Evaluation Methodology for Assessing Management System Establishment Support Tools

Anja Wiedemann*

TÜV Informationstechnik GmbH (TÜViT), Langemarckstr. 20, 45141 Essen, Germany

Abstract: The establishment and operation of a certified management system (e.g. for Quality Management or Information Security Management) according to an international standard is a complex task for an organization. Hence, organizations usually search for support in order to successfully establish the management system and pass the certification procedure. This support is represented by consultants and / or by appropriate software tools. These software tools are designed to support the implementation and operation of management systems within organizations. This article presents an evaluation methodology for such software tools. An evaluation of such software tools for the establishment of management systems in organizations provides trust into these tools to the users of the tools, and it also provides a confirmation to the manufacturers of these tools that the evaluated aspects are straight.

Keywords: Management system, ISMS, ITSM, QMS, Support tools, Compliance, Certification, Trust.

INTRODUCTION

The establishment of a management system according to an international standard within an organization is a sophisticated task. Numerous standards for management systems exist, such as ISO 9001:2008 [1] for Quality Management Systems (QMS), ISO 27001:2005 [2] for Information Security Management Systems (ISMS) or ISO 20000-1:2005 [3] for IT Service Management (ITSM), etc. However, the setup and operation of such a management system within an organization according to the corresponding standards is a complex task requiring significant amounts of time and resources in terms of costs and labor. The reason is that these standards either intervene with an organization's processes or require the establishment of new processes. [1-3] also require the overall implementation of a Plan-Do-Check-Act (PDCA) cycle for the management system. A PDCA cycle implies that the management system is appropriately planned, implemented, checked and monitored. Under consideration of the monitored results, activities are performed in order to improve the overall management system.

Establishment and operation of a management system also require a lot of documentation effort (e.g. for guidelines, handbooks, policies, notes and records, meeting reports, reports from internal evaluations of the management system, etc.). This documentation has to be directed, it has to be maintained and controlled. The organization of this documentation itself might already require appropriate software for this particular task. Nevertheless, this software itself only helps to organize the documentation related to the management system – it does not provide any further support with regard to the overall establishment of the management system within the organization.

*Address correspondence to these authors at the TÜV Informationstechnik GmbH (TÜViT), Langemarckstr. 20, 45141 Essen, Germany;
E-mail: A.Wiedemann@tuvit.de

However, the management system has to be well-established within the organization, as otherwise a certification of this management system will fail. The process is as follows (see the glossary for definitions of *audit*, *auditor*, *certificate*, *certification*, *certification body* and *compliance*):

- The organization establishes a management system (e.g. a QMS, an ISMS, etc.).
- When the management system is established, the organization requests the certification of this management system from a certification body.
- The certification body opens the certification procedure and determines auditors.
- The auditors are requested to evaluate the compliance of the organization's management system with the international standard. In this context, the auditors assess the documentation of the management system as well as the implementation and operation of the management system on-site (i.e. at the organization's site).
- Depending on the findings of the auditors, the auditors recommend the certification, or they recommend the rejection of the certification of the management system to the certification body. If the certification is initially rejected by the auditors, the organization gets the chance for improvement and a re-evaluation by the auditors.
- If certification is recommended, the certification body checks the audit results with the intention to confirm that the management system fulfills the international standard.
- If the certification body confirms that the management system fulfills the international standard, a certificate is issued to the organization.
- The organization can visualize the certificate, which provides trust into the organization's management system, to its clients and customers.

1874-107X/09

- The certification procedure also requires surveillance and re-certification audits – these audits are mandatory in order to keep up the certification of the management system.

Hence, organizations, which want to or are required to implement management systems according to international standards, usually seek for further support in order to successfully pass the certification procedure. On the one hand, this support might be provided by specific consultants for the management systems of interest during particularly challenging phases. On the other hand, the organization might be supported by the application of particular management system establishment (MSE) support tools. These MSE support tools are expected to facilitate the establishment and the operation of a management system within an organization. MSE support tools exist for various international standards. A subset of examples for such MSE support tools are [4-6] for ISO 9001, [7-9] for ISO 27001 or [10-12] for ISO 20000.

By an application of a MSE support tool, the organization expects:

- guidance with regard to the implementation of the international standard within the organization.
- avoidance of significant mistakes with regard to the implementation of the standard which otherwise might prohibit the certification of the organization.
- facilitation of the overall certification process (e.g. automatic generation of the documentation out of the tool).
- a decrease of time, costs and resources required for the establishment of the management system and the certification.
- savings with regard to the participation of consultants.
- to have and to administrate the overall management system within the support tool.

Under consideration of these expectations the question arises: *Will these MSE support tools satisfy the expectations of organizations? How to verify, whether these expectations are met or not?*

These questions will be subject of the subsequent section of this contribution.

REQUIREMENTS OF MSE SUPPORT TOOLS

The requirements (Req.), which have to be made to MSE support tools, can be specified as follows:

Req. 1) The MSE support tool shall fully comprise the contents of the international standard.

Req. 2) The MSE support tool shall represent the international standard correctly with regard to the tool's functionality.

Req. 3) If the MSE support tool is provided in terms of Software as a Service (SaaS), particular aspects have to be ensured, such as appropriate disjunction of clients, privacy, application security, appropriate security on-site (i.e. at the provider's site).

Req. 4) The MSE support tool shall provide classical quality features of software products, such as functional correctness of the software product, appropriate usability / user-friendliness, robustness, extensibility, maintainability, reusability, compatibility, portability, integrity and appropriate performance.

If Req. 1) and Req. 2) are not met, the organization might not be able to appropriately establish the management system. A certification of this management system might be prohibited, because norm elements are violated or not fully implemented. This means that costs, resources and time for the establishment and for the expensive certification process are wasted.

If Req. 3) is not met, a significant risk arises that highly sensitive information of the organization is disclosed.

If functional correctness of the software product and usability (cf. Req. 4)) are not met, the usage of the MSE support tool will cause additional problems instead of support functionality or facilitation of the implementation process of the management system.

Is the consequence of these considerations of requirements, which might not be met by these MSE support tools, that the usage of MSE support tools shall be avoided? – The answer to this questions is "no", but trust has to be provided into these MSE support tools in terms of an evaluation of these tools by independent and objective technical experts and auditors of the international management system standards. If the MSE support tool passes the evaluation procedure, a certificate is assigned to the tool manufacturer as a visible sign that the tool is trustworthy and can be applied for the establishment of the corresponding management system.

The next section deals with this evaluation procedure of MSE support tools. An evaluation of MSE support tools will provide trust to the users as well as to the manufacturers of these tools – they can have confidence that evaluated tools meet the aforementioned requirements.

EVALUATION METHODOLOGY

The evaluation methodology for MSE support tools is designed as a generic methodology, i.e. the methodology can be applied to any MSE support tool – no matter of the international standard which is focused.

The time frame, which is necessary to perform the evaluation appropriately, varies with the complexity of the MSE support tool. If, for instance, the MSE support tool is designed to work as a standalone installation at customer's site, the evaluation will be less complex than in case of a MSE support tool which is provided to the customer in terms of SaaS. However, for a careful and reasonable evaluation of a MSE support tool, at least 20 man days are assumed.

The evaluation methodology covers 9 evaluation modules. The number of evaluation modules, which are applied within the assessment of the MSE support tool, depends on the complexity of the tool. If, for instance, the MSE support tool is offered in terms of SaaS (as an example of a very complex solution), it will need the application of more evaluation modules than a support tool which is operated as

a standalone installation at the customer's site (as an example of a less complex solution) (cf. Fig. **1**).

For an evaluation of a MSE support tool, an evaluation package is tied up under consideration of the tool's particularities. This evaluation package consists of a meaningful (sub)set of the aforementioned 9 evaluation modules. However, if the evaluation process discloses that further analyses are reasonable, the evaluation of the MSE support tool can flexibly be extended by additional modules out of the 9 evaluation modules.

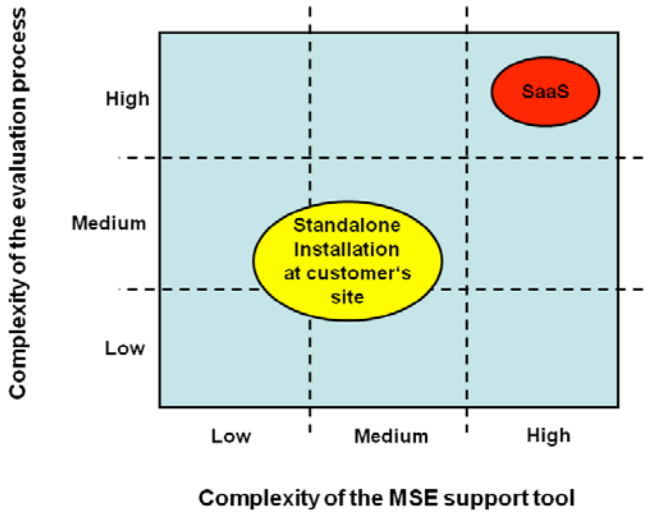

Fig. (1). Complexity of MSE support tool and evaluation process.

The evaluation modules (Mod.) 1) to 9) are described subsequently.

Mod. 1) Compliance with the International Standard

Within this evaluation module, the MSE support tool and the corresponding international standard, on which the tool focuses, are object of investigation. This part of the evaluation is performed by an auditor of the corresponding international standard as follows:

- The MSE support tool manufacturer has to provide a requirements catalogue which shows how the requirements of the international standard (e.g. ISO 9001:2008, ISO 27001:2005, etc.) are mapped to the MSE support tool (i.e. the manufacturer has to show within the requirements catalogue, how and where the requirements of the international standard can be found within the MSE support tool). This requirements catalogue is evaluated, whether it fully comprises the contents of the international standard.
- The next step is the evaluation within the MSE support tool, whether the aforementioned requirements are implemented within the tool as described in the requirements catalogue.
- Furthermore, all tool output (e.g. Statement of Applicability (SoA) and Risk Assessment Methodology in case of a MSE support tool for ISO 27001:2005) is evaluated under consideration of the requirements imposed by the international standard.
- Within this evaluation module, it is also checked, whether the MSE support tool represents the international standard correctly with regard to the tool's functionality.

Mod. 2) Quality of the MSE Support Tool Software and the Software Development Process

- The development process of the MSE support tool software has to follow a documented, process oriented approach and has to be quality-assured (e.g. by the execution of reviews, inspections, walk-throughs after each phase of the software development process and/or after each quality gate). Furthermore, verification and validation have to be part of a quality-assured software development process. Documentation, related to the software development process, is also evaluated.
- Regarding the software development process of the MSE support tool, the test process is particularly inspected. The test documentation, test methodology and the coverage of the tests are evaluated. Moreover, a software engineer / test specialist might specify and conduct own tests with the MSE support tool under consideration of particularly significant cases. In case of functional tests, applicable standards are also considered (e.g. ISO 25051:2006 [13]), although they might not be fully applied, as the overall evaluation shall remain affordable.
- This evaluation module comprises an on-site process audit (i.e. an audit at the manufacturer's site) of the software development process under consideration of the aforementioned quality assurance issues. This process audit is performed according to the rules of quality assurance audits.

Mod. 3) Usability of the MSE Support Tool

- Within this evaluation module, an expert evaluation of the usability of the MSE support tool is conducted (i.e. a usability expert works with the tool and gathers observations).
- Key personnel at the customer's site are observed by a usability expert, when working with the tool. Instead of this observation or additionally, questionnaires are evaluated, which are passed to and filled in by key personnel of the manufacturer and the customer.
- For this usability evaluation, applicable standards are considered (e.g. ISO 9241:200x [14]), although they might not be fully applied, as the overall evaluation shall remain affordable.

Mod. 4) Privacy Issues

- Within this evaluation module, it is analyzed which kind of personal data is collected.
- It is evaluated, whether this personal data is protected appropriately.
- Furthermore, the processes, in which personal data is collected, are analyzed in terms of an on-site process audit.
- For this privacy evaluation, applicable sets of rules are considered (e.g. Privacy Seal of the Independent Centre

for Privacy Protection Schleswig-Holstein (IPP) [15], European Privacy Seal (EuroPriSe) [16]), although they might not be fully applied, as the overall evaluation shall remain affordable.

This module particularly applies, if data from the MSE support tool is stored at the manufacturer's site.

Mod. 5) Application Security

- If the MSE support tool makes use of web applications (e.g. in case of SaaS), these web applications are evaluated by a security specialist for vulnerabilities.
- In case of application security, particular specifications are also considered (e.g. Open Web Application Security Project (OWASP) specifications [17, 18]).

Mod. 6) Specific Security Analyses

- The installation of the MSE support tool at the customer's site might imply the necessity for specific security analyses. For instance, in case of database usage with the MSE support tool, the security of the database will be object of investigation. In general, the security management and the infrastructure-related, organizational, personal and technical security measures, which are needed in order to establish and maintain security, are considered. However, the activities within this evaluation module highly depend on specifics either on the customer's or on the manufacturer's site. Hence, these activities are customized under consideration of existing requirements.

Mod. 7) Specific Requirements of Particular Branches of Trade or Government Authorities

Particular branches of trade (e.g. finance sector) or government authorities might have specific requirements to the MSE support tool, which have to be implemented by the tool's manufacturer and have to be fulfilled by the tool.

Mod. 8) On-Site Audit

- An auditor visits the manufacturer's site for an on-site audit. During this on-site audit, particular evaluations, which are reasonable under consideration of the MSE support tool, are performed (e.g. network security, security of interfaces, etc.).

This module particularly applies, if parts of the MSE support tool or the complete tool or customer data from the MSE support tool is operated / stored at the manufacturer's site (e.g. in case of SaaS).

Mod. 9) Certification

- The results and findings of the evaluated modules (*Mod. 1)* to *Mod. 8))* are documented in a comprehensible way. The findings of the evaluated modules are re-evaluated by the certification body which is fully independent of auditors, software / test engineers and security experts.
- If the MSE support tool successfully passes the evaluated modules (*Mod. 1)* to *Mod. 8))* and the re-evaluation by the certification body, a certificate for the evaluated operational environment and version of the MSE support tool will be provided by the certification body (i.e. the certificate only applies for a defined operational environment and version of the MSE support tool).
- Surveillance / re-certification are also part of this procedure in order to keep up the certification for the MSE support tool.

Fig. (**2**) shortly summarizes the evaluation methodology.

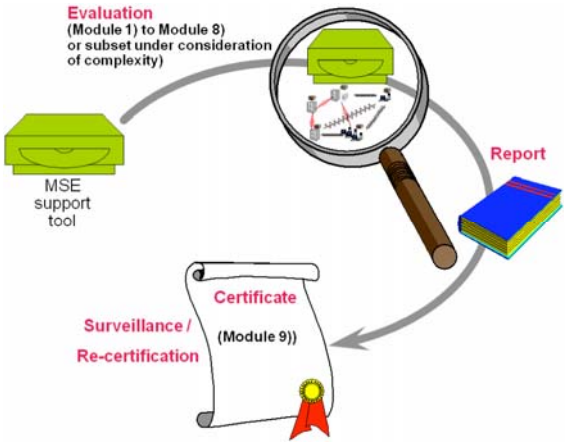

Fig. (2). Evaluation methodology of MSE support tools

Practical experience shows that customers, interested to establish management systems, are also interested in tool support. Under consideration of the variety of available MSE support tools, customers search for decision support in order to choose from the range of existing tools. However, at this point of time, there is not much support available for customers, such as, for instance [19-21]. Consequently, the author feels that there is a lack of support for customers, when faced with the task to make a decision for a particular MSE support tool. The evaluation of MSE support tools, which is made round by a certification of the investigated tool, effectively supports the customer during the decision process for a particular tool. As a certification process is a transparent process, the customer is able to comprehend the criteria, which form the basis for the evaluation and certification of the MSE support tool.

INITIAL RESULTS

Initial analyses on demo versions of several ISO 27001 MSE support tools provided various findings. A subset of these findings is depicted hereafter.

- The tools do not fully cover the ISO 27001 standard.
- The tools display the standard in an erroneous and faulty way.
- The tools generate SoAs which will not be accepted by an auditor.
- The risk assessment methodology of the tools is faulty. It suffers from a lack of plausibility (e.g. risks are calculated for weaknesses without existence of a corresponding threat) and outrages the standard (e.g. no residual risk is calculated).
- Regarding the risk treatment plan, no priorities are assigned and there is no possibility for the tool's user to assign priorities.

- The handling of some of the analyzed tools needs improvement with regard to a user-friendly usability design.
- Some of the analyzed tools showed unknown error messages which might be traced back to an inchoate test process.
- The highly sensitive ISMS data of companies, who decide to use tools in terms of SaaS, is stored on servers in Brazil or in the US without any information on these servers' environment (e.g. trusted data centers, etc.).

The discovered findings comprise significant observations which can seriously affect an organization that decides to apply one of these non-certified MSE support tools. For instance, the certification of an organization's ISMS might be jeopardized or sensitive intra-organizational information might be misused, if the MSE support tool is faulty or vulnerable. Consequently, an evaluation and certification of such MSE support tools is desirable with benefits for the manufacturer as well as for the customer.

BENEFITS

Tool manufacturers as well as the customer benefit from an evaluation of the MSE support tool plus certification.

- An objective and neutral assessment is performed, i.e. the MSE support tool is objectively checked and analyzed by an independent third party.
- Expert evaluations are performed, i.e. the analysis of the tool is performed by declared experts. These experts are objective and neutral auditors as well as software quality, usability / test / security experts. The involvement of auditors of the corresponding international standard is especially advantageous – as these are the experts who finally audit the established management systems and recommend for a certification or not.
- The results of the evaluation are reproducible, comparable and comprehensible, as a defined and published set of rules is applied.
- Market entrance / penetration can be facilitated for the manufacturer of the MSE support tool, because customers can trust evaluated and certified products.
- Failures with regard to the implementation of the corresponding international standard within the MSE support tool can be identified and eliminated. If these failures within the MSE support tool are significant, they will result in failures within the organization's management system and might prevent the institution from getting certified. A failed certification, which can be traced back to a failure within the applied ISMS tool, might result in serious difficulties. In this context, it has to be considered that the institution, which applied the tool, already had purchase costs for the tool. Time and resources were spent to get familiar with tool usage and model the management system with the tool, and furthermore, the costly certification process itself might be broken off.

  Weaknesses of the MSE support tool (e.g. within the software development process or with regard to usability, privacy, security, etc.) can be identified and can be optimized or eliminated subsequently, which ensures an early reaction to possibly disadvantageous developments in the future.
- With a certified tool, the manufacturer of the MSE support tool can significantly increase the likelihood of the customer that a certification of the management system can be accomplished by competent and proper use of a certified tool. Nevertheless, a certified tool cannot guarantee certification (e.g. the user of the tool might make significant mistakes which prohibit certification, and moreover, a management system has to be established as an agile system within the organization – this cannot be achieved by the mere application of a tool).
- The certificate itself is the visible sign of a successful evaluation according to comprehensible criteria and provides a public-oriented confirmation of state-of-the-art development processes resulting in high product quality as well as trust into the assessed MSE support tool. Consequently, customers can have confidence in certified MSE support tools.

CONCLUSION

The establishment and operation of a certified management system according to an international standard is a complex project for an organization. Support is desired and can be represented by consultants and / or by MSE support tools.

This article presented an evaluation methodology plus certification scheme for MSE support tools. Under consideration of initial evaluation results of some MSE support tools, evaluation and certification of MSE support tools is recommendable in order to implement the described benefits into these tools. An organization can have confidence in MSE support tools which are certified according to comprehensible and revealed criteria.

In the near future, the author intends to further elaborate on the presented approach in order to also evaluate other types of support software, such as support tools for project management or process management. As the aforementioned management tasks also pose challenges to organizations, tool support is also desirable. However, in order to get maximum benefit from the usage of support tools, the application of *certified* tools is recommended.

ACKNOWLEDGEMENTS

The author wants to acknowledge fruitful discussions and / or valuable contributions of Adrian Altrhein, Hans Günter Siebert, Antonius Sommer, Tim Reichert, Thomas Sterzenbach, Werner Achtert, Herbert Schippers, Wolfgang Hampe-Neteler, Christoph Sutter, Christian Freckmann and Simone Achtert – all with TÜV Informationstechnik GmbH (TÜViT).

GLOSSARY

Audit

Evaluation whether international standards are maintained. Evaluation of documents and on-site visits are included, and the results are documented.

Auditor

An examiner, who is registered and monitored by a certification body for particular international standards. Auditors are recognized experts who have to fulfill strong requirements (e.g. significant professional experience, continuous trainings, experience exchanges organized by the certification body, monitoring by the certification body, etc.). The auditor is allowed to perform audits.

Certificate

The visible sign that a product, a procedure or a service fulfills specified requirements (e.g. requirements from international standards). The certificate is passed to the manufacturer / provider of the product, procedure or service and can be published.

Certification

The certification body critically assesses an evaluation of a product, procedure or service and its results. Depending on the results of this assessment, the certification body confirms / does not confirm that a product, a procedure or a service fulfills specified requirements.

Certification Body

An independent third party which performs certifications.

Compliance

Fulfillment of an international standard or normative requirements.

REFERENCES

[1] Deutsches Institut für Normung e.V. (DIN), Quality management systems – Requirements (ISO 9001:2008), Trilingual version EN ISO 9001:2008, DIN, 2008.

[2] International Standardization Organization (ISO). Information technology — Security techniques — Information security management systems — Requirements (ISO 27001:2005), ISO/IEC, 2005.

[3] International Standardization Organization (ISO), Information technology — Service management — Part 1: Specification (ISO 20000-1:2005), ISO/IEC, 2005.

[4] Compliance Express: ISO 9000:2000 Express™2008, December 2008. [Online] Available: www.complianceexpress.com [Accessed Dec. 17, 2008].

[5] Ovitz Taylor Gates: The ISO 9000 Toolkit, December 2008. [Online] Available: www.manager-tool.com/TheISO9000Toolkit.html [Accessed Dec. 17, 2008].

[6] easy9001.com, All-In-One Easy ISO 9001 Toolkit™, December 2008. [Online] Available: www.iso9001.com [Accessed Dec. 17, 2008].

[7] realiso, RealISMS, December 2008. [Online] Available: www.realiso.com/realisms/ [Accessed Dec. 17, 2008].

[8] SerNet, Verinice, December 2008. [Online] Available: www.verinice.org [Accessed Dec. 17, 2008].

[9] plan42 gmbh it consulting, taurus27001, December 2008. [Online] Available: www.plan42.com/de/ [Accessed Dec. 17, 2008].

[10] EasyAccess Business Solutions Inc., Biz, December 2008. [Online] Available: www.EasyAccess.biz [Accessed Dec. 17, 2008].

[11] iET Solutions, iET ITSM, December 2008. [Online] Available: www.iet-solutions.de [Accessed Dec. 17, 2008].

[12] plan42 gmbh it consulting, taurus20000, December 2008. [Online] Available: www.plan42.com/de/ [Accessed Dec. 17, 2008].

[13] International Standardization Organization (ISO), Software Engineering – Software Product Quality Requirements and Evaluation (SQuaRE) – Requirements for Quality of Commercial-Off-The-Shelf (COTS) Software Product and Instructions for Testing (ISO 25051:2006), ISO/IEC, 2006.

[14] International Standardization Organization (ISO), Ergonomics of human-system interaction (series of norms), (ISO 9241:200x), ISO/IEC, 2002-2008.

[15] Independent Centre for Privacy Protection Schleswig-Holstein (ICPP), Privacy Seal, December 2008. [Online] Available: www.datenschutzzentrum.de/ [Accessed Dec. 20, 2008].

[16] European Privacy Seal (EuroPriSe), December 2008. [Online] Available: https://www.european-privacy-seal.eu/ [Accessed Dec. 20, 2008].

[17] Open Web Application Security Project (OWASP), A Guide to Building Secure Web Applications and Web Services, December 2008. [Online] Available: www.cgisecurity.com/owasp/html/. [Accessed Dec. 20, 2008].

[18] Open Web Application Security Project (OWASP), OWASP Testing Guide v2, December 2008. [Online]Available: www.owasp.org/index.php/OWASP_Testing_Guide_v2_Table_of_Contents [Accessed Dec. 20, 2008].

[19] H.K.N. Leung, K.C.C. Chan, C. Poon. "Software tools for ISO 9000 certification", *Managerial Auditing Journal*, Vol. 4(12), pp. 51-57, July 1999.

[20] C.K. Cabak. "Choosing quality management software for ISO 9000", Quality Digest, November 1997. [Online] Available: www.qualitydigest.com/nov97/html/cover.html [Accessed March 15th 2009].

[21] Simple Quality, Frequently Asked Questions About ISO 9000, March 2009. [Online]Available: www.simplyquality.org/faq09.htm [Accessed March 15th 2009].

Received: December 31, 2008 Revised: March 30, 2009 Accepted: April 03, 2009