Fachhochschule Brandenburg
University of Applied Sciences

Fachbereich Wirtschaft

Security Management

Sommersemester 2012

Semesterarbeit 2

Dozent:

Professor Dr. Friedrich Holl

Thema:

Ermittlung von Qualitätsanforderungen für Prozessimplementierungen des informationssicherheitsbezogenen Risikomanagements

Autor: Patrick Sauer
Matrikelnummer: 20108005
Datum: 07.06.2012

Inhaltsverzeichnis

1 Einleitung 3
2 Vorgehensmodelle für ein Risikomanagement 4
2.1 Allgemeine Ablaufbeschreibung 4
2.2 ISO 27005 5
2.3 NIST SP 800-30 7
2.4 BSI 100-3 8
2.5 OCTAVE-Methode der Carnegie Mellon University 9
3 Zusammenfassung und Fazit 10
4 Literaturverzeichnis 11
5 Abbildungsverzeichnis 12

1 Einleitung

Unter dem Begriff „Informationssicherheit“ wird das Sicherstellen der „Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen“[1] verstanden. Informationen sind verschiedenen Risiken ausgesetzt, die einen Verlust in den zuvor genannten Kategorien bewirken können.[2] Eines dieser Risiken besteht dabei immer aus einer Bedrohung, die durch eine vorhandene Schwachstelle ein Informationsgut gefährdet[3] und einem Unternehmen dadurch Schaden zufügen kann. Zentraler Bestandteil eines allgemeinen Informationssicherheitsmanagements ist deshalb ein Information Security Risk Management.[4] Ein solches wird je nach Vorgehensmodell, zu beachtenden Standards oder internationaler Normen unterschiedlich umgesetzt.[5] Grundsätzlich aber beinhaltet jedes Risikomanagement einen kontinuierlichen Verbesserungsprozess und kann nicht mit einer nur einmaligen Risikoanalyse umgesetzt werden.[6]

In seinem Buch „The Failure of Risk Management“ stellt der Verfasser Douglas W. Hubbard die Effektivität von Risikomanagementmodellen in Frage, da im Allgemeinen von Unternehmen nicht geprüft wird, ob ihre Managementmodelle die Sicherheit tatsächlich erhöhen.[7] Er erhebt deshalb die Forderung, dass eine Organisation wissen muss, ob ihr Risikomanagement funktioniert und über die notwendige Qualität verfügt.[8] Man kann zwar verschiedene Kennzahlen zur IT-Sicherheit ermitteln; diese sind jedoch oftmals technischer Ausprägung, vernachlässigen organisationsspezifische Eigenschaften und verfügen über eine zu geringe Aussagekraft, um die ganzheitliche Sicherheit von Informationen in einem Unternehmen zu beschreiben.[9] Da, wie zuvor dargelegt wurde, die Sicherheitsbemühungen mehr als Prozess zu sehen sind, sollte eher der Prozess bewertet werden.[10]

Die vorliegende Seminararbeit hat zum Ziel, Qualitätsanforderungen für Implementierungen eines Risikomanagements zu definieren. Diese Anforderungen sollen durch die Betrachtung unterschiedlicher Ausprägungen von nationalen und internationalen Vorgehensmodellen ermittelt werden. Dazu wird zunächst das Risikomanagement allgemein definiert, um anschließend die Unterschiede von Vorgehensmodellen zu ermitteln. Soweit in der Fachliteratur dazu Meinungen von Autoren mit Praxiserfahrung vorhanden sind, sollen diese zusätzlich aufgenommen werden. In einer weiterführenden Master-Arbeit sollen – aufbauend auf diesen Qualitätsanforderungen – mögliche prozessorientierte Kennzahlen zur Messung des Risikomanagements ermittelt werden.

[1] Deutsches Institut für Normung e.V., 2008, Seite 9.
[2] Vgl. Wheeler, 2011, Seite 23.
[3] Vgl. Landoll, 2011, Seite 366.
[4] Vgl. Klipper, 2011, Seite 3.
[5] Vgl. Kouns, et al., 2010, Seite 7 f.
[6] Vgl. Klipper, 2011, Seite 24 f.
[7] Vgl. Hubbard, 2009, Seite 3.
[8] Vgl. Hubbard, 2009, Seite 37 f.
[9] Vgl. Wheeler, 2011, Seite 35 f.
[10] Vgl. Wheeler, 2011, Seite 36.

2 Vorgehensmodelle für ein Risikomanagement

Es gibt verschiedene Vorgehensmodelle des Risikomanagements, die von Behörden verschiedener Staaten, privaten Unternehmen oder internationalen Normungsgremien veröffentlicht werden.[11] Aufgrund des limitierten Umfangs dieser Semesterarbeit beschränkt sich die Darstellung auf die Vorgehensmodelle der folgenden Institutionen:

- International Organization for Standardization (ISO)
- National Institute of Standards and Technology (NIST)
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Software Engineering Institute der Carnegie Mellon University (SEI).

Durch diese Auswahl werden eine international geltende Norm der ISO, die nationalen Standards von Deutschland und den USA sowie ein weiteres Modell einer Universität vorgestellt, sodass ein breiter und internationaler Überblick von möglichen Vorgehensweisen gegeben wird.

2.1 Allgemeine Ablaufbeschreibung

Die meisten Vorgehensmodelle zum Risikomanagement definieren einen Verbesserungsprozess bzw. ein Lebenszyklusmodell und beinhalten in der Regel folgende Schritte:[12]

1. Eine Beschreibung der benötigten Ressourcen und eine Definition der Risikotoleranz in einer Organisation
2. Ein Risk Assessment, in dem Informationsgüter, Schwachstellen, Bedrohungen und Risiken identifiziert und bewertet werden
3. Einen Entscheidungsprozess, wie mit identifizierten Risiken umgegangen wird
4. Die Dokumentation vorangegangener Entscheidungen
5. Die Implementierung von geplanten Maßnahmen
6. Eine Kontrolle bzw. Validierung, ob die getroffenen Maßnahmen wirken.
7. Eine Überwachung, ob sich die Risikosituation verändert hat.

Die Risikoidentifizierung und -bewertung sowie die danach notwendige Risikobehandlung sind zentrale Bestandteile der Risikoanalyse. Zur Bewertung von Risiken ist entweder eine quantitative Datenermittlung oder eine qualitative Schätzung notwendig, um die Auswirkungen und die Eintrittswahrscheinlichkeiten zu ermitteln.[13] Nach Abschluss der Risikobewertung gibt es grundsätzlich vier Möglichkeiten, wie ein Unternehmen in der Folge mit einzelnen Risiken umgehen kann: Risikovermeidung, Risikoreduktion, Risikoakzeptanz und Risikotransfer.[14]

[11] Vgl. Kouns, et al., 2010, Seite 113.
[12] Vgl. Wheeler, 2011, Seite 46.
[13] Vgl. Wheeler, 2011, Seite 105 und 123.
[14] Vgl. Wheeler, 2011, Seite 151.

2.2 ISO 27005

Die ISO 27005 definiert im Rahmen der ISO 27000-Serie das Risikomanagement für das Informationssicherheitsmanagement nach ISO 27001[15] und ist ein zentraler Baustein des kontinuierlichen Verbesserungsprozesses Plan – Do – Check – Act dieser Norm.[16]

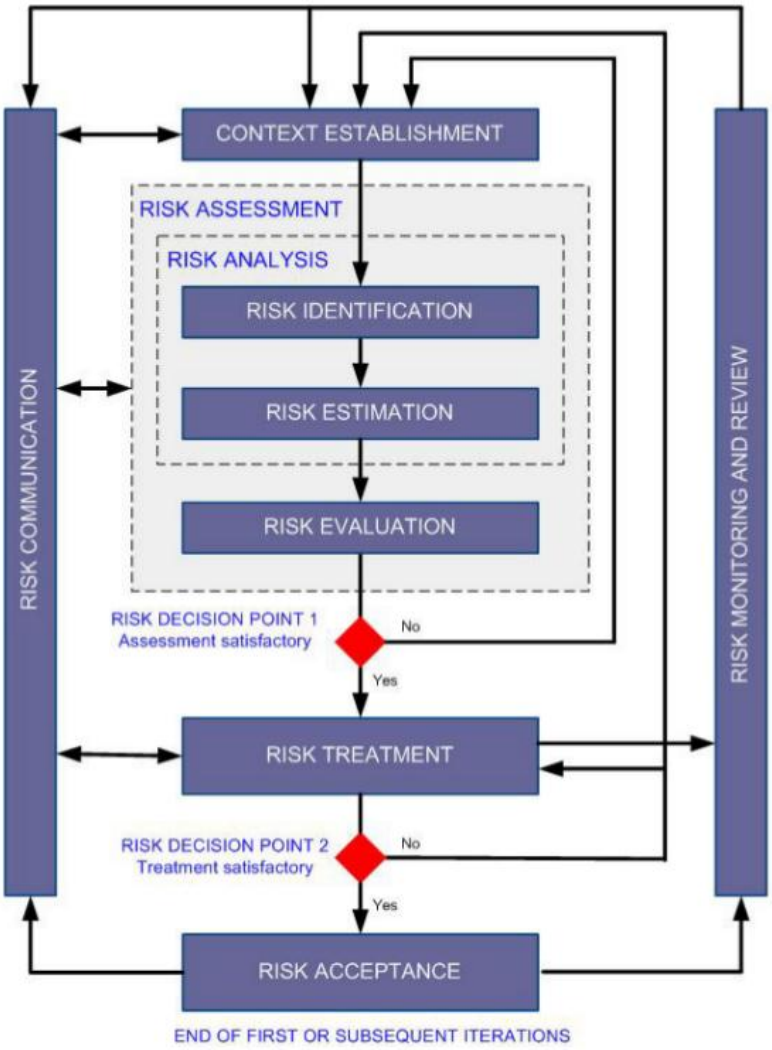

Abbildung 1: Vorgehensmodell nach ISO 27005.[17]

Vor der eigentlichen Risikoanalyse steht bei der ISO 27005 die Definition von verschiedenen Basiskriterien für den weiteren Managementprozess:[18]

- Kriterien für die Risikoevaluation
- Kriterien für Auswirkungen von Risiken
- Kriterien für eine Risikoakzeptanz.

[15] Vgl. Klipper, 2011, Seite 5.
[16] Vgl. Kouns, et al., 2010, Seite 79.
[17] Deutsches Institut für Normung e.V., 2008, Seite 5.
[18] Vgl. British Standards Institution, 2008, Seite 7 f.

In Verbindung mit der in der Risikoanalyse geforderten Identifikation der relevanten Assets[19] wird durch die Definition der Basiskriterien ein auf eine Organisation oder ein Unternehmen zugeschnittenes Risikomanagement erreicht.

Besondere Relevanz weisen die Aspekte Risikokommunikation und Risikoüberwachung auf, die in der Abbildung den optischen Rahmen für die Risikoanalyse bilden. Die Kommunikation soll sicherstellen, dass Informationen über Risiken zwischen den am Prozess Beteiligten geteilt bzw. ausgetauscht werden.[20] Sebastian Klipper, der Verfasser des Buchs ‚Information Security Risk Management; Risikomanagement mit ISO 27001, 27005 und 32010', betrachtet diesen Punkt genauer, indem er das Konfliktpotenzial der Kommunikation im Allgemeinen und jenes der Risikokommunikation speziell aufzeigt.[21] Überwachung und Kontrolle von Risiken berücksichtigen die Tatsache, dass Risiken kein statischer Zustand sind, sondern sich die Risikosituation schnell – und ohne Vorwarnung – ändern kann.[22]

Die beschriebenen Eigenschaften der ISO 27005 werden als folgende Qualitätsanforderungen aufgenommen:

- Das Risikomanagement muss durch die Definition von Basiskriterien auf die spezifische Situation einer Organisation zugeschnitten werden.
- Eine konfliktfreie Risikokommunikation ist notwendig, um den Informationsfluss über Risiken sicherzustellen.
- Risiken müssen überwacht werden, damit ein Unternehmen auf Veränderungen der Risikosituation schnell reagieren kann.

[19] Vgl. British Standards Institution, 2008, Seite 10.
[20] Vgl. British Standards Institution, 2008, Seite 21 f.
[21] Vgl. Klipper, 2011, Seite 163.
[22] Vgl. British Standards Institution, 2008, Seite 22.

2.3 NIST SP 800-30

Die Special Publication 800-30 des National Institute of Standards and Technology der USA beschreibt den Risikomanagementprozess in neun Schritten.[23] Die SP 800-30 gibt selbst Empfehlungen zur Umsetzung und definiert Erfolgsfaktoren.[24] Diese beinhalten neben in anderen Standards aufgeführte Punkten noch die folgenden:[25]

- Die Risikoanalyse sollte mindestens dreimal jährlich durchgeführt werden und auch alle größeren Änderungen der Infrastruktur zeitnah analysieren.
- Die Unterstützung des Senior Managements ist notwendig.
- Das Assessment-Team muss über eine ausreichende Kompetenz zur Durchführung von Bewertungen verfügen.

Die bisherigen Qualitätsanforderungen werden um die aufgeführten drei Aspekte erweitert.

[23] Vgl. National Institute of Standards and Technology, 2002, Seite 9.
[24] Vgl. Kouns, et al., 2010, Seite 99.
[25] Vgl. National Institute of Standards and Technology, 2002, Seite 41.

2.4 BSI 100-3

Der BSI-Standard 100-3 des Bundesamts für Sicherheit in der Informationstechnik definiert die Vorgehensweise einer Risikoanalyse auf der Basis des eigenen IT-Grundschutzes.[26] Hinter dem IT-Grundschutz steht das Konzept, dass das BSI bereits eine Risikoanalyse – ausgehend von einem normalen Schutzbedarf – durchgeführt hat, und eine weitere Risikoanalyse nur noch dann ergänzend erforderlich ist, wenn für Informationen oder IT-Systeme ein höherer oder sehr hoher Schutzbedarf im Rahmen des Sicherheitsprozesses nach BSI festgestellt wurde.[27]

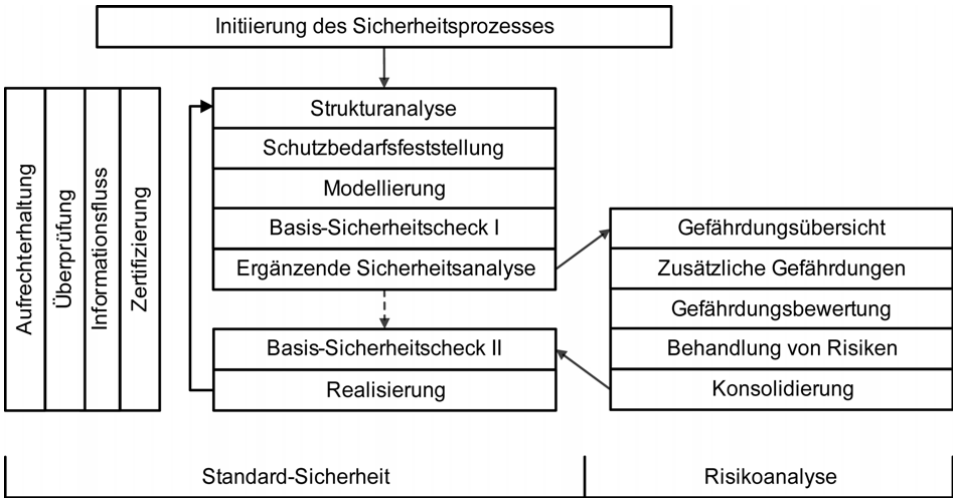

Abbildung 2: Risikoanalyse im Rahmen von IT-Grundschutz.[28]

Als Besonderheit betrachtet der Standard nicht explizit Wahrscheinlichkeiten von Risiken, sondern behandelt diese nur implizit bei der Analyse von Gefährdungen, wodurch Bedrohungen, Eintrittswahrscheinlichkeiten und Auswirkungen nicht näher differenziert werden.[29] Die Vorgehensweise des BSI 100-3 ist bei der Ermittlung von Gefährdungen inhaltlich auf die Grundschutzkataloge ausgerichtet.[30] In ihnen werden verschiedene mögliche Bedrohungen aufgelistet.[31] Durch diese Vorgehensweise wird erreicht, dass bei jeder Risikoanalyse mindestens die dort erfassten Gefährdungen und folglich dieselben Risiken bewertet werden. Aufgrund dieser Ausprägung des Standards wird folgende Qualitätsanforderung abgeleitet:

Die Sammlung von Risiken soll in ihrer Grundlage (aber nicht ausschließlich) auf anerkannten Sammlungen, Katalogen oder Checklisten zur Ermittlung von Bedrohungen aufbauen.

[26] Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2008, Seite 4 f.
[27] Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2008, Seite 34.
[28] Bundesamt für Sicherheit in der Informationstechnik, 2008, Seite 5.
[29] Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2008, Seite 5.
[30] Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2008, Seite 3.
[31] Vgl. Kouns, et al., 2010, Seite 137.

2.5 OCTAVE-Methode der Carnegie Mellon University

Die OCTAVE-Methode des Software Engineering Institute der Carnegie Mellon University besteht aus den drei folgenden Phasen:[32]

1. Erstellung von informationsgüterbezogenen Risikoprofilen
2. Identifizierung von Schwachstellen
3. Entwicklung bzw. Planung von Sicherheitsstrategien.

Zentraler Baustein der OCTAVE-Methode ist ein kleines interdisziplinäres Team, welches die Risikoanalysen durchführt. Dieses aus drei bis fünf Personen bestehende Team soll das Wissen verschiedener Unternehmensteile zusammenführen und sich aus IT-Personal sowie Betriebswirtschaftlern zusammensetzen.[33] Die Auswahl der Mitglieder dieses Analyseteams aus verschiedenen Unternehmensbereichen ist ein Grundpfeiler für eine erfolgreiche Risikoanalyse nach der OCTAVE-Methode.[34] Weitere Erfolgsfaktoren sind die Unterstützung durch das Management, die Definition der Grenzen des Analysebereichs sowie die Auswahl von Teilnehmern aus dem Unternehmen, die das Analyseteam mit ihrem Wissen unterstützen.[35] Die Relevanz der Identifizierung von Wissensträgern zeigt sich nicht zuletzt in der Tatsache, dass sich alleine drei von vier Prozessschritten der ersten Phase der Methode mit der Identifizierung von Wissen und dem Personal, bei dem es vorhanden ist, befassen.[36] Die in der OCTAVE-Methode umgesetzte Wissensbehandlung wird wie folgt als Qualitätsanforderungen aufgenommen:

- Die Analyse muss von einem interdisziplinären Team durchgeführt werden, welches das Wissen und die Personen, bei denen es vorhanden ist, im Unternehmen identifiziert und somit bei den Risiko-Bewertungen auf dieses Wissen zurückgreifen kann.

[32] Vgl. Kouns, et al., 2010, Seite 209 f.
[33] Vgl. Kouns, et al., 2010, Seite 205.
[34] Vgl. Kouns, et al., 2010, Seite 209.
[35] Vgl. CERT, Software Engineering Institute, Carnegie Mellon University, 2003, Seite 1-9.
[36] Vgl. CERT, Software Engineering Institute, Carnegie Mellon University, 2003, Seite iv.

3 Zusammenfassung und Fazit

Nach Betrachtung der Schwerpunkte der vorgestellten Vorgehensweisen ergeben sich Qualitätsanforderungen an das Risikomanagement in den folgenden Feldern: Anpassung, Kommunikation, Aktualität, Unterstützung und Kompetenz/Wissen.[37]

1. Anpassung
   Das Risikomanagement muss durch die Definition von Basiskriterien auf die spezifische Situation einer Organisation zugeschnitten werden.[38]
2. Kommunikation
   Eine konfliktfreie Risikokommunikation ist notwendig, um den Informationsfluss über Risiken sicherzustellen.[39]
3. Aktualität
   a. Risiken müssen überwacht werden, damit ein Unternehmen auf Veränderungen schnell reagieren kann.[40]
   b. Die Risikoanalyse sollte mindestens dreimal jährlich durchgeführt werden und darüber hinaus auch alle größeren Änderungen der Infrastruktur zeitnah analysieren.[41]
4. Unterstützung
   Die Unterstützung des Senior Managements ist für die Risikoanalyse notwendig.[42]
5. Kompetenz/Wissen
   a. Die Sammlung von Risiken soll in ihrer Grundlage (aber nicht ausschließlich) auf anerkannten Sammlungen, Katalogen oder Checklisten zur Ermittlung von Bedrohungen aufbauen.[43]
   b. Das Assessment-Team muss über eine ausreichende Kompetenz zur Durchführung von Bewertungen verfügen.[44]
   c. Die Analyse muss von einem interdisziplinären Team durchgeführt werden, welches das Wissen und die Personen, welche darüber verfügen, im Unternehmen identifiziert und somit bei den Risiko-Bewertungen auf dieses Wissen zurückgreifen kann.[45]

Die in der Einleitung genannte Zielsetzung wurde erreicht, indem unterschiedliche Anforderungen aus den Standards und Normen extrahiert werden konnten. In weiteren Arbeiten bleibt jedoch zu klären, welche Auswirkungen die ermittelten Anforderungen auf die Effizienz eines Risikomanagements haben, und inwieweit die Umsetzung der Anforderungen messbar ist.

---

[37] Die Reihenfolge der Schwerpunktfelder hat keine Relevanz.
[38] Die Anforderung wurde der ISO 27005 entnommen.
[39] Die Anforderung wurde der ISO 27005 entnommen.
[40] Die Anforderung wurde der ISO 27005 entnommen.
[41] Die Anforderung wurde der NIST SP 800-30 entnommen.
[42] Die Anforderung wurde der NIST SP 800-30 entnommen.
[43] Die Anforderung wurde der BSI 100-3 entnommen.
[44] Die Anforderung wurde der NIST SP 800-30 entnommen.
[45] Die Anforderung wurde der OCTAVE entnommen.

4 Literaturverzeichnis

British Standards Institution. 2008. *BS ISO/IEC 27005: Information security risk management.* 2008.

Bundesamt für Sicherheit in der Informationstechnik. 2008. *BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz. Version 2.5.* 2008.

Bundesamt für Sicherheit in der Informationstechnik. 2008. *BSI-Standards 100-1: Managementsysteme für Informationssicherheit.* 2008.

CERT, Software Engineering Institute, Carnegie Mellon University. 2003. *OCTAVE Method Implementation Guide Version 2.0.* 2003. Abgerufen am 02.04.2012. http://www.cert.org/octave/.

Deutsches Institut für Normung e.V. 2008. *DIN ISO/IEC 27001:2008 Informationssicherheit-Managementsysteme.* 2008.

Hayden, Lance. 2010. *IT Security Metrics.* New York : McGraw-Hill, 2010.

Hubbard, Douglas W. 2009. *The Failure of Risk Management.* New Jerse : John Wiley & Sons, 2009.

Jaquith, Andrew. 2007. *Security Metrics.* Boston : Pearson, 2007.

Klipper, Sebastian. 2011. *Information Security Risk Management.* Wiesbaden : Vieweg+Teubner, 2011.

Kouns, Jake und Minoli, Daniel. 2010. *Information Technology Risk Management In Enterprise Environments.* New Jersey : John Wiley & Sons, 2010.

Landoll, Douglas J. 2011. *The Security Risk Assessment Handbook.* Boca Raton : CRC Press, 2011.

National Institute of Standards and Technology. 2002. *NIST SP 800-30: Risk Management Guide for Information Technology Systems.* 2002.

Wheeler, Evan. 2011. *Security Risk Management.* Waltham : Syngress, 2011.

5 Abbildungsverzeichnis

Abbildung 1: Vorgehensmodell nach ISO 27005. 5
Abbildung 2: Risikoanalyse im Rahmen von IT-Grundschutz. 8