Thema:

IT-Sicherheit nach ISO 27002 bei öffentlichen Auftraggebern

Bachelorarbeit

Institut für Technische und Betriebliche Informationssysteme (ITI)
Arbeitsgruppe Wirtschaftsinformatik III – Managementinformationssysteme

Themensteller: Prof. Dr. rer. pol. Hans-Knud Arndt
Betreuer: Sascha Siepe
Michael Köhler
Jörg Eschweiler

vorgelegt von: Benjamin Wilhelms

Abgabetermin: 05.03.2010

Inhaltsverzeichnis

Verzeichnis der Abkürzungen und Akronyme

BSI	Bundesamt für Sicherheit in der Informationstechnik
CIO	Chief Investment Officer
COBIT	Control Objectives for Information and Related Technology
ISO	International Organization of Standardization
IT	Informationstechnik
ITIL	IT Infrastructure Library
NATO	North Atlantic Treaty Organization (deutsch: Nordatlantische Vertragsorganisation)
ÖAG	Öffentlicher Auftraggeber
PDCA	Plan Do Act Check
VSA	Verschlusssachenanweisung
ZDV	Zentrale Dienstvorschriften

Abbildungsverzeichnis

Tabellenverzeichnis

Formelverzeichnis

Kurzfassung

Aufgrund sich stets wandelnder Geschäftsanforderungen für Unternehmen sind diese zunehmend auf eine möglichst flexible Ausrichtung von Informationstechnik (IT) an eigene Strategien und Ziele gebunden. Durch diesen reallen Wert von Informationstechnik im Unternehmen benötigen heutige Unternehmen Werkzeuge für das Management in Form von Sicherheitskonzepten.

Diese Werkzeuge unterliegen einem ständigen Wandel, da äußere Einflüsse des Unternehmens jederzeit andere Anforderungen an Geschäftsprozesse, Infrastruktur und die Organisationsstruktur eines Unternehmens stellen. Mithilfe der Standards ISO 27002, COBIT und ITIL soll dieser ständig andauernde Lebenszyklus in der Informationssicherheit von Unternehmen handhabbar gemacht werden. Gerade in Hinblick auf öffentliche Auftraggeber spiegelt sich ein eher selten untersuchtes Anwendungsfeld wider, welches im Rahmen dieser Arbeit untersucht werden soll.

Aufgrund des öffentlichen Vergaberechts spielt die ISO 27001 in Verbindung mit der ISO 27002 gerade in Hinblick auf IT-Sicherheit bei öffentlichen Auftraggebern eine wesentliche Rolle. Zur Untersuchung von konkreten Umsetzungen von Maßnahmen nach ISO 27002 wird anhand des Beispiels der Bundeswehr eine Gegenüberstellung mit der „ZDV 54/100 –IT-Sicherheit in der Bundeswehr“ durchgeführt.

Ein abschließender quantitativer Vergleich stellt teilweise erhebliche Lücken bei Maßnahmen innerhalb der ZDV 54/100 fest. Aufgrund von sehr verteilten Verordnungsstrukturen innerhalb der Bundeswehr ist hier jedoch keine eindeutige Aussage über die Erfüllbarkeit der geforderten Maßnahmen nach ISO 27002 möglich. Es wird jedoch deutlich, welchen Stellenwert Best-Practices[1] auch bei öffentlichen Auftraggebern besitzen, um die Umsetzung von IT-Sicherheit in der Praxis zu gewährleisten. Aufgrund der verhältnismäßig hohen Sicherheitsanforderungen der Bundeswehr bezüglich Verfügbarkeit, Datenintegrität und Authentizität, ist davon auszugehen, dass es bislang sehr wenige Stellen der öffentlichen Hand gibt, mit vergleichbaren Umsetzungen von Best-Practices.

[1] In deutsch: bestes Verfahren bzw. Erfolgsrezept

1 Einleitung

Die Informationstechnologie (IT) ist ein wesentlicher Faktor für die Unterstützung von betrieblichen Geschäftsprozessen. Ohne sie wären in der heutigen Zeit eine Vielzahl von Prozessen nicht mehr möglich. *„In einigen Fällen findet die Durchführung eines Geschäftsprozesses inzwischen nur durch elektronische Systeme und ohne manuelle Bearbeitungsschritte statt. Als Beispiele hierfür können „Web-Shops" oder das „Online Banking" herangezogen werden. Die Qualität, Funktionalität und Leistungsfähigkeit dieser IT-Unterstützung prägt maßgeblich das Erscheinungsbild der gesamten Organisation nach außen zum Kunden."* [Buchsein et al. 2007, S. 12]. Aus diesem Grund gehört der Betrieb und die Einführung von IT im Unternehmen sowie im öffentlichen Sektor zu wichtigen Einflussgrößen der Gesamtstrategie und den Zielen von Unternehmen (Sichtwort ‚Business IT-Alignment').

Darüber hinaus gibt es eine Vielzahl von gesetzlichen Grundlagen wie beispielsweise: das Bundesdatenschutzgesetz (BDSG), das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) oder die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) [vgl. Speichert 2007, S. 336ff.], durch die Unternehmen Maßnahmen zur IT-Sicherheit gewährleisten müssen. Um die Komplexität von möglichen Sicherheitskonzepten beherrschbar zu machen, gibt es viele Sicherheitsstandards welche bei der Einführung eines Informationssicherheits-Managementsystems und möglichen Maßnahmen unterstützen sollen.

Die ISO/IEC 27001 und ISO/IEC 27002 sind hierbei ergänzende Standards zur Einführung von IT-Sicherheit, welche bei kommerziellen Unternehmen, Behörden und gemeinnützigen Organisationen Relevanz finden [vgl. ISO 27001 S. 7]. Die Verwendung dieser international anerkannten Standards macht diese gerade für öffentliche Auftraggeber sehr interessant. Durch die Vergleichbarkeit von Leistungen bei öffentlich-privaten Partnerschaften (ÖPP), sind Behörden und Einrichtungen an das öffentliche Beschaffungsrecht gebunden, durch welches die Chancengleichheit der technischen Anforderungen der Bieter verlangt wird [vgl. § 97 GWB]. Die ISO-Norm 2700x bietet daher eine europäisch und international allgemeingültige Grundlage, auf der Maßnahmen und Leistungen vergleichbar sind [vgl. Kersten et al. 2008, S. 6f.].

Aufgrund dieser Sonderstellung des ISO-Standards, soll die Umsetzung von Sicherheitsmaßnahmen so genannter ‚Best-Practices' nach ISO 27002 bei öffentlichen Auftraggebern untersucht werden.

2 Einführung in die IT-Sicherheit

2.1 Aktuelle Einordnung

"*But what we find most interesting is that more than half (56%) expect spending to either increase or stay the same – in spite of the worst economic downturn in decades. Or perhaps because of it.*"[2] [PricewaterhouseCoopers 2009, S. 10]

Mit diesem Worten bewerteten die Autoren von PricewaterhouseCoopers die Zahlen ihrer ‚Global State of Information Security 2010' Studie, in welcher über 7.200 CIOs, Vize-Präsidenten, IT- und IT-Security Vorstände zum Thema IT-Sicherheit befragt wurden. Anhand der Zahlen dieser Umfrage ist zu erkennen, dass Unternehmen und öffentliche Auftraggeber trotz wirtschaftlich schwierigen Zeiten stetig in die Sicherheit ihrer Informationstechnologie investieren und das Thema aktueller denn je ist [vgl. PricewaterhouseCoopers 2009, S. 10].

So beschreiben nach Abbildung 1 60,9 Prozent aller Befragten eine gleichbleibende, oder steigende Anzahl von Sicherheitsvorfällen in ihren Unternehmen zum Vorjahr (Siehe Abbildung 1).

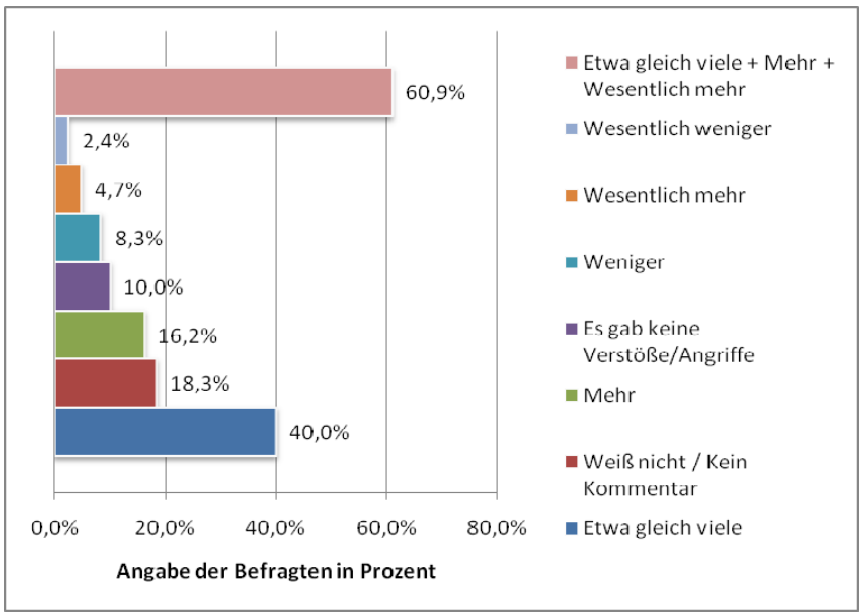

Abbildung 1: Entwicklung der Anzahl der Sicherheitsvorfälle

Quelle: in Anlehnung an IT InformationWeek 2008, S. 6

[2] Auf Deutsch: Wir finden es wesentlich erstaunlicher, dass mehr als die Hälfte (56%) erwartet, in Zukunft stetig bzw. höher in die IT-Sicherheit zu investieren – und dies während der schlechtesten Wirtschaftssituation seit Jahrzehnten. Oder vielleicht gerade deswegen.

„73 Prozent der IT-Sicherheitsbeauftragten in Unternehmen und Verbänden betonen mittlerweile die Wichtigkeit eines sicheren IT-Betriebes, um reibungslose Arbeitsabläufe in ihrer Organisation zu gewährleisten. Im Jahr 2005 waren es lediglich 66 Prozent.[..] Als Hauptgrund für Sicherheitsinvestitionen wird ein potenzieller Schaden basierend auf einer Risikobewertung angeführt. Jedoch auch die im Lagebericht 2007 vorhergesagte Zunahme gesetzlicher Vorgaben bezüglich Haftungsregelungen und Kreditvergabe wird als Grund für Investitionen im Sicherheitsbereich genannt [..].“ [BSI 2009, S. 13]

2.2 Grundlagen

2.2.1 Informationstechnik

„*Ein IT-System ist ein […] dynamisches technisches System mit der Fähigkeit zur Speicherung und Verarbeitung von Informationen*“ [Eckert 2006, S. 2]. Diese Systeme sind in einer Vielzahl von gesellschaftlichen, unternehmerischen und politischen Strukturen vorhanden und werden von unterschiedlichsten Benutzern für unterschiedlichste Aufgaben verwendet. Hierbei bilden Informationen und informationsverarbeitende Objekte die im System zu schützenden Güter. [vgl. Eckert 2006, S. 3]

IT setzt sich nach GOLTSCHE aus fünf so genannten ‚IT-Ressourcen’ (siehe Tabelle 1) zusammen, welche sich als Grundlage für Informationstechnik darstellen. [vgl. Goltsche 2006, S. 34]

Qualitätskriterium	Erläuterung
Personal	Informationssysteme und Services benötigen Menschen um durchgeführt zu werden, also um zu planen, zu organisieren, einzukaufen, zu unterstützen und zu überwachen
Applikationssysteme	Manuell durchgeführte und programmierte Prozeduren, Anwendungssoftware
Technische Infrastruktur	Enthält die Hardware, Betriebssysteme, Datenbanken, Netzwerke und Netzwerksoftware, etc.
Facilities	Das sind die Ressourcen, die benötigt werden, um die

	technische Infrastruktur aufzustellen und sowohl das Geschäft als auch die Informationssysteme zu unterstützen (Räume, Strom, Klima)
Daten	Zur Darstellung externer und interner Objekte, seien diese strukturiert oder unstrukturiert, Grafiken, Text, Audiodateien, etc.

Tabelle 1: IT-Ressourcen
Quelle: Goltsche 2006, S. 34

2.2.2 Sicherheit

Beim Begriff ‚Sicherheit' werden nach Claudia Eckert zwei Facetten unterschieden:

- Die **Funktionssicherheit** (engl. Safety) beschreibt, ob die realisierten Funktionen mit den geplanten Funktionen übereinstimmen und dass ein funktionssicheres System keinen funktional unzulässigen Zustand annimmt. *„Anders formuliert verstehen wir unter Funktionssicherheit eines Systems, dass es unter allen (normalen) Betriebsbedingungen funktioniert."* [Ecker 2006, S. 4 f.]

- Die **Informationssicherheit** (engl. Security) ist demnach die Eigenschaft nur solche Systemzustände anzunehmen, *„die zu keiner unautorisierten Informationsveränderung oder Gewinnung führen."* [vgl. Eckert 2006, S. 5]

Aktuelle Begriffe wie ‚Datensicherheit' und ‚Datenschutz' (engl. protection und privacy) sind demnach Eigenschaften der Informationssicherheit. Diese beschreiben eine Teilmenge der Systemzustände, welche nur den autorisierten Zugriff auf Ressourcen (insbesondere Daten bzw. personenbezogene Daten) zulassen. Der Schutz solcher autorisierten Übergange soll hierbei durch Filterung aller vorsätzlichen und unvorsätzlichen Aktivitäten gewährleistet werden [vgl. Eckert 2006, S. 5].

2.2.3 Schutzziele

In IT-Systemen sind Informationen bzw. Daten die zu schützende Güter. Der Zugriff soll nur für autorisierte Subjekte zugelassen sein. Hierzu erfordert es eine eindeutige Verifizierung der Identität [vgl. Eckert 2006, S. 6].

In Hinblick auf Anforderungen an den Betrieb von Informationstechnik und den Zugriff auf Daten lassen sich so genannte ‚Schutzziele' definieren. Die wesentlichen Schutzziele für die Sicherheit von Informationstechnik sind hierbei [vgl. Eckert 2006, S. 6 ff.]:

- **Authentizität** (engl. Authenticity):

  Beschreibt den ursprünglichen Herkunftsnachweis von Informationen.

- **Integrität** (engl. Integrity):

  Beschreibt die Unverfälschtheit der Daten und Informationen.

- **Privatsphäre** (engl. Privacy):

  Beschreibt den autorisierten Umgang mit personenbezogenen und personenbeziehbaren Daten.

- **Verbindlichkeit** / Nachweisbarkeit / Nicht-Abstreitbarkeit (engl. Account-ability, Non-Repudiation):

  Beschreibt die Nachweismöglichkeit bestimmter Ereignisse (vergleichbar mit einem Einschreiben – Brief ist angekommen).

- **Verfügbarkeit** (engl. Availability):

  Beschreibt den uneingeschränkten Zugriff auf Ressourcen.

- **Vertraulichkeit** (engl. Confidentiality):

  Beschreibt die Geheimhaltung bestimmter Ressourcen gegenüber unautorisierten Subjekten.

2.2.4 Schwachstelle und Bedrohung

Durch Schwachstellen können Schutzziele, wie Datenintegrität oder Verfügbarkeit eines IT-Systems beeinträchtigt werden. Unter einer Schwachstelle (engl. weakness) definiert ECKERT „*eine Schwäche eines Systems oder einen Punkt, an dem das System verwundbar werden kann.*" [Eckert 2006, S. 13f.]

Dies umfasst Möglichkeiten Sicherheitsdienste unauthorisiert durch Modifikation oder Täuschung zu umgehen. Abbildung 2 beschreibt die wesentlichen Gefährdungs-kategorien, durch welche Schwachstellen in IT-Systemen ausgenutzt werden können

[vgl. Eckert 2006, S. 14f.]. Hierbei können Schwachstellen nicht nur durch vorsätzliche Taten die Schutzziele gefährden, sonder auch fahrlässiger Umgang oder höhere Gewalt wie Blitzschläge oder Feuer.

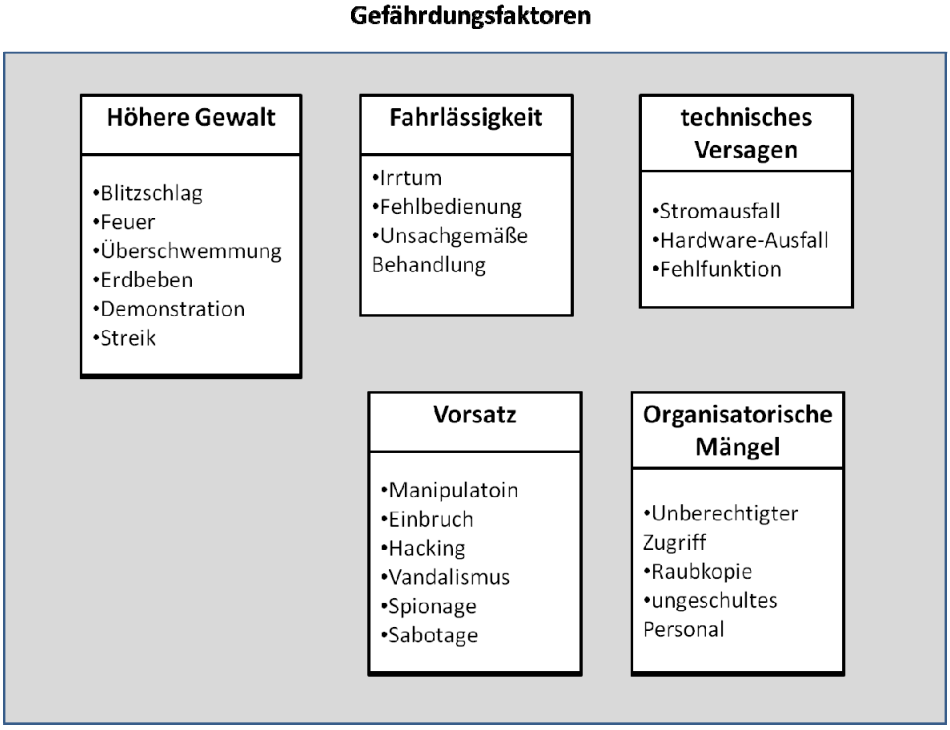

Abbildung 2: Klassifikation von Gefährdungsfaktoren

Quelle: Eckert 2006, S. 15

Eine Bedrohung beschreibt die Gefährdung der Ausnutzung von Schwachstellen die die Datenintegrität oder Verfügbarkeit beeinträchtigen kann [vgl. Ecker 2006, S. 14]. Je nach Gewichtung kann die Bedrohung von Fall zu Fall vernachlässigbar sein, oder eine ernsthafte Bedrohung für Unternehmen darstellen.

Je nach Unternehmenswert (engl. asset) gilt es eine Einschätzung bezüglich Eintrittswahrscheinlichkeit und potenziellen Schaden zu treffen. Dieser Gedanke führt zum Begriff des Risikos, welcher die relative Häufigkeit und die Schadenshöhe für den Eintritt eines Schadensereignisses angeben soll [vgl. Eckert 2006, S. 15].

Eine Messbarkeit des Risikos in einer Einheit ermöglicht folgende Risiko-Formel:

$$R = P_E \cdot S_E$$

Formel 1: Risiko-Formel

Quelle: Königs 2006, S. 11

Hierbei stellt *R* das Risiko, *P* die Wahrscheinlichkeit des Schadenseintritts und *S* das Schadensausmaß dar.

Da von einer 100-prozentigen Sicherheit und einem Risiko von null nicht auszugehen ist, spricht man beim Umgang zur Minimierung von Risiken im Unternehmen vom so genannten Risikomanagement [vgl. Königs 2006, S. 106]. Mithilfe des Risikomanagements soll zukünftiger Schaden und potentieller Verlust von Vermögen minimiert werden, indem mögliche Risiken gemessen und gesteuert werden. [vgl. Wolke 2008, S. 1f.] Wie in Abbildung 3 dargestellt ist, soll hierbei mögliche Schäden äußerer Einflüsse wie rechtlicher Rahmenbedingungen, volkswirtschaftlichen Ursachen, sowie technologischen Fortschritt entgegengewirkt werden.

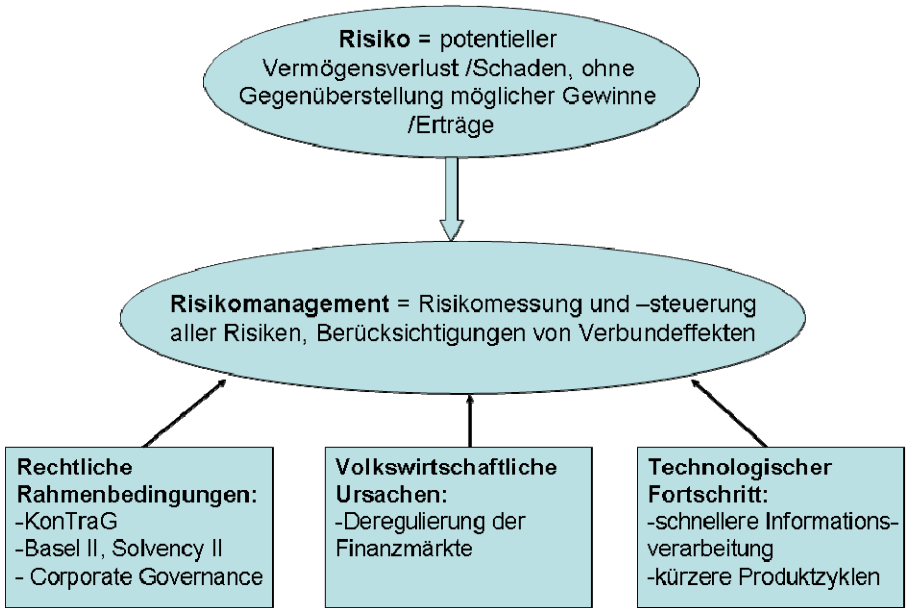

Abbildung 3: Begriffe und Gründe des Risikomanagements

Quelle: Wolke 2008, S. 3

2.3 Gesetzliche Anforderungen an die IT-Sicherheit

Je nach Branche hat die Informationssicherheit in Unternehmen einen unterschiedlich hohen Stellenwert. Dies hängt zum Teil mit einem unterschiedlichen Umfang der Informationsverarbeitung und -nutzung zusammen [vgl. Gründer et. al 2007, S. 15].

Unternehmen wie Banken, Versicherungen und Finanzinstitute haben relativ hohe Anforderungen an Verfügbarkeit und Sicherheit ihrer Informationen und werden als so genannte „reine Informationsverarbeiter" bezeichnet. Sie und Bereiche wie Verteidigung, Luft- und Raumfahrt und Energieversorgung haben eine so genannte ‚Null-Fehler-Philosophie' bezüglich eines jeden noch so kleinen Systemausfalls [vgl. Gründer et. al 2007, S. 15].

„IT-Sicherheit erfordert stets ein notwendiges Augenmaß, schließlich bestehen auch Unternehmen, deren Ansprüche an die Verfügbarkeit und Sicherheit ihrer Informationen deutlich geringer ausfallen, als in den zuvor beschriebenen Branchen. Oftmals unterschätzen und/oder vernachlässigen IT-Leiter die IT-Sicherheits-bedürfnisse aber gerade in solchen Unternehmen, da (IT-)Gefahren typischerweise nicht unmittelbar sicht- oder fühlbar sind, solange sie sich nicht verwirklicht haben. Sicherheitsmaßnahmen können bekanntlich erhebliche Ressourcen und Gelder beanspruchen, die angesichts oft knapper IT-Budgets nicht verfügbar sind." [Gründer et. al 2007, S. 16]

Im Rahmen der Sicherheit von Informationstechnologie wurden in der Bundesrepublik Deutschland (BRD) zum Ziel des einheitlichen Umgangs mehrere Gesetze eingeführt [vgl. Speichert 2007, S. 327f]. Diese dienen dem Schutz von Mitarbeitern, Kunden und Gläubigern aber auch der Übertragung von Verantwortung auf Unternehmen, Geschäftsleitungen und Mitarbeitern.

Im Folgenden werden einige wesentliche Gesetze mit den entsprechenden Vorschriften zur IT-Sicherheit in der BRD aufgezählt:

- Bundesdatenschutzgesetz (BDSG) [vgl. Speichert 2007, S. 164ff., Witt 2006, S. 7ff.]
    - Regelung des Datengeheimnisses
    - Beschreibung des Umgangs mit personenbezogenen Daten
- Strafgesetzbuch (StGB) [vgl. Speichert 2007, S. 311ff., Witt 2006, S. 14f.]
    - Strafrechtliche Verfolgung von Kompromittierung der Schutzziele

- Bürgerliches-/Handelsgesetzbuch (BGB, HGB) [vgl. Witt 2006, S. 6, S. 13]
    - Grundlagen des Datenschutzes
- Teledienstdatenschutzgesetz (TDDSG) [vgl. Speichert 2007, S. 142ff.]
    - Regelungen für den speziellen Datenschutz des Teledienstbereichs
- Telekommunikationsgesetz (TKG) [vgl. Speichert 2007, S. 121ff.]
    - Anwendung des Fernmeldegeheimnisses bei geschäftsmäßigen Telekommunikationsdienstleistern
    - Regelungen der Erlaubnisbestände bei Erhebung von Telekommunikations-daten
- Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) [vgl. Speichert 2007, S. 258, Witt 2006, S. 5]
    - Aufbewahrungspflichten von Daten und Belegen
- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) [vgl. Witt 2006, S. 4, Speichert 2007, S.218f.]
    - Verpflichtung zur Einführung eines Risikomanagementsystems
    - Reform zur ‚Corporate Governance'[3]

2.4 Bundesamt für Sicherheit in der Informationstechnik

Im Rahmen der gesetzlichen Anforderungen zur IT-Sicherheit in der BRD spielt das Bundesamt für Sicherheit (BSI) eine wesentliche Rolle. Das BSI ist eine Bundesbehörde, welche dem Bundesministerium des Innern unterstellt ist und die IT-Sicherheit in Deutschland stets auf aktuellem Stand halten soll. Aufgaben des BSI sind in dem ‚Gesetz zur Sicherheit in der Informationstechnik' (vom 14. August 2009) konkretisiert [vgl. BSI – Organisationsübersicht des BSI].

„Das BSI untersucht Sicherheitsrisiken bei der Anwendung der Informationstechnik und entwickelt Sicherheitsvorkehrungen. Es informiert über Risiken und Gefahren beim Einsatz der Informationstechnik und versucht Lösungen dafür zu finden. Dies beinhaltet

[3] Unternehmensübergreifende Grundsätze verantwortungsbewusster Unterenehmensführung [Fröhlich et. al 2007, S. 40f.]

die Prüfung und Bewertung der IT-Sicherheit von IT-Systemen, einschließlich deren Entwicklung in Kooperation mit der Industrie. Auch bei technisch sicheren Informations- und Telekommunikationssystemen können Risiken und Schäden durch unzureichende Administration und Anwendung entstehen. Um diese Risiken zu minimieren beziehungsweise zu vermeiden, wendet sich das BSI an eine Vielzahl von Zielgruppen: Es berät Hersteller, Vertreiber und Anwender von Informationstechnik. Darüber hinaus analysiert es Entwicklungen und Trends in der Informationstechnik." [BSI – Organisationsübersicht des BSI]

Hierzu führt das BSI die so genannten IT-Grundschutz-Kataloge in welchen aktuelle Sicherheitsmaßnahmen für typische Geschäftsprozesse, Anwendungen und IT-Systeme genannt werden. Diese Maßnahmen sollen einen angemessenen Schutz aller Informationen bei Institutionen und Unternehmen gewährleisten. „*IT-Grundschutz verfolgt dabei einen ganzheitlichen Ansatz. Durch die geeignete Kombination von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen wird ein Sicherheitsniveau erreicht, das für den normalen Schutzbedarf angemessen und ausreichend ist, um geschäftsrelevante Informationen zu schützen. Darüber hinaus bilden die Maßnahmen der IT-Grundschutz-Kataloge nicht nur eine Basis für hochschutzbedürftige IT-Systeme und Anwendungen, sondern liefern an vielen Stellen bereits höherwertige Sicherheit."* [BSI - IT-Grundschutz – Basis für Informationssicherheit]

3 Grundlagen IT-Sicherheitsstandards

3.1 Allgemein

„Standards und Normen dienen“ allgemein *„dazu, das Funktionieren von sozialen und technischen Systemen zu ermöglichen oder zu erhalten.“* [Fröhlich et. al 2007, S. 63] Eines der zentralen Anliegen an Modelle für IT-Standards sind die Skalierbarkeit auf Geschäftsprozesse und Umwelteinflüsse von Unternehmen. IT-Sicherheitsmodelle wie ITIL, COBIT oder ISO 27001 sind solche Standards, welche die Unternehmen bei der Einführung, Verbesserung und Überwachung von Informationstechnologie unterstützen sollen [vgl. 27001, S. 5].

Hierbei spielt der Begriff der ‚IT Governance’ eine wesentliche und aktuelle Rolle [vgl. Fröhlich et. al 2007, S. 63].

3.1.1 IT Governance

„*IT Governance umfasst prinzipielle Regelungen zu Entscheidungsrechten, Rollen, und Verantwortlichkeiten sowie zur Organisation der IT, die sich jeweils auf die Domänen Stategic Alignment, Value Delivery, Ressource Management, Risk Management und Performance Measurement*[4] *beziehen*.“ [Fröhlich et. al 2007, S. 29]

Abbildung 4 skizziert das Verständnis von FRÖHLICH ET. AL, wie sich IT im Unternehmen integriert und beschreibt in diesem Zusammenhang das Verständnis von Governance, insbesondere von IT Governance.

[4] auf Deutsch: „Harmonisierung von IT und Business, Bewertung des Beitrages der IT, Nutzung von Ressourcen, Risikomanagement und Risikovorsorge, Messbarkeit der Umsetzung“

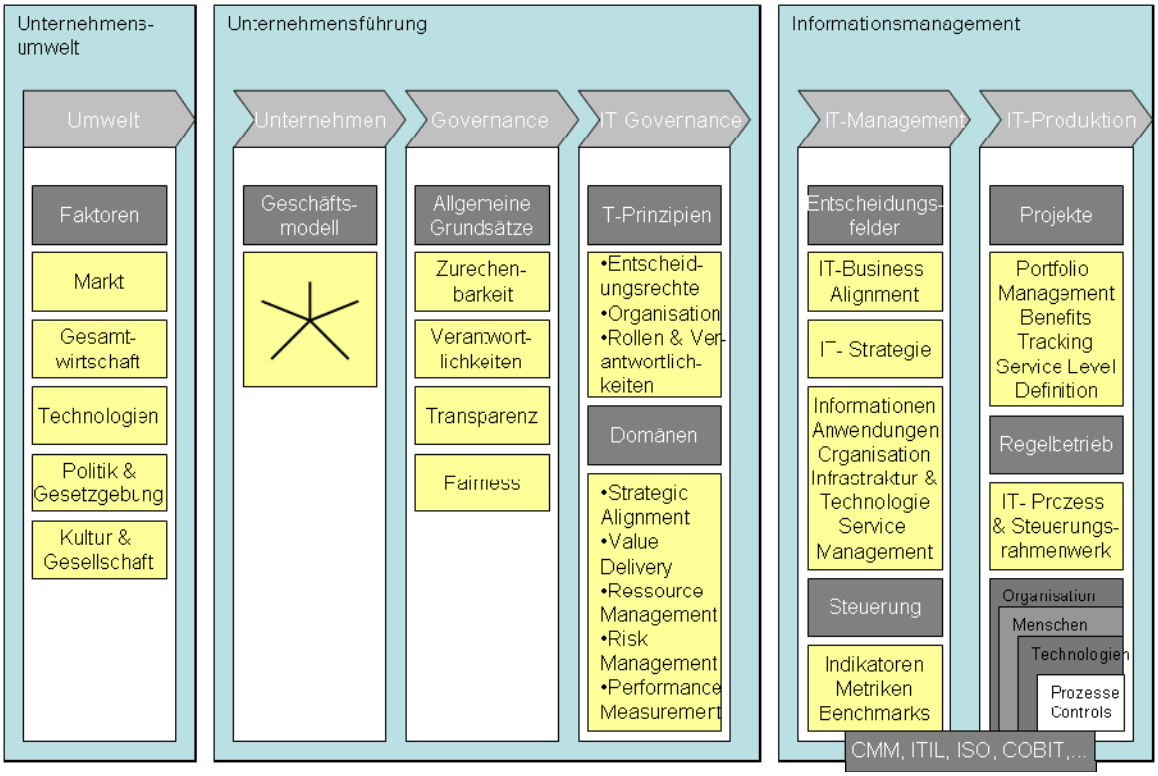

Abbildung 4: IT als integraler Bestandteil des Unternehmens

Quelle: in Anlehnung Fröhlich et. al 2007, S. 28

Die **Umwelt** des Unternehmens beschreibt die Grenzen der Handlungsmöglichkeiten, sie schränkt mögliche Aktionen durch Einflüsse wie Marktpotenziale, Regularien und Konkurrenzsituation ein.

Die **Unternehmensführung** setzte sich aus Unternehmen, Governance und IT-Governance zusammen. *„Die Unternehmensführung richtet an den durch die Umwelt vorgegebenen Möglichkeiten das Geschäftsmodell aus [...]“* [Fröhlich et. al 2007, S. 28], und legt Strategie und Geschäftsprozesse fest, welche die Schaffung einer geeigneten Organisation unterstützen. Schließlich werden hier auch Einsatz von Personal und Technologie festgelegt.

In Form der **Governance** gibt die Unternehmensleitung *„allgemeine Grundsätze zu Entscheidungskompetenzen und Verantwortlichkeiten, Regeln zur Sicherstellung von Transparenz und moralische Grundsätze (Fairness)“* [Fröhlich et. al 2007, S. 28f] vor. Die Governance beschreibt demnach alle bereichsspezifischen Governances (insbesondere IT-Governance). Während die **IT Governance** die Art und Weise des Einsatzes von IT im Unternehmen beschreibt, legt das **Informationsmanagement** das konkrete Handeln innerhalb einer Domäne fest. Dieses unterteilt sich wieder herum in ‚IT-Management’ und ‚IT-Produktion’, in denen der operative IT-Betrieb ausgeführt und gesteuert wird [vgl. Fröhlich et. al 2007, S. 29].

Auf dieser Ebene werden prozessorientierte IT-Standards und Best Practices wie ITIL, COBIT und ISO einsetzbar [vgl. Fröhlich et. al 2007, S. 30]. Der prozessorientierte Ansatz erfolgt nach dem PDCA-Modell von Deming, welcher im Folgenden genauer beschrieben wird.

3.1.2 PDCA-Zyklus

Die Grundlage einer Vielzahl von IT-Standards (ISO 27001 oder ITIL) ist der Kontrollzyklus von Deming [vgl. Goltsche 2006, S. 13f].

„Das Modell von Deming ist sehr weit verbreitet und gut bekannt. Es fokussiert auf Prozessoptimierung im industriellen Fertigungsbereich, um dadurch die Qualität der erzeugten Produkte zu steigern. Deming kreierte einen kontinuierlichen Verbesserungs-fluss [...]“ der *„häufig als Kreislauf dargestellt“* wird [Goltsche 2006, S.13f]. Dieser Kreislauf kann gemäß der Darstellung zyklisch immer wieder durchlaufen werden (siehe Abbildung 5).

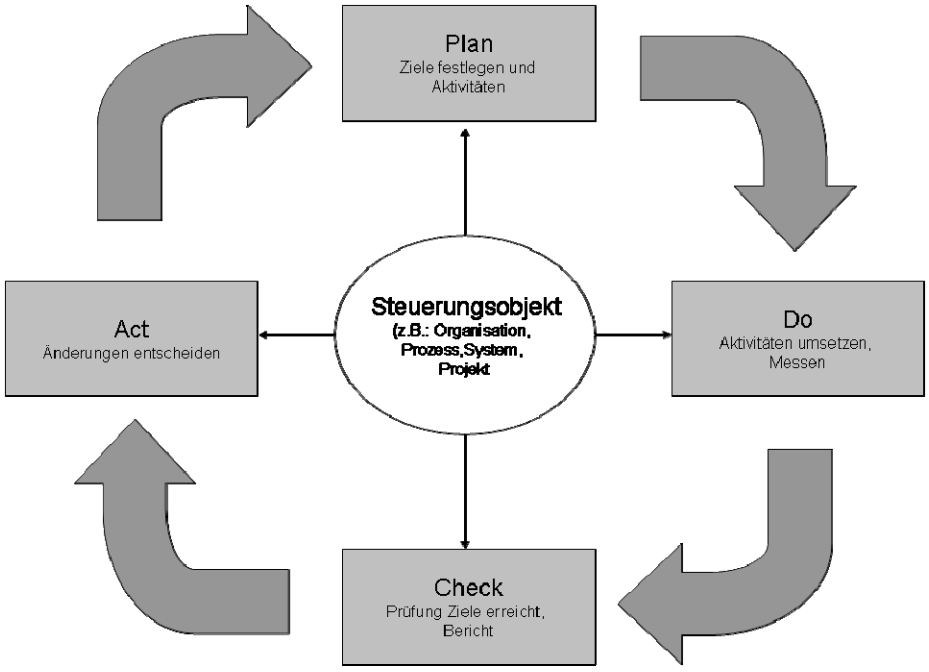

Abbildung 5: Kontrollzyklus nach Deming

Quelle: Goltsche 2006, S. 14

Die einzelnen Phasen können wie folgt beschrieben werden:

- Plan: Entwickeln oder Ändern von Geschäftsprozessen oder Teilen davon, um die Ergebnisse zu verbessern, Aufstellung eines Plans
- Do: Durchführen des Plans und Messung der Wirksamkeit
- Check: Bewerten der Messergebnisse und Berichten der Bewertungen an die Entscheider
- Act: Entscheiden über Änderungen, die notwendig sind, um den Prozess zu verbessern

Mithilfe dieses kontinuierlichen Verbesserungszyklus, sollen Unternehmen im stetigen Wandel an ihrer Unternehmensqualität arbeiten können, um stetig Leistung, Kunden- und Mitarbeiterzufriedenheit, Prozesse und Produkte zu verbessern [vgl. Goltsche 2006, S. 13f.].

Das Modell von Deming lässt sich prinzipiell auf alle Phasen eines IT-Sicherheitskonzeptes anwenden. Es bildet auch die Grundlage der Rahmenarchitekturen der ISO 2700x, insbesondere des Informationssicherheits Managementsystems (ISMS) nach ISO 27001. Diese werden im Folgenden genauer beschrieben.

3.2 ISO 2700X Familie

Die geplante ISO 27000-Familie soll eine Vielzahl von Standards zur IT-Sicherheit umfassen und Ordnung in die vielen Normen bringen. In dieser ist das Informationssicherheits Managementsystem (ISMS) nach ISO 27001 eine wesentliche Komponente. Darüber hinaus sind derzeit weitere Standards angedacht:

- ISO 27001 – Informationssicherheits-Managementsysteme
- ISO 27002:2005 (ehemals 17799:2005)
- ISO 27003 – Implementierungsrichtlinien
- ISO 27004 – Metriken und Messmöglichkeiten
- ISO 27005 – Risikomanagement
- ISO 27006:2007 - Anforderungen an Auditierungs- und Zertifizierungsinstanzen

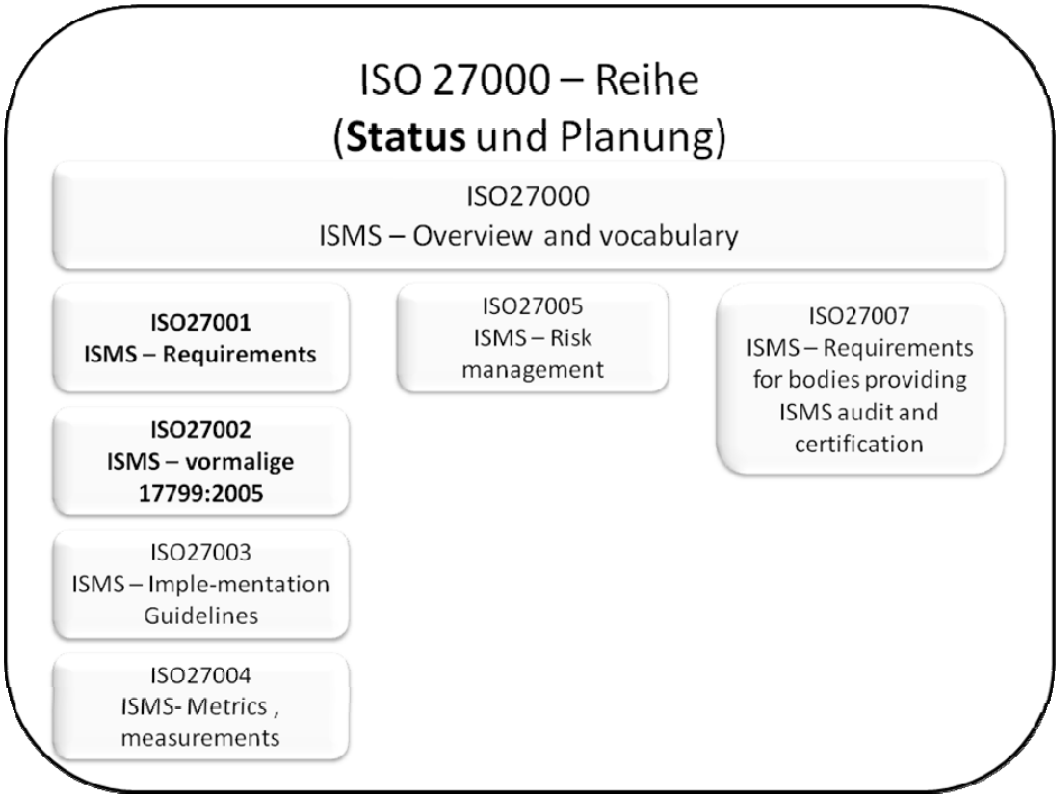

Abbildung 6: ISO 27000 – Reihe

Quelle: Müller 2008 – IT-Sicherheit mit System, S. 31

Abbildung 6 beschreibt den Abschluss und die Planung der Arbeiten an der Normenreihe ISO 27000 [vgl. Müller 2008, S. 30].

3.2.1 ISO 27001:2005

Die ISO/IEC 27001:2005 ‚Information technology – Security techniques – Information security management systems – Requirements' beschreibt Maßnahmen zur Einführung eines prozessorientierten Informationssicherheits-Managementsystems (ISMS).

Im Rahmen des IT-Sicherheitsmanagements ist seit Januar 2006 eine ISO 27001 Zertifizierung auf Basis des IT-Grundschutzes möglich, welche sowohl Anforderungen der ISO 27001 und auch des IT-Grundschutzes des BSIs erfüllt. Aus diesem Grund ist eine Zertifizierung nach ISO 27001 gerade für international tätige Unternehmen sehr wichtig. [vgl. Hofmann, Schmidt 2004, S. 261] Der Aufbau dieses Modells erfolgt in überblicksartigen Themen:

1. Begriffe und Definitionen
2. Informationssicherheitsmanagementssysteme (ISMS)
3. Verantwortung des Management

4. Interne ISMS Audits
5. Management Review des ISMS
6. Verbesserung des ISMS
7. Kontrollziele und Kontrollen (Anhang A)
8. OECD-Prinzipien und der Standard ISO/IEC 27001:2005 (Anhang B)

Die Grundlage des ISMS basiert auf den vier Phasen des PDCA-Zyklus nach Deming (siehe Kapitel 3.1.2). Hierbei beschreibt die Planungsphase (Plan) den Aufbau eines ISMS, in welcher die Organisation den Geltungsbereich definiert. Dabei sollten besonders gesetzliche, vertragliche und regulatorische Anforderungen in Betracht gezogen werden. Schließlich erfolgt eine Risikobewertung der Unternehmenswerte [vgl. Müller 2008, S. 29].

In der Durchführungsphase (Do) umfasst die ISO 27001 Maßnahmen zur Implementierung des Risokomanagements, Bewertung des Betriebs vom ISMS und Schulungen von Personal [vgl. Müller 2008, S. 29].

Die Prüfungsphase (Check) beschreibt das Monitoring von Fehlern und Sicherheitslücken im ISMS. Mithilfe von regelmäßigen Audits und Reviews sollen mögliche Verbesserungspotenziale des Systems identifiziert werden [vgl. Müller 2008, S. 29].

Abschließend wird in Verbesserungsphase (Act) die Umsetzung der Verbesserungen vorgenommen und mit einer Bewertung möglicher Zielstellungen abgeschlossen [vgl. Müller 2008, S. 29].

3.2.2 ISO 27002:2005

Die ISO/IEC 27002:2005 (ehemals ISO/IEC 17799:2000) ist inhaltliche Grundlage des British Standard Nr. 7799, Teil 1 (BS 7799-1:1999) [vgl. Müller 2008, S. 26f]. Sie besteht aus 11 Abschnitten mit Maßnahmen zur Erfüllung von IT-Sicherheitsanforderungen eines ISMS und sollen bei der Bewältigung von IT-Risiken in der Praxis unterstützen [vgl. Königs 2006, S. 141].

Im Genaueren besteht der ISO 27002-Standard aus folgenden Sicherheitskategorien:

1. Sicherheitsleitlinie

2. Organisation der Informationssicherheit
3. Management von organisationseigenen Werten
4. Sicherheit im Personalbereich
5. Physische und umgebungsbezogene Sicherheit
6. Management der Kommunikation und des Betriebs
7. Zugangskontrolle
8. Beschaffung, Entwicklung und Wartung von Informationssystemen
9. Management von Informationssicherheitsvorfällen
10. Aufrechterhaltung des Geschäftsbetriebs
11. Einhaltung von Verpflichtungen

In jedem dieser Abschnitte wird ein Maßnahmenziel beschrieben, zu dem schließlich detaillierte Informationen zur Umsetzung geschildert werden. Neben Anleitungen zur Umsetzungen werden aber auch weiterführende Angaben zu anderen Standards oder zum Beispiel gesetzliche Rahmenbedingungen veranschaulicht [vgl. 27002, S. 14f.]. Eine schematische Darstellung des Aufbaus, siehe Abbildung 7.

Im Gegensatz zur ISO 27001 wird hier also nicht der Prozess des IT-Sicherheitsmanagements beschrieben, sondern es wird eine Sammlung von ‚Best-Practices'[5] an Maßnahmen angegeben, welche zur Umsetzung implementiert werden können. Hierbei sind die Maßnahmen keine verbindlichen Forderungen, sondern sollen als „*Ausgangspunkt für die Entwicklung organisationsspezifischer Richtlinien angesehen werden.*" [27002, S. 11] Deshalb sollen Unternehmen in der Lage sein, die Maßnahmen durch ihre unternehmenseigenen Richtlinien zu ergänzen.

[5] In deutsch: bestes Verfahren bzw. Erfolgsrezept

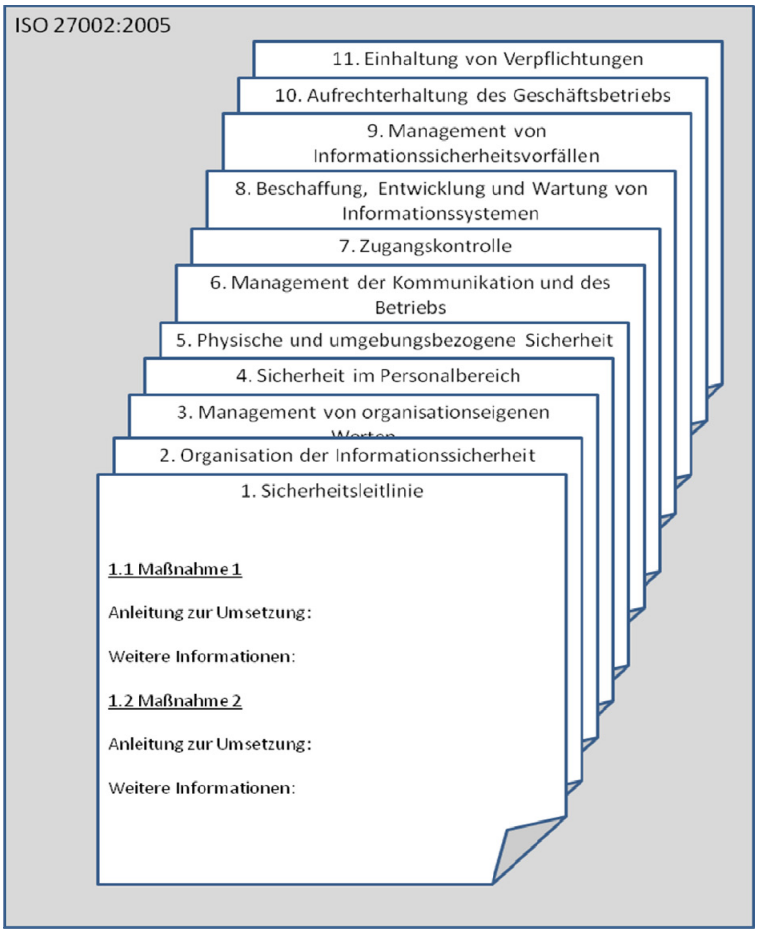

Abbildung 7: Schema ISO 27002

3.2.3 Abgrenzung zu anderen Standards

Neben der ISO 27002 ehemals 17799 gibt es weitere wichtige internationale Regelwerke wie zum Beispiel ITIL und COBIT [vgl. Königs 2006, S. 140].

COBIT umfasst hierbei ein geschäftsorientierten Framework mit Kontrollzielen für Auditoren (Revisor), Manager und „Owner“ von IT-Prozessen. Es beschreibt für 34 IT-Prozesse wesentliche Erfolgsfaktoren, Schlüsselziel-Indikatoren und Schlüssel-Leistungs-Indikatoren, auf welche die IT-Prozesse hin überprüft werden sollen [vgl. Königs 2006, S. 138].

„*COBIT unterstützt die IT-Governance, indem eine umfassende Beschreibung der Kontrollziele für IT-Prozesse geliefert wird. Diese Kontrollziele, auf englisch Control Objectives genannt, sind Aussagen zum gewünschten Ergebnis/Zweck eines Prozesses, das mit der Implementierung von Kontrollverfahren in einer bestimmten Aktivität erreicht werden soll. Vom Prinzip her benutzt COBIT damit das Kontrollmodell von*

Deming […] setzt aber auf Normen, Standards und Zielen als Inputgeber für Verbesserungen.“ [Goltsche 2006, S.12]

ITIL dagegen unterstützt einen prozessorientierten Rahmen für Betreiber von IT- und Telekommunikationsdiensten, unter Berücksichtigung einer zentralen Rolle der Benutzer [vgl. Königs 2006, S. 140]. Es besteht dabei aus einer Reihe von Büchern, welche Vorschläge für Best-Practices für das IT-Service Management beinhalten. Dabei gibt es eine Vielzahl von Empfehlungen von Aktivitäten zur Umsetzung, aber gibt keine Unterstützung bei der Umsetzung [vgl. Goltsche 2006, S. 9].

Je nach Regelwerk haben die einzelnen Standards unterschiedliche Schwerpunkte bezüglich gewisser Anwendungsgebiete wie „Planung und Organisation“, „Beschaffung und Einführung“, „Auslieferung und Unterstützung“ und „Überwachung“. Zudem bestehen auch Unterschiede in der Anleitung zur Kontrolle, dem Risiko-Management und der Maßnahmenkonzeption. Wie in Abbildung 8 dargestellt, gibt KÖNIGS die Standards in zwei Kategorien an. Umso tiefer die Unterstützungstiefe ist, desto höher ist der technische und betriebliche Detailierungsgrad des Regelwerks und umso breiter die Anwendungstiefe ist, desto vollständiger lassen sich sämtliche Sicherheitsanliegen unterstützen [vgl. Königs 2006, S.139 ff.].

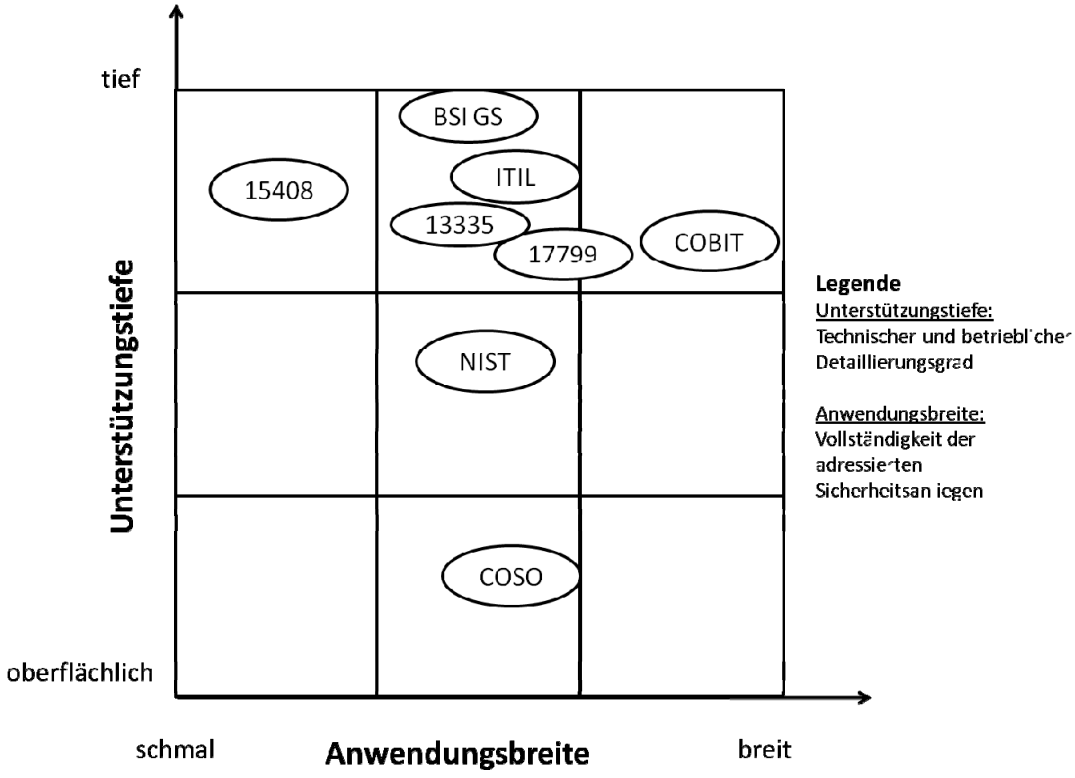

Abbildung 8: Standardübersicht

Quelle: Königs 2006, S. 141

4 IT-Sicherheit öffentlicher Auftraggeber

In diesem Abschnitt soll zunächst der Begriff des öffentlichen Auftraggebers (ÖAG) beschrieben, sowie die Bedeutung und der Grund der Untersuchung des ISO 27002 Sicherheitsstandards bei ÖAGs verdeutlicht werden.

Zur Untersuchung der IT-Sicherheitsmaßnahmen wird im Rahmen dieser Arbeit im Kapitel 5 die Umsetzung anhand des Beispiels der Bundeswehr erarbeitet und den Maßnahmen der ISO 27002 gegenübergestellt. Hierbei wird in kurzen Abschnitten auch auf die konkrete Umsetzung der genannten Maßnahmen eingegangen. Hierfür ist das zentrale Dokument die ZDV 54/100 – „IT-Sicherheit in der Bundeswehr“, welche aus sicherheitstechnischen Gründen nur in Auszügen im Anhang 2 wiederzufinden ist.

4.1 Definition öffentlicher Auftraggeber

Ein öffentliche Auftraggeber (ÖAG) ist bei Beschaffungsvorgängen an vergaberechtliche Vorschriften des Vergaberechts öffentlicher Aufträge gebunden. Hierzu unterscheidet das ‚Gesetz gegen Wettbewerbsbeschränkungen’ (GWB) sechs Gruppen öffentlicher Auftraggeber [vgl. Fabry et al. 2007, S. 23]:

1. *„Gebietskörperschaften sowie deren Sondervermögen*” [§ 98 Nr. 1 GWB]

   Zu den Gebietskörperschaften zählen der Bund, die Bundesländer, sowie Landkreise und Gemeinden. Daneben gehören hierzu auch deren ‚Sondervermögen’, in Form von organisatorisch unabhängigen und mit eigenem Haushalt ausgestatteten Eigenbetrieben. Bei diesen tritt aber stets die dahinter stehende Gebietskörperschaft als öffentlicher Auftraggeber auf [vgl. Fabry et al. 2007, S. 23].

2. *„andere juristische Personen des öffentlichen und des privaten Rechts, die zu dem besonderen Zweck gegründet wurden, im Allgemeininteresse liegende Aufgaben nichtgewerblicher Art zu erfüllen [...]“* [§ 98 Nr. 2 GWB]

   „*Hierzu zählen selbstständige- besonders privatrechtlich organisierte juristische Personen, die öffentliche Aufgaben wahrnehmen.*“ [Fabry et al. 2007, 24f.] Dieser Artikel umfasst also auch neben rechtsfähigen Körperschaften und Anstalten auch juristische Personen wie Aktiengesellschaften (AG), Gesellschaften mit beschränkter Haftung (GmbH) oder auch eingetragene Vereine (e.V.) [vgl. Fabry et al. 2007, 24f.].

3. *„Verbände, deren Mitglieder unter Nummer 1 oder 2 fallen“* [§ 98 Nr. 3 GWB]

Hinzu kommen Verbände, deren Mitglieder öffentliche Auftraggeber nach § 98 Nr. 1 oder 2 sind. Insbesondere fallen hierzu auch Zusammenschlüsse wie z.B. Wasser- und Schulverbände [vgl. Fabry et al.,S. 30f.].

4. *„natürliche oder juristische Personen des privaten Rechts, die auf dem Gebiet der Trinkwasser- oder Energieversorgung oder des Verkehrs tätig sind [...]“* [§ 98 Nr. 4 GWB]

   Zusätzlich umfasst die Vergabepflicht nicht nur organisatorische Personen wie in Artikel 2, sondern auch monopolähnliche Marktbranchen, aud die der Staat Einfluss nimmt. Hierzu zählen Auftraggeber bei denen die zu erfüllenden Aufgaben im Allgemeininteresse des Staates liegen, wie Trinkwasserversorger, Energieversorger (Elekrizität-, Gas-, und Wärmeversorgung) oder auch Verkehr [vgl. Fabry et al., S. 31].

5. *„natürliche oder juristische Personen des privaten Rechts in den Fällen, in denen sie für Tiefbaumaßnahmen, für die Errichtung von Krankenhäusern, Sport-, Erholungs- oder Freizeiteinrichtungen, Schul-, Hochschul- oder Verwaltungsgebäuden oder für damit in Verbindung stehende Dienstleistungen und Auslobungsverfahren von Stellen, die unter Nummern 1 bis 3 fallen, Mittel erhalten, mit denen diese Vorhaben zu mehr als 50 vom Hundert finanziert werden, [...]“* [§ 98 Nr. 5 GWB]

   Hierbei wird die Vergabepflicht auf natürliche und juristische Personen des Privatrechts erweitert, sofern diese staatlich finanzierte Leistungen erbringen [vgl. Fabry et al., S. 32].

6. *„natürliche oder juristische Personen des privaten Rechts, die mit Stellen, die unter die Nummern 1 bis 3 fallen, einen Vertrag über eine Baukonzession abgeschlossen haben, hinsichtlich der Aufträge an Dritte*.“ [§ 98 Nr. 5 GWB]

   Dieser Teil umfasst natürliche und juristische Personen des Privatrechts, welche mit einem öffentlichen Auftraggeber einen Vertrag über eine Bauleistung abgeschlossen haben, so ist die Leistung auf Nutzung gegenüber Dritten der Vergabepflicht unterworfen. [vgl. Fabry et al., S. 32]

Nach den europäischen Vergaberichtlinien gibt es drei Grundsätze, an denen sich die Vorschriften des Vergaberechts orientieren: das **Wettbewerbsprinzip**, das **Transparenzprinzip**, sowie das **Diskriminierungsverbot** [vgl. Fabry et al.,S. 46].

Im Sinne des Wettbewerbsprinzip soll eine Gleichbehandlung regionaler und europäischer Unternehmen zum Zweck eines einheitlichen europäischen Binnenmarktes erfolgen. „*Das Transparenzgebot verpflichtet den öffentlichen Auftraggeber, das Vergabeverfahren nach eindeutigen, nachvollziehbaren und – soweit möglich – im Voraus bestimmten Vorgaben durchzuführen.*“ [Fabry et al., S. 50] Das Ziel des Diskriminierungsverbots ist es, einen europaweiten Markt für öffentliche Aufträge zu schaffen, durch welches Diskriminierung von Auftraggebern anderer EU-Staaten unterbunden werden soll.

4.2 Bedeutung der ISO-Norm für ÖAG

„*Eine nicht zu unterschätzende Bedeutung für die Durchsetzung von Zertifizierungsmodellen kommt dem öffentlichen Beschaffungsrecht und hier insbesondere den für diesen gültigen europäischen Richtlinien zu*.“ [Kersten et al. 2008, S. 6]

Zur Einhaltung des Wettbewerbsprinzips bei Ausschreibungen von technischen Anforderungen von Managementsystemen werden bestimmte Normen bevorzugt, die es ermöglichen nationale und europäische Normen umzusetzen. Doch obwohl ISO 27001, der IT-Grundschutz und der Code of Practice (COBIT) in einzelnen EU-Richtlinien Erwähnung finden, kann hierbei im Sinne des öffentlichen Beschaffungsrechts nicht von gleichwertigen Modellen ausgegangen werden [vgl. Kersten et al. 2008, S. 6f.]. Wenn also ein öffentlicher Auftraggeber bei einer internationalen Ausschreibung den Grundschutznachweis alter Form des BSI einfordert, würde dies ein Handelshindernis darstellen und andere ausländische Bieter diskriminieren.

Wenn also die Einführung eines Managementsystems die Zulassungskriterien für das europäische Beschaffungsrecht erfüllen soll, ist eine Verwendung und Vergleichbarkeit durch DIN ISO/IEC 27001 ratsam [vgl. Kersten et al. 2008, S. 6f.].

Zur Unterstützung der Umsetzung von ISO 27001 gibt die ISO 27002 (ehemals 17799) eine umfangreiche Anleitung mit möglichen Maßnahmen. Diese Maßnahmen spielen für die Anwendung der ISO 27001 eine so große Rolle, dass sie in der Anlage A in kurzer Form beschrieben werden [vgl. 27002, S. 7ff.]. Dadurch bietet die ISO 27002 eine entscheidene Grundlage für die Vergleichbarkeit von Umsetzungen eines ISMS nach ISO 27001. Aus diesem Grund wird im Rahmen dieser Arbeit die Umsetung von Maßnahmen der Bundeswehr nach ISO 27002 untersucht.

4.3 IT-Sicherheit ÖAG am Beispiel der Bundeswehr

Um eine Umsetzung von Anforderungen der IT-Sicherheit von ÖAG zu untersuchen, ist die Bundeswehr ein sehr gutes und anschauliches Beispiel. Durch die sehr hohen und umfangreichen Anforderungen an die Erfüllung ihrer Schutzziele bietet sich die Untersuchung des Sicherheitskonzeptes der ZDV 54/100 an.

Nach dem Beitritt der BRD in die NATO und der Gründung der Bundeswehr im Jahre 1956 hat sich ihr Einsatz bis heute wesentlich verändert. Erhebliche Modernisierungen durch die Einführung betriebswirtschaftlicher Steuerungs- und Managementmethoden versprechen eine effizientere und effektivere Organisation [vgl. Richter 2007, S. 15]. Eine Vielzahl von öffentlichen Aufträgen „*bis zur Privatisierung von Aufgaben im Servicebereich der Streitkräfte*“ [Richter 2007, S. 15] haben demnach auch im Bereich der IT wesentliche Veränderungen gebracht.

So werden im Rahmen des Projektes ‚Herkules‘ „*Rechenzentren, Software und Anwendungen, Computer, Telefone sowie Sprach- und Datennetze auf den neuesten Stand*“ [Heise Online] gebracht. Dies ist mit einem Volumen von 7,1 Milliarden Euro eines der derzeit größten Public-Private-Partnership in Europa [vgl. ebd.].

Die IT-Systeme (IT-SysBw) der Bundeswehr umfassen eine Vielzahl von vielschichtigen Systemen für die unterschiedlichsten Aufgaben. Abbildung 9 verdeutlicht die wesentlichen Bestandteile des IT-SysBw.

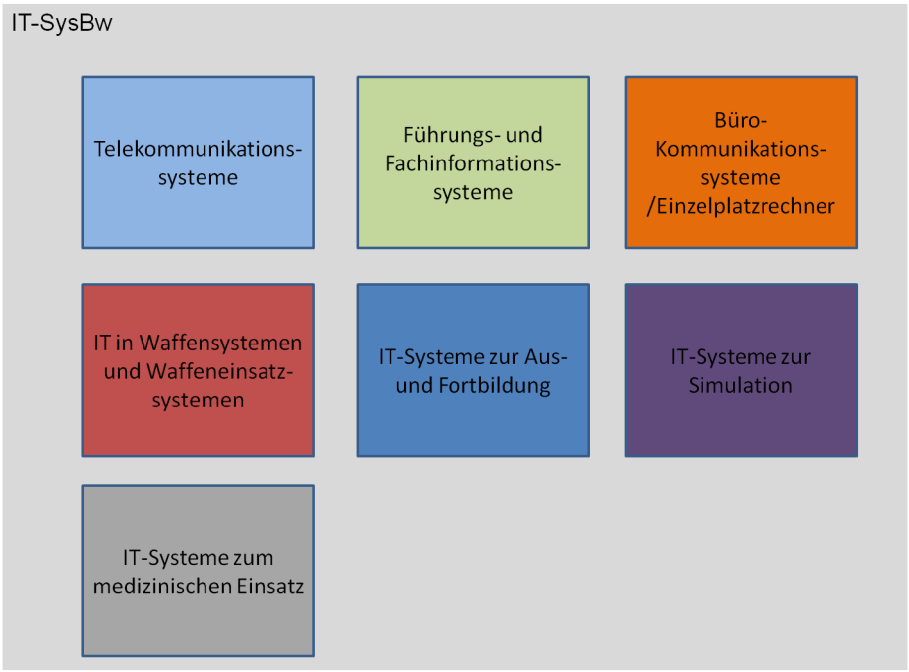

Abbildung 9: Aufbau IT-SysBw

Quelle:Eigene Darstellung in Anlehnung an ZDV 54/100, S. 10

Durch den stetig wachsenden Einsatz von IT in wesentlichen Prozessen der Bundeswehr, spielt der Schutz von Daten und Informationen auch hier eine immer größere Rolle. Im Rahmen dieser Arbeit hat die Bundeswehr eine Vielzahl von gesetzlichen Bestimmungen einzuhalten, welche für eine Vielzahl anderer öffentlicher Einrichtungen ebenfalls von Bedeutung sind wie z. B. StGB, Informations- und Kommunikationsdienstegesetz (IuKDG), Teledienstegesetz (TDG), Teledienstedatenschutzgesetz (TDDSG), Zugangskontrolldiensteschutzgesetz (ZKDSG) und BDSG.

Die wesentlichen Schutzziele der IT-Systeme der Bundeswehr bestehen aus dem Erhalt von Integrität, Verfügbarkeit, Verbindlichkeit und Vertraulichkeit von Informationen bei politischen und militärischen Entscheidungs- und Führungsprozessen. Die Maßnahmen zur IT-Sicherheit sollen aber auch die Beeinträchtigung der Funktionsfähigkeit von Führungsmitteln durch Fremdeinflüsse ausschließen, zu einer Kontinuität der Arbeitsabläufe der Bundeswehr beitragen und im Schadensfall negative Auswirkungen minimieren [vgl. ZDV 54/100, S.11].

Wesentlicher Bestandteil für IT-Sicherheit im Unternehmen, aber auch in der Bundeswehr ist eine klare organisatorische Struktur der Kompetenzen. Abbildung 10 verdeutlicht die Organisationsstruktur der Bundeswehr, insbesondere des IT-AmtBws und der ministeriellen Weisung durch die Abteilung M II im Bundesministerium für Verteidigung.

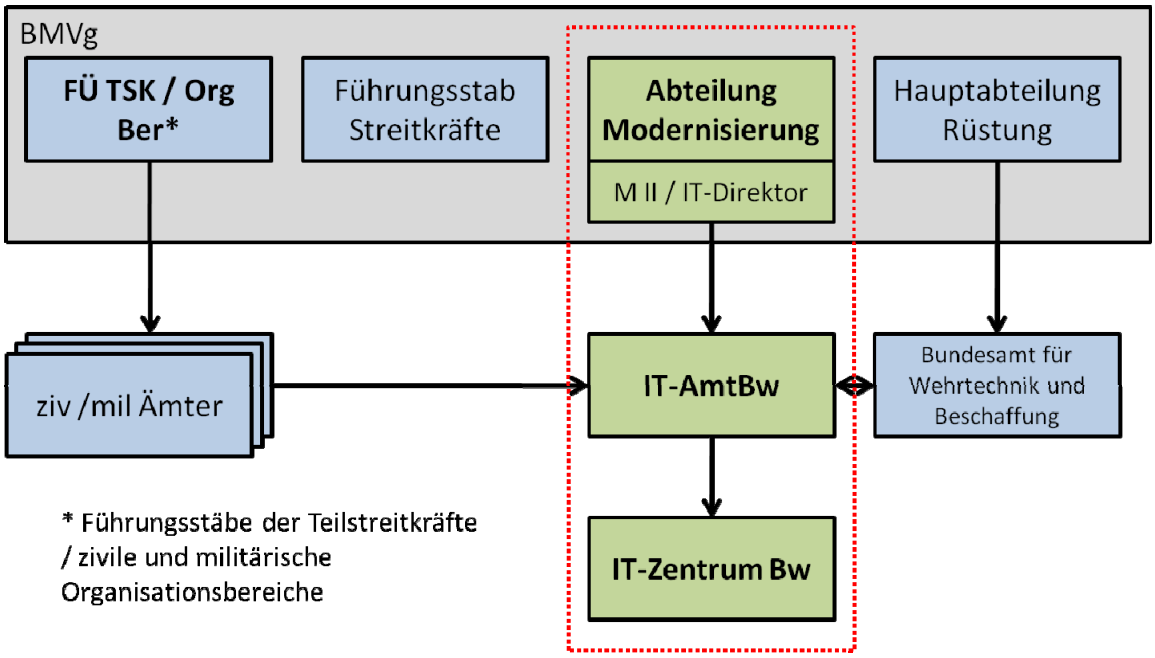

Abbildung 10: Organisatorische Einbindung IT-AmtBw

Quelle: IT-AmtBw

5 IT-Sicherheit der Bundeswehr nach ZDV 54/100

Im Rahmen der Untersuchung der Maßnahmen der ZDV 54/100 wird in dieser Arbeit eine Gegenüberstellung erarbeit, um die Frage zu beantworten, ob ein ÖAG die Maßnahmen der ISO 27002 erfüllt. Neben den Tabellen zur Gegenüberstellung der geforderten Maßnahmen, werden in kurzen Abschnitten die angewandten Maßnahmen der Bundeswehr beschrieben, welche in den oben genannten Verweisen im Anhang nachzulesen sind.

Die Struktur und Nummerierung der Tabellen erfolgt hierbei aus Sicht der ISO 27002-Norm und beginnt mit den ersten Maßnahmen im Abschnitt 4. Im weiteren Verlauf wird aus Gründen einer besseren Lesbarkeit bei Beschreibungen aus der ZDV 54/100 nur von der ZDV gesprochen. Das Gleiche gilt für die Verwendung des Begriffs ISO für den Sicherheitsstandard nach ISO 27002.

5.1 Sicherheitsrichtlinie

		ISO 27002	**ZDV 54/100**
5.		**Sicherheitsleitlinie**	
	5.1.	Informationssicherheits-leitlinie	
	5.1.1.	Leitlinie zur Informationssicherheit	ZDV 54/100 bildet Dokument der Sicherheitsrichtlinie und umfasst: LfNr. 1, 2, 3, 4
	5.1.2.	Überprüfung der Informationssicherheits-linie	LfNr. 7, 8, 9, 10

Tabelle 2: Sicherheitsrichtlinie

Die ZDV 54/100 ist die Leitlinie für die Informationssicherheit. Diese Dienstvorschrift umfasst neben IT-Sicherheitsmaßnahmen, die IT-Sicherheitskonzepte für Dienststellen und Projekte, Anforderungen an Hard- und Software und auch allgemeine Grundlagen zur IT-Sicherheit.

Die Durchführung von Sicherheitsmaßnahmen wird in Anlage 21 der ZDV dokumentiert. Diese wird in unregelmäßigen Abständen aktualisiert. Dieses Dokument wird neben anderen auch im Intranet der Bundeswehr (IntranetBw) zur Einsichtnahme veröffentlicht. Zusätzlich besteht die Möglichkeit im Rahmen eines Änderungsvorschlags Maßnahmen zur Korrektur der Sicherheitsrichtlinie einzureichen.

5.2 Organisation der Informationssicherheit

		ISO 27002	**ZDV 54/100**
6.		**Organisation der Informationssicherheit**	
	6.1.	Interne Organisation	
	6.1.1.	Engagement des Managements für Informationssicherheit	Kapitel 2 „Organisation IT Sicherheit“ LfNr. 2001- 2006
	6.1.2.	Koordination der Informationssicherheit	LfNr. 4001-4005
	6.1.3.	Zuweisung der Verantwortlichkeiten für Informationssicherheit	LfNr. 1004, 1035
	6.1.4.	Genehmigungsverfahren für informations-verarbeitende Einrichtungen	LfNr. 1031ff : Neues Siko für Dst und Prj.
	6.1.5.	Vertraulichkeits-vereinbarung	LfNr. 1014- 1015: Informationen LfNr. 1019- 1020: Vertraulichkeit
	6.1.6.	Kontakt zu Behörden	Anlage 12 – BSI
	6.1.7.	Kontakt zu speziellen	Keine Angabe

		ISO 27002	ZDV 54/100
		Interessensgruppen	
	6.1.8.	Unabhängige Überprüfung der Informationssicherheit	3.1.1 unabhängigePrüfung durch IT-Zentrum CertBw
	6.2.	Externe	
	6.2.1.	Identifizierung von Risiken in Zusammenhang mit externen Mitarbeitern	LfNr. 1025-1031: Auslandseinsätze (Anlage 21 20.1.3)
	6.2.2.	Adressieren von Sicherheit im Umgang mit Kunden	Anlage 21: 15.3 - Wartungspersonal
	6.2.3.	Adressieren von Sicherheit in Vereinbarung mit Dritten	Keine Angabe

Tabelle 3: Organisation von Informationssicherheit

Die Organisation der IT-Sicherheit innerhalb der Bundeswehr ist in Kapitel 2 – ‚Organisation IT-Sicherheit' beschrieben. Demnach ist die Organisationsstruktur hierarchisch aufgebaut und die ministerielle Verantwortung liegt beim Bundesministerium für Verteidigung, welche durch die Gruppen ‚M II' für Informationsmanagement und ‚Org 2' für den Datenschutz unterstützt werden.

Auf Ämterebene ist das IT-AmtBw A6 für IT-Sicherheit und deren Umsetzung zuständig. Zu ihren Aufgaben zählen:

- Bearbeitung der Grundlagen zur IT-Sicherheit
- Prüfung von Phasen- und Stufendokumenten von Projekten
- Mitprüfung der IT-Sicherheitskonzepte
- Durchführung organisationsübergreifender Sicherheitsinspektionen und -prüfungen

Die praktische Umsetzung von Maßnahmen liegt in den Händen des jeweiligen Projektleiters bzw. der Dienststellenleiter in Unterstützung eines ihm beigestellten IT-

Sicherheitsbeauftragten (IT-SiBe). Dies gilt auch für die Analysephase neuer Projekte oder bei der Einrichtung neuer Dienststellen.

Grundsätzlich sind im Sinne der Vertraulichkeit sämtliche IT-gestützen Informationen im Sinne der ZDV 54/100 zu schützen. Laut nach dem Grundsatz *„Kenntnis nur wenn nötig“* werden Informationen im Geschäftsbereich der BMVg in zwei Kategorien gefasst:

- Verschlusssachen
- Personenbezogene Daten

Schließlich ist auch der Kontakt zu Behörden wie dem BSI organisatorisch geregelt. Demnach umfasst die Beratung des BSIs an die Bundeswehr Grundsatzprobleme, den Einsatz von Standardsoftware, Sicherheitsprobleme von IT-Systemen und Mitwirkung von Schulungs- und Informationsveranstaltungen.

⊖ Kontakt zu speziellen Interessensgruppen

Um eine geeignete und objektive Überprüfung der Sicherheitsmaßnahmen zu gewährleisten sind die Verantwortungen für den Systembetrieb und das Audit stets getrennt. Während der Systembetrieb vom Dienstellenleiter oder Projektleiter verwaltet wird, ist das IT-AmtBw bzw. das ITZ-Zert mit dem Prüfzentrum für IT-Sicherheit für die Durchführung von Systemprüfungen und Audits zuständig.

Risiken und Gefahren gegenüber Dritten wird im Rahmen der ZDV 54/100 nicht getroffen. Lediglich eine Maßnahme zur Verpflichtung von externem Wartungspersonal auf das Datengeheimnis des § 5 des BDSG wird hier festgelegt.

⊖ Adressieren von Sicherheit in Vereinbarung mit Dritten

5.3 Management von Organisationswerten

		ISO 27002	**ZDV 54 / 100**
7.		**Management von organisationseigenen Werten**	
	7.1.	Verantwortung für	

		ISO 27002	ZDV 54 / 100
		organisationseigene Werte (Assets)	
	7.1.1.	Inventar der organisationseigen Werte (Assets)	Keine Angabe
	7.1.2.	Eigentum von organisationseigenen Werte (Assets)	Keine Angabe
	7.1.3.	Zulässiger Gebrauch von organisationseigenen Werten (Assets)	Tragbarer PC: Anlage 19 Behandlung Datenträger: Anlage 20 1/2
	7.2.	Klassifizierung von Informationen	
	7.2.1.	Regelungen von Klassifizierung	LfNr. 1014,: VS, PersDat (A, B)
	7.2.2.	Kennzeichnung von und Umgang mit Informationen	LfNr. 1015- Umgang Verschlusssachen Anhang 21

Tabelle 4: Management von Organisationswerten

⊖ Inventarisierung von organisationseigenen Werten

Es wird lediglich der zulässige Umgang mit tragbaren PCs und Datenträgern beschrieben.

Eine Klassifikation von Informationen findet in zwei Kategorien statt. Zum einen den personenbezogenen Daten und zum anderen den Verschlusssachen. Hierbei wird im Genaueren auf die Kennzeichnung und den Umgang mit solchen Informationen eingegangen.

5.4 Personalsicherheit

		ISO 27002	ZDV 54 / 100
8.		**Personalsicherheit**	**Kapitel 4**
	8.1.	Vor der Anstellung	
	8.1.1.	Aufgaben und Verant-wortlichkeiten	LfNr. 4007- 4009
	8.1.2.	Überprüfung	Personal Abstrahlsicherheit LfNr. 4019
	8.1.3.	Arbeitsvertragsklauseln	Kapitel 4 V Belehrung und Verpflichtung
	8.2.	Während der Anstellung	
	8.2.1.	Verantwortung des Managements	LfNr. 4030 – jährliche Unterzeichnung der Belehrung nach Anlage 17
	8.2.2.	Sensibilisierung, Ausbildung und Schulung für Informationssicherheit	LfNr. 4006 Spezifizierung Anhang 21
	8.2.3.	Disziplinarverfahren	Keine Angabe
	8.3.	Beendigung und Änderung der Anstellung	Kapitel 4 VI
	8.3.1.	Verantwortlichkeiten bei der Beendigung	LfNr. 4031-4032 Verpflichtung IT-SiBe nach Anlage 18
	8.3.2.	Rückgabe von organisationseigenen Werten	Übergabe/ Löschung nach 4032 Erklärung nach Anlage 18
	8.3.3.	Zurücknahme von Zugangsrechten	LfNr. 4032: Übergabe/ Löschung

Tabelle 5: Personalsicherheit

Dem IT-Personal soll neben Kenntnissen über Bedrohungen auch die Notwendigkeit von IT-Sicherheit vermittelt werden. Die Ausbildung des Personals soll auf Grundlage der ZDV 54/100 erfolgen.

Personal, welches im Abstrahlprüfdienst tätig ist, muss sich einer Sicherheitsüberprüfung nach Ü3 (§ 10 Sicherheitsüberprüfungsgesetz – SÜG) unterziehen. Nutzer und IT-Personal haben Gesetz, Vorschriften und Weisungen einzuhalten und je nach Tätigkeit und Zugang zu Informationen sind Mitarbeiter auf die Einhaltung der Sicherheitsrichtlinie nach ZDV 54/100 zu verpflichten (Anlage 17). Personal welches Zugriff auf VS-geschützen Daten beseitzt, wird einmal im Jahr auf die Einhaltung der Sicherheitsrichtlinie belehrt und verpflichtet.

Alle Nutzer und sämtliches IT-Personal sollen im Sinne der IT-Sicherheit fach- und ebenengerecht aus- und fortgebildet werden.

⊖ Disziplinarverfahren

Beim Ausscheiden des Personals sind Zugangs- und Zutrittsrechte aufzuheben und dem zuständigen Sicherheitsbeauftragten der Dienststelle anzugeben. Dieser ist für die Durchführung von Zurücksetzen des Passwortes, Löschen nicht mehr benötigter Daten und Prüfung auf Virenfreiheit verantwortlich.

5.5 Physische und umgebungsbezogene Sicherheit

		ISO 27002	**ZDV 54 / 100**
9.		**Physische und umgebungsbezogene Sicherheit**	**Kapitel 3**
	9.1.	Sicherheitsbereiche	LfNr. 3008- 3009
	9.1.1.	Sicherheitszonen	Anlage 21: 1.1.4, 1.1.5, 1.1.6 LfNr. 3008- 3009
	9.1.2.	Zutrittskontrolle	Anlage 21: 1.1.4, 1.1.5, 1.1.6 LfNr. 3008- 3009

		ISO 27002	ZDV 54 / 100
	9.1.3.	Sicherung von Büros, Räumen und Einrichtungen	LfNr. 6002- 6003, Zutritt zu Räumen und Gebäuden
	9.1.4.	Schutz vor Bedrohungen von außen und aus der Umgebung	Anlage 21: 13.2.8, 13.2.9, 13.2.10
	9.1.5.	Arbeiten in Sicherheitszonen	Anlage 21: 1.1.2
	9.1.6.	Öffentlicher Zugang, Anlieferungs- und Ladezonen	Keine Angabe
	9.2.	Sicherheit von Betriebsmitteln	
	9.2.1.	Platzierung und Schutz von Betriebsmitteln	z.B. Anlage 21: 1.1.1, 1.2.3, 1.2.5, 2.1.1
	9.2.2.	Unterstützende Versorgungseinrichtungen	Anlage 21: 13.2.2, 13.2.4, 13.2.5
	9.2.3.	Sicherung der Verkabelung	Anlage 21: 10.2.2, 10.2.3, 10.2.4
	9.2.4.	Instandhaltung von Gerätschaften	Anlage 21: 15.1.1
	9.2.5.	Sicherheit von außerhalb des Standorts befindlicher Ausrüstung	Anlage 21: 4-Datenträger Evtl- Laptops
	9.2.6.	Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln	Anlage 20: 1-4

		ISO 27002	ZDV 54 / 100
	9.2.7.	Entfernung von Eigentum	Anlage 21. 4.1.7- Datenträger

Tabelle 6: Physische und umgebungsbezogene Sicherheit

Server und zentrale Einrichtungen der IT sind nur in zutrittsbeschränkten Räumen zulässig. Der Dienststellenleiter vergibt hierfür die nötigen Zutrittsberechtigungen. Die Sicherung von Räumen, Büros und Einrichtungen müssen zusätzlich weiteren infrastrukturellen Anforderungen im Sinne der physischen Sicherheit entsprechen (Türschlösser, Fenster, Handfeuerlöscher, Brandschutzpläne und Blitzschutzanlagen).

⊖ Öffentliche Anlieferung, Ladezonen

Zum besseren Schutz von Betriebsmitteln, sind IT-Systeme im Erdgeschoss nur aufzustellen, wenn die Einrichtung besonders gegen Einbruch geschützt ist. Desweiteren ist bei der Platzierung der Betriebsmittel eine unbefugte Kenntnisnahme von dargestellten und ausgedruckten Informationen zu beachten und dieser entgegenzuwirken.

Server und IT-Systeme sind gegenüber Stromausfall zu schützen. Ein System soll nach einen Stromausfall jederzeit wieder fehlerfrei in den Ursprungszustand zurücksetzbar, sowie eine Notstromversorgung für die Einrichtungen implementiert sein.

Zum Schutz der Verkabelung sollen lediglich Lichtwellenleiter oder geschirmte Kupferkabel verwendet werden. Falls die Stromversorgung aus dem öffentlichen Netz erfolgt, ist die Notwendigkeit nach einem Netzfilter zu prüfen.

IT-Systeme sind grundsätzlich zu warten. Die Wartung darf nur von sicherheitsüberprüftem Wartungspersonal durchgeführt werden. Mit der Wartung beauftragte Unternehmen sind der Geheimschutzbetreuung unterlegen und haben sich bei Zugriffsmöglichkeit auf personenbezogene Daten nach § 5 BDSG zu verpflichten.

Schließlich ist im Rahmen der ZDV 54/100 auch der Umgang und Entsorgung von mobilen Betriebsgeräten wie Datenträgern und Notebooks konkret beschrieben. Maßnahmen zur Aufbewahrung sind im Rahmen der ZDV nicht genannt.

5.6 Betriebs- und Kommunikationsmanagement

		ISO 27002	ZDV 54/100
10.		**Betriebs- und Kommunikations-management**	
	10.1.	Verfahren und Verant-wortlichkeiten	
	10.1.1.	Dokumentierte Betriebs-prozesse	Keine Angabe
	10.1.2.	Änderungsverwaltung	LfNr. 8029, 9005
	10.1.3.	Aufteilung von Verantwortlichkeiten	Anlage 21: 3.1.1.
	10.1.4.	Trennung von Entwicklungs-, Test- und Produktiveinrichtungen	In Teilen Anhang 21: 16.1.2
	10.2.	Management der Dienst-leistungserbringung von Dritten	
	10.2.1.	Erbringungen von Dienst-leistungen	LfNr. 1133, 1134
	10.2.2.	Überwachung und Überprüfung der Dienstleistung von Dritten	LfNr. 1133, 1134
	10.2.3.	Management von Änderungen an Dienst-leistungen von Dritten	LfNr. 1133
	10.3.	Systemplanung und Abnahme	

		ISO 27002	ZDV 54/100
	10.3.1.	Kapazitätsplanung	Keine Angabe
	10.3.2.	Systemabnahme	L fNr. 1044-1050
	10.4.	Schutz vor Schadsoftware und mobilem Programmcode	
	10.4.1.	Maßnahmen gegen Schadsoftware	LfNr. 6009-6010 und Anlage 21: Abschnitt 11
	10.4.2.	Schutz vor mobiler Software (mobile Agenten)	Anlage 21: 11.2
	10.5.	Backup	
	10.5.1.	Backup von Informationen	Anlage 21: Abschnitt 14
	10.6.	Management von Netzsicherheit	LfNr. 1121-1124: Netzbetriebskonzept & Anlage 21: Abschnitt 7
	10.6.1.	Maßnahmen für Netze	Anlage 21: 7.1.2
	10.6.2.	Sicherheit von Netz-diensten	Anlage 21: 7.1.3, 7.1.4, 7.1.5
	10.7.	Handhabung von Speicher- und Auf-zeichnungsmedien	
	10.7.1.	Verwaltung von Wechselmedien	LfNr. 6006, 6007 Anlage21: 4.1.2 & Anlage 20
	10.7.2.	Entsorgung von Medien	LfNr. 6006

		ISO 27002	ZDV 54/100
			Anlage 21: 4.1.2 & Anlage 20
	10.7.3.	Umgang mit Informationen	LfNr. 6006 Anlage 21: 4.1.2 & Anlage 20
	10.7.4.	Sicherheit der Systemdokumentation	Anlage 21: 14.1.9
	10.8.	Austausch von Informationen	
	10.8.1.	Leitlinien und Verfahren zum Austausch von Informationen	teilweise in Anlage 21: Abschnitt 7, 8 und 9
	10.8.2.	Vereinbarung zum Austausch von Informationen	VS:LfNr. 6008, Anlage 21: Abschnitt 7 insbesondere 7.2.1; 7.2.2;7.2.3 (nicht Abstreitbarkeit)
	10.8.3.	Transport physischer Medien	Anlage 21: 4.2.1., 4.2.2
	10.8.4.	Elektronische Mitteilungen / Nachrichten (Messaging)	Keine Angabe
	10.8.5.	Geschäftsinformations-systeme	Keine Angabe
	10.9.	E – Commerce - Anwendungen	
	10.9.1.	E - Commerce	Keine Angabe
	10.9.2.	Online - Transaktionen	Keine Angabe
	10.9.3.	Öffentlich verfügbare Informationen	Keine Angabe

		ISO 27002	ZDV 54/100
	10.10.	Überwachung	
	10.10.1.	Auditprotokolle	Anlage 21: 12.1ff
	10.10.2.	Überwachung der System-nutzung	Schnittstellenüberwachung nach außerhalb bei CERTBw (LfNr. 2023)
	10.10.3.	Schutz von Protokollinformationen	Anlage 21: 12.2.4, 12.2.5
	10.10.4.	Administrator- und Betreiberprotokolle	Anlage 21: 16.1.6
	10.10.5.	Fehlerprotokolle	Keine Angabe
	10.10.6.	Zeitsynchronisation	Keine Angabe

Tabelle 7: Betriebs- und Kommunikationsmanagement

⊖ Dokumentation von Betriebsprozessen

Eine Fortschreibung des Sicherheitskonzeptes von Projekten und Dienststellen erfolgt bei technischen Änderungen, Baumaßnahmen, Änderungen der Gefährdungslage oder Gesetzes- und Vorschriftenänderungen. Nachträgliche Änderungen im Sicherheits-konzept sind in der IT-Sicherheitsdokumentation festzuhalten (Anlage 6). Die Freigabe technischer Sicherheitsmaßnahmen wird durch den Projektleiter überprüft und angeordnet.

Die Verantwortlichkeiten für den Betrieb und des Audits von IT-Systemen sind nach Anlage 21 strickt zu trennen. Diese Anlage trennt die Instanzen der Umsetzung von Maßnahmen und der Verwaltung/Durchführung von Sicherheitsüberprüfungen und schützt vor unbefugten oder vorsätzlichen Missbrauch.

Im Sinne der Trennung von Test-, Entwicklung-, und Produktiveinrichtung schreibt die ZDV 54/100 lediglich die Trennung von Test- und Produktivdaten nach dem Gebot der getrennten Verarbeitung vor. Weiterführende Maßnahmen zur Überführung von Software, Testumgebungen oder sensitiven Daten gibt es nicht.

⊖ Trennung von Entwicklungs-, Test- und Produktiveinrichtungen

Bei Verträgen über Dienstleistungen von Dritten sind die IT-Sicherheitsbestimmungen grundlegender Vertragsbestandteil. Hierbei wird die Vorgehensweise von Fortschreibungen wesentlicher Anpassungen im IT-Sicherheitskonzeptes im Vertrag aufgenommen. Die Bundeswehr hält sich jederzeit offen unregelmäßige Prüfungen von Systemen, welche Bundeswehrdaten speichern oder verarbeiten, vorzunehmen.

⊖ Kapazitätsplanung

Für eine Systemabnahme und Inbetriebnahme ist eine Freigabe durch den Projektleiter bzw. Dienststellenleiter erforderlich. Hierbei werden die Realisierung von materiellen, organisatorischen, technischen Maßnahmen und das Vorliegen der IT-Sicherheits-dokumentation und die Freigabe zur Nutzung überprüft. Bei Mängeln, die nicht die Verarbeitung von VS-Material betreffen, darf der Projektleiter in einigen Fällen der Risikobewertung eine vorläufige Freigabe erteilen.

Zur Wahrung von der Integrität, Verfügbarkeit und Vertraulichkeit ist der Schutz gegen Softwareanomalien wesentlicher Bestandteil des IT-SysBw. So soll jede Ausbreitung von Schadcode (Viren, Malware, etc.) verhindert werden, indem alle ein und ausgehenden Datanträger auf Virenbefall geprüft werden und auf allen IT-Systemen Programme zur Erkennung von Softwareanomalien installiert sind. Diese Software muss regelmäßig wirken und von Systembenutzern nicht zu umgehen sein.

Im Bereich der Datensicherung sind regelmäßige Backups vorgesehen, welche örtlich getrennt und vor äußeren Einflüssen wie Feuer oder Wasserschäden geschützt sind. Sicherungen sind hierbei je nach Datentyp in unterschiedlichen Intervallen durchzuführen (täglich, monatlich).

Für den Betrieb aller IT-Netze in Einrichtungen der Bundewehr ist ein so genanntes Netzbetriebskonzept zu erstellen. Hier werden Zuständigkeiten für den Betrieb, Regelungen für Nutzer, Regeln für die Datensicherung und Regelungen zur IT-Sicherheit (z. B. Verschlüsselung) beschrieben.

Die Verwendung von Datenträgern wie USB-Sticks oder CDs spielt eine immer größer werdende Rolle im sicheren Umgang von Daten. So wird in der ZDV neben der Kennzeichnung und dem Umgang mit Datenträgern auch auf die Entsorgung eingegangen.

Regeln für den Austausch von Informationen werden in dem gesonderten Merkblatt für die Behandlung von Verschlusssachen des Geheimhaltungsgrades behandelt. Lediglich der Umgang von VS-geschützten Material findet in der ZDV Erwähnung. Demnach

sind alle VS geschützten Dokumente kryptiert zu verschicken. Detailliertere Auskunft gibt aber das oben genannte Merkblatt.

Die IT-Systeme der Bundeswehr müssen stets über eine Funktion zum dokumentierten Datenaustausch verfügen, sodass jederzeit ein eindeutiger Sendenachweis zur Verfügung steht.

Bei physischem Transport von Informationen auf Datenträgern, sind diese mit zugelassenen Anwendungen des BMVg zu verschlüsseln und zu signieren.

- Elektronische Mitteilungen / Nachrichten (Messaging)
- Geschäftsinformationssysteme
- E – Commerce - Anwendungen
- E - Commerce
- Online - Transaktionen
- Öffentlich verfügbare Informationen

Bei Auditprotokollen von Sicherheitsüberprüfung sind im Rahmen der ZDV die geltenden datenschutzrechtlichen Bestimmungen zu beachten. Demnach sind die Protokolldaten nach Ablauf der Aufbewahrungsfrist unverzüglich von Auditoren oder Sicherheitspersonal zu vernichten. Ausgenommen sind hierbei Daten, welche aufgrund von straf-/disziplinartechnischen Verfahren noch benötigt werden.

Instanz für die Systemnutzungsüberwachung in der Bundeswehr ist das CERTBw. Ihre Aufgaben werden im Dokument „Weisung zum Einsatz des Computer Emergency Response Teams der Bundeswehr (CERTBw)“ - BMVg – IT 3 VS-NfD konkretisiert.

Protokollinformationen von Sicherheitsüberprüfung sind auf gesonderten nicht manipulierbaren Datenträgern zu sichern, auf welche nur Auditoren und IT-Sicherheitspersonal Zugriffsrechte besitzen.

Protokolle von Zugriffen der Administratoren (Administrator- und Betreiberprotokolle) sind alle 2 Monate zu überprüfen.

- Fehlerprotokolle
- Zeitsynchronisation

5.7 Zugangskontrolle

		ISO 27002	ZDV 54/100
11.		**Zugangskontrolle**	**Anlage 21: Abschnitt 2**
	11.1.	Geschäftsanforderungen für die Zugangskontrolle	LfNr. 3008 & Anlage 21: Abschnitt 2
	11.1.1.	Leitlinie zur Zugangskontrolle	LfNr. 3008
	11.2.	Benutzerverwaltung	Anlage 21: Abschnitt 2
	11.2.1.	Benutzerregistrierung	Anlage 21: 2.1.4 , 3.1.2, 3.1.3
	11.2.2.	Verwaltung von Sonderrechten	Anlage 21: 2.1.9
	11.2.3.	Verwaltung von Benutzerpasswörtern	LfNr. 6004, Anlage 21: Abschnitt 2 Anlage 14: 5
	11.2.4.	Überprüfung von Benutzerberechtigungen	Keine Angabe
	11.3.	Benutzerverantwortung	
	11.3.1.	Passwortverwendung	Anlage 21: 2.2.6
	11.3.2.	Unbeaufsichtigte Benutzerausstattung	Anlage 21: 2.2.8, 2.1.8, 2.1.3
	11.3.3.	Der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms	Teilweise in Anlage 21 2.1.3
	11.4.	Zugangskontrolle für Netze	
	11.4.1.	Regelwerk zur Nutzung	LfNr. 1123, Anlage 21: 2.2.1, 2.2.2

		ISO 27002	ZDV 54/100
		von Netzdiensten	
	11.4.2.	Benutzerauthentisierung für externe Verbindungen	LfNr. 1123, Anlage 21: Abschnitt 2.2.1
	11.4.3.	Geräteidentifikation von Netzen	Keine Angabe
	11.4.4.	Schutz der Diagnose- und Konfigurationsports	Keine Angabe
	11.4.5.	Trennung von Netzen	Anlage 21: Abschnitt 5
	11.4.6.	Kontrolle von Netz-verbindungen	LfNr. 3010 durch Filter
	11.4.7.	Routingkontrolle für Netze	Keine Angabe
	11.5.	Zugriffskontrolle auf Betriebssysteme	Siehe auch ISO 27002 Abschnitt 11.2
	11.5.1.	Verfahren für sichere Anmeldung	Siehe auch ISO 27002 Abschnitt 11.2
	11.5.2.	Benutzeridentifikation und Authentisierung	Siehe auch ISO 27002 Abschnitt 11.2
	11.5.3.	Systeme zur Verwaltung von Passwörtern	Siehe auch ISO 27002 Abschnitt 11.2
	11.5.4.	Verwendung von Systemwerkzeugen	Keine Angabe
	11.5.5.	Session Time-Out	Siehe auch ISO 27002 Abschnitt 11.2
	11.5.6.	Begrenzung der Verbindungszeit	Keine Angabe
	11.6.	Zugangskontrolle zu Anwendung und	Allgemein zu IT Anlage 21: Abschnitt

		ISO 27002	ZDV 54/100
		Information	2
	11.6.1.	Einschränkung von Informationszugriffen	Siehe oben
	11.6.2.	Isolation sensitiver Systeme	Keine Angabe
	11.7.	Mobile Computing und Telearbeit	Keine Telearbeit, aber Verwendung von mobilen Geräten: Anlage 19
	11.7.1.	Mobile Computing und Kommunikation	Keine Angabe
	11.7.2.	Telearbeit	Keine Angabe in ZDV 54/100 BMVg – Org 1 Rahmenweisung zur Einführung der Telearbeit im GeschäftsZDv 54/100 Im Bereich des Ministerium der Verteidigung

Tabelle 8: Zugangskontrolle

Für alle Zugriffe eines Nutzers des IT-SysBw auf Informationen ist ein Nutzeridentität notwendig. Hierbei sind eindeutige, personenbezogene Nutzerkonten zu verwenden, welche je nach Sicherheitsniveau höchstens zwei Systemanmeldungen zulassen.

Die Registrierung und spätere Löschung von Benutzerkonten ist nur durch den zuständigen Administrator möglich. Der Vorgang erfolgt durch schriftliche Beantragung und wird durch den Dienstellenleiter genehmigt. Die Zugriffsrechte der Nutzer basieren auf einem Rollenmodell, indem die Nutzer zu bestimmten Kennzeichnungen zugeordnet werden, welche den Kontext des Nutzers zum IT-System beschreibt. Hierbei sind die Zugriffsrechte und Rollen so zu wählen, dass nur der notwendige Funktions- und Informationszugang für den Nutzer zugänglich sind („Need-to-Know“ Prinzip).

Besondere Beachtung finden die anlassbezogenen Sonderrechte für sensible Systeme. Hier ist lediglich eine Systemanmeldung zulässig und nach Wegfall des Zugangsgrundes, sind die Zugangsrechte unverzüglich zu löschen.

Im Sinne der „Zehn Regeln zur IT-Sicherheit am Arbeitsplatz“ – Anlage 14 dürfen Passwörter von Benutzern grundsätzlich nicht weitergegeben werden. Standard-passwörter vom Hersteller sind ebenfalls sofort zu ändern.

Zum Schutz vor unautorisiertem Zugriff haben Benutzerpasswörter bestimmte Eigenschaften wie Länge, Verwendung von Sonderzeichen oder Zahlen zu erfüllen und müssen alle 30 Tage erneuert werden.

⊖ Überprüfung von Benutzerberechtigung

In nicht abschließbaren Räumlichkeiten sind Einzelplatzrechner bei kurzzeitigem Verlassen automatisch durch einen Bildschirmschoner zu sperren und Notebooks zusätzlich gegen Diebstahl zu schützen.

⊖ Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms

Maßnahmen zur Zugangskontrolle von Netzen werden im zentralen Netzbetriebs-konzept zusammengefasst. Hier werden Regeln für die Zugangsrechte und die An- und Abmeldung der Nutzer, Zuständigkeiten für den Betrieb, sowie Regeln für die IT-Sicherheitsmaßnahmen (Verschlüsselung) innerhalb des IT-SysBw und auch von externen Verbindungen beschrieben.

⊖ Geräteidentifikation von Netzen

⊖ Schutz der Diagnose- und Konfigurationsports

Zum Schutze von einzelnen Netzdomänen werden innerhalb des IT-SysBw zwischen Bereichen mit unterschiedlichen Sicherheitsanforderungen so genannte Sicherheits-gateways implementiert. Dies gilt auch für Schnittstellen zwischen Bw-Netzen und öffentlicher Betreiber oder andere Streitkräfte. Die Sicherheitsgateways sind demnach so zu konfigurieren, dass nur benötigte Ports und IP-Adressen freigeschaltet werden. Dies gewährleistet durch den richtigen Einsatz von Sicherheits- und Filterfunktionen nur autorisierte Zugriffe zwischen Netzen mit unterschiedlichen Sicherheitsniveaus.

⊖ Routingkontrolle für Netze

Wie auch bei den Vorschriften für IT-Systeme und Netze sind diese Regeln, von Anlage 2 Abschnitt 2, auch für Regelungen zu Betriebssystemen gültig.

- Verwendung von Systemwerkzeugen
- Begrenzung der Verbindungszeit
- Zugangskontrolle für Anwendungen und Informationen

Zum Schutz von Daten und Informationen des IT-SysBw sind auch für Notebooks, Palmtops und PDAs besondere Schutzmaßnahmen vor unzulässigem Zugriff zu treffen. Die Anlage 19 beschreibt den ordnungsmäßigen Umgang

- Mobile Computing und Kommunikation
- Telearbeit

5.8 Beschaffung, Entwicklung und Wartung von Informationssystemen

		ISO 27002	**ZDV 54 / 100**
12.		**Beschaffung, Entwicklung und Wartung von Informations-systemen**	
	12.1.	Sicherheitsanforderungen von Informationssystemen	
	12.1.1.	Analyse und Spezifikation von Sicherheits-anforderungen	LfNr. 9005: IT-SiKo fortschreiben 1051- 1060, 8016, 8017
	12.2.	Korrekte Verarbeitung in Anwendungen	
	12.2.1.	Überprüfung von Eingabedaten	Keine Angabe
	12.2.2.	Kontrolle der internen Verarbeitung	Keine Angabe
	12.2.3.	Integrität von Nachrichten	Keine Angabe

		ISO 27002	ZDV 54 / 100
	12.2.4.	Überprüfung von Ausgabedaten	Keine Angabe
	12.3.	Kryptographische Maßnahmen	ZDV 54/110 VS-NfD „Behandlung und Einsatz von Kryptomitteln“ LfNr. 1098- 1105 und Anlage 21: Abschnitt 8
	12.3.1.	Leitlinie zur Anwendung von Kryptographie	Siehe oben
	12.3.2.	Verwaltung kryptographischer Schlüssel	Siehe oben
	12.4.	Sicherheit von Systemdateien	
	12.4.1.	Kontrolle von Software im Betrieb	Anlage 24: Kapitel 7
	12.4.2.	Schutz vor Test-Daten	Keine Angabe
	12.4.3.	Zugangskontrolle zu Quellcode	Keine Angabe
	12.5.	Sicherheit bei Ent-wicklungs- und Unter-stützungsprozessen	
	12.5.1.	Änderungskontrollverfahre n	LfNr. 1047- erneute Freigabe Anlage 25 Abschnitt 5
	12.5.2.	Technische Kontrolle von Anwendungen nach Änderungen am Betriebssystem	Keine Angabe

		ISO 27002	ZDV 54 / 100
	12.5.3.	Einschränkung von Änderungen an Softwarepaketen	Keine Angabe
	12.5.4.	Ungewollte Preisgabe von Informationen	Keine Angabe
	12.5.5.	Ausgelagerte Softwareentwicklung	Keine Angabe
	12.6.	Umgang mit Schwachstellen	
	12.6.1.	Kontrolle technischer Schwachstellen	LfNr. 2024, 2025, 2026 Anlage 23: LfNr. 23, Anlage 24: LfNr. 30

Tabelle 9: Beschaffung, Entwicklung und Wartung von Informationssystemen

Bei Neubeschaffung oder Erweiterung von Informationssystemen sind die Maßnahmen zur Fortschreibung des Sicherheitskonzeptes zu beachten. IT-Anteile sind gemäß eines Antrages zur Abnahmeerklärung und einer Genehmigung zur Nutzung durch den Projektleiter bzw. der Projektleiterin freizugeben. Neben der Beschreibung der Lösungsarchitektur, der Durchführung einer Bedrohungs- und Risikoanalyse und der Beschreibung des Restrisikos sind auch die Kosten für die Umsetzung höherwertiger Sicherheitsmaßnahmen zu berücksichtigen. Die Evaluierung von IT-Produkten der Lösungsbeschreibung erfolgt durch die Zertifizierungsbehörde des BSIs.

⊖ Korrekur der Verarbeitung in Anwendungen

Die Leitlinie der Kryptographie steht in einem eigenen Dokument der ZDV 54/110 – Behandlung und Einsatz von Kryptomitteln.

Zum einheitlichen Umgang mit eingesetzter Software an Clienten und Servern ist vor der Abnahme jedes IT-Systems ein konkreter Hardware- und Softwarekonfigurations-stand festzulegen.

⊖ Schutz von Testdaten

⊖ Zugangskontrolle zu Quellcode

Entwicklungsarbeiten erfordern bei erheblichen Änderungen am IT-System eine erneute Freigabe des Sicherheitskonzeptes durch den Projekt- bzw Dienststellenleiter. Neben der Verantwortung für personelle, organisatorische und technische Maßnahmen, ist er ebenfalls für die Fortschreibung der Sichterheitsdokumentation zuständig.

- Technische Kontrolle von Anwendungen nach Änderungen am Betriebssystem
- Einschränkung von Änderungen an Softwarepaketen
- Ungewollte Preisgabe von Informationen
- Ausgelagerte Softwareentwicklung

Das Auftreten von Schwachstellen in der Lösungsarchitektur ist stets zu dokumentieren und bei der nächsten Bedrohungs- und Risikoanalyse zu bewerten. Zuständig für die Untersuchung sind die Prüfteams technische IT-Sicherheit des IT-Amtes Bw. Bei Lösungen, welche höherwertige Geheimhaltungsgrade (VS-Vertraulich) betreffen, kann auch durch das IT-AmtBw die Einschaltung des BSIs beantragt werden.

5.9 Umgang mit Informationssicherheitsvorfällen

		ISO 27002	**ZDV 54/100**
13.		**Umgang mit Informationssicherheits-vorfällen**	
	13.1.	Melden von Informations-sicherheitsereignissen und Schwachstellen	
	13.1.1.	Melden von Informations-sicherheitsereignissen	LfNr. 1083-1086 und Anlage 21: Abschnitt 24 Umgang mit Sicherheitsvorfällen
	13.1.2.	Melden von Sicherheitsschwachstellen	LfNr. 1083, 1084 und Anlage 21: 24.1.1
	13.2.	Umgang mit Informations-sicherheitsvorfällen und	

		ISO 27002	ZDV 54/100
		Verbesserungen	
	13.2.1.	Verantwortlichkeiten und Verfahren	LfNr. 1085 und Anlage 21: Abschnitt 24
	13.2.2.	Lernen von Informationssicherheits-vorfällen	Keine Angabe
	13.2.3.	Sammeln von Beweisen	Keine Angabe

Tabelle 10: Umgang mit Informationssicherheitsvorfällen

IT-Sicherheitsvorfälle sind bei Verdacht sofort dem IT-Sicherheitsbeauftragten in schriftlicher Form (Email, Fax) zu melden. Wenn sich bei näherer Untersuchung der Verdacht bestätigt, ist der Vorfall dem zuständigen Projekt- bzw. Dienststellenleiter umgehend zu berichten. Bei Verdachtsmomenten auf terroristische und extremistische Vorfälle ist im weiteren Verlauf der MAD (Militärische Abschirmdienst) zu benachrichtigen.

Verstöße gegen das Melden von Sicherheitsvorfällen können als Dienstvergehen bewertet und als Ordnungswidrigkeiten oder Straftaten verfolgt werden.

⊖ Umgang mit Informationssicherheitsvorfällen und Verbesserung

5.10 Sicherstellung des Geschäftsbetriebs (Business Continuity Management)

		ISO 27002	ZDV 54/100
14.		**Sicherstellung des Geschäftsbetriebs (Business Continuity Management)**	**Notfallkonzept**
	14.1.	Informationssicherheits-aspekte bei der Sicher-	LfNr. 1117-1120 , Anlage 10, Anlage 23: Kapitel 10 und Anlage 21:

		ISO 27002	ZDV 54/100
		stellung des Geschäft-betriebs (Business Continuity Management)	Abschnitt 13
	14.1.1.	Einbeziehung der Informationssicherheit in den Prozess zur Sicherstellung des Geschäftsbetriebs	Aktionsplan in Anlage 10 Punkt 5 Prozessgetriebener Wiederanlauf
	14.1.2.	Sicherstellung des Geschäftsbetriebs und Risikoeinschätzung	Anlage 21: 13.2, Anlage 10 Abschnitt 13 a
	14.1.3.	Entwicklung und Umsetzen von Plänen zu Sicherstellung des Geschäftsbetriebs, die Informationssicherheit enthalten	Anlage 10 Punkt 5, oder Punkt 13 c
	14.1.4.	Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs	Anlage 10
	14.1.5.	Testen, Instandhaltung und Neubewertung von Plänen zur Sicherstellung des Geschäftsbetriebs	Anlage 10 Punkt 16: regelmäßige Prüfung (einmal im Jahr) und anlassbezogene Überprüfung

Tabelle 11: Sicherstellen des Geschäftsbetriebs (Business Continuity Management)

Jedes Sicherheitskonzept von Projekten und Dienststellen besitzt ein so genanntes Konzept zur Notfallplanung. Im so genannten Notfallhandbuch, welches Teil der Systemdokumentation ist, beschreibt ein Wiederanlaufplan den prozesstechnischen Ablauf von Maßnahmen nach einem Sicherheitsvorfall. Im allgemeinen Teil des Handbuches werden ebenfalls Szenarien und Strategien für Maßnahmen auf mögliche Ereignisse wie Brand, Blitzschlag, Sabotage, Viren oder Trojanische Pferde betrachtet.

Je nach Ereignis und Ausfallszenario sind ebenfalls die Ausfallzeiten von Gebäuden, Abteilungen oder IT-Systemen zu betrachten, wie auch die Wiederanlaufzeit vom Notbetrieb bis zur endgültigen Wiederherstellung des Ursprungzustands.

Als Modell für ein Notfallkonzept und die Erstellung eines Notfallhandbuches dient die Anlage 10 der ZDV 54/100, in welchem der wesentliche Aufbau einer einheitlichen Struktur dieser Dokumente vorgegeben wird.

Einmal pro Jahr oder bei besonderen Anlässen wird das Notfallhandbuch einer Überprüfung unterzogen, um stets einen aktuellen und wirksamen Stand sicherzustellen.

5.11 Einhaltung von Vorgaben (Compliance)

		ISO 27002	**ZDV 54 / 100**
15.		**Einhaltung von Vorgaben**	
	15.1.	Einhaltung gesetzlicher Vorgaben	
	15.1.1.	Identifikation der anwendbaren Gesetze	Anlage 4
	15.1.2.	Rechte an geistigem Eigentum	Keine Angabe
	15.1.3.	Schutz von organisations-eigenen Aufzeichnungen	LfNr. 1014-1015 und Anlage 21: 12.1.6
	15.1.4.	Datenschutz und Vertraulichkeit von personalbezogenen Informationen	LfNr.1068, 7005 und Anlage 21: 12.1.4
	15.1.5.	Verhinderung des Missbrauchs von informations-verarbeitenden	Keine Angabe

		ISO 27002	ZDV 54 / 100
		Einrichtungen	
	15.1.6.	Leitlinien zu kryptographischen Verfahren	Angaben in ZDV 54/110
	15.2.	Einhaltung von Sicherheitsleitlinien und -standards, und technischer Vorgaben	
	15.2.1.	Einhaltung von Sicherheitsleitlinien und -standards	LfNr. 1067 i.v.m 2011
	15.2.2.	Prüfung der Einhaltung technischer Vorgaben	LfNr. 2011 und 2024 Anlage 21: 12.1.5, 12.2.3
	15.3.	Überlegungen zu Revisionsprüfungen von Informationssystemen	
	15.3.1.	Maßnahmen für Audits von Informationssystemen	Anlage 21: 12.1.8
	15.3.2.	Schutz von Revisionswerkzeugen für Informationssysteme	Anlage 21: 12.2.3

Tabelle 12: Einhaltung von Vorgaben (Compliance)

Die im IT-SysBw relevanten Gesetze werden in der ZDV Anlage 4 genannt und sind in den Sicherheitsmaßnahmen direkt zu berücksichtigen. Dies geschieht entweder auf direkte Weisung und Anordnung der Bundeswehr oder wird direkt von den Sicherheitsbeauftragten in ihrem Verantwortungsbereich umgesetzt.

⊖ Rechte am geistigen Eigentum

Grundsätzlich gilt, dass alle nicht gekennzeichneten Informationen zu schützen sind. Die Bundeswehr unterteilt Informationen in zwei Kategorien:

a) Verschlusssachen (VS)

   Verschlusssachen sind in erster Linie geheimhaltungsbedürftige Informationen.

b) Personenbezogene Daten (PersDat)

   Angaben über persönliche oder sachliche Verhältnisse einer Person

   - Allgemeine Arten von personenbezogenen Daten (APersDat)

     Dies sind Angaben, welche den nicht besonderen Arten von personenbezogenen Daten zuzuordnen sind.

   - Besondere Arten von personenbezogenen Daten (BPersDat)

     Angaben einer Person zu religiöser Überzeugung, politischer Meinung, rassischer und ethnischer Herkunft, Gesundheits- und Sexualleben.

Für Protokolldaten von Sicherheitsüberprüfungen gelten ebenfalls die datenschutzrechtlichen Regelungen. Die Protokolldaten dürfen nur bei Verstößen länger als vom Datenschutzgesetz vorgeschrieben zur Beweissicherung aufbewahrt werden.

Zur Sicherung der gesetzlich geforderten Maßnahmen des Datenschutzes unterstützt ein administrativer Datenschutzbeauftragter (ADSB) die IT-Sicherheitsinspektionen.

⊖ Verhinderung des Missbrauchs von informationsverarbeitenden Einrichtungen

Der gesetzeskonforme Umgang mit kryptographischen Verfahren ist nicht Teil der ZDV 54/100, aber sollte Teil der Allgemeinen Leitlinie von kryptographischen Verfahren der ZDV 54/110 sein.

Die Einhaltung von Maßnahmen gemäß der Sicherheitsrichtlinie sind regelmäßig durch Sicherheitsüberprüfungen zu dokumentieren. Dies soll sicherstellen, dass Verfahren in allen Verantwortungsbereichen der Leitlinie korrekt angewandt und entsprechende Maßnahmen umgesetzt werden. Darüber hinaus werden auch die technischen Anforderungen und Umsetzungen von im Betrieb befindlichen Systemen überprüft.

Vor den Sicherheitsüberprüfungen sind die Nutzer von Art und Umfang der Dokumentation im System zu belehren. Der Zugriff auf die Werkzeuge zur Analyse der

Protokolle ist nur den Auditoren und IT-Sicherheitsbeauftragten erlaubt. Dadurch wird die Gefahr einer Manipulierung minimiert.

5.12 Zusammenfassung

Zum Abschluss der Gegenüberstellung aller 11 Abschnitte der ISO 27002 mit der Sicherheitsvorschrift ZDV 54/100 der Bundeswehr soll der Frage nachgegangen werden in welchem Umfang die Best-Practices der ISO umgesetzt wurden. Innerhalb der 11 großen Abschnitte werden 133 Maßnahmen genannt, welche in Tabelle 13 quantitativ mit den in vorherigen Abschnitten überprüften Maßnahmen der Bundeswehr verglichen werden.

Nr.	Abschnitt	Anzahl Maßnahmen ISO 27002	Anzahl Maßnahmen ZDV 54/100
4.	Risikoeinschätzung und -behandlung	2	2
5.	Sicherheitsletilinie	2	2
6.	Organisation der Informationssicherheit	11	9
7.	Management von organisationseigenen Werten	5	3
8.	Personalsicherheit	9	9
9.	Physische und umgebungsbezogene Sicherheit	13	12
10.	Betriebs- und Kommunikationsmanagement	32	23
11.	Zugangskontrolle	25	17
12.	Beschaffung, Entwicklung und Wartung von Informationssystemen	16	6
13.	Umgang mit Informationssicherheitsvorfällen	5	3
14.	Sicherstellung des Geschäftsbetriebs	5	5
15.	Einhaltung der Vorgaben	10	8
	Gesamt	133	97

Tabelle 13: Quantitative Gegenüberstellung aller Maßnahmen

Wie aus Tabelle 13 hervorgeht, gibt es wesentliche Übereinstimmungen der ISO 27002 mit den Maßnahmen der ZDV 54/100. Nach Abschluss der Untersuchung sind 97 von 133 Maßnahmen in der ZDV in Teilen oder vollständig wiederzufinden. Teilweise sind jedoch die empfohlenen Maßnahmen der ISO wesentlich komplexer, als sie in der zentralen Dienstvorschrift beschrieben werden. Es ist davon auszugehen, dass schließlich auch eine Vielzahl von Maßnahmen in anderen Verordnungen und Vorschriften der Bundeswehr beschrieben werden. Aus diesem Grund ist ein direkter Vergleich und die Frage, ob ein die Bundeswehr ISO 27002 erfüllt, in Hinblick auf diese Untersuchung nicht eindeutig zu beantworten.

6 Fazit der Kernaussage

Nach der Gegenüberstellung von ZDV 54/100 und ISO 27002 (vgl. Kapitel 5) wird deutlich, dass sich nicht alle Maßnahmen in der Umsetzung der Bundeswehr wiederfinden lassen. Insbesondere die Dokumentation von Prozessen, die Inventarisierung von Unternehmenswerten oder die Verarbeitung in Anwendungssystemen sind hier gar nicht bzw. nur in sehr kleinen Teilen beschrieben. Dies muss allerdings nicht zwingend bedeuten, dass diese Maßnahmen nicht erfüllt werden, sondern kann auch durch die Beschreibung in anderen Vorschriften und Verordnungen zu erklären sein.

Doch was die Gegenüberstellung zeigt, ist, dass sich für die wesentlichen Punkte der ISO 27002 vergleichbare Maßnahmen bei der Bundeswehr finden. Die Frage nach der Erfüllung der geforderten Maßnahmen nach ISO 27002 lässt sich dadurch aber nicht eindeutig beantworten, zeigt dennoch die Tragweite von Best-Practices in der Praxis.

Die Einführung eines ISMS nach ISO 27001 bildet zwar die Grundlage für IT-Sicherheit in heutigen Unternehmen der öffentlichen Hand, gibt aber zu wenig greifbare Umsetzungsmöglichkeiten mit. Bei der Gegenüberstellung von ZDV 54/100 und ISO wird deutlich, dass die Dokumentation von Best-Practices in Anlehnung an ISO 27002 unerlässlicher Bestandteil der Umsetzung eines ISMS in der Praxis ist. Dieses Regelwerk gilt es schließlich, wie in Kapitel 3.2.2 beschrieben, nicht zu erfüllen, sondern soll Unternehmen anleiten unternehmenseigene Richtlinien festzuhalten. Gerade die Checkliste der Anlage 21 enthält wesentliche und gut strukturierte Maßnahmen der Bundeswehr, welche auch mit eigenen Inhalten ergänzt wurden.

Bei öffentlichen Auftraggebern sind dies Vorschriften zum Umgang mit Verschlusssachen nach der Geheimschutzordnung des Deutschen Bundestages bzw. die dabei zu erfüllenden Vorschriften nach dem Sicherheitsüberprüfungsgesetz (SÜG). Mit diesen zusätzlichen Vorschriften grenzen sich öffentliche Auftraggeber von reinen Wirtschaftsunternehmen ab. Hier wird der Umgang mit sensiblen Daten unternehmensintern gelöst und der Umgang wird nicht vom Gesetzgeber direkt festgelegt.

Da die Bundeswehr seit je her eine komplexe Vorschriften- und Verordnungsdokumentation führt, ist die Dokumentation von Best-Practices wie in der ISO 27002 angeleitet bei der Bundeswehr keine Neuerung. Aufgrund der hohen Sicherheitsansprüche der Bundeswehr gegenüber der IT-Sicherheit ist davon auszugehen, dass die ZDV 54/100 eine Vorreiterrolle unter den Sicherheitsdokumentationen bei öffentlichen Auftraggebern einnimmt. Die Untersuchung von

Umsetzungen bei weiteren öffentlichen Auftraggebern wäre wünschenswert gewesen, doch hätte die Komplexität der Ausarbeitung den Rahmen dieser Arbeit überschritten.

7 Literaturverzeichnis

Literatur

- Buchsein, R.; Günther, H.; Machmeier, V.; Victor, F. (2007): IT-Management mit ITIL® V3. Strategien Kennzahlen Umsetzung /// Strategien, Kennzahlen, Umsetzung. 1. Aufl., Wiesbaden.
- Eckert, C. (2006): IT-Sicherheit. Konzepte - Verfahren - Protokolle /// Konzepte, Verfahren, Protokolle. 4., überarb. Aufl. München - Oldenbourg.
- Fabry, B.; Meininger, F.; Kayser, K.(2007): Vergaberecht in der Unternehmenspraxis. Erfolgreich um öffentliche Aufträge bewerben. 1. Aufl. Wiesbaden.
- Fröhlich, M.; Glasner, K. (2007): IT Governance. Leitfaden für eine praxisgerechte Implementierung. (Springer-11775 /Dig. Serial]). Online verfügbar unter http://dx.doi.org/10.1007/978-3-8349-9364-9.
- Gesetz gegen Wettbewerbsbeschränkungen (GWB) vom 20.07.2005.
- Goltsche, W. (2006): COBIT kompakt und verständlich. Der Standard zur IT Governance \2014 So gewinnen Sie Kontrolle über Ihre IT \2014 So steuern Sie Ihre IT und erreichen Ihr Ziele. Wiesbaden.
- Gründer, T.; Bauer, M. (2007): Managementhandbuch IT-Sicherheit. Risiken, Basel II, Recht. Berlin.
- Hofmann, J.; Schmidt, W. (2004): Kompaktkurs IT-Management. Das Wissen für die erfolgreiche Praxis - Grundlagen und beispielhafte Umsetzung - Für Studenten und Praktiker. 1. Aufl. Wiesbaden.
- International Organization for Standardization (Hg.) (2005): ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management. o.O..
- International Organization for Standardization (Hg.) (2005): ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements. o.O..
- IT Governance Institute (Hg.) (2008): Aligning CobiT, ITIL and ISO 27002 for Business Benefit.o.O..
- IT InformationWeek (Hg.) (2008): IT-Security. Studienband 2008. Online verfügbar unter http://i.cmpnet.com/informationweek.de/2008/mtkResearch/it-security-2008_vorabauszuege.pdf, zuletzt aktualisiert am 21.12.2009
- Kersten, H.; Klett, G. (2008): Der IT-Security-Manager /// Der IT Security Manager. Expertenwissen für jeden IT-Security-Manager - von namhaften Autoren praxisnah vermittelt. 2., aktualis. u. erw. Aufl. Wiesbaden.
- Müller, K.-R. (2008): IT-Sicherheit mit System. Sicherheitspyramide - Sicherheits-, Kontinuitäts- und Risikomanagement - Normen und Practices - SOA und Softwareentwicklung .3., erweiterte und aktualisierte Auflage. Wiesbaden.

- Richter, G. (Hg.) (2007): Die ökonomische Modernisierung der Bundeswehr. Sachstand, Konzeptionen und Perspektiven.o.O.
- Speichert, H.; Fedtke, S. (2008): Praxis des IT-Rechts. Praktische Rechtsfragen der IT-Sicherheit und Internetnutzung. 2., aktualisierte u. erw. Aufl., unveränd. Nachdr. Wiesbaden.
- Witt, B. (2006): IT-Sicherheit kompakt und verständlich. Eine praxisorientierte Einführung.Wiesbaden.

Internetquellen

- Bundesamt für Sicherheit in der Informationstechnik - BSI: Organisationsübersicht des BSI. Online verfügbar unter https://www.bsi.bund.de/cln_183/DE/DasBSI/Aufgaben/aufgaben_node.html, zuletzt geprüft am 03.11.2009.
- Bundesamt für Sicherheit in der Informationstechnik – BSI: IT-Grundschutz – Basis für Informationssicherheit. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/Allgemeines/Einstiegskapitel/einstiegskapitel_node.html, zuletzt geprüft am 15.02.2010.
- Bundesamt für Sicherheit in der Informationstechnik - BSI (Hg.) (2009): Die Lage der IT-Sicherheit in Deutschland 2009. Online verfügbar unter https://www.bsi.bund.de/cae/servlet/contentblob/476182/publicationFile/30725/Lagebericht2009_pdf.pdf, zuletzt geprüft am 21.12.2009.
- Heise Online (Hg.): Siemens und IBM erhalten Milliarden-Auftrag "Herkules". Online verfügbar unter http://www.heise.de/newsticker/meldung/Siemens-und-IBM-erhalten-Milliarden-Auftrag-Herkules-129698.html, zuletzt geprüft am 09.01.2010.
- IT InformationWeek (Hg.) (2008): IT-Security. Studienband 2008. Online verfügbar unter http://i.cmpnet.com/informationweek.de/2008/mtkResearch/it-security-2008_vorabauszuege.pdf, zuletzt geprüft am 21.12.2009.
- IT AmtBw (Hg.): Das IT-AmtBw. Bundesamt für Informationsmanagement und Informationstechnik der Bundesweg. Online verfügbar unter http://www.it-amtbw.de/portal/a/itamtbw/kcxml/04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKLNzKK93JyAclB2I6B-pFw0aCUVH1vfV-P_NxU_QD9gtyIckdHRUUAtTd8bg!!/delta/base64xml/L3dJdyEvd0ZNQUFzQUMvNElVRS82XzIyX0pCVA!!zuletzt geprüft am 11.02.2010.
- PrivatehouseCoopers: Key findings from the 2010 Global State of Information Security Survey®. Public Sector. Online verfügbar unter http://www.pwc.com/en_GX/gx/information-security-survey/pdf/global_info_survey_public_sector_2010.pdf zuletzt geprüft am 16.02.2010

Anlagenverzeichnis

Anlage 1: Verschlusssachenanweisung (VS-Anweisung/VSA)

Anlage 2: ZDV 54/100

Anlage 3: Abschließende Erklärung

Anlage 4: Daten-CD

Merkblatt für die Behandlung von Verschlusssachen (VS) des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)

Das VS-NfD-Merkblatt legt die Behandlung von nationalen Verschlusssachen (VS) des Geheimhaltungsgrades VS -NUR FÜR DEN DIENSTGEBRAUCH sowie von ausländischen VS und VS zwischenstaatlicher Organisationen (z.B. NATO, OCCAR) von vergleichbarem Geheimhaltungsgrad – nachfolgend VS-NfD -im Bereich der Wirtschaft fest. Eine Liste vergleichbarer Geheimhaltungsgrade sowie weitere Informationen über VS-NfD Regelungen können bei dem/der Sicherheitsbevollmächtigten (SiBe) oder – soweit diese/r nicht bestellt ist – beim VS-Auftraggeber angefordert werden. Spezielle Fragen können an das Bundesministerium für Wirtschaft und Arbeit (Referat VI B 3) unter folgender E-Mail-Adresse gerichtet werden: buero-vib3@bmwa.bund.de.

I. Allgemeines

1. Zugangsberechtigung und Weitergabe

1.1.VS des Geheimhaltungsgrades VS-NfD dürfen nur Personen zugänglich gemacht werden, die im Zusammenhang mit der Auftragsdurchführung oder bei der Auftragsanbahnung Kenntnis erhalten müssen (Grundsatz „Kenntnis nur, wenn nötig“). Den zugangsberechtigten Personen ist dieses Merkblatt vor dem Zugang zu solchen VS nachweislich bekannt zu geben; sie werden auf ihre besondere Verantwortung für den Schutz der VS gemäß diesem Merkblatt sowie eventuelle strafrechtliche oder vertragsrechtliche Konsequenzen bei Zuwiderhandlung hingewiesen.

> Weitergehende Maßnahmen wie ein Geheimschutzverfahren des BMWA, Sicherheitsüberprüfungen oder formale Besuchsanmeldungen sind nicht erforderlich.

1.2.Über den Inhalt der VS ist Verschwiegenheit gegenüber Nichtbeteiligten zu wahren. Mitarbeiter, die sich zum Umgang mit solchen VS als ungeeignet erwiesen oder gegen die Verpflichtung zur Geheimhaltung verstoßen haben, sind von der Bearbeitung solcher VS auszuschließen.

1.3.Die Weitergabe von als VS-NfD eingestuften VS darf nur an Regierungsstellen, zwischenstaatliche Organisationen oder Auftragnehmer erfolgen, die an einem Programm/Projekt/Auftrag beteiligt sind und die Zugang zu den Informationen im Zusammenhang mit der Bearbeitung des Programms/Projekts/Auftrags haben müssen. Vor der Weitergabe von VS-NfD eingestuften VS an nicht beteiligte zwischenstaatliche Organisationen oder Auftragnehmer aus nicht beteiligten Ländern ist die schriftliche Einwilligung des amtlichen VS-Auftraggebers der VS einzuholen. Grundsätzlich bedarf es hierbei einer Geheimschutzvereinbarung.

1.4.In Deutschland kann sich das BMWA beim VS-Auftragnehmer über die Einhaltung der Bestimmungen dieses Merkblattes vergewissern.

1.5.Die VS-Einstufung ist dreißig Jahre nach dem 1. Januar des auf die Einstufung folgenden Jahres aufgehoben, sofern keine andere Frist bestimmt ist. Bei internationalen Aufträgen ist BMWA zu konsultieren, sofern keine Programm-oder Projektvereinbarungen bestehen.

2. Bearbeitungsmaßnahmen

2.1.Kennzeichnung und Handhabung bzw. Verwahrung

Dokumente und Material des Geheimhaltungsgrades VS-NfD sind wie folgt zu kennzeichnen, zu behandeln und zu verwahren:

2.1.1. Dokumente sind durch schwarzen oder blauen Stempelaufdruck, Druck „VS – NUR FÜR DEN DIENSTGEBRAUCH“ am oberen Rand jeder beschriebenen Seite sowie aller entsprechend eingestuften Anlagen zu kennzeichnen bzw. im Falle internationaler oder ausländischer VS mit der entsprechenden deutschen Kennzeichnung umzustempeln. Bei Büchern, Broschüren u.ä. genügt die Kennzeichnung auf dem Einband und dem Titelblatt. Trägt jede beschriebene Seite eines ausländischen Buches oder einer ausländischen Broschüre den ausländischen Geheimhaltungsgrad, genügt die Kennzeichnung mit dem deutschen Geheimhaltungsgrad auf dem Einband oder dem Titelblatt.

2.1.2. VS-NfD eingestuftes Material (z.B. Gerät, Ausrüstung) oder Datenträger (z.B. Disketten, CD`s, Mikrochips, Mikrofiche) sind ebenfalls entweder deutlich sichtbar am Material selbst oder – falls dies nicht möglich ist – an den Aufbewahrungsbehältnissen des Materials zu kennzeichnen bzw. grundsätzlich umzustempeln.

2.1.3. Die VS sind in verschlossenen Räumen oder Behältern (Schränken, Schreibtischen usw.) zu verwahren. Außerhalb von solchen Räumen oder Behältnissen sind sie stets so aufzubewahren bzw. zu behandeln, dass Unbefugte keinen Zugang zu oder Einblick in die VS haben.

2.1.4. VS-Zwischenmaterial (z.B. Vorentwürfe, Stenogramme, Tonträger, Folien) ist gegen Einsichtnahme Unbefugter in derselben Weise zu schützen wie das Bezugsdokument. VS-Zwischenmaterial, das nicht an Dritte weitergegeben und unverzüglich vernichtet wird, muss nicht als VS gekennzeichnet werden.

2.2.Weitergabe

2.2.1. Die Weitergabe in Deutschland erfolgt durch Boten oder Versand durch Zustelldienste in einfachem verschlossenen Umschlag bzw. Behältnis. Der Umschlag bzw. das Behältnis erhalten keine VS-Kennzeichnung.

2.2.2. VS können durch private Zustelldienste als gewöhnlicher Brief bzw. Paket oder auch als Luft-oder Seefracht in das Ausland versendet werden, es sei denn, der VS-Auftraggeber hat dieser Versendungsart ausdrücklich widersprochen oder andere Modalitäten für den Auslandsversand festgelegt. Dabei sind vom VS-Auftraggeber zwischenstaatliche Vereinbarungen bzw. besondere Programm-oder Projektvereinbarungen zu berücksichtigen.

2.3.Vernichtung/Rückgabe

2.3.1. Um größere Bestände von VS zu vermeiden, sind nicht mehr benötigte VS zu vernichten oder an den VS-Auftraggeber zurückzugeben.

2.3.2. VS, auch VS-Zwischenmaterial, sind so zu vernichten, dass der Inhalt nicht mehr erkennbar ist und nicht mehr erkennbar gemacht werden kann.

2.4 Verlust, unbefugte Weitergabe, Auffinden von VS oder Nichtbeachtung des Merkblatts

Der Verlust, die unbefugte Weitergabe sowie das Auffinden von VS oder die Nichtbeachtung dieses Merkblattes ist unverzüglich über den/die SiBe – soweit bestellt – dem deutschen VS-Auftraggeber und BMWA (Referat VI B 3) mitzuteilen, um einen eventuell entstandenen Schaden zu begrenzen und den Vorfall aufzuklären.

2.5. Besuche

Besuche in das oder aus dem Ausland mit Zugang zu VS-NfD oder vergleichbarem Geheimhaltungsgrad werden in der Regel unmittelbar zwischen der entsendenden und der zu besuchenden Einrichtung vereinbart. Es gibt keine besonderen Formvorschriften.

2.6. Aufträge

2.6.1. Alle VS-Auftragnehmer/-Unterauftragnehmer sind vom VS-Auftraggeber vertraglich zu verpflichten, die Regelungen dieses Merkblattes zu beachten. Dabei ist darauf hinzuweisen, dass eine Nichtbeachtung die Auflösung des Vertrages bzw. von Teilen des Vertrages zur Folge haben kann.

2.6.2. Bei Angeboten bzw. der Aufforderung zur Abgabe von Angeboten und nach Auftragsdurchführung sind VS bis zur Aufhebung der Einstufung vorschriftsmäßig zu verwahren, baldmöglichst zu vernichten oder zurück zu geben.

2.6.3. VS-Auftragnehmer/-Unterauftragnehmer im Ausland sind vertraglich zu verpflichten, die Vorschriften ihrer zuständigen Sicherheitsbehörde für die Behandlung von VS vergleichbaren Geheimhaltungsgrades zu beachten.

Gibt es keinen vergleichbaren Geheimhaltungsgrad in dem Land eines VS-Auftragnehmers/-Unterauftragnehmers, ist BMWA (Referat VI B 3) einzuschalten, das Regelungen für den Schutz mit der zuständigen ausländischen Sicherheitsbehörde vereinbart. Die Weitergabe darf dann erst nach Zustimmung des BMWA erfolgen.

II. Nutzung von Informationstechnik (IT)

1. Bearbeitung

1.1. Wird IT für die Bearbeitung von VS-NfD eingestuften VS genutzt, sind zum Schutz der VS (entsprechend Teil I 1.1 und 1.2) geeignete informationstechnische Maßnahmen und / oder materielle und organisatorische Maßnahmen zu treffen .

1.2. Vor der Bearbeitung oder Speicherung von VS-NfD eingestuften VS ist sicherzustellen, dass das Gerät oder das interne Netzwerk nicht unmittelbar (z.B. ohne Schutz durch eine Firewall) mit dem Internet verbunden ist, sofern nicht weitergehende Maßnahmen entsprechend 3.3 aufgeführt, ergriffen worden sind.

1.3. Bei der Bearbeitung von VS-NfD eingestuften VS kommen insbesondere folgende Maßnahmen in Betracht:

- Übersicht über die Zugriffsberechtigungen,
- Nutzung von Identifizierungs-und Authentisierungsmechanismen (z.B. Login, Passwort),
- geeignete IT-Sicherheitsanweisung (einzelplatz-oder .unternehmensbezogen)

Funktastaturen und Funk-Netzwerke dürfen nur eingesetzt werden, wenn sie vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassen sind.

1.4 Werden für die Bearbeitung oder Speicherung von VS-NfD eingestuften Daten tragbare IT-Systeme (z.B. Notebooks oder Handhelds) eingesetzt, sind die verwendeten Speichermedien durch vom BSI zugelassene Produkte zu verschlüsseln.

1.5 Transportable Datenträger (z.B. Disketten, CD's, Wechselplatten), die VS-NfD eingestufte Daten unkryptiert[1] enthalten, sind gemäß Teil I 2.1.2 zu kennzeichnen und gemäß Teil I 2.1.3 aufzubewahren.

1.6 Das Löschen von Datenträgern hat mit Hilfe von Softwareprodukten zu erfolgen, die mindestens ein zweifaches Überschreiben vorsehen. Hierbei soll auf vom BSI empfohlene Produkte zurückgegriffen werden.

1.7 Informationstechnik und Datenträger sind auf Virenbefall (insbesondere Trojanische Pferde oder Würmer) zu überprüfen bevor VS-NfD damit bearbeitet werden. Diese Prüfung ist in regelmäßigen Zeitabständen zu wiederholen.

1.8 Private Informationstechnik (z.B. Laptops), Software oder Datenträger dürfen nicht für die Bearbeitung eingesetzt werden. In für VS-NfD genutzten Informationssystemen dürfen keine private Software oder private Datenträger verwendet werden.

1.9 Auf fest installierten Datenträgern, die VS-NfD eingestufte Daten unkryptiert enthalten, sind die Verschlusssachen gemäß 1.6 zu löschen, bevor die Datenträger im Rahmen von Wartungs-oder Reparaturarbeiten an IT-Systemkomponenten den Bereich der zugriffsberechtigten Personen verlassen. Ist eine Löschung nicht möglich, sind die Datenträger auszubauen und zurückzubehalten bzw. ist die Wartungs-/Reparaturfirma vertraglich auf die Einhaltung der Regeln dieses Merkblattes zu verpflichten..

[1] Kryptieren = verschlüsseln oder codieren. Um auf materielle Sicherheitsmaßnahmen (VS-Kennzeichnung, sichere Aufbewahrung usw.) verzichten zu können, muß das für die Kryptierung genutzte Kryptosystem vom Bundesamt für Sicherheit in der Informationstechnik zugelassen und/oder vom BMWA freigegeben sein.

2. Übertragung

2.1. Bei der elektronischen Übermittlung auf Telekommunikations-oder anderen technischen Kommunikationsverbindungen (einschließlich Onlinedienste wie WWW, FTP, TELNET, email etc.) in Deutschland sind die VS mit einem vom BSI zugelassenen und/oder von BMWA freigegebenen Kryptosystem zu kryptieren.

Abweichend davon ist ausnahmsweise eine unkryptierte Übertragung zulässig:

a) innerhalb von Festnetzen bei Telefongesprächen, bei Videokonferenzen und bei Fernkopien und Fernschreiben, wenn zwischen Absender und Empfänger für die erforderliche Übertragungsart keine Kryptiermöglichkeit besteht und der VS-Auftraggeber bei der Auftragsvergabe nicht ausdrücklich eine Kryptierung verlangt. Die absendende Stelle hat sich vor der Übertragung zu vergewissern, dass sie mit dem richtigen Empfänger verbunden ist.

b) innerhalb eines geschlossenen Netzes (LAN), wenn es ausschließlich auf einem örtlich zusammenhängenden firmeneigenen Gelände betrieben wird und die Übertragungseinrichtungen gegen unmittelbaren Zugriff Unbefugter geschützt sind.

2.2. Bei grenzüberschreitenden elektronischen Übermittlungen müssen die Verschlüsselungsverfahren zwischen den nationalen Sicherheitsbehörden der beteiligten Staaten abgestimmt werden. Sofern in einem Programm/Projekt besondere Sicherheitsanweisungen für die Übermittlung vereinbart wurden, sind diese zu beachten.

Bei Bedarf erteilt BMWA (Referat VI B 3) weitere Auskünfte.

3. Maßnahmen zum Schutz der Vertraulichkeit von VS mit der Einstufung VS-NfD bei der Nutzung von (IT)

Die im Folgenden empfohlenen Maßnahmen sollen die Vertraulichkeit der elektronisch gespeicherten VS sicherstellen. Sie dienen nicht in erster Linie dazu, die Integrität und die Verfügbarkeit der Daten zu gewährleisten.

Drei unterschiedliche Ausgangsituationen sind zu unterscheiden:

3.1.Einzelplatz PC oder Netzwerke mit geschlossenen Nutzergruppen, die nicht mit anderen Netzen verbunden sind

-Das Betriebssystem muss ein differenziertes Benutzerprofil und Zugriffschutz bis auf Dateiebene gewährleisten, damit der Grundsatz „Kenntnis nur, wenn nötig“ sichergestellt wird (z. B. Unix/Linux; Win NT; Win 2000, Win XP).

- Es muss ein Login und ein Passwort vorhanden sein. Das Passwort muss mindestens 6 Stellen, alphanumerisch (Sonderzeichen); Groß-und Kleinbuchstaben enthalten. -Das BIOS muss ebenfalls Passwort geschützt sein. -Ein Booten des IT-Systems darf grundsätzlich nur von der Festplatte aus möglich sein. -Es sollte – falls möglich – eine RAM-Disk für die Temp-Dateien enthalten (Nutzungshilfe). -Ein aktuelles Virenprogramm muss eingesetzt sein.

-Bei Netzwerken sollte eine eigene Partition zum Speichern der VS-Daten auf dem Server installiert werden.

3.2.Geschlossene Netze mit E-Mail-Anschluss nach außen

Zusätzlich zu den unter Nr. 3.1 festgelegten Punkten müssen

-ein Serverbasiertes Netz vorhanden sein, bei dem der Server im zugangsgeschützten Bereich steht, -eine Firewall vorhanden sein, entweder auf dem Server oder als eigenes IT-System
(und ggfs. zusätzlich E-Mailserver) auch im zugangsgeschützten Bereich, -ein Paketfilter eingesetzt werden; ein Applikations-Gateway ist möglich, -jede weitere IP-Adresse, außer der Server-IP, nach außen verborgen werden (DNS-
Server),
-die Übertragung von VS-NfD verschlüsselt erfolgen, wobei für die Verschlüsselung nur vom BMWA zugelassene Produkte eingesetzt werden dürfen; Schlüssel sind grundsätzlich nicht auf der Festplatte abzulegen.
Es müssen verbindliche Anwenderregelungen innerhalb des Unternehmens festgelegt und geschult werden.
Die neuesten Sicherheits-Updates der genutzten Software sind nach Verfügbarkeit insbesondere auch an der Firewall einzubinden.

3.3.Standalone-PC oder Geschlossene Netze mit E-Mail-und Internetanschluss

Zusätzlich zu den unter Nr. 3.1 und Nr. 3.2 festgelegten Punkten müssen -eine Firewall und Applikation-Gateway vorhanden sein, -die Regelungen des BSI-Grundschutzhandbuchs für Passwörter angewendet werden, -VS-NfD-Daten auf dem Server in einer eigenen Partition bzw. in einem speziell
geschützten Datenbereich gehalten werden; die dadurch gegebenen Schutzmechanismen sind entsprechend anzuwenden. Je nach Umfang ist die Einrichtung eines eigenen VPN z.B. für eine Nutzergruppe oder ein Projekt erforderlich.

Anlage 2

Die Anlage 2 der ZDV 54/100 ist durch die Bestimmungen der Geheimschutzordnung der Bundesrepublik Deutschland als Verschlusssache (VS-Nfd) eingestuft. Sie darf deshalb nicht im Rahmen dieser öffentlichen Arbeit, als Anlage beigefügt werden. Zu wissenschaftlichen Zwecken und zum näheren Verständis der Arbeit kann sie aber über das Streitkräfteamt der Bundeswehr eingesehen werden.

Kontakt finden sie unter der Pressestelle der Bundeswehr:

Bundesministerium der Verteidigung
Leiter des Presse- und Informationsstabes
Stauffenbergstraße 18
10785 Berlin
Tel.: +49 (0) 1888 24 8232
Fax: +49 (0) 1888 24 8240

http://www.streitkraefteamt.bundeswehr.de

Abschließende Erklärung

Ich versichere hiermit, daß ich die vorliegende Bachelorarbeit selbständig, ohne unzulässige Hilfe Dritter und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Magdeburg, der 05.03.10

Daten-CD