Exposé der Bachelorarbeit

Forschungsgruppe Knowledge Engineering

Fakultät für Informatik

Universität Wien

TITEL:

Name:
Matrikelnummer:
Erstellung des Exposés:
Studiengang: Wirtschaftsinformatik
Betreuer: o. Univ.Prof. Dr. Dimitris Karagiannis

1. Konzept

1.1. Ausgangslage und Zielsetzung

Es gibt derzeit schon viele ISMS-Tools auf dem Markt, doch nicht alle erfüllen den selben Standard oder beinhalten dieselben Komponenten. Eines der Ziele dieser Bachelorarbeit ist es, einen Überblick über die aktuell auf dem Markt verfügbaren ISMS-Tools zu geben und diese nach einem selbst erstellten Kriterienkatalog zu vergleichen. Diese Kriterien umfassen u.a. die unterstützten Informationssicherheitsstandards, die unterstützten Workflows und die verfügbaren Reports.

Das zweite Ziel ist es, ein konzeptionelles Metamodell zu erstellen, in dem eine Integration des Metamodells von ISMS-Lösungen mit dem von EA-Standards stattfindet. Teile dieses konzeptionelle Metamodell werden dann mittels ADOxx implementiert und durch aussagekräftige Beispielmodelle präsentiert. Bereits vorhanden sind hier ein paar EA-Frameworks, die einen ISMS-Standard integriert haben oder Erweiterungen anbieten, wie z.B. das Zachman-Framework mit SABSA, sowie TOGAF und Archimate mit Erweiterungen, die Teile der ISMS-Anforderungen abdecken.

Als Informationsgrundlage wird diese Arbeit auch Theorie zu ISMS, ISMS-Standards und ISMS-Frameworks umfassen, in denen erläutert wird, was ein ISMS ist, warum es notwendig ist und wie man es zertifizieren lässt. Außerdem wird erklärt was sowohl die ISMS-Standards ISO/IEC 27001 und BSI IT-Grundschutz, als auch die ISMS-Frameworks SABSA, ITIL und COBIT 5 alles beinhalten.

1.2. Methoden und Vorgehen

Bezüglich der Informationsgrundlage wird eine ausführliche Literaturrecherche mittels U:Search, IEEE Xplore, Springer und ScienceDirect durchgeführt. Außerdem werden im Rahmen einer Onlinerecherche die Webseiten der verschiedenen Standards und auch andere Internetquellen herangezogen, um die aus den anderen Quellen erworbenen Informationen zu unterstreichen.

Um den derzeitigen Stand der ISMS-Tools auf dem Markt zu ermitteln wird eine Google-Suche mit den Stichwörtern ‚ISMS-Tools', ‚Information Security Management System Tools', ‚ISO 27001 Tools' und ‚IT-Grundschutz Tools' vorgenommen. Hier nutze ich ebenfalls schon vorhandene Tool-Vergleiche, und die Webseiten der Tool-Anbieter. Für weitere Informationen über die Tools bzw. Demo-Versionen, werde ich, falls nicht vorhanden, bei dem Anbieter anfragen.

Um die Tools optimal vergleichen zu können, wird am Anfang ein aussagekräftiger Kriterienkatalog erstellt, der sowohl allgemeine (z.B. Kosten, Zielgruppe und Support), funktionale (z.B. verfügbare Reports und unterstützte Workflows), als auch technische (z.B. Systemanforderungen) Kriterien enthalten wird. Je nachdem ob es möglich ist die Tools auszuprobieren, wird auch die Benutzeroberfläche und -freundlichkeit bewerten. Anschließend werde ich alle gefundenen Tools mittels der Kriterien vergleichen.

Um mich mit ADOxx auseinander zu setzen, werde ich einerseits die Software runterladen, andererseits die auf der Webseite verfügbaren Dokumentationen und Tutorials heranziehen. Nach einer Einarbeitungszeit werde ich dann das konzeptionelle Metamodel in ADOxx implementieren.

1.3. Erwartete Ergebnisse

Das erwartete Ergebnis dieser Bachelorarbeit ist ein Kriterienkatalog und ein Vergleich der vorhandenen ISMS-Tools anhand dieser Kriterien. Außerdem soll am Ende ein konzeptionelles Metamodell und eine prototypische Implementation dieses Metamodells mit ADOxx vorhanden sein.

1.4. Zielgruppe

Die Zielgruppen dieser Bachelorarbeit sind sowohl alle Unternehmen, die Interesse an einem Informationssicherheitsmanagement-System haben, als auch Hersteller von ISMS-Tools, die sich einen Überblick über die derzeitige Marktsituation bzgl. ISMS-Tools machen möchten bzw. Leser, die sich über die ISMS-Standards ISO/IEC 27001 und BSI IT-Grundschutz oder die ISMS-Frameworks SABSA, COBIT 5 und ITIL informieren möchten. Auch Forscher, die mehr über die Integration von ISMS-Lösungen in EA-Standards erfahren möchten, sind bei diesem Paper richtig.

1.5. Erfordernisse

Für den Toolvergleich werde ich einige der Tools als Demo-Version zum Testen benötigen. Falls das nicht möglich ist, werde ich meine Vergleiche rein aus den vorhandenen Informationen ziehen. Für das Metamodel und die Implementierung werde ich ADOxx benötigen.
Für die Literatur- und Onlinerecherche benötige ich die Zugriffsberechtigungen auf den Literaturbestand der Universität Wien und Internetzugang.

1.6. Eigene Motivation

Informationssicherheit ist ein wichtiges Thema in der heutigen Gesellschaft und wird immer wichtiger. Deshalb ist es so wichtig Informationssicherheitsmanagement-Systeme in das Unternehmen zu integrieren. Das klingt einfach, ist es jedoch nicht. Mit dieser Bachelorarbeit kann ich Unternehmen eine grobe Übersicht über alle notwendigen Informationen und Tools geben, die sie benutzen können. Außerdem ist es derzeit noch nicht allgemein üblich, dass eine ISMS-Lösung in ein EA-Standard integriert wird. Deshalb ist es spannend dies mithilfe von ADOxx auszuprobieren.

Da ich mich sowohl für das Thema Sicherheit als auch für das Thema Enterprise Architecture während des Studiums zu interessieren begonnen habe, ist diese Kombination genau das richtige für mich.

2. Zeitplan

	Tätigkeit	**Von**	**bis**
1	Literatur- und Onlinerecherche	05.10.2017	10.10.2017
2	Kriterienkatalog, Toolrecherche, Exposé	11.10.2017	17.10.2017
3	Einleitung, Related Work, ISMS (Kapitel1-3)	18.10.2017	25.10.2017
4	ISMS-Standards (Kapitel 4)	26.10.2017	31.10.2017
5	ISMS-Frameworks (Kapitel 5)	01.11.2017	05.11.2017
6	Marktübersicht Tools (Kapitel 6)	06.11.2017	20.11.2017
7	Informieren über EA-Frameworks	21.11.2017	26.11.2017
8	Integration mit EA-Framework (Kapitel 7)	27.11.2017	18.12.2017
9	Installation und Einarbeitung in ADOxx	19.12.2017	24.12.2017
10	Prototypische Implementierung (Kapitel 8)	25.12.2017	31.01.2017

3. Gliederung

1. Introduction
2. Related Work
3. Information Security Management System
    a. What is an ISMS?
    b. Why do you need an ISMS?
    c. Certification
4. ISMS-Standards
    a. ISO /IEC 27001
    b. BSI IT-Grundschutz
5. ISMS-Frameworks
    a. SABSA
    b. ITIL
    c. COBIT 5
6. Market overview of the current tools
    a. Criteria
    b. Selected tools
    c. Comparison of the tools
7. Integration with EA-Frameworks/Solutions
    a. Meta model of ISMS-Solutions
    b. Meta model of EA-Standards
    c. Conceptual meta model
8. Prototypical Implementation
    a. ADOxx
    b. Preparation and Approach
    c. Implementation
9. Conclusion

References

4. Auswahlbibliografie

Onlinesicherheit – iso/iec. https://www.onlinesicherheit.gv.at/experteninformation/normen_und_standards/iso-iec_27000/71519.html. Accessed: 2017-10-10

ISO/IEC 2016. International standard iso/iec 27000, information technology - security techniques - information security management systems - overview and vocabulary. Fourth edition, 02 2016

Reza Alavi, Shareeful Islam and Haralambos Mouratidis. A Conceptual Framework to Analyze Human Factors of Information Security Management System (ISMS) in Organizations, pages 297 – 305. Springer International Publishing, Cham, 2014.

A. Asosheh, P. Hajinazari, and H. Khodkari. A practical implementation of isms. In 7th International Converence on e-Commerce in Developing Countries: with focus on e-Security, pages 1-17, April 2013.

Kristian Beckers, Maritta Heisel, Bjornar Solhaug, and Ketil Stolen. ISMS-CORAS: A Structured Method for Establishing an ISO 27001 Compliant Information Security Management System, pages 315-344, Springer International Publishing, Cham, 2014.

Gerd Brunner. Neue Version Cobit 5 untestützt Security nach ISO 27001. Computerwelt, 2013(10).

Jason S. Burkett. Business security architecture: Weaving information security into your organization's enterprise architecture through sabsa. Information Security journal: A Global Perspective, 01 January 2012, Vol. 21(1), p.47-54.

Alan Calder. ISO 2700 and ISO 17799, pages 169-179. John Wiley Sons, Inc., 2008.

Z. Cosic and M. Boban. Information security management x2014; defining approaches to information security policies in isms. In IEEE 8th International Symposium on Intellligent Systems and Informatics, pages 83-85, Sept 2010.

Georg Disterer. Iso/iec 27000, 27001 and 27002 for information security management. Journal of Information Security, 2013, Vol.07(02), pp.92-100.

Bundesamt für Sicherheit in der Informationstechnik. Bsi-standard 200-1. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_1.pdf?__blob=publicationFile&v=2. Accessed: 2017-10-11.

Bundesamt für Sicherheit in der Informationstechnik. Bsi-standard 200-2. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.pdf?__blob=publicationFile&v=3. Accessed: 2017-10-11.

Bundesamt für Sicherheit in der Informationstechnik. Bsi-standard 200-3. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_3.pdf?__blob=publicationFile&v=3. Accessed: 2017-10-11.

Constantine Gikas. A general comparison of fisma, hipaa, iso 27000 and pci-dss standards. Information Security Journal: A Global Perspective, 19(3):132-141; 2010.

V. Hensel and K. Lempke-Rust. On an integration of an information security management system into an enterprise architecture. In 2010 Workshops on Database and Expert Systems Applications, pages 354-358; Aug 2010.

Edward Humphreys. Information security management system standards. Datenschutz und Datensicherheit – DuD, 35(1):7-11, Jan 2011.

Martina Jakabova, Jana Urdzikova, and Emilia Mironovova. Standardization of information security management system: Iso/iec 27001:2005, itil, cobit. International Journal of Recent Contributions from Engineering, Science IT (iJES), 11/9/2013, Vol.1(2), p.11.