

- Business continuity processes are not correctly defined, documents and tested.
- Suppliers are not sufficiently considered and evaluated regarding information security.
- The annual "Management Review" does not meet the minimum requirements.
- The handling and disposal of old equipment or defective media devices does not meet the defined requirements.
- The process for employee offboarding does not document or does not cover all requirements.
- The risk analysis and treatment were not planned or performed correctly.
- Overdue or not existing non-disclosure agreements with suppliers as defined by process.
- The "Statement of Applicability" does not correctly document the status of applicability of controls.
- There is no documentation of emergency contacts.

Organizational changes.

Changes within the organization affect the implementation or performance of the ISMS:

- The position of Information Security Officer has been newly filled.
- Reorganization, integration into new company structures
- New site with unfinished security measures.

Insufficient task management.

Tasks to regularly check, implement measures or improve the ISMS are not carried out:

- Internal audits were not planned correctly with an audit program or insufficient performed / tracked.
- Not all non-conformities from last audits were tracked correctly.
- The risk management planning contains overdue mitigation measures.
- ISMS measures with an overdue or no completion date.
- No measuring and monitoring of ISMS performances and its objectives.
- No regular documented review of user rights and access permissions
- The regular information security awareness trainings were not tracked or not performed correctly.

Lack of employee awareness.

During sample checks of information security, findings were made due to insufficient employee awareness or employees generally not adhering to the rules:

- Unlocked doors in security areas.
- Violation of guidelines for handling access information
- Inadequate handling when sending / printing / saving data.
- Confidential documents and material were left on desks.

Lack of resources.

Due to a lack of resources, information security tasks or implementations were not carried out:

- Dual roles as representatives for management systems
- Resignations and vacancies in the area of ISMS responsibilities
- No budgeting for external independent support
- The communication processes and responsibilities inside ISMS team are not defined or documented correctly.
- There are not for all processes owners defined or there is a lack of resources.

The breakdown of the share of each of the above-mentioned root causes category in the total number of identified non-conformities is depicted below, in Figure 3.

Figure SEQ Figure * ARABIC 3. Share of root causes of identified non-conformities in total

Source: Authors' own research.

Determining the correlations of non-conformities regarding requirements and company size

The statistical view depicted below in Table 5 shows the relationship between the size of the company and the number of findings as well as the level of improvement which was accomplished from one year to the next in order to fix the issues.

Table 5: Correlation between company size and number of findings

Company size	Share from total number	Number of findings Current Year	Number of findings Last Year	Average nb of findings	Trend LY to CY
Small	23%	15	27	3	-80%
Medium	50%	43	44	3,9	-2%
Large	27%	21	25	3,5	-19%
Legend: CY=Current Year, LY=Last Year					

Source: Authors' own research.

As shown above, small companies were able to fix a share of identified issues from the previous year that is significantly greater than medium and large companies. Furthermore, medium companies from the analyzed sample were only able to improve slightly their performance, achieving a very small percentage improvement compared not only to small companies but also to the large ones.

This could mean that the resources and importance of ISMS in general is higher for small and large companies than for medium companies, so the former are able to improve their systems in a shorter time.

The statistics shows that companies with many years of audit experience and a long time of implementing the requirements of the standard reduce the number of risks and thus increase their security level but still remain at a residual level.

The deviations and therefore non-conformities in the information security audits relate to similar areas, with the most frequent unfulfilled requirements being found in the areas of insufficient implementation of the required / defined process and in action tracking for regular tasks in the management system.

A distinction must be made as to whether these measures have not been sufficiently implemented for financial reasons, organizational reasons or due to a lack of know-how.

Determining the process maturity level in the ISMS area, taking into account continuous improvement

Dealing with non-conformities is a task of the continuous improvement process within the management systems. Both improvements and the elimination of non-conformities are intended to ensure the implementation of requirements and thus the required process maturity.

Use of maturity models

Some industry standards already require a maturity level to be specified, e.g. for critical infrastructures or in the automotive industry.

There are also industry standards that have already recognized this gap and provide a maturity level as an overview of the status of the information security management system, for example:

- Maturity level for TISAX: for the ENX standard and the VDA, a maturity level of 3 is defined within the VDA_ISA questionnaire for the fulfillment of the given requirements (VDA, 2023)
- Maturity level for critical infrastructure audits by BSI, Federal Office for Information Security in Germany: BSI in Germany has also already established a maturity level for a quick assessment of checks carried out. Here, the complete implementation of MUST and Should requirements have to be scored in the classification. A maturity level of 3 indicates a fully established ISMS.

The objective of determining the maturity level is to achieve an overall view of the fulfillment of the criteria with individual scores. Acting as a KPI, this serves to preventively record and control further improvement measures. If an approach with a maturity model has to be introduced for an ISMS in accordance with ISO/IEC 27001, then a self-assessment should be used as part of the reviews.

Systematic measures planning

As with other standards, strict and consistent action management is an essential point within the management of an ISMS. This applies to systems in which time-based organization of tasks is required.

Most findings from companies that are already well familiar with the technology and content of their management system over the years can be found in action tracking processes.

There are several ways to track ISMS measures, such as project management tools, ticket systems, SharePoint lists, Excel tables or calendar tasks.

Since, according to many years of audit experience, most tasks can rely on planning and repetition in operational tasks, the recommended implementation is the use of ticket or project management systems, as time tracking and integration of approvals and notifications is already implemented here using workflows.

Regular information security reviews

One requirement for maintaining an ISMS is the regular review through internal audits. These are intended to maintain conformity during the year and before the 3rd party surveillance or repeat audit.

Ideally, all problems and non-conformities are found and rectified before the 3rd party audit, so that only a few issues potentially relevant to certification remain.

By conducting them at shorter intervals and having objective assessment by more external support, a significant improvement can be achieved over the years.

Overview of information security with performance indicators

On the one hand, KPIs are used to measure the achievement of ISMS objectives, but on the other hand they also serve as a means of monitoring the current security level.

A critical development of the level of information security, especially on an operational basis, is also possible through a suitable selection of key figures.

There are various recommendations as to which topics can be monitored and how (M. M. Naumann et al., 2023).

Self-Assessments

In specific industries or for defined standards, such as TISAX with the VDA-ISA, a self-assessment is already mandatory before audits.

This provides a good initial overview, which can also be carried out together with external service providers. In most cases, a rough summary of the classification is then made based on maturity levels, for example.

Conclusion

In this paper, we were able to show that an accumulation of non-conformities can be found in repetitive tasks, but also in non-compliant process implementations within the information security management systems.

Based on the statistical survey and the need to consider the improvement of standard tasks and measures management identified therein, it should be noted that there is a considerable need to continuously improve the level of information security, even in systems that have been in place for many years. This is partly due to cost and resource considerations, but also to a lack of overview of the resulting risks.

Further evaluations and investigations would then also offer opportunities for business process optimization, as correlations between the size of the companies and the general weighting and objective of information security also play a role.

As the number of samples surveyed and examined is not sufficient to allow even more precise details or mapping to all companies and areas, these points should be examined in more detail with further statistical surveys.

There is also a need to track key figures with more details and ideally to apply maturity models.

This would ensure a more sustainable and therefore higher level of information security than the current short-term view of companies. In addition, there would be cost savings due to the elimination of rework, the freeing up of resources and a general reduction in information security risks.

The point of early detection and permanent monitoring of trends and non-conformities should be considered with further research into the use of maturity models for the information security management system implemented according to the ISO 27001:2022 international standard and thus the visualization of inadequate process implementations and associated risks.

References

BSI. (2020). *Orientation guide to documentation of compliance according to Section 8a (3) BSIG*.

European Commission (2003). *SME definition*. https://single-market-economy.ec.europa.eu/smes/sme-definition_en

European Commission (2021). *Commission staff working document evaluation of Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (2003/361/EC)*, https://ec.europa.eu/transparency/documents-register/detail?ref=SWD(2021)279&lang=en.

Ionescu, R. C., Olaru M., Sargut K. (2019). Study of the Information Security Impact on the Business Continuity, in *Proceedings of the 34th International Business Information Management Association Conference (IBIMA), Madrid, Spain*, 11/13-14/2019, Pag.: 4279-4287, ISBN: 978-0-9998551-3-3, https://apps-webofknowledge-com.am.e-nformation.ro/full_record.do?product=WOS&search_mode=GeneralSearch&qid=1&SID=F1Popqoibfu8upwkh1Q&page=1&doc=2

Ismail, U. M., Islam, S. (2020). A unified framework for cloud security transparency and audit. *Journal of Information Security and Applications*, *54*, 102594. https://doi.org/10.1016/j.jisa.2020.102594

ISO (2018). *ISO 19011:2018—Guidelines for auditing management systems*. https://www.iso.org/standard/70017.html

ISO (2023). *ISO - The circular economy: Building trust through conformity assessment*. https://www.iso.org/insights/circular-economy-building-trust

Mandrakov, E. S., Vasiliev, V. A., Dudina, D. A. (2020). Non-conforming Products Management in a Digital Quality Management System. *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, 266–268. https://doi.org/10.1109/ITQMIS51053.2020.9322931

Mejias, P. (2023). Adding value to audits of management systems. https://www.quality.org/article/adding-value-audits-management-systems

Naden, C. (2020). Words to the wise on conformity assessment. *ISO*. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/news/2020/05/Ref2519.html

Naumann, J. (2022). *ISO/IEC 27001 ISO/IEC 27002 und IT-Grundschutz*. Books on Demand.

Naumann, M. M., Olaru, S. M., Lampe, G. S., Pitz, F. (2023). Measuring and indicating the level of information security - an analysis of current approaches. *Ecoforum Journal*, *12*(2). http://www.ecoforumjournal.ro/index.php/eco/article/view/1739

Qusef, A., Arafat, M., & Al-Taher, S. (2018). Organizational management role in information security management system. *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*, 1–8. https://doi.org/10.1145/3231053.3231064

Stefanova-Stoyanova, V., & Danov, P. (2022). Comparative Analysis of Specialized Standards and Methods on Increasing the Effectiveness and Role of PDCA for Risk Control in Management Systems. *2022 10th International Scientific Conference on Computer Science (COMSCI)*, 1–4. https://doi.org/10.1109/COMSCI55378.2022.9912583

Sven, L.G., Maftei, M., Surugiu, I., Bitan, G, Ionescu, R. C. (2020) Study of Information Security Management System and Business Continuity Management in the Context of the Global Crisis, *The 6th BASIQ International Conference on New Trends in Sustainable Business and Consumption, Messina, Italia, 2020*, vol. 01, pg. 942-949, ISSN 2457-483X, https://www-webofscience-com.am.e-nformation.ro/wos/woscc/full-record/WOS:000630165800121

VDA (2023). *Information security*. https://www.vda.de/en/topics/digitization/data/information-security