

Zürcher Hochschule
für Angewandte Wissenschaften



Zürcher Hochschule für Angewandte Wissenschaften

**School of Engineering
Departement T - Studiengang Informatik**

SEMESTERARBEIT

Audit-Methode zur Gefahrenanalyse einer KMU IT-Infrastruktur

Vorgelegt von: Sandro Brunner
Geissbergstr. 5
8302 Kloten

Betreuer: Dr. Ralf Mock

Selbständigkeitserklärung

Ich versichere hiermit, dass ich meine Semesterarbeit mit dem Thema

Audit-Methode zur Gefahrenanalyse einer KMU IT-Infrastruktur

selbständig verfasst und keine anderen als die unten angegebenen Quellen und Hilfsmittel benutzt habe. Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch nicht veröffentlicht.

Die Ergebnisse der Arbeit stehen ausschliesslich dem auf dem Deckblatt angeführten Unternehmen zur Verfügung (Arbeit mit Sperrvermerk).

Mir ist bekannt, dass ich meine Semesterarbeit zusammen mit dieser Erklärung fristgemäss im Sekretariat der ZHAW abzugeben habe.

Zürich, den 25.05.2012

Unterschrift

Kurzfassung

Im Rahmen eines F&E-Projektes entwickelt die Zürcher Hochschule für Angewandte Wissenschaft (ZHAW) zusammen mit einem Industriepartner am Beispiel des Brandschutzes eine generische Audit-Methode zur Gefahren- und Risikoberechnung [11]. Die von einem Auditor zu bewertenden Prüfungskriterien werden dabei anhand mehrerer Attribute beschrieben. In dieser Semesterarbeit wird die Methode zuerst formell beschrieben und dann mit Hilfe von IT-Security-Standards, Leitfäden sowie IT-Security-Surveys an die IT-Branche angepasst. Zur Benutzung der Methode wurde mit HTML5 Web-Technologien ein Prototyp entwickelt. Ziel der in dieser Arbeit entwickelten Methode ist es dabei, die IT-Security eines KMU-Unternehmens auf ein Grundschutz-Niveau zu heben bzw. zu halten.

Inhaltsverzeichnis

1	Glossar	1
2	Einleitung	2
2.1	Ausgangslage	2
2.2	Ziel der Arbeit	2
2.2.1	Aufgabenstellung	2
2.2.2	Rahmenbedingungen	3
2.3	Vorgehen	3
3	Methodik des Brandschutz- und Risikoaudits	4
3.1	Aufbau	4
3.2	Bewertung	5
3.3	Auswertung	6
3.3.1	Beispiel	8
4	Anpassung der Methode	9
4.1	Ermittlung der Prüfungskriterien	9
4.1.1	Leitfaden Informationssicherheit (BSI)	10
4.1.2	ISO/IEC 27002:2005	10
4.1.3	Vergleich der Listen vom Leitfaden Informationssicherheit und ISO 27002 Standard	11
4.1.4	Vergleich der Standards mit IT-Security-Surveys	11
4.1.5	Definition Prüfungskriterien	15
4.2	Definition der Attribute (Schadensdimensionen)	15
4.3	Definition der PK-Konsequenzen und PK-Gewichtung	16
4.3.1	Fazit	17
5	Entwicklung des Prototyps	18
5.1	Vorgehen	18
5.2	Mockups und Anforderungen	19
5.2.1	Index Mockup	20
5.2.2	Audit Mockup	21
5.2.3	Auswertung Mockup	22
5.3	Use Cases	23
5.4	Architektur / Technologien zur Umsetzung	24
5.4.1	Voraussetzung Browser-Versionen	24
5.5	Projektmanagement	25
5.5.1	Installation	25
5.6	Fazit	25
6	Case Study - Test der Funktionalität und Anwendbarkeit	27

7	Schlussfolgerungen	29
A	Projektplan Semesterarbeit	30
B	Anhang Methodik	32
B.1	Berechnungsparameter Detailliert	32
B.2	Methode Excel-Umsetzung mit Variablenbeschriftung	33
C	Leitfaden Informationssicherheit : Zusammengefasste Prüfungskriterien	36
C.1	Szenarien und Massnahmen	36
C.2	Häufige Versäumnisse	36
C.3	Wichtige Sicherheitsmassnahmen	37
D	ISO/IEC 27002:2005 : Zusammenfassung Objectives	41
D.1	Security Policy	41
D.2	Organization of information security	41
D.3	Asset management	42
D.4	Human resources security	43
D.5	Physical and environmental security	44
D.6	Communications and operations management	45
D.7	Access control	47
D.8	Information systems acquisition, development and maintenance	49
D.9	Information security incident management	50
D.10	Business continuity management	51
D.11	Compliance	51
E	Prüfungskriterien der Methode	53
F	Dokumente zur Softwareentwicklung	58
F.1	Anforderungen an den Prototyp	58
F.2	Use Cases - Detailbeschreibung	60
F.2.1	Use Case U.1 - Audit initialisieren	60
F.2.2	Use Case U.2 - Audit durchführen	61
F.2.3	Use Case U.3 - Audit auswerten	62
F.3	Datenmodell	62
F.4	Dateien / Dateistruktur	64
F.4.1	HTML	64
F.4.2	JavaScript (Logik)	64
F.4.3	CSS (Darstellung)	65
F.4.4	Bilder	65
F.4.5	Tests	65
F.5	Bilder des Prototyps	65
	Literaturverzeichnis	69

1 Glossar

Datenschutz: “Unter Datenschutz versteht man den Schutz personenbezogener Daten vor dem Missbrauch durch Dritte.” [1]

Datensicherheit: “Mit Datensicherheit wird der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet. Ein anderer Begriff dafür ist *Informationssicherheit*. “ [1]

Datensicherung (engl. Backup): “Bei einer Datensicherung werden zum Schutz vor Datenverlust Sicherungskopien von vorhandenen Datenbeständen erstellt.“ [1]

Integrität: “Schutz vor unzulässiger Veränderung oder Zerstörung von Informationen. Beinhaltet die Sicherstellung der Nichtabstreitbarkeit (non-repudiation) sowie der Authentizität” [44 U.S.C., Sec. 3542]

ISMS: “Steht für Information Security Management System oder auf Deutsch: Managementsystem für Informationssicherheit.” [1]

Risikoanalyse (engl. Risk Assessment/Analysis): “Mit einer Risikoanalyse wird untersucht, wie wahrscheinlich das Eintreten eines bestimmten Schadens ist und welche negativen Folgen der Schaden hätte.” [1]

Sicherheitsrichtlinie(engl. Security Policy): “In einer Sicherheitsrichtlinie werden Schutzziele und allgemeine Sicherheitsmaßnahmen im Sinne offizieller Vorgaben eines Unternehmens oder einer Behörde formuliert.” [1]

Use-Case: Ein *Use Case* ist ein Fall (oder Situation), in welchem ein System dazu verwendet wird, einen oder mehrere gestellte Anforderungen (requirements) zu erfüllen. Ein *Use Case* beschreibt eine Funktionalität die das System anbietet. (Aus [7] S. 20)

Verfügbarkeit: “Sicherstellung, dass zu einen vorgegeben (beliebigen) Zeitpunkt auf Informationen zugegriffen werden kann bzw. Informationen verwendet werden können” [44 U.S.C., Sec. 3542]

Vertraulichkeit: “Bewahrung/Sicherstellung von autorisierten Einschränkungen auf Zugriff sowie Veröffentlichung von Informationen zuzüglich der Möglichkeit Informationen, die die Privatsphäre betreffen zu schützen” [44 U.S.C., Sec. 3542]

2 Einleitung

2.1 Ausgangslage

Das Institut für angewandte Informationstechnologie (InIT) der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) erarbeitet zur Zeit zusammen mit einem Ingenieurbüro eine Methode zur Erfassung sowie dem Vergleich (Benchmarking) von Gefahren und Risiken. Die Methode wird am Beispiel des Brandschutzes entwickelt, ist aber darauf ausgelegt, generisch, und damit auch für IT-Audits, anwendbar zu sein.

2.2 Ziel der Arbeit

Das Ziel dieser Arbeit ist es, die bereits entwickelte Methode so zu ändern bzw. anzupassen, dass es möglich ist, Gefahren einer IT-Infrastruktur aufzuzeigen, sowie die Programmierung eines webbasierten Prototyps mit dem dies ausgeführt und dargestellt werden kann. Die Grösse der Firma, in der diese Methode schlussendlich zum Einsatz kommen soll, beschränkt sich vorerst auf KMUs. Als Ergebnis ist es vorgesehen, dass einem IT-Verantwortlichen eines KMUs ein Werkzeug zur Verfügung gestellt werden kann, mit welchem es ihm möglich ist, die IT-Security seines Unternehmens auf ein Grundschutz-Niveau zu heben bzw. zu halten. Dies soll zudem möglichst zeit- sowie ressourcenschonend sein.

2.2.1 Aufgabenstellung

Im Rahmen dieser Arbeit müssen folgende Aufgaben gelöst werden:

- Ermittlung der Prüfungskriterien anhand von IT-Security-Standards, -Studien, -Surveys und Literatur.
- Definition einer Bewertungsskala.
- Ermittlung von Attributen, um Konsequenzen zu beschreiben.
- Programmierung eines Prototyps unter Anwendung eines professionellen Entwicklungsprozesses (z. B. : SCRUM).
- Erprobung der Methode an einem realen Beispiel (Fallbeispiel).

2.2.2 Rahmenbedingungen

Zusammengefasst werden folgende Anforderungen an die Methode gestellt:

- **Ausrichtung:** Die Methode ist auf KMUs ausgerichtet. Dazu zählen laut Definition Betriebe, die weniger als 250 Mitarbeiter angestellt haben (Jahresarbeits Einheit) und entweder einen Jahresumsatz von weniger als 50 Mio. Euro erzielen oder eine Jahresbilanzsumme von weniger als 43 Mio. Euro vorweisen können. [6]
- **Dauer:** Die Anwendung der Methode sollte ungefähr 4 und auf keinen Fall länger als 8 Stunden dauern (Audit inkl. Auswertung).
- **Bereiche:** Die Methode soll Gefahren einer IT-Infrastruktur ersichtlich machen. Damit gemeint sind *technische* sowie *organisatorische* Aspekte der IT-Security.

2.3 Vorgehen

Um die Ziele zu erreichen, wird folgendermassen vorgegangen:

1. **Methodik:** Beschreibung des methodischen Konzeptes des genannten Ansatzes für ein Brandschutz-Audit samt Risk Assessment. Dieses Konzept bildet die Grundlage für die in dieser Semesterarbeit zu entwickelnde Methode eines IT-Security-Audits.
2. **Anpassung der Methode:** Die Methode wird an die IT-Branche angepasst. Es wird gezeigt, wie die Methode konzeptionell an die in dieser Arbeit gestellten Anforderungen angepasst wird. Dazu zählen die Ermittlung und Bewertung der Prüfungskriterien, die Definition der Bewertungsskala sowie die Ermittlung der Attribute, mit welchen Konsequenzen beschrieben werden.
3. **Entwicklung des Prototyps:** In diesem Punkt geht es um das Konzept sowie die anschliessende Umsetzung der Methode.
4. **Case-Study:** Zum Schluss wird die Methode bzw. der Prototyp an einem Beispiel getestet. Hier geht es darum aufzuzeigen, ob die Methode praxistauglich ist und ob es Verbesserungsmöglichkeiten gibt.

3 Methodik des Brandschutz- und Risikoaudits

Die Methodik des zugrundeliegenden Brandschutz- und Risikoaudits ist konzeptionell soweit ausgereift, dass damit erste Praxiserfahrungen gesammelt werden können. Damit liegt auch eine Basis für eine entsprechende Entwicklung im Bereich der IT-Security vor.

3.1 Aufbau

Eine Checkliste unerwünschter Ereignisse, wie sie aus einer Branche bekannt sind oder aus Standards abgeleitet wurden, bildet die Grundlage des Risiko-Audits. Diese Ereignisse bilden die Prüfkriterien (PK) der Checkliste. Die PK werden in Klassen zusammengefasst:

- **Prüfungskriterium:** Ist ein in der Branche häufig auftretender Mangel.
- **Sicherheitsaspekt:** Logischer Bund von mehreren zusammengehörigen Prüfungskriterien.
- **Bereich:** Logischer Bund von mehreren zusammengehörigen Sicherheitsaspekten.
- **Branche:** Oberstes Glied der Hierarchie. Umfasst und beinhaltet alle vorher beschriebenen Stufen. Beschreibt eine spezifische Branche.

Die Branche sowie die Prüfungskriterien werden über Attribute beschrieben. Diese Attribute müssen einen Schaden möglichst vollständig beschreiben. Der Ansatz im Brandschutz nutzt die Attribute *Personenschaden*, *Gebäudeschaden*, *Sachschaden* und *Unterbruchschaden*. Die Bewertung dieser Attribute auf Branchen-Level (*Attribut-Gewichtung Branche*) sagt aus, wie wichtig das jeweilige Attribut für die Branche ist. Auf PK-Level (*Attribut-Konsequenz*), bekommt jedes Attribut einen Wert zwischen 0 und 1 zugewiesen. Dieser Wert drückt die potentiellen Konsequenzen auf dieses Attribut aus, sollte ein Mangel auftreten bzw. vorhanden sein. Je höher der Wert, desto höher sind die erwarteten potentiellen Konsequenzen.

Um potentielle Schäden genauer bewerten zu können, werden die Prüfungskriterien zusätzlich untereinander gewichtet. Jedes Prüfungskriterium erhält somit ein weiteres Attribut (*PK-Gewichtung*). Es sagt aus, wie wichtig das PK im Vergleich zu anderen PKs ist. Auch dieses Attribut erhält einen Wert zwischen 0 und 1. Der potentielle Schaden eines Prüfungskriteriums, das mit einer 1 bewertet worden ist, ist dabei doppelt so gross wie bei einem Prüfungskriterium, das mit 0.5 bewertet worden ist. Die Werte die dieses Attribut annehmen kann sind in einer Wertemenge definiert. Der Ansatz im Brandschutz hat hierfür zum Beispiel drei verschiedene Werte definiert: „*grosser Mangel*“ = 1, „*mittlerer Mangel*“ = 0.5 und „*kleiner Mangel*“ = 0.25.

In einem ersten Schritt muss eine Liste von Prüfungskriterien erstellt werden, in welcher jene Mängel enthalten sind, die in einer Branche besonders häufig auftreten. Danach müssen die Attribute aller Prüfungskriterien mit Werten hinterlegt werden. Dieser Teil stellt die Grundlage für die Berechnung des Gefahrenpotentials dar und ist daher von elementarer Wichtigkeit.

3.2 Bewertung

Nachdem das Grundgerüst der Prüfungskriterien, Attribute und Gewichtungen vorliegt, können die Prüfungskriterien bewertet werden. Dem Auditor stehen dafür mehrere Bewertungsmöglichkeiten (*PK-Bewertung*) zur Verfügung. Den Bewertungsmöglichkeiten werden Werte zwischen 0 und 1 zugeteilt, wobei 1 ausdrückt, dass der Mangel nicht besteht bzw. keine Gefahr für den Betrieb darstellt und 0, dass durch den Mangel die grösstmöglichen Konsequenzen zu erwarten sind. Jedes Prüfungskriterium kann auch als „nicht relevant“ bewertet werden. In der Berechnung wird ein Prüfungskriterium, das als „nicht relevant“ bewertet wurde, ignoriert. Zusätzlich gibt es das Bewertungskriterium „nicht beurteilbar“. Diese Bewertung wird dann abgegeben, wenn ein Prüfungskriterium zwar vorhanden, aber nicht adäquat überprüfbar ist.

In Tabelle 3.1 sind alle Komponenten der Berechnung aufgeführt.

Variabel	Bezeichnung
i	Prüfungskriterium (PK)
s	Sicherheitsaspekt (SA)
j	Attribut (Schadensdimension)
k	Relative Gewichtung
l	Bewertung
a_j	Attribut-Gewichtung Branche
$c_{s,i,j}$	Attribut-Konsequenz
$w_{s,i,k}$	PK-Gewichtung
$b_{s,i,l}$	PK-Bewertung

Tab. 3.1: Methode: Berechnungskomponenten (Für Details siehe Anhang B.1)

Nachdem ein Auditor alle Prüfungskriterien bewertet hat, können alle weiteren Berechnungen durchgeführt werden. Die in Tab. 3.1 definierten Variablen bilden die Grundlage für diese Berechnungen.

3.3 Auswertung

Als Resultat erhält jedes Prüfungskriterium für jedes Attribut einen spezifischen Wert. Pro Prüfungskriterium erhält man schlussendlich also so viele Werte bzw. Resultate wie es Attribute gibt. Ein Resultat ist jeweils das Ergebnis der Multiplikation der drei Faktoren $c_{s,i,j}$ (*Attribut-Konsequenz*), $w_{s,i,k}$ (*PK-Gewichtung*) und $b_{s,i,l}$ (*PK-Bewertung*):

$$r_{s,i,j} = c_{s,i,j} \cdot w_{s,i,k} \cdot b_{s,i,l} \quad (3.1)$$

Der Wert $r_{s,i,j}$ drückt aus, wie wichtig ein Attribut eines Prüfungskriteriums ist. Da die Faktoren jeweils höchstens einen Wert von 1 annehmen können, ist auch das Ergebnis auf einen Höchstwert von 1 begrenzt. An dieser Zahl erkennt man die Wichtigkeit im Bezug auf alle anderen in der Methode berechneten Werte.

In einem ersten Schritt werden alle Resultate r , die zu demselben Attribut j und Sicherheitsaspekt s gehören, aufsummiert (Spaltensumme).

$$z_{s,j} = \sum_{i=1}^n r_{s,i,j} \quad (3.2)$$

$z_{s,j}$ ist die Summe aller Resultate $r_{s,i,j}$ des Sicherheitsaspektes s und Attributes j aus Gl. 3.1. Um diese Zahl in einen Kontext zu stellen und bewertbar zu machen, wird sie durch die maximal erreichbare Summe $z_{Max,s,j}$ dividiert. Um diese Zahl zu erhalten wird der Faktor b der Gleichung 3.1 auf 1 gesetzt. Dadurch wird die prozentuale Erfüllung eines Attributes eines Sicherheitsaspektes sichtbar gemacht.

Danach werden alle berechneten $z_{s,j}$ und $z_{Max,s,j}$ aufsummiert. Damit wird das Total an erreichten Punkten t_j eines Attributes sowie die maximale Punktzahl, die bei diesem Attribut erreicht werden kann erhalten.

$$t_j = \sum_{s=1}^n z_{s,j} \quad (3.3)$$

$$t_{Max,j} = \sum_{s=1}^n z_{Max,s,j} \quad (3.4)$$

Anschliessend wird zuerst t_j durch $t_{Max,j}$ dividiert. Das Resultat davon ist die prozentuale Erfüllung eines Attributes über die gesamte Branche hinweg gesehen. Zum Schluss wird diese Zahl mit a_j , der Branchengewichtung des Attributes j , multipliziert. Dies ist die Endbewertung des Attributes j über die gesamte Branche. Je höher dieser Erfüllungsgrad ist, desto geringer ist die Gefahr eines Schadens einzustufen.

Die Berechnung dieser Zahl wird in folgender Gleichung dargestellt

$$u_j = \frac{t_j}{t_{Max,j}} \cdot a_j \quad (3.5)$$

u_j ist dabei im besten Fall gleich gross a_j (falls $t_j = t_{Max,j}$). In diesem Fall besteht für dieses Attribut keine Gefahr im Betrieb.

Den Gesamterfüllungsgrad des Betriebes über alle Attribute hinweg betrachtet wird berechnet, indem die Summe des Erfüllungsgrades jedes Attributes (u_j) durch die Summe der Attribut-Gewichtungen dividiert wird:

$$v = \frac{\sum_{j=1}^n u_j}{\sum_{j=1}^n a_j} \quad (3.6)$$

In der bereits entwickelten Methode gibt es für die *PK-Gewichtung* (Tab. 3.2) sowie die *PK-Bewertung* (Tab. 3.3) bereits definierte Gewichtungs- bzw. Bewertungsmöglichkeiten. Diese werden für diese Arbeit übernommen. Die PK-Bewertungsmöglichkeit „*Nicht Beurteilbar*“ wurde noch nicht klar definiert. Sie wird komplett weggelassen.

k	Definition	$w_{s,i,k}$
0	Kleiner Mangel	0.25
1	Mittlerer Mangel	0.5
2	Grosser Mangel	1

Tab. 3.2: PK-Gewichtungsmöglichkeiten

l	Definition	$b_{s,i,l}$
0	Nicht akzeptabel	0
1	Akzeptabel	0.5
2	In Ordnung	1
3	Nicht Relevant	Leere Menge $\{\}$
4	Nicht Beurteilbar	?

Tab. 3.3: PK-Bewertungsmöglichkeiten

3.3.1 Beispiel

Mit einem Rechenbeispiel aus dem Brandschutz soll die Funktion der Methode verdeutlicht werden. Die Werte wurden zufällig ausgewählt.

In diesem Beispiel wird im Brandschutz ein Schaden - und somit sämtliche Prüfungskriterien - mit den vier Attributen, **P**: *Personenschaden*, **G**: *Gebäudeschaden*, **S**: *Sachschaden* und **U**: *Unterbruch* beschrieben. Das Beispiel-Prüfungskriterium sei “*Abschottungen in Treppenhäusern und Fluchtkorridoren fehlen*” und wurde folgendermassen bewertet:

PK-Konsequenz: P	0.8
PK-Konsequenz: G	0.4
PK-Konsequenz: S	0.4
PK-Konsequenz: U	0
PK-Gewichtung:	1 (grosser Mangel)
PK-Bewertung:	0.5 (akzeptabel)

Tab. 3.4: Beispielbewertungen

Die PK-Bewertung sei vom Auditor durchgeführt worden. Das Resultat ($r_{s,i,j}$) wird mit Hilfe von Gl. 3.1 berechnet, was zu einem Resultat pro Attribut, also insgesamt vier Resultaten führt:

- $P = 0.8 \cdot 1 \cdot 0.5 = 0.4$
- $G = 0.4 \cdot 1 \cdot 0.5 = 0.2$
- $S = 0.4 \cdot 1 \cdot 0.5 = 0.2$
- $U = 0 \cdot 1 \cdot 0.5 = 0$

Diese Berechnung wird für jedes Prüfungskriterium durchgeführt. Die Auswertung besteht dann im wesentlichen im aufsummieren dieser Resultate. Um die Attribute miteinander vergleichen zu können, wird eine prozentuale Erfüllung berechnet, die erst ganz zum Schluss noch mit der *Attribut-Gewichtung Branche* multipliziert wird, um den als wichtig bewerteten Attributen mehr Gewicht im Gesamtergebnis zu geben. Angenommen die Attribut-Gewichtung Branche wäre $P = 4$ und $G = 3$ und die Gesamt-Erfüllung der Attribute (u_j) sei $P = 0.6$ und $G = 0.7$. Das Endresultat für P wäre $4 \cdot 0.6 = 2.4$ und für $G = 3 \cdot 0.7 = 2.1$. P hätte trotz seiner niedrigen Erfüllung einen höheren Einfluss auf das Gesamtergebnis als G .

4 Anpassung der Methode

Es wurde beschrieben, aus was für Elementen die Methode besteht und wie man Eingaben eines Auditors bzw. einen Audit auswertet. In diesem Kapitel werden nun die variablen Elemente an die IT-Branche angepasst. Dazu zählen die Prüfungskriterien sowie die Attribute. PK-Gewichtungs- und PK-Bewertungsmöglichkeiten sowie die dazugehörigen Werte werden aus der bereits entwickelten Methode übernommen (Tab. 3.2, Tab. 3.3).

4.1 Ermittlung der Prüfungskriterien

Zur Bestimmung der Prüfungskriterien werden etablierte IT-Security-Standards und Leitfäden sowie IT-Security-Umfragen (Surveys) von renommierten Unternehmen zur Rate gezogen. Ziel ist es, eine Liste von 40 bis 70 Prüfungskriterien zu erhalten. Diese beschränkte Anzahl an Prüfungskriterien soll den zeitlich begrenzten Rahmen der Methode gewährleisten. Im Vergleich zu Kriterien oder Checklisten die in IT-Security-Standards gefunden werden können, ist diese Menge an Prüfungskriterien sehr begrenzt. Nicht selten haben Standards eine Länge von mehreren hundert Seiten und gehen bei der Beschreibung von Fehlerquellen tief ins Detail. Zur Ableitung von Prüfungskriterien wird der „Leitfaden Informationssicherheit“ [1] vom Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Standard „27002:2005“ [3] der internationalen Standardisierungsorganisation (ISO) verwendet. [1] ist im deutschsprachigen Raum und [3] international anerkannt. Beide Dokumente sind zudem auf einen *Best Practice*-Ansatz angelegt, was dem Sinn der Methode entspricht. In einem ersten Schritt werden aus den in diesen beiden Dokumenten vorkommenden Vorschlägen bezüglich IT-Security je eine Liste erstellt. Punkte, die in beiden Listen vorkommen, werden als mögliche Prüfungskriterien betrachtet. In einem zweiten Schritt werden IT-Security-Umfragen (Surveys) studiert. Sie sollen aufzeigen, mit welchen Aspekten der IT-Security Unternehmen die grösste Mühe bzw. am meisten Probleme haben. Diese Umfragen sollen dabei helfen, die Prüfungskriterien, die in [1] sowie [3] vorkommen, zu bestätigen.

4.1.1 Leitfaden Informationssicherheit (BSI)

Dieses Dokument wurde vom BSI geschrieben, um kleinen und mittleren Unternehmen (KMUs), welche über beschränkte finanzielle und personelle Ressourcen verfügen, einen leicht überschaubaren Einstieg in die Thematik der IT-Security zu bieten. Dieser Leitfaden gibt einen umfassenden und verständlichen Überblick über die wichtigsten Belange der IT-Security. Das BSI ist zudem eine renommierte Behörde, deren Standards und Massnahmenkataloge die Grundlage der IT-Security-Strategie vieler Firmen bilden. Aus diesen Gründen eignet sich dieses Dokument ausgezeichnet für diese Arbeit.

Der Leitfaden fängt damit an, zu erklären, weshalb Informationssicherheit in der heutigen Zeit so wichtig ist und zählt grundlegend falsche Ansichten auf, die oft immer noch vorhanden sind. Einige der häufig gehörten Aussagen seien:

- „Bei uns ist noch nie etwas passiert.“
- „Was soll bei uns schon zu holen sein, so geheim sind unsere Daten nicht.“
- „Unser Netz ist sicher.“
- „Unsere Mitarbeiter sind vertrauenswürdig.“

Es werde zum Beispiel angenommen, dass, wenn man die Sicherheit in der IT steigern wolle, dies mit hohen Kosten und der Anstellung von hoch qualifiziertem Personal verbunden sei. Die wichtigsten Faktoren seien jedoch „ein gesunder Menschenverstand, durchdachte organisatorische Regelungen sowie zuverlässige und gut informierte Mitarbeiter, die selbstständig Sicherheitserfordernisse diszipliniert und routiniert beachten“[1]. Anschliessend werden wichtige Begriffe erklärt und gesetzliche Vorschriften aufgezeigt. Danach folgen Szenarien, häufige Versäumnisse und Sicherheitsmassnahmen. Diese stellen mögliche Prüfungskriterien dar bzw. könnten zu Prüfungskriterien abgeleitet werden. Sie wurden zusammengetragen und können im Anhang C gefunden werden.

4.1.2 ISO/IEC 27002:2005

Der ISO 27002 Standard ist Teil der 27000 Standard-Familie der ISO, welche sich dem Thema der IT-Security verschrieben hat. Er gibt Anleitung und beschreibt allgemeine Prinzipien zur Initialisierung, Implementierung, Instandhaltung und Verbesserung eines IT-Security-Managementsystems. Diese gelten als allgemein anerkannt, müssen jedoch nicht zwingend für jede Firma relevant sein. Der einleitende Teil besteht aus einer Vorstellung, einer Beschreibung des Rahmens sowie Begriffsdefinitionen. Der Hauptteil geht detaillierter auf IT-Security-Aspekte ein und ist wie folgt aufgebaut: Die Basis bilden 39 Sicherheitsaspekte, sogenannte *control objectives*, welche in 11 Kategorien eingeteilt sind (*security control clauses*). Jeder dieser Sicherheitsaspekte beschreibt zum einen, was erreicht werden soll (*control objective*) und zeigt einen oder mehrere Möglichkeiten (*controls*) auf, wie dieses Ziel erreicht werden kann.

Im Standard gibt es hunderte dieser „Best Practice“ Anleitungen, wie die IT-Security einer Firma geschützt bzw. verbessert werden kann. Diese reichen von „Trivial“ bis hin zu „Sehr spezifisch“. Diese *controls* sowie die dazugehörigen Umsetzungsanleitungen (*Implementation guidance*) könnten sich also gut als Prüfungskriterien eignen. Sie werden in einer Liste zusammengefasst und können im Anhang D gefunden werden. Sie werden im nächsten Abschnitt mit der aus dem Leitfaden Informationssicherheit des BSI [1] erstellten Liste (Anhang C) verglichen. Punkte die auf beiden Listen vorkommen sind Kandidaten, um in der Methode als Prüfungskriterien übernommen zu werden.

4.1.3 Vergleich der Listen vom Leitfaden Informationssicherheit und ISO 27002 Standard

Nach der Durchsicht der beiden Dokumente und der Niederschrift der sich darin befindenden Punkte bezüglich IT-Security, hat sich gezeigt, dass er ISO 27002 Standard um einiges detaillierter auf die IT-Security-Aspekte eingeht als dies der BSI-Leitfaden tut. Der BSI Leitfaden enthält eine Untermenge der von im ISO 27002 beschriebenen Punkte und drückt diese zumeist verständlicher aus. Da bei der Auswahl Punkte gewählt werden, die in beiden Dokumenten vorkommen, kann somit hauptsächlich auf Punkte aus dem BSI Leitfaden geachtet werden, wobei Punkte aus dem ISO 27002 zur genaueren Beschreibung der jeweiligen Aspekte gebraucht werden können. Sollten in den IT-Security-Umfragen spezielle Aspekte erwähnt werden, die nicht im BSI-Leitfaden erwähnt werden, so kann der ISO 27002 zu genaueren Definition dieser Aspekte verwendet werden.

4.1.4 Vergleich der Standards mit IT-Security-Surveys

Durch den Vergleich des ISO 27002 Standards mit dem BSI Leitfaden hat eine Liste mit circa 60 Prüfungskriterien erstellt werden können. Es werden nun noch einige IT-Security-Surveys studiert, um zu sehen, ob die bisher erarbeiteten Prüfungskriterien relevant sind und auch, um vielleicht einige zusätzliche Punkte, welche weder in [1] noch [3] vorkommen, zur Liste hinzuzufügen. Die betrachteten Surveys sollen dabei nicht älter als 3 Jahre sein. Wenn möglich sollen die in den Surveys befragten Unternehmen KMUs sein, da die hier entwickelte Methode auf diese Zielgruppe ausgelegt ist.

Bei der ersten untersuchten IT-Security-Umfrage handelt es sich um die *IT-Sicherheitslage im Mittelstand 2011* der Organisation „Deutschland sicher im Netz (DsiN)“[9]. Alle weiteren Informationen bzw. Zitate in diesem und dem nächsten Absatz stammen aus dieser Quelle. Wie bereits im Titel erkennbar, wurde diese Studie 2011 durchgeführt. Zudem ist es das Zitat: „Ziel des DsiN-Sicherheitschecks, den aktuellen Stand der Informationssicherheit in kleinen und mittleren Unternehmen (KMUs) in Deutschland zu ermitteln und daraufhin Handlungsempfehlungen zu geben“. Die Studie wurde online durchgeführt. Es nahmen insgesamt 1400 Unternehmen daran Teil. Diese Studie ist aktuell, wurde in Deutschland durchgeführt und konzentriert sich auf KMUs. Sie passt somit optimal ins Schema der hier zu untersuchenden IT-Security-Surveys.

Die Studie kommt zum Ergebnis, dass die Entwicklung der IT-Security insgesamt eine positive ist. Die letzte DsiN-Studie dazu wurde 2008 durchgeführt. Zum einen sei die Verantwortung für IT-Security in Unternehmen klarer zugeordnet und Sicherheitslösungen wie Firewall, Anti-Virus und Anti-Spam-Lösungen inzwischen Standard geworden.

Daneben gibt es auch einige sicherheitsrelevante Punkte, welche Firmen verstärkt beachten sollten:

- “Stärkung des Umgangs mit Compliance-Vorgaben.”
- “Verwendung von sicherer E-Mail.”
- “Schützen von mobilen Daten”
- “Gewährleistung der Funktionsfähigkeit der IT-Infrastruktur”

Das Verwenden sicherer E-Mails ist noch nicht Teil der Liste an Prüfungskriterien, wird jedoch nun hinzugefügt. Eine weitere, in der Studie aufgeführte Empfehlung, welche noch nicht in der Liste der Prüfungskriterien vorkommt, ist die Benutzung einer sicheren gemeinsamen Dateiablage (Datentresor). Diese kann verwendet werden, wenn häufig eine organisationsübergreifende Kommunikation notwendig ist. Diese Empfehlung ist ein potentieller Kandidat um auf die Liste der Prüfungskriterien zu gelangen. Ein weiterer Punkt bei dem Handlungsbedarf zu bestehen scheint, sind die organisatorischen Massnahmen bezüglich IT-Security. Laut Studie haben lediglich 24% der befragten Unternehmen eine dokumentierte Sicherheitsrichtlinie, 30% ein von der Geschäftsleitung getragenes Sicherheitskonzept und 31% haben gar keine organisatorische Massnahmen definiert. Diese Punkte sind bereits in der Liste der Prüfungskriterien erhalten und bestätigen deren Relevanz. Bei der Definition der Konsequenzen dieser Punkte, kann ihnen jedoch aufgrund dieses Befundes eine höhere Wichtigkeit gegeben werden.

Der nächste betrachtete Survey hat den Namen „Global IT Security Risk“ [4] und wurde von Kaspersky Lab in Zusammenarbeit mit B2B International, einem internationalen Forschungsinstitut, durchgeführt. Es wurden insgesamt 1300 Informatik-Spezialisten aus kleinen, mittleren sowie grossen Unternehmen aus 11 Ländern befragt. Die Studie fand im Jahr 2011 statt. Alle weiteren Informationen bzw. Zitate in diesem und dem nächsten Absatz stammen aus dieser Quelle.

Laut Studie ist die IT-Security-Strategie für einen Grossteil der Unternehmen eines der wichtigsten Anliegen, für viele kommt sie noch vor der Finanz-, Marketing- oder Personalstrategie. Dies vor allem, weil die Unternehmen bzw. deren Geschäftsprozesse ohne IT nicht funktionieren könnten und ein erfolgreicher Angriff zu einem Betriebsunterbruch, einem Reputationsverlust der Firma oder dem Diebstahl geistigen Eigentums führen kann. Dennoch gibt es Verbesserungspotenzial. Nur etwas mehr als die Hälfte aller befragten Unternehmen gaben an, einen organisierten, systematischen Umgang bezüglich IT-Security-Fragen umgesetzt zu haben. Für 33% der Befragten seien IT-Sicherheitsvorkommnisse zu unberechenbar und 28% sind der Ansicht, dass sie dieses Thema nicht betreffe. Diese Firmen reagieren grundsätzlich reaktiv. Sie investieren erst in die IT-Sicherheit, nachdem etwas passiert ist.

Hier zeigt sich, dass obwohl eine generelle Akzeptanz bezüglich der Wichtigkeit der IT-Security besteht, vielerorts noch Nachholbedarf besteht und Aufklärungsarbeit betrieben werden sollte. Auch die Tatsache, dass IT-Security nicht nur für sich steht, sondern in Geschäftsprozesse zu integrieren und ganzheitlich zu betrachten ist, scheint nicht immer klar zu sein.

Zum Schluss gibt Kaspersky Lab folgende 5 Empfehlungen ab:

1. "Wählen Sie eine Sicherheitslösung die zu Ihrem Unternehmen passt."
2. "Investieren Sie in die Ausbildung (Security Awareness) Ihrer Mitarbeiter."
3. "Auf allen IT-Systemen (inkl. mobilen Geräten) sollte ein Anti-Virenprogramm installiert sein."
4. "Benützen Sie ein zentralisiertes Management-System für alle Endpoint-Devices."
5. "Schützen Sie die Kommunikation ihrer Benutzer anstatt sie zu beschränken."

Punkt Nummer vier kommt noch nicht in der Liste der Prüfungskriterien vor und wäre ein Kriterium, das hinzugenommen werden könnte. Der Punkt, Kommunikation zu schützen (z.B. mit Verschlüsselung), wurde bereits in [9] genannt. Schadsoftware (Viren, Trojaner etc.) wurde als die gefährlichste externe Bedrohung ausgemacht. 10% der erfolgreichen Angriffe führten zum Verlust von sensiblen Daten. Ein unternehmensweites Anti-Virus System sollte also Pflicht sein. Nichtsdestotrotz gaben 30% aller an der Studie teilnehmenden Unternehmen an, über keine bzw. nur eine teilweise (nicht unternehmensweite) Anti-Viren-Lösung zu verfügen. Das Bewusstsein der Mitarbeiter ist auf der Liste der Empfehlungen der einzige nicht technische Punkt. Gerade deshalb scheint er dem Autor wichtig. Er ist bereits auf der Liste der Prüfungskriterien enthalten. Bei der Definition der Konsequenzen, eine Aufgabe die später in dieser Arbeit zu lösen ist, wäre dies ein Grund, ihm eine hohe Bewertung zu geben.

Die dritte untersuchte Umfrage bezüglich IT-Security ist der „Information Security Breaches Survey (ISBS) 2010“ [10]. Die Umfrage wurde 2010 von Infosecurity Europe in Auftrag gegeben und gemeinsam mit Pricewaterhouse Coopers durchgeführt. Insgesamt nahmen 539 Firmen aus ganz England an der Befragung teil, wovon 55% KMUs waren. Alle weiteren Informationen bzw. Zitate in diesem und den nächsten vier Absätzen stammen aus dieser Quelle.

Dieser sehr interessante Bericht zeigt bei der Auswertung der Resultate klar auf, wie kleine und wie grosse Unternehmen geantwortet haben. Auch die Resultate der gleichen, im Jahre 2008 durchgeführten Umfrage sind jeweils ersichtlich. So bekommt man zusätzlich zu den Auswertungen der Fragen eine Einsicht in die Unterschiede zwischen kleinen und grossen Unternehmen und sieht zugleich die Entwicklung, die in den letzten 3 Jahren stattfand. Es folgt ein Auszug aus den Erkenntnissen dieser Umfrage.

77% der Geschäftsleiter der befragten Unternehmen bewerteten die IT-Security mit einer grossen bzw. sehr grossen Wichtigkeit. Interessant daran ist, dass dennoch jedes siebte dieser Unternehmen keine offizielle Informationssicherheitsrichtlinie hat. Das Prüfungskriterium, ob eine Sicherheitsrichtlinie vorhanden ist, ist bereits auf der momentan noch nicht definitiven Liste. Bei der Bewertung der Wichtigkeit der Sicherheitsrichtlinie soll deshalb ein hoher Wert gewählt werden. Interessant sind auch die Treiber / Beweggründe um IT-Security-Massnahmen auszubauen. Die vier wichtigsten sind: Schutz von Kundeninformationen (28%), Vorbeugung von Systemausfällen (19%), Einhaltung von Gesetzen und Vorschriften (13%), sowie, um den Ruf der Firma zu schützen (11%). Diese Punkte könnten sich als Attribute für die Methode eignen. Die Sicherheitskultur in den Firmen, kleinen wie grossen, hat deutlich zugenommen. Eine dauerhafte Schulung der Mitarbeiter hingegen führt nur knapp die Hälfte aller Unternehmen durch. Es wird dargelegt, dass allein durch technische Massnahmen keine Sicherheit erlangt werden kann. Auch den erheblichen, positiven Einfluss, den die Unterstützung der Geschäftsleitung bezüglich IT-Security hat, wird hervorgehoben. Der Autor ist der Ansicht, dass diese Einsichten auch in der Methode widergespiegelt werden sollten, was heisst, dass organisatorischen Massnahmen zur Verbesserung der IT-Security eine hohe Wichtigkeit zuzusprechen ist. Ein weiterer wichtiger Punkt ist der Verlust bzw. der Diebstahl von Daten. Eine Möglichkeit, dem entgegen zu wirken ist der Gebrauch von Verschlüsselung. Hier fällt auf, dass vor allem ein grosser Anteil der KMUs zu wenig auf Verschlüsselung setzt (Notebook Harddisks 57%, Kundentransaktionen auf Firmenwebseite 42%, Smartphones 23%). Hardwareausfälle, Virenbefall sowie von Mitarbeitern ausgelöste Probleme zählen zu den häufigsten Vorfällen. Bei den Mitarbeitern scheint es hierbei ausschlaggebend zu sein, ob und wie gut sie die Sicherheitsrichtlinie verstehen. Vor allem die steigende Komplexität der Systeme ist Ursache vieler Probleme und Fehler. Die Auswirkung von Sicherheitsvorfällen wird in der Studie anhand von Kosten, jedoch auch anhand des Einflusses auf den Ruf gemessen. Für einige Firmen (z. B. Banken) ist die Wahrung ihres guten Rufes wichtiger als ein finanzieller Verlust. Die Schädigung des Rufes ist demnach ein geeigneter Kandidat für eine Schadensdimension (Attribut). Der Unterbruch der Geschäftstätigkeiten war die häufigste Folge von Sicherheitsvorfällen, wobei Viren und andere Schadsoftware die grössten Übeltäter waren.

Abschliessend ist zu diesem Bericht zu sagen, dass er zwar keine neue Prüfungskriterien hervorgebracht hat, jedoch viele der in [1] und [3] vorkommenden Punkte bestätigte. Es sticht klar hervor, dass zu einem erfolgreichen Management der IT-Security nicht nur technische, sondern auch, und vor allem, organisatorische Massnahmen zählen. Die Mitarbeiter spielen hierbei eine tragende Rolle. Des weiteren hat der Bericht dabei geholfen, schon jetzt die Konsequenz einiger Prüfungskriterien besser einschätzen zu können und zeigt mögliche Schadensdimensionen (Attribute), wie zum Beispiel die Schädigung des Rufes, auf.

4.1.5 Definition Prüfungskriterien

Durch den Vergleich vom „BSI-Leitfaden Informationssicherheit“ [1] mit dem „ISO Standard 27002:2005“ [3] wurde eine Liste von möglichen Prüfungskriterien erstellt. Mit Hilfe diverser IT-Security-Surveys ([9],[4],[10]) wurde dann geprüft, ob die Liste relevant ist und ob zusätzliche Prüfungskriterien von Nöten sind. Es kann gesagt werden, dass die Punkte dieser provisorischen Liste beibehalten werden konnten und um ein paar wenige Punkte ergänzt wurden. Die definitive Liste der Prüfungskriterien, die die Grundlage der Methode bildet und im weiteren Verlauf dieses Kapitels mit Werten versehen wird, kann im Anhang E gefunden werden.

4.2 Definition der Attribute (Schadensdimensionen)

Bei der Definition der Attribute geht es darum, die Schäden, die Prüfungskriterien verursachen können, festzulegen. Wenn es um das Thema IT-Security geht, landet man zwangsläufig bei den Begriffen *Vertraulichkeit* (Confidentiality), *Integrität* (Integrity) und *Verfügbarkeit* (Availability) (CIA). Bei diesen Begriffen handelt es sich um die Grundwerte der IT-Security ([3] Kap. 2.5). Diese drei Werte bieten sich somit als Attribute an. Es stellt sich nun eine Frage. Ist es möglich, sinnvolle Werte für die Attribut-Konsequenzen jedes einzelnen Prüfungskriteriums zu bestimmen? Zum Beispiel für das Prüfungskriterium „*Verstösse gegen die Sicherheitsrichtlinie werden nicht geahndet*“. Hier ist es schwierig, spezifische Konsequenz-Werte für die Integrität, die Verfügbarkeit und die Vertraulichkeit zu bestimmen. Hat dieses Prüfungskriterium nun mehr Einfluss auf die Integrität, die Verfügbarkeit oder die Vertraulichkeit von Daten? Das Prüfungskriterium an sich ist wichtig, die Bestimmung von Konsequenzen jedoch schwierig. In diesem Fall ist es einfacher, eine Konsequenz auf die Gesamtsicherheit (CIA) zu bestimmen, da die Erfüllung dieses Kriteriums sich klar positiv auf alle auswirkt. Dies ist jedoch nicht bei jedem Prüfungskriterium so: Bei einigen lassen sich problemlos Bewertungen bezüglich der Konsequenz vornehmen. Als Lösung für diese Problem wird in Fällen, in denen sich die Konsequenzen für die einzelnen Attribute nicht genau bestimmen lassen, allen Attributen der gleiche Wert gegeben. Ein weiterer Aspekt ist, ob es noch mehr Attribute braucht, oder ob diese drei bereits ausreichen. In [10] z. B. wird dargelegt, dass die Bestrebungen, die IT-Security im Betrieb zu verbessern, bei vielen Firmen den Grund hat, ihren Ruf zu schützen. Für Banken z. B. würde sich ein erfolgreicher Angriff, bei dem Kundendaten bzw. Kundengelder gestohlen werden, verheerend auf das Geschäft auswirken. Hat es nun Sinn, ein Attribut „*Verlust des Ansehens*“ hinzuzufügen? Subjektiv betrachtet ja, aber es stellt sich jedoch gleich wieder die Frage, wie man ein Prüfungskriterium nach diesem Attribut bewerten soll bzw. welche Prüfungskriterien zu einem Verlust an Ansehen führen können. In der gesamten Liste gibt es kein Prüfungskriterium bei dem man sage könnte, dass es direkt einen Verlust des Ansehens zur Folge hat. Letztlich könnten alle dazu führen.

Stellt man jedoch die Integrität, Verfügbarkeit sowie Vertraulichkeit sicher, so kann man davon ausgehen, dass die Wahrscheinlichkeit sinkt, dass es zu einem Sicherheitsvorfall kommt bzw. dass ein solcher zu einem Verlust des Ansehens führt. Die Möglichkeit an Ansehen zu verlieren ist bereits in den klassischen Sicherheitsattributen enthalten. Da es sich bei allen anderen Prüfungskriterien gleich verhält, werden keine weiteren Attribute hinzugefügt.

Die von der Methode verwendeten Attribute sind somit bestimmt. Es sind dies:

- **Verfügbarkeit:** “Sicherstellung, dass zu einen vorgegeben (beliebigen) Zeitpunkt auf Informationen zugegriffen werden kann bzw. Informationen verwendet werden können” [44 U.S.C., Sec. 3542]

Hierunter fallen auch Systemausfälle (Business Continuity)

- **Vertraulichkeit:** “Bewahrung/Sicherstellung von autorisierten Einschränkungen auf Zugriff sowie Veröffentlichung von Informationen zuzüglich der Möglichkeit Informationen die die Privatsphäre betreffen zu schützen” [44 U.S.C., Sec. 3542]
- **Integrität:** “Schutz vor unzulässiger Veränderung oder Zerstörung von Informationen. Beinhaltet die Sicherstellung der Nichtabstreitbarkeit (non-repudiation) sowie der Authentizität” [44 U.S.C., Sec. 3542]

4.3 Definition der PK-Konsequenzen und PK-Gewichtung

Nachdem die Prüfungskriterien definiert wurden, müssen sie gewichtet werden. Es gilt, für jedes Prüfungskriterium die PK-Konsequenz von jedem Attribut sowie die PK-Gewichtung zu bestimmen. Mit der PK-Konsequenz wird ausgedrückt, was für eine Konsequenz ein Mangel auf ein bestimmtes Attribut hat. Mit der PK-Gewichtung wird die Wichtigkeit eines Prüfungskriteriums im Vergleich zu allen anderen Prüfungskriterien beschrieben. Die Zahlenwerte der PK-Gewichtung werden direkt von der bereits bestehenden Methode übernommen (grosser Mangel = 1, mittlerer Mangel = 0.5, kleiner Mangel = 0.25). Die Werte (PK-Konsequenz & PK-Gewichtung) der Prüfungskriterien zu bestimmen ist nicht trivial. Nehmen wir als Beispiel das Prüfungskriterium: „*Es ist nicht auf allen IT-Systemen ein Viren-Schutzprogramm installiert*“. Dies ist ein Prüfungskriterium, mit einer hohen Wichtigkeit. Die PK-Gewichtung sollte 1 (*grosser Mangel*) sein. Auch die Konsequenz wird dementsprechend, in diesem Fall für alle Attribute, hoch sein. Doch wie hoch genau? Ist die Konsequenz auf die Verfügbarkeit mit einer 0.7, 0.8 oder gar einer 0.9 zu bewerten? Wo liegt der beste Wert, um ein am Schluss sinnvolles Resultat zu gewährleisten? Diese Bewertungen sollten optimalerweise von mehreren Experten vergeben und mit einer mathematischen Methode auf einen gemeinsamen Nenner gebracht werden. Um diese Aufgabe im Rahmen dieser Arbeit zu vereinfachen, werden mögliche Konsequenzen in Klassen eingeteilt und diesen Klassen Werte zugewiesen. Diese sind in der folgenden Tabelle hinterlegt.

Die Klassen wurden aus [5] entnommen, die dazugehörigen Zahlenwerte nach eigenen Einschätzungen vergeben. Sollten sich diese als ungeeignet herausstellen, können sie angepasst werden.

PK-Konsequenz	Wert
Keine	0
Geringfügig / Tolerabel	0.3
Erheblich	0.6
Existentiell bedrohend	0.9

Tab. 4.1: Konsequenz-Klassen

Im Rahmen dieser Arbeit wird die PK-Konsequenz sowie die PK-Gewichtung aller 59 Prüfungskriterien vom Autor bewertet. Mit diesen bewerteten Prüfungskriterien als Grundlage wird im weiteren Verlauf der Prototyp sowie dessen Anwendbarkeit getestet und bewertet. Die detaillierte List der Prüfungskriterien mit Konsequenz- und Gewichtungswerten kann im AnhangE gefunden werden.

4.3.1 Fazit

Zu bestimmen, wie hoch eine mögliche Konsequenz eines Mangels für ein bestimmtes Attribut (C, I, A) eines Prüfungskriterium ist bzw. sein könnte, hat sich als schwierig herausgestellt. Grund dafür ist unter anderem die nicht immer gegebene Unabhängigkeit zwischen den Attributen. Ist z. B. bei einem Mangel die Vertraulichkeit betroffen, leiden möglicherweise auch Verfügbarkeit und Integrität darunter. Die Einteilung der PK-Konsequenz-Bewertungen in Klassen, hat bei der Bewertung geholfen, der Autor hat sie jedoch viele Male als zu einschränkend wahrgenommen. Ein weiterer Punkt ist, dass der Autor die meisten Prüfungskriterien als „*grosser Mangel*“ bewertet hat. Da es ein Ziel der Arbeit ist, das geprüfte Unternehmen auf ein Grundschutz-Niveau zu heben, scheint es nur eine logische Folge zu sein, dass die meisten Punkte auf der Liste auch grosse Mängel darstellen. Soll diese Methode für einen Einsatz in der Industrie weiterentwickelt bzw. umgesetzt werden, so müssten nach Ansicht des Autors mehrere IT-Security-Experten an der Bewertung der Prüfungskriterien teilnehmen und die gesammelten Werte mit einer mathematischen Methode zusammengefasst werden. Dabei sollten die Bewertungen nicht mit Klassen, sondern mit einer genaueren Methode erfasst werden können. Zudem sollte nochmals überdenkt werden, ob es Sinn macht, die Prüfungskriterien untereinander zu gewichten.

5 Entwicklung des Prototyps

Die Methode ist bereits in Excel umgesetzt. Dies erlaubt es, die Funktionalität aufzuzeigen, sowie rasch Anpassungen vornehmen zu können. Dieses Vorgehen hat jedoch auch Nachteile. Zum einen nimmt die Übersichtlichkeit bei einer hohen Anzahl an Prüfungskriterien ab und zum anderen stösst man bei der Programmierung der Auswertung rasch an Grenzen. Excel erlaubt zwar diverse Kontrollstrukturen (z. B. IF ELSE) mit deren Hilfe man eine gewisse Logik einbauen kann, der dafür notwendige Code wird jedoch rasch komplex und unübersichtlich. Zwischenresultate, die es für die Auswertung häufiger braucht, müssen zudem in zusätzliche Felder abgespeichert werden. Diese können dann zwar „versteckt“ werden, fügen dem Excel-Blatt jedoch nur noch mehr, für den Endbenutzer nicht relevante Informationen hinzu. Eine derartige Umsetzung ist zwar während der Entwicklung einer Methode, wenn diese sich rasch ändert und angepasst werden muss, praktisch, für einen Endbenutzer jedoch heutzutage ungeeignet. Im Rahmen dieser Arbeit soll daher ein Prototyp entwickelt werden. Ziel ist es, einem IT-Sicherheitsverantwortlichen oder IT-Administrator eines KMUs ein Programm zur Verfügung zu stellen, welches die bereits entwickelte Methode umsetzt und zugleich zugänglicher und einfacher bedienbar macht. Das Programm soll sich dabei an folgende Grundsätze halten:

- Beim Programm muss es sich um ein Web-Tool handeln.
- Das Programm muss einfach zu beziehen/installier-/bedienbar sein.
- Der Benutzer soll keine zusätzliche Software installieren müssen. (Eine aktuelle Version eines Web-Browser gilt wird hierbei nicht als zusätzliche Software)

Mit diesen Grundsätzen soll sichergestellt werden, dass eine möglichst hohe Anzahl an Benutzern erreicht werden kann.

5.1 Vorgehen

Der Autor selbst hat nur geringe Erfahrung in der Softwareentwicklung und stützt sich deshalb bei der Entwicklung dieses Prototyps auf [8]. Zur Beschreibung, was ein Programm können muss, werden in dieser Quelle sogenannte *User-Stories* verwendet. Dies sind ein wenig informellere *Use Cases*. Zur genaueren Beschreibung, was das Programm können muss, werden deshalb in diesem Projekt *Use Cases* anstatt *User-Stories* verwendet. Um *Use Cases* korrekt anzuwenden, wird sich an [7] gehalten.

Um die Vorstellung, wie der Prototyp aussehen soll zu konkretisieren, werden in einem ersten Schritt Mockups erstellt. Mockups sind visuelle Darstellungen des Prototyps. Sie bilden die Grundlage der Entwicklung. In einem ersten Schritt werden daraus die Anforderungen (Requirements), die der Prototyp erfüllen soll, definiert.

Daraus werden *Use Cases* abgeleitet die beschreiben, wie die Anforderungen umgesetzt werden sollen bzw. wie der Benutzer mit dem System interagiert.

Nachdem festgelegt wurde, was das Programm können und was zu dessen Realisierung getan werden muss, wird der eigentliche Prototyp entwickelt. Dazu muss entschieden werden, was für Technologien (Programmiersprache, Framework etc.) zum Einsatz kommen sollen.

Zusammengefasst wird der Prototyp in folgenden Schritte umgesetzt:

1. Erstellen der Mockups.
2. Ableitung der Anforderungen und Use Cases aus den Mockups.
3. Festlegen, mit welchen Technologien der Prototyp umgesetzt wird.
4. Erstellung des Prototyps gemäss Anforderungen und Architektur.

5.2 Mockups und Anforderungen

Die Mockups sind dafür zuständig, bereits vor der Umsetzung eine Vorstellung davon zu erhalten, wie das fertige Produkt aussehen soll. Daraus lassen sich direkt Anforderungen ableiten. Die formalisierten Anforderungen können in Anhang F.1 gefunden werden. Die Mockups wurden mit Hilfe des Web-Tools¹ der Firma *Balsamiq* erstellt.

¹<http://www.balsamiq.com/products/mockups>

5.2.1 Index Mockup

A Web Page

file:///C:/User/Data/Audit/index.html

Audit

Schutzziel-Definition:

C: I: A:

Persönliche Daten:

Firma:

Abteilung:

Datum:

Name:

Benutzeranleitung:

Audit Links:

[Audit ausführen](#) [Auswertung Audit](#)

Abb. 5.1: Index Mockup

1. Der Benutzer muss auf dieser Seite die Schutzziel-Erfüllung eingeben können. Das heisst, dass er für jedes Attribut einen Wert zwischen 1 und 10 eingeben kann, der ausdrückt, wie wichtig ihm das jeweilige Attribut ist.
2. Der Benutzer muss diverse persönliche Daten eingeben können. Welche genau ist noch nicht genau definiert. Diese persönlichen Daten müssen in der Auswertung des Audits wieder dargestellt werden.
3. Auf der Start-Seite muss sich auch eine kurze Anleitung zur Verwendung des Audits finden.

4. Auf der Start-Seite müssen sich 2 Links befinden. Einer führt zum Audit selbst, der andere zu dessen Auswertung.

5.2.2 Audit Mockup

A Web Page

file:///C:/User/Data/Audit/audit.html

Audit

Sicherheitsaspekt 1	
Sicherheitsaspekt 2	
Prüfungskriterium 2.1	Ja
Prüfungskriterium 2.2	Nein
Prüfungskriterium 2.3	Teilweise
Prüfungskriterium 2.4	Nicht relevant
Sicherheitsaspekt 3	
Sicherheitsaspekt 4	

Erfüllung-Total:
C: 45%
I: 30%
A: 55%

Audit auswerten
Audit zurücksetzen
Startseite

Abb. 5.2: Audit Mockup

1. Der Benutzer muss die Möglichkeit haben, alle Prüfungskriterien aller Sicherheitsaspekte nach den definierten Bewertungsmöglichkeiten zu bewerten.
2. Der Benutzer soll zu jeder Zeit die Gesamt-Erfüllung des Audits sehen.
3. Der Benutzer hat 3 Links zur Verfügung. Er kann den Audit auswerten oder zurücksetzen lassen, oder zur Startseite zurück gelangen.

5.2.3 Auswertung Mockup

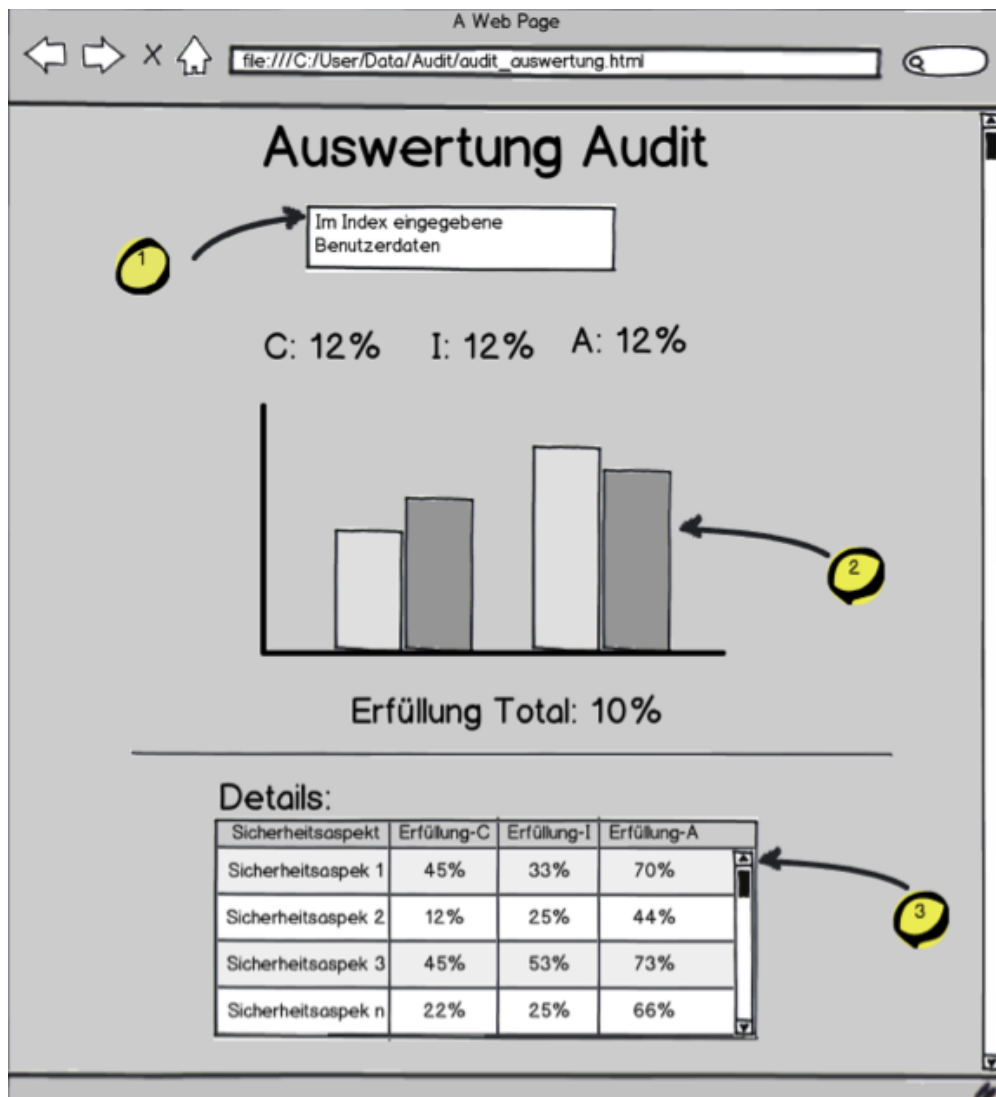


Abb. 5.3: Auswertung Mockup

1. Der Benutzer sieht seine auf der Index-Seite eingegebenen persönlichen Daten.
2. Die Gesamt-Erfüllung der Attribute soll graphisch dargestellt werden. Zusätzlich soll die Gesamt-Erfüllung des Audits ersichtlich sein.
3. Die Detail-Erfüllung der einzelnen Sicherheitsaspekte soll in einer Tabelle dargestellt werden.

5.3 Use Cases

Aus den Anforderungen können nun *Use Cases* abgeleitet werden. Es wurde eine Rolle identifiziert welche mit dem System interagiert, der *Benutzer*.

Benutzer: Der Benutzer führt den Audit durch und veranlasst eine Auswertung desselben.

Die *Use Cases* sind in folgendem Diagramm dargestellt:

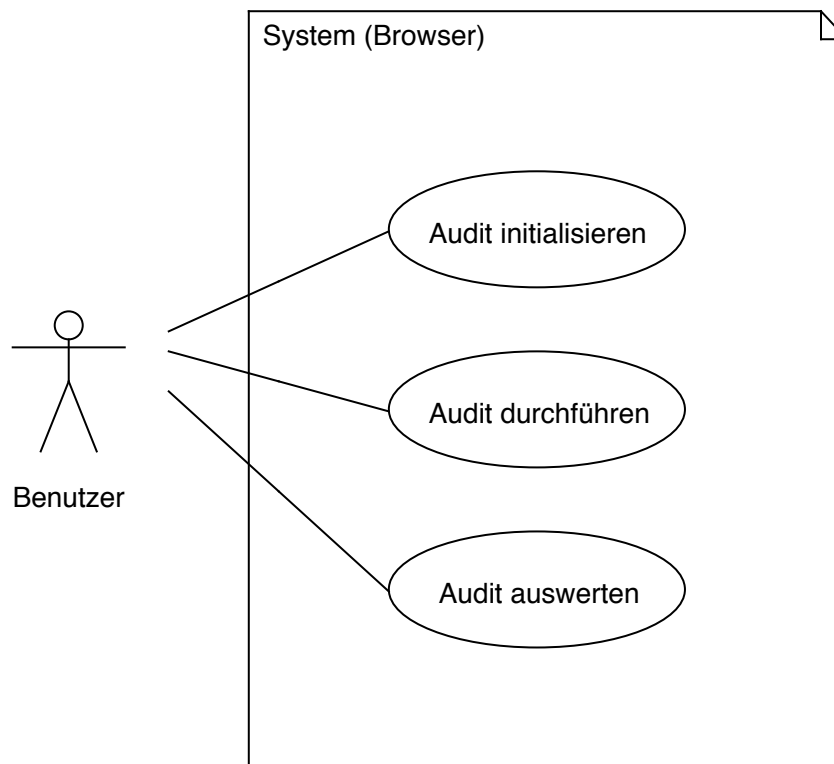


Abb. 5.4: Prototyp - Use Cases

Use-Case U.1: Audit initialisieren:

Der Benutzer definiert die Schutzziel-Definitionen, gibt seine persönliche Daten ein und wird über die Benutzung des Tools informiert.

Use-Case U.2: Audit durchführen:

Der Benutzer bewertet alle Prüfungskriterien und sieht während der Bewertung die Gesamt-Erfüllung aller Attribute.

Use-Case U.3: Audit auswerten:

Der Benutzer lässt den Audit auswerten und bekommt einen Report dargestellt, in dem seine persönlichen Daten, die Gesamt-Erfüllung der Attribute sowie die Detail-Erfüllung der einzelnen Sicherheitsaspekte dargestellt werden.

Die detaillierte Beschreibung der Use Cases kann im Anhang F.2 gefunden werden.

5.4 Architektur / Technologien zur Umsetzung

Aufgrund der in Kap. 5.1 definierten Grundsätze wird der Prototyp als HTML5-Web-Applikation umgesetzt. Jegliche Daten werden auf dem Client gespeichert. Einzige Voraussetzung zur Verwendung des Prototyps ist ein somit moderner Web-Browser (Tab. 5.1). Zur Umsetzung werden folgende Technologien verwendet.

Daten Die für den Audit benötigte Datenstruktur wird als JSON-Objekt in einem File abgelegt und zur persistenten Speicherung im *Local Storage* abgelegt. Der *Local Storage* ist ein HTML5 Feature, welches eine lokale Speicherung von bis zu 5MB an Daten erlaubt und wurde bereits von allen Web-Browserherstellern implementiert [2][12]. Es erlaubt, dass der Benutzer, obwohl er keine Datenbank installieren muss, ausgefüllte Audits nicht verliert.

Logik Die Client-Sprache der Browser ist *JavaScript*. Die gesamte Logik bzw. Umsetzung der Methode wird in dieser Sprache programmiert. Zur Vereinfachung der Programmierarbeit und Sicherstellung einer hoher Web-Browser-Kompatibilität werden für diverse Aufgaben die *JQuery*² und *JQuery UI*³ Bibliotheken eingesetzt.

Darstellung Für die Darstellung der Webseiten wird CSS verwendet. Um die Auswertung zu zeichnen wird das von HTML5 angebotene *Canvas*-Objekt verwendet. Es wird wie der Local Storage bereits von allen Web-Browserherstellern implementiert [12].

Eine detaillierte Beschreibung der JSON-Datenstruktur kann im Anhang F.3 gefunden werden. Eine Beschreibung aller zum Prototyp gehörenden Files ist im Anhang F.4 abgelegt.

5.4.1 Voraussetzung Browser-Versionen

Die beiden verwendeten HTML5 Features, *Local Storage* und *Canvas*, werden von allen bekannten Web-Browserherstellern implementiert. Anbei eine Spezifikation aus [2], bezüglich welche Versionen dieser Browser diese HTML5 Features und somit die Verwendung dieses Prototyps unterstützen.

²<http://www.jquery.com>

³<http://www.jqueryui.com>

OS	MAC				Windows				
Hersteller	Safari	Firefox	Opera	Chrome	Safari	IE	Firefox	Opera	Chrome
Version	5.1	11	11.62	18	5.1	9	11	11.61	18
Test	O	O	O	O	O	X	O	O	O

Tab. 5.1: Unterstützte Web-Browser-Versionen

Die Funktionalität wurde auf allen in der Tabelle vorkommenden Browsern getestet. Das Resultat dieses Tests ist in der dritten Zeile ersichtlich. *O* steht für erfolgreiche Tests und *X* für nicht erfolgreiche Tests. Auf allen Browser bis auf den *Internet Explorer 9* funktioniert es. Grund dafür ist, dass der InternetExplorer 9 das LocalStorage Feature für lokale Files nicht erlaubt.

5.5 Projektmanagement

Zur Versionenkontrolle wird Git⁴ verwendet. Alle Files des Prototypen sind auf dem öffentlichen github-Repository <https://github.com/sandorkan/Semesterarbeit> abgelegt.

5.5.1 Installation

Auf dem oben erwähnten github-Repository befindet sich ein Zip-File (Audit_Prototyp.zip), welches alle Files enthält, die es zur Verwendung des Prototyps braucht. Zur Benutzung des Prototyps lädt man sich dieses Zip-File herunter, entpackt es und öffnet das *Index.html* File mit einem Browser seiner Wahl.

5.6 Fazit

Der Prototyp wurde aufgrund der in Kap. 5.1 definierten Grundsätze, welche sich auch aus der Aufgabenstellung ableiteten, als HTML5 Web-Applikation erstellt. Daraus ergeben sich folgende Vorteile:

- Zur Benutzung des Programmes werden lediglich die Dateien benötigt.
- Die Datenstruktur mit JSON ist sehr intuitiv und zur Verwendung mit JavaScript geeignet.
- Dank HTML5 Technologien kommt man ohne Datenbank aus.
- Da zur Benutzung nur einen Web-Browser benötigt wird, ist das Programm betriebssystemunabhängig anwendbar.

⁴<http://git-scm.com/>

- Die Lösung bleibt übersichtlich. Es muss kein Framework eingesetzt werden. Es braucht keinen Web-Server auf welchem die Applikation gehostet wird.

Dass der Prototyp so einfach wie möglich zu installieren ist und möglichst einfach vielen Benutzern zur Verfügung stehen soll, waren bei der Entwicklung des Prototyps für den Autoren die wichtigsten Eigenschaften. Zudem waren die eingesetzten Technologien bereits aus anderen Arbeiten bekannt. Die Lösung unterscheidet sich von der klassischen Implementation einer Web-Applikation (z.B. PHP & MySql) wodurch sich auch einige Nachteile ergeben:

- Durch den Einsatz einer relationalen Datenbank wären spätere Auswertungen der Audits möglich gewesen.
- Das *Local Storage* Feature bietet einen Speicherplatz von 5MB. Wenn es möglich sein soll, mehrere Audits zu speichern, könnte dieser Speicherplatz knapp werden.
- Daten die im *Local Storage* gespeichert sind, sind nur von dem Web-Browser mit dem sie erstellt wurden abrufbar. Der Benutzer ist somit an einen bestimmten Web-Browser gebunden, wenn er auf einen bereits ausgefüllten Audit zugreifen will.

Ein Prototyp ist dafür gedacht, aufzuzeigen, wie eine mögliche Umsetzung aussehen könnte. Mit dem in dieser Arbeit entwickelten Prototyp ist dies gelungen. Soll die in dieser Arbeit dargelegte Methodik jedoch professionell eingesetzt werden, sollte nach Ansicht der Autors eine gehostete Web-Applikation mit einer relativen Datenbank erstellt werden. Hätte man eine Datenbank zur Verfügung, könnte man bereits ausgefüllte Audits auswerten und so interessante Erkenntnisse bezüglich der IT-Security in KMU's in der Schweiz gewinnen. Auch eine Anpassung von Prüfungskriterien oder Bewertungen der Prüfungskriterien wären dann denkbar.

6 Case Study - Test der Funktionalität und Anwendbarkeit

Der entwickelte Prototyp wird nun auf seine Funktionalität sowie Anwendbarkeit getestet. Die Funktionalität wird anhand der aufgestellten Anforderungen (Anhang F.1) und Use Cases (Anhang F.2) überprüft. Die Anwendbarkeit wird mit einem komplett durchgeführten Audit bewertet. Dabei wird versucht Stärken und Schwächen des Prototyps bzw. der Methode zu finden.

Für den Test des Prototyps wird die IT eines ehemaligen Arbeitgebers des Autors bewertet. Es wird der dem Autor letzte bekannte Stand der IT bewertet.

Da die Firma eine grosse Menge an vertraulichen Kundendaten besitzt, mit denen sie täglich Arbeiten muss, wird bei der Schutzziel-Definition sowohl der Vertraulichkeit sowie auch der Verfügbarkeit einen hohen Wert zugewiesen. Die Schutzziel-Definitionen für den Test-Audit wurden wie folgt definiert: *Vertraulichkeit: 8, Integrität: 4, Verfügbarkeit: 8*

Funktionalität

Sämtliche in Anhang F.1 gestellten Anforderungen sind umgesetzt. Die in Anhang F.2 beschriebenen Use Cases sind allesamt funktionsfähig.

Schwächen

Die negative Formulierung der Prüfungskriterien passt nicht zu den Bewertungsmöglichkeiten. In der entwickelten Methode wurde definiert, dass Prüfungskriterien häufig auftretende Mängel sind und negativ formuliert werden. Als Bewertungsmöglichkeiten wurden *“In Ordnung”*, *“Akzeptabel”* und *“Nicht akzeptabel”* übernommen. Mit *“Nicht akzeptabel”* wird ausgedrückt, dass ein Mangel vorhanden ist. Hat man aber ein Prüfungskriterium wie *“Verstösse gegen die Sicherheitsrichtlinie werden nicht geahndet”* und will ausdrücken, dass der Mangel besteht, passt die Bewertung *“Nicht akzeptabel”* nicht. Einer solchen Aussage würde man nicht eine solche Bewertung geben. Es verhält sich mit allen anderen Prüfungskriterien gleich. Der Autor ist der Ansicht, dass es hier passender wäre, Prüfungskriterien positiv zu formulieren und die Bewertungsmöglichkeiten in *“Ja”*, *“Nein”* und *“Teilweise”* abzuändern.

Bei manchen Sicherheitsaspekten wäre es sinnvoll, auf dem Level des Sicherheitsaspektes definieren zu können, ob der Sicherheitsaspekt überhaupt vorhanden ist. Ein Beispiel dafür ist der Sicherheitsaspekt *“Sicherheitsrichtlinie”*. Hat eine Firma keine Sicherheitsrichtlinie, bräuchte man die dazu gehörigen Prüfungskriterien eigentlich nicht zu bewerten. Man könnte eine Regel definieren die besagt, dass wenn ein Sicherheitsaspekt nicht vorhanden ist, alle zum Sicherheitsaspekt gehörenden Prüfungskriterien so schlecht wie möglich bewertet werden.

Nach dem Ausfüllen des Audits stellt sich die Frage, ob die Bewertungsmöglichkeit *“Nicht relevant”* gebraucht wird. Sie wurde einzig beim PK *“Ausfall von Lieferanten oder Dienstleister”* gebraucht. Bei den meisten anderen Prüfungskriterien handelt es sich jedoch um so grundlegende Komponenten der IT-Security, dass diese Bewertungsmöglichkeit sehr wahrscheinlich fast nie gebraucht wird.

Bei einigen Prüfungskriterien wäre es hilfreich, eine Art Hilfe-Knopf anbieten zu können, der dazu verwendet werden kann, Prüfungskriterien genauer zu beschreiben.

Einige Prüfungskriterien passen nicht wirklich in den Sicherheitsaspekt, in dem sie aufgeführt sind. Das Prüfungskriterium *“Es werden keine externen Sicherheitsexperten damit beauftragt, kritische Bereiche der internen IT-Sicherheit zu überprüfen”* zum Beispiel ist unter dem Sicherheitsaspekt *“Sicherheitsrichtlinie”*, passt aber weder dort, noch in irgend einen anderen Sicherheitsaspekt.

Stärken

Obwohl es an die 60 Prüfungskriterien gibt, ist deren Darstellung im Prototyp sehr kompakt und übersichtlich gehalten. Zudem sieht man jederzeit, wie hoch die Erfüllung der Sicherheitsaspekte und der Attribute ist. Dies hilft einem zu sehen, wie sich ein einzelnes Prüfungskriterium auf den Sicherheitsaspekt bzw. das Gesamt-Resultat auswirkt.

Bei der Auswertung des Audits gibt einem die Darstellung der Gesamt-Erfüllung der Schutzziele einen raschen und übersichtlichen Überblick über den Zustand der IT-Security eines Unternehmens.

Bei der Auswertung des Audits zeigt die Tabelle schön auf, bei welchen Sicherheitsaspekten noch Verbesserungspotential besteht. Hier wäre es vielleicht hilfreich, Sicherheitsaspekte die eine besonders niedrige Erfüllungsrate haben hervorzuheben.

Anpassungen des Prototyps

Aufgrund der bei dem Test der Anwendbarkeit aufgedeckten Schwächen, wurden folgende Anpassungen des Prototyps vorgenommen.

- Der Sicherheitsaspekt *“Sicherheitsrichtlinie”* wird in *“Organisatorische Sicherheit”* umbenannt.
- Alle Prüfungskriterien werden anstatt negativ nun positiv formuliert. Z. B. :
 - Alt: *“Das Gebäude ist nicht vor Einbrechern geschützt.”*
 - Neu: *“Das Gebäude ist vor Einbrechern geschützt.”*
- Die Formulierung der Bewertungskriterien wird geändert um besser auf die Prüfungskriterien zu passen.
 - Alt: *“In Ordnung”* Neu: *“Ja”*
 - Alt: *“Akzeptabel”* Neu: *“Teilweise”*
 - Alt: *“Nicht akzeptabel”* Neu: *“Nein”*

7 Schlussfolgerungen

Es hat sich gezeigt, dass die von der ZHAW entwickelte Methode generisch anwendbar ist und sich an die IT-Branche anpassen lässt. Die Anwendung von Attributen zur Beschreibung von möglichen Schäden erlaubt eine vollständige und akkurate Beschreibung von Gefahren. Für die Methode in dieser Arbeit wurden zur Beschreibung eines Schadens die klassischen IT-Security-Grundsätze *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* gewählt. Es wären aber durchaus auch andere Attribute, wie *Kosten* oder *Reputation* denkbar. Zur Bestimmung einer Liste relevanter Prüfungskriterien wurden mit dem *ISO 27002* sowie dem *BSI Leitfaden Informationssicherheit* zwei anerkannte IT-Security-Standards zu Rate gezogen. Diverse IT-Security-Surveys bestätigten und erweiterten diese Liste. In der bereits entwickelten Methode werden Prüfungskriterien als Mängel definiert und negativ formuliert (z. B. : *“Es ist keine Sicherheitsrichtlinie vorhanden”*). Dies hat sich für die Befragung als nicht passend herausgestellt und wurde abgeändert. Die Bewertung der Prüfungskriterien wurden vom Autor selbst durchgeführt. Als Prototyp, mit dem diese Methode getestet werden kann, wurde eine HTML5 Web-Applikation entwickelt, die komplett auf dem Client läuft. Die von der Methode vorgegebenen Berechnungsfunktionen liessen sich ohne Probleme implementieren und liefern die erwarteten Resultate.

Die von der ZHAW entwickelte Methode funktioniert auf einer theoretischen Ebenen ohne Probleme. Das Grundgerüst der Methode - die Attribute, die Prüfungskriterien sowie deren Bewertung - sollte idealerweise in Zusammenarbeit mit mehreren Experten erstellt werden. Nur so lässt sich sicherstellen, dass die Methode verlässliche und aussagekräftige Resultate generiert. Die in dieser Arbeit definierten Prüfungskriterien und Attribute sowie deren Bewertung könnte man als anzupassende Start-Menge verwenden. Der Prototyp sollte in einem nächsten Schritt in eine auf einem Server laufende Web-Applikation mit einer Datenbank weiterentwickelt werden. So wäre die Sammlung und Auswertung mehrerer Audits möglich. Dadurch könnte ein Bild der IT-Security-Lage von KMUs gewonnen werden. Weiter könnten KMUs von sich aus Inputs bezüglich Prüfungskriterien sowie Attributen liefern und somit die Methode aktuell und relevant halten.

Die gesetzten Ziele wurden erreicht. Die Methode wurde formell beschrieben, jedes Element ist nun durch eine Variabel und jede Berechnung durch eine Gleichung ausgedrückt. Attribute und Prüfungskriterien wurden mit Hilfe von Standards und Surveys definiert. Ein funktionierender Prototyp lässt die Methode anwenden. Die Arbeit hat sich jedoch als aufwendiger als erwartet herausgestellt. Zur zufriedenstellender Anpassung der Methode bräuchte es mehr Zeit als die für diese Arbeit vorgegebenen 15 Tage. So könnten noch mehr Standards und Surveys berücksichtigt werden. Zusätzlich sollten Experten-Befragungen definiert und durchgeführt werden.

A Projektplan Semesterarbeit

Dies ist der konzeptionelle Projektplan der Semesterarbeit. Die Arbeit selbst wurde nach den in dem Plan definierten Schritten, jedoch über einen Zeitraum von mehreren Monaten durchgeführt.

ID	Aufgabe	Dauer	29 Apr 2012		6 Mai 2012							13 Mai 2012							20 Mai 2012							27 Mai 2012				
			4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28			
1	Detailplanung	1T																												
2	Beschreibung der Methode	3T																												
3	Anpassung der Methode	5T																												
4	Literaturrecherche	1T																												
5	Definition der Prüfungskriterien und Attribute	3T																												
6	Bewertung der Prüfungskriterien	1T																												
7	MS: Bewertete Liste von Prüfungskriterien	1T																												
8	Entwicklung des Prototyps	7T																												
9	Erstellen des Konzeptes (Anforderungen, Use Cases)	2T																												
10	Definition Umsetzungstechnik	1T																												
11	Entwicklung Prototyp	4T																												
12	MS: Fertigstellung Prototyp	1T																												
13	Erstellen Dokumentation	15T																												
14	MS: Abgabe Arbeit																													

Abb. A.1: Projektplan Semesterarbeit

B Anhang Methodik

B.1 Berechnungsparameter Detailliert

Bezeichnung	Prüfungskriterium
Variabel	i
Bedeutung	Bezeichnet ein Prüfungskriterium
Detail	$i = \{1, \dots, n\}$ $n = \text{Anzahl an Prüfungskriterien}$

Tab. B.1: Definition Variabel für Prüfungskriterien

Bezeichnung	Sicherheitsaspekt
Variabel	s
Bedeutung	Bezeichnet einen Sicherheitsaspekt
Detail	$s = \{1, \dots, n\}$ $n = \text{Anzahl Sicherheitsaspekte}$

Tab. B.2: Definition Variabel für Sicherheitsaspekt

Bezeichnung	Attribut-Gewichtung Branche
Variabel	a_j ($0 \leq a \leq 10$)
Bedeutung	Gewichtung des Attributes j über gesamte Branche
Detail	$j = \{1, \dots, n\}$ $n = \text{Anzahl an Attributen.}$ $\sum a_j = 10$

Tab. B.3: Definition Attribut-Gewichtung Branche

Bezeichnung	Attribut-Konsequenz
Variabel	$c_{s,i,j}$ ($0 \leq c \leq 1$)
Bedeutung	Konsequenz von PK i aus SA s auf Attribut j
Detail	$j = \{1, \dots, n\}$ $n = \text{Anzahl an Attributen}$

Tab. B.4: Definition Attribut-Konsequenz

Bezeichnung	PK-Gewichtung
Variabel	$w_{s,i,k}$ ($0 \leq w \leq 1$)
Bedeutung	Relative Wichtung k von PK i aus SA s
Detail	$k = \{1, \dots, n\}$ $n = \text{Anzahl Gewichtungsmöglichkeiten}$

Tab. B.5: Definition PK-Gewichtung

Bezeichnung	PK-Bewertung
Variabel	$b_{s,i,l}$ ($0 \leq b \leq 1$)
Bedeutung	Bewertung l von PK i aus SA s
Detail	$l = \{0, \dots, n\}$ $n = \text{Anzahl Bewertungsmöglichkeiten}$

Tab. B.6: Definition PK-Bewertung

B.2 Methode Excel-Umsetzung mit Variablenbeschriftung

Die rein textliche Beschreibung der Methode wird rasch komplex. Die folgenden zwei Abbildungen sollen hierbei Abhilfe schaffen, indem sie zeigen, wie die Methode in Excel umgesetzt wurde und wo die jeweiligen Variablen zum Einsatz kommen. Die erste Abbildung zeigt die Grundlage der Methode: Die Prüfungskriterien sowie deren Bewertung, die festgelegt werden müssen bevor ein Audit stattfinden kann. Die zweite Abbildung ist praktisch identisch mit der ersten, zeigt jedoch die Methode aus Sicht des Auditors. Dort sieht man, dass dem Auditor Bewertungsmöglichkeiten zur Verfügung stehen (hellblau markierte Felder), sowie bereits die berechneten Resultate.

		Gewichtung Attribute				PK-Gewichtung
		Attribut 1 $j = 1$ $a_1 = 4$	Attribut 2 $j = 2$ $a_2 = 3$	Attribut 3 $j = 3$ $a_3 = 2$	Attribut 4 $j = 4$ $a_4 = 1$	
Sicherheitsaspekte	Gesamtgewichtung Attribute =>					
BEREICH 1						
Sicherheitsaspekt 1	$s = 1$	Attribut Konsequenzen				
	Prüfungskriterium 1 $i = 1$	$c_{1,1,1} = 0.8$	$c_{1,1,2} = 0.4$	$c_{1,1,3} = 0.4$	$c_{1,1,4} = 0$	$w_{1,1,2} = 1$
	Prüfungskriterium 2 $i = 2$	$c_{1,2,1} = 0$	$c_{1,2,2} = 0.5$	0	0.7	$w_{1,2,2} = 1$
	Prüfungskriterium 3 $i = 3$	$c_{1,3,1} = 0$	0.4	0	0.8	$w_{1,3,1} = 0.5$
	Prüfungskriterium 4 $i = 4$	$c_{1,4,1} = 0$	0.4	0.6	0.6	$w_{1,4,1} = 0.5$
	Prüfungskriterium 5 $i = 5$	$c_{1,5,1} = 0$	0.4	0.6	0.6	$w_{1,5,0} = 0.25$
Sicherheitsaspekt 2	$s = 2$					
Sicherheitsaspekt 3	$s = 3$					
BEREICH 2						
Sicherheitsaspekt 4	$s = 4$					
	Prüfungskriterium 6 $i = 6$	$c_{4,6,1} = 0.7$	$c_{4,6,2} = 0$	$c_{4,6,3} = 0$	$c_{4,6,4} = 0.5$	$w_{4,6,2} = 1$
	Prüfungskriterium 7 $i = 7$	$c_{4,7,1} = 0$	$c_{4,7,2} = 0.8$	0.4	0	$w_{4,7,1} = 0.5$
	Prüfungskriterium 8 $i = 8$	$c_{4,8,1} = 0.4$	0.5	0.5	0.4	$w_{4,8,1} = 0.5$
	Prüfungskriterium 9 $i = 9$	$c_{4,9,1} = 0$	0	0.8	0.7	$w_{4,9,0} = 0.25$
	Prüfungskriterium 10 $i = 10$	$c_{4,10,1} = 0$	0.6	0.4	0.3	$w_{4,10,0} = 0.25$
Sicherheitsaspekt 5	$s = 5$					
Sicherheitsaspekt 6	$s = 6$					
BEREICH 3						
Sicherheitsaspekt 7	$s = 7$					
Kriterium 8	$s = 8$					
BEREICH 4						
Kriterium 9	$s = 9$					
Kriterium 10	$s = 10$					

Abb. B.1: Excel-Umsetzung: Definition

EINGABE	Felder mit dieser Farbe können manipuliert werden				
	Gesamtgewichtung PGSU				PK Bewertung
	Gesamtgewichtung Attribute =>	Attribut 1	Attribut 2	Attribut 3	
Sicherheitsaspekte		4	3	2	1
BEREICH 1					
Sicherheitsaspekt 1					
Prüfungskriterium 1		$r_{1,1,1} = 0.8$	$r_{1,1,2} = 0.4$	$r_{1,1,3} = 0.4$	$r_{1,1,4} = 0$
Prüfungskriterium 2		$r_{1,2,1} = 0$	$r_{1,2,2} = 0.25$	0	0.35
Prüfungskriterium 3		$r_{1,3,1} = 0$	0	0	0
Prüfungskriterium 4		$r_{1,4,1} = 0$	0.1	0.15	0.15
Prüfungskriterium 5		$r_{1,5,1} = 0$	0.1	0.15	0.15
Positive Summe Brandabschnitt		$z_{1,1} = 0.8$	$z_{1,2} = 0.85$	$z_{1,3} = 0.7$	$z_{1,4} = 0.65$
Maximum nach Abzug der nicht rel. Attribute		$z_{Max1,1} = 0.8$	$z_{Max1,2} = 1.4$	$z_{Max1,3} = 0.85$	$z_{Max1,4} = 1.55$
Prozentuale Erfüllung Attribut		1	0.61	0.82	0.42
Sicherheitsaspekt 2					
Sicherheitsaspekt 3					
BEREICH 2					
Sicherheitsaspekt 4					
Prüfungskriterium 6		$r_{4,6,1} = 0$	$r_{4,6,2} = 0$	$r_{4,6,3} = 0$	$r_{4,6,4} = 0$
Prüfungskriterium 7		$r_{4,7,1} = 0$	$r_{4,7,2} = 0.4$	0.2	0
Prüfungskriterium 8		$r_{4,8,1} = 0.1$	0.125	0.125	0.1
Prüfungskriterium 9		$r_{4,9,1} = 0$	0	0.2	0.175
Prüfungskriterium 10		$r_{4,10,1} = 0$	0.15	0.1	0.075
Prozentuale Erfüllung Attribut		0.41	0.84	0.83	0.37
Attribut Verhältnis Max		1	1	1	1
Sicherheitsaspekt 5					
Sicherheitsaspekt 6					
BEREICH 3					
Sicherheitsaspekt 7					
Sicherheitsaspekt 8					
BEREICH 4					
Sicherheitsaspekt 9					
Sicherheitsaspekt 10					
SUMME		$r_1 = 0.9$	$r_2 = 1.525$	$r_3 = 1.325$	$r_4 = 1$
Summe Maximum		$f_{Max1} = 1.7$	$f_{Max2} = 2.2$	$f_{Max3} = 1.6$	$f_{Max4} = 2.5$
PGSU Ausgleich / Prozentuale Erfüllung		0.53	0.89	0.83	0.4
PGSU Gewichtung / Endbewertung		$u_1 = 2.12$	$u_2 = 2.07$	$u_3 = 1.66$	$u_4 = 0.4$
TOTAL					$v_4 = 6.25$
					10

Abb. B.2: Excel-Umsetzung: Auswertung

C Leitfaden Informationssicherheit : Zusammengefasste Prüfungskriterien

C.1 Szenarien und Massnahmen

- **Szenario 1: Kein Backup**

Massnahmen

- Regelmässige Überprüfung der Backup-Bänder
- Rücksicherung prüfen und üben
- Lagerung von Sicherungsbändern ausserhalb der eigenen Büroräume

- **Szenario 2: Befall durch Computer-Viren**

Massnahmen

- Update-Konzept für Sicherheits-Updates erstellen
- „IT-Inseln“ innerhalb des Unternehmens nicht vergessen

- **Szenario 3: Ausfall des Administrators**

Massnahmen

- System-Einstellungen und -Parameter ausführlich dokumentieren
- Passwörter sicher hinterlegen
- Notfallplan mit Anweisungen für die Verfahrensweise bei den wichtigsten Schadensfällen erstellen
- Vertretungsregeln einrichten

- **Szenario 4: Hackerangriff aus dem Internet**

Massnahmen

- Internet-Zugänge sichern
- vertrauliche Daten verschlüsseln

- **Szenario 5: Innentäter**

Massnahmen

- Räume und Gebäude gegen unbefugten Zutritt sichern
- wichtige Daten verschlüsseln

C.2 Häufige Versäumnisse

1. **Unzureichende Informationssicherheitsstrategie**

- Sicherheit hat einen zu geringen Stellenwert
- Dauerhafte Prozesse zur Beibehaltung des Sicherheitsniveaus fehlen

- Sicherheitsvorgaben sind nicht dokumentiert
- Kontrollmechanismen und Aufklärung im Fall von Verstößen fehlen

2. Schlechte Konfiguration von IT-Systemen

- Die Rechtevergabe wird nicht restriktiv genug gehandhabt
- IT-Systeme sind schlecht konfiguriert

3. Unsichere Vernetzung und Internet-Anbindung

- Sensitive Systeme sind gegen offene Netze unzureichend abgeschottet

4. Nichtbeachtung von Sicherheitserfordernissen

- Sicherheitsmaßnahmen werden aus Bequemlichkeit vernachlässigt
- Anwender und Administratoren sind mangelhaft geschult

5. Schlechte Wartung von IT-Systemen

- Verfügbare Sicherheits-Updates werden nicht eingespielt

6. Sorgloser Umgang mit Passwörtern und Sicherheitsmechanismen

- Mit Passwörtern wird zu sorglos umgegangen
- Vorhandene Sicherheitsmechanismen werden nicht genutzt

7. Mangelhafter Schutz vor Einbrechern und Elementarschäden

- Räume und IT-Systeme werden nur ungenügend gegen Diebstahl oder Elementarschäden geschützt

C.3 Wichtige Sicherheitsmassnahmen

Angemessene Berücksichtigung von Informationssicherheit

1. Informationssicherheitsaspekte müssen bei allen Projekten frühzeitig und ausreichend berücksichtigt werden
2. Im Falle mangelnder Ressourcen sollten alternative Lösungsansätze in Erwägung gezogen werden

Schritt für Schritt zu mehr Informationssicherheit

1. Die Informationssicherheitsziele müssen festgelegt werden, damit angemessene Maßnahmen definiert werden können
2. Zu jedem vorhandenen Sicherheitsziel und jeder zugehörigen Maßnahme sollten geeignete Regelungen getroffen werden

3. Ein Handlungsplan mit klaren Prioritäten der Sicherheitsziele und -maßnahmen sollte erstellt werden
4. Besonders umständliche Sicherheitsanforderungen sollten vermieden werden
5. Zuständigkeiten müssen festgelegt werden
6. Bestehende Richtlinien und Zuständigkeiten müssen bekannt gemacht werden

Kontrolle und Aufrechterhaltung der Informationssicherheit

1. Die Informationssicherheit sollte regelmäßig überprüft werden
2. Vorhandene Arbeitsabläufe und Sicherheitsrichtlinien sollten regelmäßig hinsichtlich Zweckmäßigkeit und Effizienz überprüft werden

Weiterführende Schritte

1. Langfristig sollte ein umfassendes Sicherheitsmanagement aufgebaut werden
2. Alle bestehenden Sicherheitsrichtlinien sollten schriftlich in einem Sicherheitskonzept dokumentiert werden

Sicherheit von IT-Systemen

1. Vorhandene Schutzmechanismen sollten genutzt werden
2. Viren-Schutzprogramme müssen flächendeckend eingesetzt werden
3. Datenzugriffsmöglichkeiten sollten auf das erforderliche Mindestmaß beschränkt werden
4. Allen Systembenutzern sollten Rollen und Profile zugeordnet werden
5. Administratorrechte sollten auf das erforderliche Maß eingeschränkt werden
6. Programmprivilegien sollten begrenzt werden
7. Die Standardeinstellungen gemäß Auslieferungszustand sollten geeignet angepasst werden
8. Handbücher und Produktdokumentationen sollten frühzeitig gelesen werden
9. Ausführliche Installations- und Systemdokumentationen müssen erstellt und regelmäßig aktualisiert werden

Vernetzung und Internet-Anbindung

1. Zum Schutz von Netzen muss eine Firewall verwendet werden
2. Eine sichere Firewall muss bestimmten Mindestanforderungen genügen
3. Nach außen angebotene Daten sollten auf das erforderliche Mindestmaß beschränkt werden
4. Nach außen angebotene Dienste und Programmfunktionalität sollten auf das erforderliche Mindestmaß beschränkt werden

5. Beim Umgang mit Web-Browsern ist besondere Vorsicht geboten, riskante Aktionen sollten unterbunden werden
6. Bei E-Mail-Anhängen ist besondere Vorsicht notwendig
7. Ein gesonderter Internet-PC zum Surfen ist eine kostengünstige Lösung für die meisten Sicherheitsprobleme bei der Internet-Nutzung
8. Faktor Mensch: Kenntnis und Beachtung von Sicherheitserfordernissen
9. Sicherheitsrichtlinien und -anforderungen müssen beachtet werden
10. Am Arbeitsplatz sollte Ordnung herrschen und sensitive Informationen nicht frei zugänglich sein
11. Bei Wartungs- und Reparaturarbeiten sind besondere Vorsichtsmaßnahmen zu beachten
12. Mitarbeiter müssen regelmäßig geschult werden
13. Nur eine ehrliche Selbsteinschätzung hilft weiter: Manchmal muss Expertenrat eingeholt werden
14. Für alle bestehenden Sicherheitsvorgaben sollten Kontrollmechanismen aufgebaut werden
15. Konsequenzen für Sicherheitsverstöße sollten festgelegt und veröffentlicht werden
16. Erkannte Sicherheitsverstöße sollten auch tatsächlich sanktioniert werden

Wartung von IT-Systemen: Umgang mit sicherheitsrelevanten Updates

1. Sicherheits-Updates müssen regelmäßig eingespielt werden
2. Zu den Sicherheitseigenschaften verwendeter Software sollten in regelmäßigen Abständen ausführliche Recherchen durchgeführt werden
3. Es sollte ein Aktionsplan zum Einspielen erforderlicher Sicherheits-Updates erstellt werden
4. Softwareänderungen sollten getestet werden

Verwendung von Sicherheitsmechanismen: Umgang mit Passwörtern und Verschlüsselung

1. Sicherheitsmechanismen sollten sorgfältig ausgesucht werden
2. Es müssen gut gewählte (sichere) Passwörter eingesetzt werden
3. Voreingestellte oder leere Passwörter sollten geändert werden
4. Arbeitsplatzrechner sollten bei Verlassen mit Bildschirmschoner und Kennwort gesichert werden
5. Sensitive Daten und Systeme müssen geschützt werden

Schutz vor Katastrophen und Elementarschäden

1. Notfallpläne sollten erstellt werden und jedem Mitarbeiter bekannt sein
2. Alle wichtigen Daten müssen regelmäßig gesichert werden (Backup)
3. IT-Systeme müssen angemessen gegen Feuer, Überhitzung, Wasserschäden und Stromausfall geschützt sein
4. Maßnahmen zum Zutrittsschutz und zum Schutz vor Einbrechern müssen umgesetzt werden
5. Der gesamte Bestand an Hard und Software sollte in einer Inventarliste erfasst werden

D ISO/IEC 27002:2005 :

Zusammenfassung Objectives

Der Standard beschreibt 11 Grundlegende Sicherheitsaspekte.

- Security Policy
- Organizing Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

Zu jedem dieser Aspekte gibt es eine Erklärung, was genau erreicht werden soll (*Control Objective*). Des weiteren gibt es jeweils einen oder mehrere praktische Vorschläge, wie der Aspekt umgesetzt bzw. erreicht werden kann (*Control(s)*). Diese, als Prüfungskriterium infrage kommenden Punkte, werden nun aufgelistet. Die detaillierte Beschreibung der einzelnen Punkte und wie sie umgesetzt werden können werden nicht aufgeführt.

D.1 Security Policy

Information Security Policy: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

1. An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.
2. The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

D.2 Organization of information security

Internal Organization: To manage information security within the organization

1. Management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.
2. Information security activities should be co-ordinated by representatives from different parts of the organization with relevant roles and job functions.
3. All information security responsibilities should be clearly defined.
4. A management authorization process for new information processing facilities should be defined and implemented.
5. Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified and regularly reviewed.
6. Appropriate contacts with relevant authorities should be maintained.
7. Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.
8. The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures) should be reviewed independently at planned intervals, or when significant changes to the security implementation occur.

External Parties: To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties

1. The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access.
2. All identified security requirements should be addressed before giving customers access to the organization's information or assets.
3. Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information facilities, or adding products or services to information processing facilities should cover all relevant security requirements.

D.3 Asset management

Responsibility for assets: To achieve and maintain appropriate protection of organizational assets

1. All assets should be clearly identified and an inventory of all important assets drawn up and maintained.

2. All information and assets associated with information processing facilities should be owned by a designated part of the organizations.
3. Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented.

Information classification: To ensure that information receives an appropriate level of protection

1. Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.
2. An appropriate set of procedures for information labeling and handling should be developed and implemented in accordance with the classification scheme adopted by the organization.

D.4 Human resources security

Prior to employment: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

1. Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy.
2. Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classifications of the information to be accessed, and the perceived risks.
3. As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security

During employment: To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

1. Management should require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.
2. All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.
3. There should be a formal disciplinary process for employees who have committed a security breach.

Termination or change of employment: To ensure that employees, contractors and third party users exit and organization or change employment in an orderly manner.

1. Responsibilities for performing employment termination or change of employment should be clearly defined and assigned.
2. All employees, contractors and third party users should return all of the organization's assets in their possession upon termination of their employment, contract or agreement.
3. The access rights of all employees, contractors and third party users to information or information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.

D.5 Physical and environmental security

Secure areas: To prevent unauthorized physical access, damage, and interference to the organization's premises and information.

1. Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.
2. Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
3. Physical security for offices, rooms, and facilities should be designed and applied
4. Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.
5. Physical protection and guidelines for working in secure areas should be designed and applied.
6. Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

Equipment Security: To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

1. Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities access.
2. Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.
3. Power and telecommunications cabling carrying data or supporting information services should be protected from interception.

4. Equipment should be correctly maintained to ensure its continued availability and integrity.
5. Security should be applied to off-site equipment taking into account the different risks of working outside the organization's premises.
6. All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.
7. Equipment, information or software should not be taken off-site without prior authorization.

D.6 Communications and operations management

Operational procedures and responsibilities: To ensure the correct and secure operation of information processing facilities.

1. Operating procedures should be documented, maintained, and made available to all users who need them.
2. Changes to information processing facilities and systems should be controlled.
3. Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
4. Development, test, and operational facilities should be separated to reduce the risks of unauthorized access or changes to the operational system.

Third party service delivery management: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

1. It should be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.
2. Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

System planning and acceptance: To minimize the risk of systems failures

1. The use of resources should be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.
2. Acceptance criteria for new information systems, upgrades, and new versions should be established and suitable tests of the system(s) carried out during development and prior to acceptance.

Protection against malicious and mobile code: To protect the integrity of software and information

1. Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.
2. Where the use of mobile code is authorized, the configuration should ensure that the authorised mobile code operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing.³

Back-up: To maintain the integrity and availability of information and information processing facilities.

1. Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.

Network security management: To ensure the protection of information in networks and the protection the the supporting infrastructure.

1. Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
2. Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided inhouse or are outsourced.

Media handling: To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.

1. There should be procedures in place for the management of removable media.
2. Media should be disposed of securely and safely when no longer required, using formal procedures.
3. Procedures for the handling and storage of information should be established to protect this information from unauthorized disclosure or misuse.
4. System documentation should be protected against unauthorized access.

Exchange information: To maintain the security of information and software exchanged within an organization and with any external entity

1. Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities.
2. Agreements should be established for the exchange of information and software between the organization and external parties.
3. Media containing information should be protected against unauthroized access, misuse or corruption during transportation beyond an organization's physical boundaries.

4. Information involved in electronic messaging should be appropriately protected.
5. Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems.

Electronic commerce services: To ensure the security of electronic e commerce services, and their secure use

1. Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.
2. Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
3. The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification.

Monitoring: To detect unauthorized information processing activities

1. Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.
2. Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly.
3. Logging facilities and log information should be protected against tampering and unauthorized access.
4. System administrator and system operator activities should be logged.
5. Faults should be logged, analysed, and appropriate action taken.
6. The clocks of all relevant information processing systems within an organization or security domain should be synchronized with an agreed accurate time source.

D.7 Access control

Business requirement for access control: To control access to information

1. An access control policy should be established, documented and reviewed based on business and security requirements for access.

User access management: To ensure authorized user access and to prevent unauthorized access to information systems.

1. There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.
2. The allocation and use of privileges should be restricted and controlled.

3. The allocation of passwords should be controlled through a formal management process.
4. Management should review users' access rights at regular intervals using a formal process.

User responsibilities: To prevent unauthorized user access, and compromise or theft of information and information processing facilities.

1. Users should be required to follow good security practises in the selection and use of passwords.
2. Users should ensure that unattended equipment has appropriate protection.
3. A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.

Network access control: To prevent unauthorized access to networked services.

1. Users should only be provided with access to the services that they have been specifically authorized to use
2. Appropriate authentication methods should be used to control access by remote users.
3. Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment
4. Physical and logical access to diagnostic and configuration ports should be controlled.
5. Groups of information services, users, and information systems should be segregated on networks
6. For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications.
7. Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

Operating system access control: To prevent unauthorized access to operating systems.

1. Access to operating systems should be controlled by a secure log-on procedure.
2. All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.
3. Systems for managing passwords should be interactive and should ensure quality passwords.

4. The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.
5. Inactive sessions should shut down after a defined period of inactivity.
6. Restrictions on connection times should be used to provide additional security for high-risk applications.

Application and information access control: To prevent unauthorized access to information held in application systems.

1. Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy.
2. Sensitive systems should have a dedicated (isolated) computing environment.

Mobile computing and teleworking: To ensure information security when using mobile computing and teleworking facilities.

1. A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.
2. A policy, operational plans and procedures should be developed and implemented for teleworking activities.

D.8 Information systems acquisition, development and maintenance

Security requirements of information systems: To ensure that security is an integral part of information systems

1. Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls.

Correct processing of applications: To prevent errors, loss, unauthorized modification or misuse of information in applications.

1. Data input to applications should be validated to ensure that this data is correct and appropriate.
2. Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
3. Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented.
4. Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

Cryptographic controls: To protect confidentiality, authenticity or integrity of information by cryptographic means.

1. A policy on the use of cryptographic controls for protection of information should be developed and implemented.
2. Key management should be in place to support the organization's use of cryptographic techniques.

Security of system files: To ensure the security of system files.

1. There should be procedures in place to control the installation of software on operational systems.
2. Test data should be selected carefully, and protected and controlled.
3. Access to program source code should be restricted.

Security in development and support processes: To maintain security of applications system software and information.

1. The implementation of changes should be controlled by the use of formal change control procedures.
2. When operating systems are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
3. Opportunities for information leakage should be prevented.
4. Outsourced software development should be supervised and monitored by the organization.

Technical Vulnerability Management__ To reduce risks resulting from exploitation of published technical vulnerabilities.

1. Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

D.9 Information security incident management

Reporting information security events and weaknesses: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

1. Information security events should be reported through appropriate management channels as quickly as possible.
2. All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services.

Management of information security incidents and improvements: To ensure a consistent and effective approach is applied to the management of information security incidents.

1. Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.
2. There should be mechanisms in place to enable the types, volumes, and costs of information security incident to be quantified and monitored.
3. Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

D.10 Business continuity management

Information security aspects of business continuity management: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

1. A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.
2. Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security.
3. Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.
4. A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.
5. Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective.

D.11 Compliance

Compliance with legal requirements: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

1. All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.
2. Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.
3. Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.
4. Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.
5. Users should be deterred from using information processing facilities for unauthorized purposes.
6. Cryptographic controls should be used in compliance with all relevant agreements, laws, and regulations.

Compliance with security policies and standards, and technical compliance:

To ensure compliance of systems with organizational security policies and standards

1. Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.
2. Information systems should be regularly checked for compliance with security implementation standards.

Information systems audit considerations: To maximize the effectiveness of and to minimize interference to/from the information systems audit process.

1. Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes.
2. Access to information systems audit tools should be protected to prevent any possible misuse or compromise.

E Prüfungskriterien der Methode

Die aus dem BSI-Leitfaden, dem ISO/IEC 27002:2005 Standard sowie den Surveys [4], [9], [10] entstandene Liste von Prüfungskriterien. Zu jedem Prüfungskriterium ist zusätzlich noch seine PK-Konsequenz-Bewertung sowie PK-Gewichtung angegeben. Die PK-Konsequenz-Bewertung wurde mit Hilfe von Tab. 4.3 vergeben, die PK-Gewichtungen wurden aus der bereits definierten Methode übernommen und sind in Tab. 3.2 ersichtlich.

- **Sicherheitsrichtlinie**

1. Die Sicherheitsrichtlinie wird vom Management unterstützt.
 - **C: 0.6, I: 0.6 A: 0.6, PK-Gewichtung: 0.5**
2. Es werden bzw. wurden externe Sicherheitsexperten damit beauftragt, kritische Bereiche der internen IT-Sicherheit zu überprüfen.
 - **C: 0.6, I: 0.6 A: 0.6, PK-Gewichtung: 0.5**
3. Mitarbeiter sind verpflichtet, die Sicherheitsrichtlinie durch ihre Unterschrift zur Kenntnis zu nehmen.
 - **C: 0.6, I: 0.6 A: 0.6, PK-Gewichtung: 1**
4. Verstösse gegen die Sicherheitsrichtlinie werden geahndet.
 - **C: 0.9, I: 0.9 A: 0.9, PK-Gewichtung: 1**
5. Es gibt Kontrollmechanismen für bestehende Sicherheitsvorgaben.
 - **C: 0.6, I: 0.6 A: 0.6, PK-Gewichtung: 0.5**
6. Die Sicherheitsrichtlinie wird regelmässig auf ihre Aktualität geprüft.
 - **C: 0.3, I: 0.3 A: 0.3, PK-Gewichtung: 0.5**

- **Awareness**

1. Die in der Sicherheitsrichtlinie definierten Richtlinien sind in der Firma bekannt.
 - **C: 0.6, I: 0.3 A: 0.3, PK-Gewichtung: 0.5**
2. Die Mitarbeiter wissen, an wen sie sich bei Sicherheitsfragen wenden können.
 - **C: 0.3, I: 0.3 A: 0.3, PK-Gewichtung: 0.5**
3. Das Bewusstsein (Awareness) der Mitarbeiter bezüglich Informationssicherheit wird regelmässig geschult/trainiert.
 - **C: 0.6, I: 0.6 A: 0.6, PK-Gewichtung: 1**

4. Die Arbeitsplatzrechner werden bei Verlassen mit Bildschirmschoner und Kennwort gesichert.

– **C:** 0.6, **I:** 0.3 **A:** 0.3, **PK-Gewichtung:** 0.5

5. Mitarbeiter sind informiert, wann sich Handwerker, Servicetechniker und Reinigungspersonal im Haus befinden.

– **C:** 0.6, **I:** 0.3 **A:** 0.6, **PK-Gewichtung:** 0.5

- **Backup**

1. Es gibt eine klar definierte Backup-Strategie.

– **C:** 0, **I:** 0 **A:** 0.9, **PK-Gewichtung:** 1

2. Notebooks und nicht vernetzte Systeme werden regelmässig gesichert.

– **C:** 0, **I:** 0 **A:** 0.9, **PK-Gewichtung:** 1

3. Es wird eine regelmässige Rücksicherung der Daten geübt.

– **C:** 0, **I:** 0 **A:** 0.9, **PK-Gewichtung:** 1

4. Der Backup- und der Rücksicherungsprozess ist dokumentiert.

– **C:** 0, **I:** 0 **A:** 0.9, **PK-Gewichtung:** 0.5

5. Die Backup-Bänder werden sicher ausserhalb des Büros gelagert.

– **C:** 0, **I:** 0 **A:** 0.9, **PK-Gewichtung:** 1

- **Viren / Schadprogramme**

1. Es ist auf allen IT-Systemen ein Viren-Schutzprogramm (Malware/Schadsoftware) installiert.

– **C:** 0.9, **I:** 0.6 **A:** 0.9, **PK-Gewichtung:** 1

2. Viren-Schutzprogramm-Updates können automatisiert durchgeführt werden.

– **C:** 0.9, **I:** 0.6 **A:** 0.9, **PK-Gewichtung:** 1

3. System-Updates (Betriebssysteme, Programme) können automatisiert durchgeführt werden.

– **C:** 0.6, **I:** 0.6 **A:** 0.6, **PK-Gewichtung:** 1

4. System- und Viren-Schutzprogramm-Updates werden regelmässig durchgeführt?

– **C:** 0.9, **I:** 0.6 **A:** 0.9, **PK-Gewichtung:** 1

5. E-Mails sowie jeglicher Internetverkehr wird zentral auf Viren / Schadprogramme überprüft.

– **C:** 0.9, **I:** 0.6 **A:** 0.9, **PK-Gewichtung:** 1

- **Passwörter**

1. Benutzerpasswörter genügen den gängigen Sicherheitsanforderungen. (Mind. 8 Zeichen, Gross- und Kleinbuchstaben, Mind. 1 Zahl, Sonderzeichen)

– **C:** 0.6, **I:** 0.6 **A:** 0.3, **PK-Gewichtung:** 1

2. Passwörter müssen regelmässig geändert werden.

– **C:** 0.6, **I:** 0.6 **A:** 0.6, **PK-Gewichtung:** 1

- **Vernetzung Internet-Anbindung**

1. Es gibt eine Firewall?

– **C:** 0.9, **I:** 0.9 **A:** 0.9, **PK-Gewichtung:** 1

2. Konfiguration und Funktionsfähigkeit der Firewall werden regelmässig kritisch überprüft und kontrolliert?

– **C:** 0.9, **I:** 0.9 **A:** 0.9, **PK-Gewichtung:** 1

3. Es gibt ein Konzept, welche Daten nach aussen angeboten werden müssen.

– **C:** 0.6, **I:** 0.6 **A:** 0.6, **PK-Gewichtung:** 0.5

- **Zugriff auf Daten**

1. Der Zugriff auf Daten ist nach dem Need-To-Know Prinzip geregelt?(Jeder Benutzer hat genau Zugriff auf die Dateien die er zur Erledigung seiner Arbeit benötigt Zugriff).

– **C:** 0.9, **I:** 0.6 **A:** 0.3, **PK-Gewichtung:** 1

2. Zugriffsberechtigungen werden über Rollen und Profile verwaltet (Bsp. Benutzer A hat Zugriff auf Dateien der Abteilung Verkauf, Gruppe A hat Zugriff auf Dateien der Abteilung Produktion, etc.)

– **C:** 0.9, **I:** 0.6 **A:** 0.3, **PK-Gewichtung:** 1

3. Es gibt einen Prozess, der sicherstellt, dass vergebene Rechte nach dem Austritt eines Mitarbeiters wieder entfernt werden.

– **C:** 0.6, **I:** 0.6 **A:** 0.6, **PK-Gewichtung:** 0.5

4. Zusätzlich beantragte Rechte eines Mitarbeiters, müssen von seinem Vorgesetzten genehmigt werden.

– **C:** 0.6, **I:** 0.6 **A:** 0.6, **PK-Gewichtung:** 0.5

5. Es ist klar definiert, welche Funktion was für Rechte benötigt?
 - **C:** 0.6, **I:** 0.6 **A:** 0.6, **PK-Gewichtung:** 0.5
6. Es gibt verschiedene Rollen und Profile für Administratoren. (Ein Administrator darf nicht alles)
 - **C:** 0.6, **I:** 0.6 **A:** 0.6, **PK-Gewichtung:** 1
7. Ist bekannt und geregelt, welche Rechte und Privilegien Programme haben?
 - **C:** 0.6, **I:** 0.6 **A:** 0.6, **PK-Gewichtung:** 0.5

- **Daten-Sicherheit**

1. Es gibt ein Konzept zur Klassifikation von Daten (öffentlich, geheim, intern, extern, Abteilung A und B, Abteilung C etc.)
 - **C:** 0.6, **I:** 0.6 **A:** 0.3, **PK-Gewichtung:** 1
2. Als geheim/sensitiv klassifizierte Daten werden verschlüsselt gespeichert.
 - **C:** 0.9, **I:** 0.6 **A:** 0.3, **PK-Gewichtung:** 1
3. Manipulationen (Lesen, Schreiben, Löschen) an Daten werden protokolliert.
 - **C:** 0.6, **I:** 0.9 **A:** 0.3, **PK-Gewichtung:** 1
4. Notebooks werden komplett verschlüsselt.
 - **C:** 0.6, **I:** 0.6 **A:** 0.6, **PK-Gewichtung:** 1
5. E-Mails werden verschlüsselt. Auf die Sicherheit von Informationen in E-Mails wird geachtet.
 - **C:** 0.6, **I:** 0.6 **A:** 0.6, **PK-Gewichtung:** 1

- **Infrastruktur** (df. kritische IT-Infrastruktur)

1. Das Gebäude ist vor Einbrechern geschützt.
 - **C:** 0.3, **I:** 0 **A:** 0.9, **PK-Gewichtung:** 1
2. Der Serverraum ist nur für Befugte betretbar.
 - **C:** 0.6, **I:** 0 **A:** 0.9, **PK-Gewichtung:** 1
3. Externe IT-Arbeiter werden nur beaufsichtigt im Serverraum gelassen.
 - **C:** 0.6, **I:** 0 **A:** 0.6, **PK-Gewichtung:** 0.5
4. Kritische IT-Infrastruktur ist gegen Überhitzung geschützt.
 - **C:** 0, **I:** 0 **A:** 0.9, **PK-Gewichtung:** 0.5

5. Kritische IT-Infrastruktur ist gegen Feuer geschützt.
 - **C:** 0, **I:** 0 **A:** 0.9, **PK-Gewichtung:** 1
6. Kritische IT-Infrastruktur ist gegen Stromausfälle geschützt.
 - **C:** 0, **I:** 0 **A:** 0.9, **PK-Gewichtung:** 0.5
- **Notfallpläne** Es gibt Notfallpläne für:
 1. Grippewelle, Ausfall vom Grossteil der Mitarbeiter.
 - **C:** 0, **I:** 0 **A:** 0.9, **PK-Gewichtung:** 0.5
 2. Ausfall von Lieferanten oder Dienstleister.
 - **C:** 0, **I:** 0 **A:** 0.9, **PK-Gewichtung:** 0.5
 3. Ausfall des IT Managers.
 - **C:** 0, **I:** 0 **A:** 0.9, **PK-Gewichtung:** 0.5
 4. Virusbefall mehrerer / dem Grossteil der Rechner.
 - **C:** 0, **I:** 0 **A:** 0.9, **PK-Gewichtung:** 0.5
 5. Ausfall einer kritischen IT-Infrastruktur.
 - **C:** 0, **I:** 0 **A:** 0.9, **PK-Gewichtung:** 0.5
 6. Die Notfallpläne sind allen involvierten Leuten bekannt.
 - **C:** 0, **I:** 0 **A:** 0.9, **PK-Gewichtung:** 0.5
 7. Das Vorgehen der Notfallpläne wird regelmässig durchgespielt.
 - **C:** 0, **I:** 0 **A:** 0.6, **PK-Gewichtung:** 0.5
- **Dokumentation / Stellvertreter**
 1. Der IT-Administrator hat einen Stellvertreter.
 - **C:** 0.3, **I:** 0.3 **A:** 0.9, **PK-Gewichtung:** 0.5
 2. Die Administratoren-Passwörter sind hinterlegt.
 - **C:** 0.3, **I:** 0.3 **A:** 0.9, **PK-Gewichtung:** 0.5
 3. Sämtliche IT-Systeme sind ausreichend dokumentiert (Installation, Bedienung, Behandlung von Fehlern)
 - **C:** 0.3, **I:** 0.3 **A:** 0.9, **PK-Gewichtung:** 0.5
 4. Es gibt ein Inventar sämtlicher IT-Systeme (Hard- und Software).
 - **C:** 0.6, **I:** 0.6 **A:** 0.6, **PK-Gewichtung:** 0.5

F Dokumente zur Softwareentwicklung

F.1 Anforderungen an den Prototyp

Die Anforderungen an den Prototyp wurden aus den erstellten Mockups (Kap. 5.2) abgeleitet.

Bezeichnung	Anforderung A.1
Beschreibung	Der Benutzer muss die Schutzziel-Definitionen bestimmen können. Das heisst, dass er für jedes Attribut einen Wert zwischen 1 und 10 definieren kann, welcher die Wichtigkeit dieses Attributes ausdrückt.

Tab. F.1: Anforderung A.1

Bezeichnung	Anforderung A.2
Beschreibung	Der Benutzer muss persönliche Daten, wie seinen Namen, das Datum, die Firma sowie die Abteilung eintragen können.

Tab. F.2: Anforderung A.2

Bezeichnung	Anforderung A.3
Beschreibung	Dem Benutzer muss eine Erklärung, wie der Audit funktioniert und wie er anzuwenden ist zur Verfügung stehen.

Tab. F.3: Anforderung A.3

Bezeichnung	Anforderung A.4
Beschreibung	Der Benutzer muss die Liste der Prüfungskriterien (Anhang E) nach vordefinierten Bewertungsmöglichkeiten (Tab. 3.3) bewerten können.

Tab. F.4: Anforderung A.4

Bezeichnung	Anforderung A.5
Beschreibung	Der Benutzer muss, während er einen Audit ausfüllt, jederzeit sehen, wie hoch die Gesamt-Erfüllung der Attribute ist.

Tab. F.5: Anforderung A.5

Bezeichnung	Anforderung A.6
Beschreibung	Der Benutzer muss einen Audit auswerten lassen können. Die Auswertung muss nach der in dieser Arbeit definierten Methodik ausgeführt werden.

Tab. F.6: Anforderung A.6

Bezeichnung	Anforderung A.7
Beschreibung	Die Auswertung der Gesamt-Erfüllung der Attribute muss graphisch dargestellt werden. Die Erfüllung der einzelnen Sicherheitsaspekte muss in einer Tabelle dargestellt werden.

Tab. F.7: Anforderung A.7

F.2 Use Cases - Detailbeschreibung

Die Art der Beschreibungen der *Use Cases* wurde [7] entnommen.

F.2.1 Use Case U.1 - Audit initialisieren

Use Case Name	Audit initialisieren
Referenz-Nr. Use Case	U.1
Zugehörige Anforderungen:	A.1, A.2, A3
Ziel	Definition der persönlichen Daten und Schutzziele durch Benutzer.
Voraussetzungen	-
Wann erfolgreich?	Wenn der <i>Benutzer</i> persönliche Daten und Schutzziele definieren kann.
Wann nicht erfolgreich?	Wenn der <i>Benutzer</i> persönliche Daten und Schutzziele nicht definieren kann.
Primäre Rollen	Benutzer
Sekundäre Rollen	-
Auslöser	Der <i>Benutzer</i> öffnet die Start-Seite (Index) der Audit-Applikation.
Main Flow	
Schritt	Aktion
1	Der <i>Benutzer</i> öffnet die Start-Seite (Index) der Audit-Applikation.
2	Das Programm kreiert die Eingabemaske für die Schutzziel-Def. und die persönlichen Daten des <i>Benutzers</i> . Hat der Benutzer diese Informationen bereits einmal ausgefüllt, werden diese Informationen geladen.
3	Der Benutzer definiert/ändert seine persönlichen Angaben sowie Schutzziel-Definitionen.
4	Der <i>Benutzer</i> kann den Audit starten bzw. einen bereits ausgefüllten Audit begutachten.

Tab. F.8: Detailbeschreibung Use Case : Audit initialisieren

F.2.2 Use Case U.2 - Audit durchführen

Use Case Name	Audit durchführen
Referenz-Nr. Use Case	U2
Zugehörige Anforderungen:	A.4, A.5
Ziel	Ermöglichen der Erfassung eines Audits für einen <i>Benutzer</i> .
Voraussetzungen	-
Wann erfolgreich?	Wenn der <i>Benutzer</i> alle Prüfungskriterien hat bewerten können.
Wann nicht erfolgreich?	Wenn der <i>Benutzer</i> nicht alle Prüfungskriterien bewerten kann.
Primäre Rollen	Benutzer
Sekundäre Rollen	-
Auslöser	Der <i>Benutzer</i> startet einen neuen Audit oder öffnet einen bereits begonnenen
Main Flow	
Schritt	Aktion
1	Der <i>Benutzer</i> startet einen neuen oder einen bereits angefangenen Audit.
2	Das System erstellt eine Liste aller Prüfungskriterien und stellt diese dem <i>Benutzer</i> zur Bewertung (vordefinierte Auswahl an Bewertungsmöglichkeiten) zur Verfügung.
3	Der <i>Benutzer</i> bewertet alle Prüfungskriterien.
4	Das System zeigt dem <i>Benutzer</i> nach jeder Bewertung die Gesamterfüllung der Attribute an und speichert das Resultat.

Tab. F.9: Detailbeschreibung Use Case : Audit durchführen

F.2.3 Use Case U.3 - Audit auswerten

Use Case Name	Audit auswerten
Referenz-Nr. Use Case:	U.3
Zugehörige Anforderungen:	A.6, A.7
Ziel	Auswertung des erfassten Audits mit Hilfe der entwickelten Methodik
Voraussetzungen	-
Wann erfolgreich?	Wenn dem <i>Benutzer</i> eine visuelle Darstellung des Audit-Ergebnisses gezeigt wird.
Wann nicht erfolgreich?	Wenn trotz kompletter Ausfüllung des Audits kein Ergebnis gezeigt wird bzw. berechnet werden kann.
Primäre Rollen	Benutzer
Sekundäre Rollen	-
Auslöser	Der Benutzer startet die Audit-Auswertung
Main Flow	
Schritt	Aktion
1	Der Benutzer startet die Audit-Auswertung.
2	Das Programm bezieht die aus dem Audit berechneten Resultate
3	Das Programm bezieht die persönlichen Daten des Benutzers
4	Das Programm kreiert eine grafische Darstellung des Ergebnisses und stellt diese sowie die persönlichen Daten dem Benutzer zur Verfügung.

Tab. F.10: Detailbeschreibung Use Case : Audit auswerten

F.3 Datenmodell

Alle für den Audit erforderlichen Daten werden in einem JSON-Objekt gespeichert, auf welches diverse JavaScript Funktionen zugreifen. Die Datenstruktur ist dabei wie folgt aufgebaut.

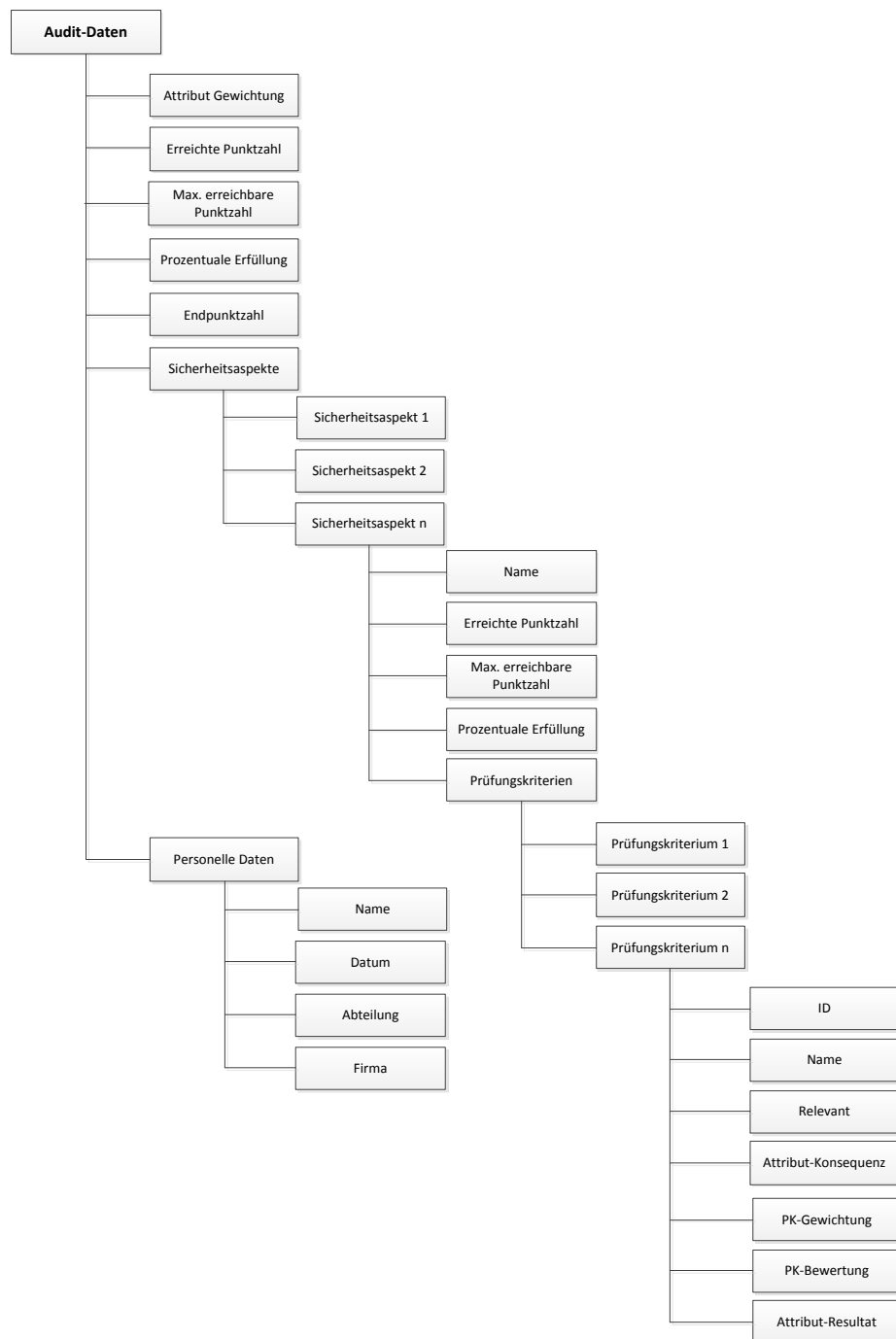


Abb. F.1: JSON-Datenstruktur

F.4 Dateien / Dateistruktur

Die Files für die Webseiten (HTML) befinden sich im Stammverzeichnis (Root). Files für die Darstellung (CSS), Logik und Daten (JavaScript), Bilder sowie Tests sind in separaten Ordnern abgelegt. In diesem Kapitel soll aufgezeigt werden, aus was für Files der Prototyp besteht und was die Aufgabe des jeweiligen Files ist.

F.4.1 HTML

Befinden sich im Stammverzeichnis '/'.

/index.html Start-Seite des Prototyps. Auf ihr können Schutzziele definiert und persönliche Daten eingegeben werden. Man gelangt von ihr auf den Audit (*/audit.html*) oder die Audit-Auswertung (*/audit_auswertung.html*)

/audit.html Stellt die Liste mit den Prüfungskriterien dar, die der Auditor bewerten kann.

/audit_auswertung.html Stellt die Auswertung des Audits dar. Auf ihr werden die in der Start-Seite (*/index.html*) eingegebenen persönlichen Daten sowie Schutzziel-Definitionen wiedergegeben.

F.4.2 JavaScript (Logik)

Die gesamte Logik des Prototyps befindet sich unter '/js'.

/js/audit_data.js In diesem File ist die gesamte Datenstruktur des Audits gespeichert. Alle Felder für Sicherheitsaspekte, Prüfungskriterien, Resultate und für die Berechnung benötigte Parameter sind in diesem File vorhanden (Siehe auch Abb. F.1).

/js/audit_index.js Dieses File wird zur Erstellung der Start-Seite (*/index.html*) benötigt. Sind bereits persönliche Daten und Schutzziel-Definitionen im lokalen Speicher vorhanden, so werden diese Einträge auf der Seite entsprechend geladen. Geht ein Benutzer das erste Mal auf diese Seite, so wird die Datenstruktur aus */js/audit_data.js* in den lokalen Speicher (*Local Storage*) gespeichert und so den anderen Seiten zur Verfügung gestellt.

/js/audit.js In diesem File sind die Funktionen gespeichert, die es zur Berechnung des Audits braucht. Sobald ein Prüfungskriterium bewertet wird, setzt eine Funktion die entsprechenden Werte in der Datenstruktur und berechnet den Audit. So stehen immer die neuesten Ergebnisse zur Darstellung zur Verfügung.

/js/audit_auswertung.js Dieses File ist dafür zuständig, die berechneten Resultate darzustellen. Die Daten bezieht sie aus der lokal abgespeicherten Datenstruktur. Zur Darstellung der Gesamt-Erfüllung der Attribute wird hierbei mit dem *Canvas*-Objekt (HTML5) gearbeitet.

/js/jquery-ui-1.8.19.custom.min.js Dieses *jQuery UI*¹ File wird für die Darstellung der Sicherheitsaspekte und Prüfungskriterien gebraucht (Accordion).

/js/jquery-1.7.2.min.js Diese *jQuery*² Bibliothek wird teilweise für JavaScript Programmierarbeiten eingesetzt. Hauptsächlich jedoch wird es vom *jQuery UI*-File benötigt, damit das Accordion funktioniert.

F.4.3 CSS (Darstellung)

Die Files für die Darstellung der Webseiten befinden sich unter **'/css'**.

/css/ui-lightness/ In diesem Ordner befinden sich die Files, die für die Darstellung der Liste der Prüfungskriterien zuständig sind. Sie sind Bestandteil der *jQuery UI*-Bibliothek.

/css/index.css Dieses File ist für die Darstellung der */index.html* Files zuständig

/css/audit.css Dieses File ist für die Darstellung des */audit.html* Files zuständig.

/css/audit_auswertung Dieses File ist für die Darstellung des */audit_auswertung.html* Files zuständig.

F.4.4 Bilder

Die verwendeten Bilder befinden sich unter **'/img'**.

/img/backArrow.png Bild von einem nach links zeigenden Dreieck. Wird für die Navigation verwendet.

/img/forwardArrow.png Bild von einem nach rechts zeigenden Dreieck. Wird für die Navigation verwendet.

F.4.5 Tests

Das File mit den Tests befindet sich unter **'/tests'**

/tests/unit_tests_berechnungsMethoden.html In diesem File befinden sich die Tests für die Berechnungsmethoden. Es werden die Grund-Berechnungsfunktionen, auf welchen der gesamte Audit aufbaut, getestet. Dazu gehört das Berechnen des PK-Resultates (Gl. 3.1), des Sicherheitsaspekt-Resultates (Gl.3.2) sowie des Audit-Resultates (Gl. 3.3, 3.4, 3.5, 3.6).

F.5 Bilder des Prototyps

Folgend die Bilder des fertig entwickelten Prototyps

¹<http://www.jqueryui.com>

²<http://www.jquery.com>

Audit

Schutzziel-Definition

Geben Sie hier, je nach dem, wie wichtig Ihnen eines dieser Attribute ist, jeweils einen Wert zwischen 1-10 ein.

Vertraulichkeit: Integrität: Verfügbarkeit:

Persönliche Daten

Firma:
Abteilung:
Datum:
Name:

Benutzeranleitung

Beim Audit handelt es sich um eine Liste von Prüfungskriterien aus verschiedenen Sicherheitsaspekten wie z.B. "Backup", "Awareness" etc. Jedes Prüfungskriterium beschreibt eine Anforderung an die IT-Security ihres Unternehmens. Mit den Bewertungsoptionen geben Sie an, ob eine Anforderung erfüllt ist ("Ja"), teilweise erfüllt ist ("Teilweise") oder nicht erfüllt ist ("Nein", Standardwert). Sie sehen dabei den Grad der Erfüllung des Sicherheitsaspektes in derselben Zeile wie der Sicherheitseffekt. Die Gesamt-Erfüllung von Ihnen definierten Schutz-Ziele sehen sie in einer Box neben der Liste. Wollen sie die Auswerten des Audits sehen, so können Sie entweder auf das schwarze nach rechtszeigende Dreieck oder den entsprechenden Link klicken.


Audit Links

Folgen Sie diesen Links um den Audit auszufüllen oder, wenn sie den Audit bereits ausgefüllt haben, um die Auswertung zu betrachten.

[Audit ausfüllen](#)

[Auswertung Audit](#)

Abb. F.2: Index-Seite Prototyp



▼ **Organisatorische Sicherheit - C: 92%, I: 92%, A: 92%**

Die Sicherheitsrichtlinie wird vom Management unterstützt.	Ja ▼
Es werden externe Sicherheitsexperten damit beauftragt, kritische Bereiche der internen IT-Sicherheit zu überprüfen.	Ja ▼
Verstösse gegen die Sicherheitsrichtlinie werden geahndet.	Ja ▼
Es gibt Kontrollmechanismen für bestehende Sicherheitsvorgaben.	Teilweise ▼
Die Sicherheitsrichtlinie wird regelmässig auf ihre Aktualität geprüft.	Ja ▼

▶ Awareness - C: 47%, I: 46%, A: 46%

▶ Backup - C: -, I: -, A: 48%

▶ Viren / Schadprogramme - C: 71%, I: 70%, A: 71%

▶ Passwörter - C: 0%, I: 0%, A: 0%


▶ Vernetzung / Internet-Anbindung - C: 0%, I: 0%, A: 0%

▶ Zugriff auf Daten - C: 0%, I: 0%, A: 0%

▶ Infrastruktur - C: 0%, I: 0%, A: 0%

▶ Notfallpläne (Es gibt Notfallpläne für..) - C: 0%, I: 0%, A: 0%

▶ Dokumentation / Stellvertreter - C: 0%, I: 0%, A: 0%



Erfüllung Total:

C: 35%

I: 35%

A: 29%

[Audit auswerten](#)
[Audit zurücksetzen](#)
[Start-Seite](#)

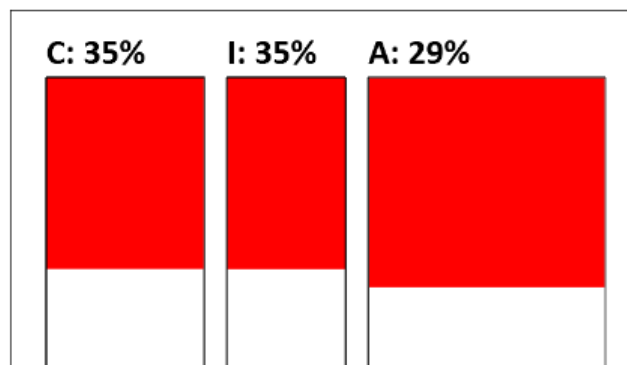
Abb. F.3: Audit-Seite Prototyp

Auswertung Audit

Persönliche Daten:

Firma:	Firefox
Abteilung:	TestAbteilung
Datum:	TestDatum
Name:	TestName

Gesamt-Erfüllung: 32%



Detail-Auswertung:

Sicherheitsaspekt	Erfüllung-C	Erfüllung-I	Erfüllung-A	Erfüllung-Total
Organisatorische Sicherheit	92%	92%	92%	92%
Awareness	47%	46%	46%	46%
Backup	0%	0%	48%	48%
Viren / Schadprogramme	71%	70%	71%	71%
Passwörter	0%	0%	0%	0%
Vernetzung / Internet-Anbindung	0%	0%	0%	0%
Zugriff auf Daten	0%	0%	0%	0%
Infrastruktur	0%	0%	0%	0%
Notfallpläne (Es gibt Notfallpläne für...)	0%	0%	0%	0%
Dokumentation / Stellvertreter	0%	0%	0%	0%
Total	35%	35%	29%	32%

Abb. F.4: Audit_Auswertung-Seite Prototyp

Literaturverzeichnis

- [1] BSI. Leitfaden Informationssicherheit. Technical Report BSI-Bro10/311, BSI, 2008.
- [2] Robson E. Freeman R. *Head First HTML5 Programming*. O'Reilly, 2011.
- [3] ISO/IEC. Information technology - security techniques - code of practice for information security management. Technical Report INTERNATIONAL STANDARD ISO/IEC 27002:2005(E), ISO/IEC, 2007.
- [4] Kaspersky. Global it security risks. Technical report, Kaspersky Lab, B2B International, 2011.
- [5] Klett G. Kersten. H. *Der IT Security Manager*. Vieweg + Teubner Verlag, 2008.
- [6] EU Kommission. Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen. Technical Report 2003/361/EG, EU, 2003.
- [7] Hamilton K. Miles R. *Learning UML 2.0*. O'Reilly, 2006.
- [8] Miles R. Pilone D. *Head First - Software Development*. O'Reilly, 2008.
- [9] Stefan Brandl Prof. Dr. Sachar Paulus. IT-Sicherheitslage im Mittelstand 2011. Technical report, DsiN, 2011.
- [10] PWC. Information security breaches survey 2010. Technical report, Infosecurity Europe, Price Water House Coopers, 2010.
- [11] Mock R. Computer-assisted risk assessment audit on operation level. *PSAM 11 & ESREL 12*, 2012.
- [12] Deep Blue Sky web design and consultancy. HTML5 & CSS3 Support. Technical report, <http://www.findmebyip.com/litmus>, 2010.

Abbildungsverzeichnis

5.1	Index Mockup	20
5.2	Audit Mockup	21
5.3	Auswertung Mockup	22
5.4	Prototyp - Use Cases	23
A.1	Projektplan Semesterarbeit	31
B.1	Excel-Umsetzung: Definition	34
B.2	Excel-Umsetzung: Auswertung	35
F.1	JSON-Datenstruktur	63
F.2	Index-Seite Prototyp	66
F.3	Audit-Seite Prototyp	67
F.4	Audit_Auswertung-Seite Prototyp	68

Tabellenverzeichnis

3.1	Methode: Berechnungskomponenten (Für Details siehe Anhang B.1)	5
3.2	PK-Gewichtungsmöglichkeiten	7
3.3	PK-Bewertungsmöglichkeiten	7
3.4	Beispielbewertungen	8
4.1	Konsequenz-Klassen	17
5.1	Unterstützte Web-Browser-Versionen	25
B.1	Definition Variabel für Prüfungskriterien	32
B.2	Definition Variabel für Sicherheitsaspekt	32
B.3	Definition Attribut-Gewichtung Branche	32
B.4	Definition Attribut-Konsequenz	32
B.5	Definition PK-Gewichtung	33
B.6	Definition PK-Bewertung	33
F.1	Anforderung A.1	58
F.2	Anforderung A.2	58
F.3	Anforderung A.3	58
F.4	Anforderung A.4	58
F.5	Anforderung A.5	58
F.6	Anforderung A.6	59
F.7	Anforderung A.7	59
F.8	Detailbeschreibung Use Case : Audit initialisieren	60
F.9	Detailbeschreibung Use Case : Audit durchführen	61
F.10	Detailbeschreibung Use Case : Audit auswerten	62