Aufbau eines zertifizierten Information Security Management Systems

Secorvo White Paper

Case Study
Aufbau und Zertifizierung eines ISMS nach BS7799-2:2002/ISO 27001

Version 1.3
Stand 24. September 2006

Klaus Kühner (POET Service GmbH)
Jörg Völker (Secorvo)

Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
D-76137 Karlsruhe

Tel. +49 721 255171-0
Fax +49 721 255171-100

info@secorvo.de
www.secorvo.de

Inhaltsübersicht

Abkürzungen

ASP	Application Service Provider/Providing
BS	British Standard
CMS	Conten Management System
COBIT	Control Objectives for Information and related Technology
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITIL	IT Infrastructure Library
PDCA	Plan-Do-Check-Act Model
RA	Risiko Analyse
RZ	Rechenzentrum
SOA	Statement of Applicability
SSE-CMM	System Security Engineering Capability Maturity Model

Historie

Version	Datum	Änderung	Autor
1.0	10.08.06	Erste Fassung	Jörg Völker
1.1	23.08.06	Überarbeitung	Klaus Kühner
1.2	25.08.06	Fassung zur Freigabe	Jörg Völker
1.3	24.09.06	Erste publizierte Fassung	Jörg Völker, Dirk Fox

1 Einleitung

Seit Ende der 90er Jahre des letzten Jahrhunderts existiert ein weltweit anerkannter Standard zum Aufbau und Betrieb eines Information Security Management Systems zur Sicherstellung einer angemessenen Sicherheitspolitik für Unternehmen und Behörden.

Dieser zweiteilige, ursprünglich britische Standard BS 7799 zum Management von Informationssicherheit enthält eine umfassende Sammlung von Maßnahmen, die dem Best Practice-Ansatz in der Informationssicherheit genügen. Teil 1 des Standards (BS7799-1) hat die Aufgabe, diese Maßnahmen darzustellen; Teil 2 (BS7799-2) bildet eine Basis für die Beurteilung eines Informationssicherheits-Managementsystems, die für ein formales Verfahren zur Zertifizierung herangezogen werden kann.

Bereits im Jahr 2000 wurde BS 7799-1 als ISO Standard ISO 17799:2000 veröffentlicht und 2005 einer gründlichen Revision unterzogen. Ebenfalls im Jahr 2005 wurde BS7799-2 als ISO 27001 publiziert. ISO ist nun bestrebt alle sich mit Information Security relevanten Standards in der 27000 Serie zu integrieren. Die Überführung von ISO 17799:2005 nach ISO 2700x ist für 2007 geplant. Eine Einführung in die Inhalte von ISO 17799:2005, BS7799-2 und ISO 27001 findet sich bspw. in [4].

Gerade die Möglichkeit, sein Information Security Management System zertifizieren zu lassen, verhalf dem BS 7799-2 zu relativ rascher internationaler Verbreitung (305 Zertifizierungen bis Oktober 2003, 2.746 Zertifizierungen bis August 2006). In Deutschland verlief die Verbreitung nicht ganz so rasch (38 Zertifizierungen bis Juni 2005, 58 Zertifizierungen bis August 2006). Doch die Nachfrage nimmt auch hier langsam, aber stetig zu. Insbesondere bei IT-Dienstleistern und Betreibern von Rechenzentren sowie Application Service Providern (ASP) erfreuen sich BS 7799-2 / ISO 27001 großer Attraktivität. Lässt sich so doch recht anschaulich der professionelle und effektive Umgang mit Sicherheitsfragen gegenüber internen und externen Kunden darstellen.

Dies bewog im Jahr 2005 auch das Unternehmen ems ePublishing Service GmbH, eine Zertifizierung nach BS 7799-2 anzustreben. Die ems ePublishing Service GmbH, inzwischen umfirmiert in POET Service GmbH (kurz POET), ist IT- und Servicedienstleister und 100%ige Tochter der POET AG und bietet unter anderem ASP und Managed Services an. Die POET AG ist seit Jahren zuverlässiger Partner für FORTUNE 500 Unternehmen wie ABB Inc., DaimlerChrysler AG, EADS, IBM, ThyssenKrupp AG und Volkswagen AG sowie marktführende mittelständische Unternehmen wie Kaiser + Kraft Europa GmbH, Koch, Neff & Volckmar GmbH und Cornelsen mit den Kataloglösungen X-Solutions und X-Procure für einkaufende Unternehmen und Marktplätze, Content Services und dem Betrieb von Marktplätzen. Ausschlaggebend für die Zertifizierung nach BS 7799-2 statt IT-Grundschutz waren die internationale Anerkennung des Standards (gerade im Hinblick auf die international aufgestellte Kundschaft der POET) sowie das prozessorientierte Vorgehensmodell, das BS 7799-2 zugrunde liegt.

Zeitgleich mit POET strebte auch die PhonoNet GmbH, ein Kunde von POET, die Zertifizierung nach BS 7799-2 an. Die PhonoNet GmbH wurde vom Bundesverband der Phonographischen Wirtschaft e.V. gegründet, um den Datenaustausch zwischen Handel, Medien und Industrie zu standardisieren und damit entscheidend zu vereinfachen. Heute unterstützt PhonoNet durch den Datenaustausch in zahlreichen Formaten und mit Katalogdatenbanken die Distribution und Vermarktung von physischen und digitalen Produkten. Hierzu betreibt PhonoNet die Plattform „Order Clearing“ für den elektronischen Datenaustausch der deutschen Musikbranche; gehostet wird die Plattform bei POET.

Von einer gleichzeitigen Durchführung beider Zertifizierungsprojekte versprach man sich einige Synergien und entsprechende Kostenersparnisse aufgrund der engen Verzahnung der Geschäftsprozesse.

Die Secorvo Security Consulting GmbH wurde beauftragt, POET und PhonoNet bei Aufbau, Inbetriebnahme und Überprüfung eines ISMS nach BS7799-2 zu unterstützen. Im Vordergrund der Beratungstätigkeit sollte dabei stehen, POET in die Lage zu versetzen, alle wesentlichen Aktivitäten selbst durchführen zu können und den dafür erforderlichen Know-How-Transfer während des Projektes sicherzustellen.

Ein ehrgeiziger Zeitplan sah vor, die Zertifizierung sowohl von PhonoNet als auch von POET noch im Jahr 2005 erfolgreich abzuschließen.

2 Ausgangslage

Die BS7799-2 Zertifizierung wurde für POET auf den Bereich ASP Service begrenzt. Dieser Bereich umfasst den Rechenzentrumsbetrieb zur Bereitstellung der Produkte für externe Kunden von POET. Seitens PhonoNet wurde die Zertifizierung auf das Order Clearing beschränkt.

Da es sich bei BS7799-2 um einen prozessorientierten Standard zur Etablierung eines Information Security Management Systems handelt, stehen im Fokus des Standards nicht (nur) die Umsetzung bestimmter Security Maßnahmen, sondern vor allem die Etablierung von Prozessen zur Sicherstellung eines effektiven und effizienten Managementsystems zur Aufrechterhaltung von Informationssicherheit.

3 Vorgehensweise

3.1 Projektphasen

Die vom BS7799-2 propagierte, prozessorientierte Vorgehensweise basiert auf dem so genannten PDCA-Model (PLAN-DO-CHECK-ACT, siehe Abbildung 1).

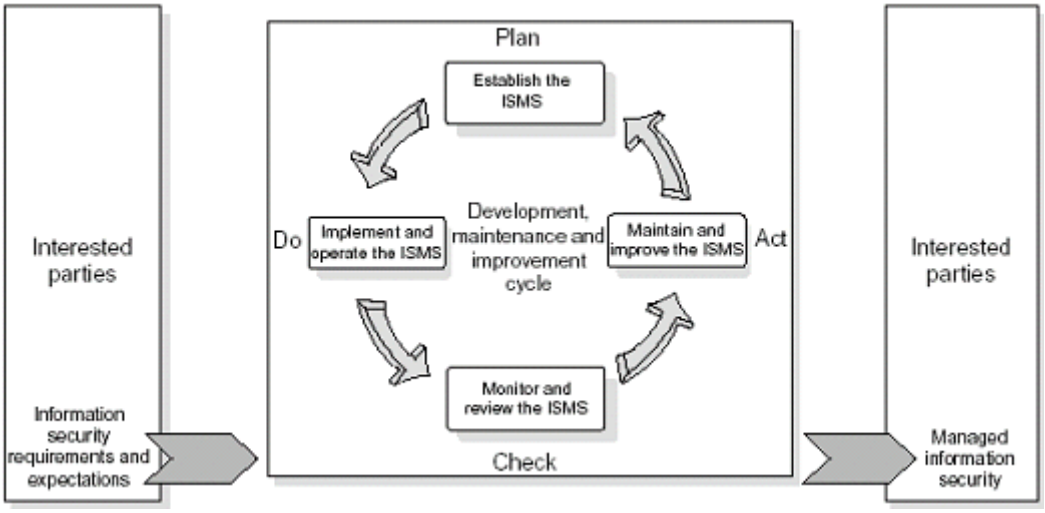


Abbildung 1: PDCA-Model (Quelle: BS 7799-2)

Den Sachverhalt, dass im Vordergrund des Projekts die Etablierung von Prozesse steht, galt es frühest möglich allen Projektbeteiligten zu vermitteln. Das gelang überraschenderweise nicht ad hoc: Es bedurfte einiger Zeit, bis alle Projektbeteiligten das gleiche Verständnis von der bevorstehenden Aufgabe hatten.

Es zeigte sich, dass es durchaus sinnvoll ist, sich im Rahmen des Umsetzungsprojektes an diese Vorgehensweise zu halten und die Projektphasen daran auszurichten.

Auf dieser Basis wurde dann der folgende allgemeine Projektphasenplan erarbeitet:

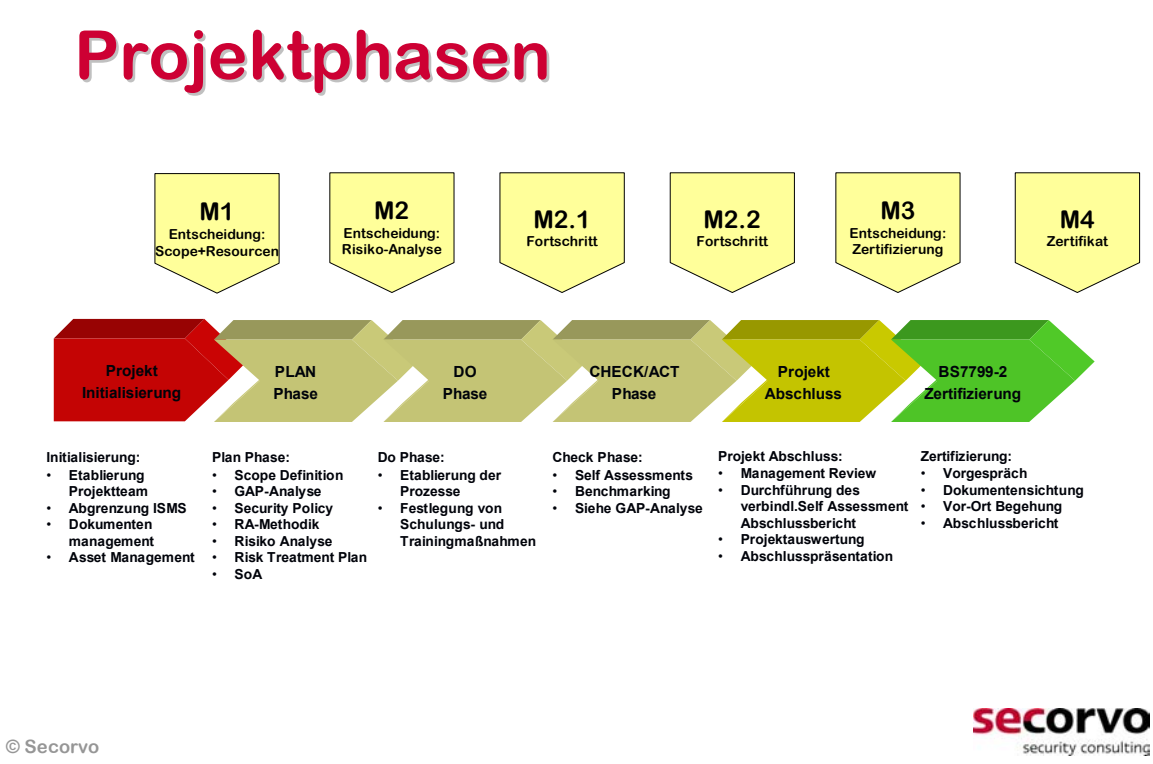


Abbildung 2: Projektphasenplan

Die einzelnen Projektphasen umfassten die folgenden Aufgabenschwerpunkte:

- **Projektinitialisierung**

Sie diente in erster Linie der Konstituierung des Projektteams und der Festlegung von Formalien (z.B. der Definition von Templates etc.). Des Weiteren erfolgte in dieser Phase die Bestimmung und Festlegung von Ressourcen (wie viel interne und externe Unterstützung wird benötigt, welche Bereiche sind betroffen und müssen entsprechende Unterstützungs-leistungen erbringen), sowie die Festlegung des Zeit- und Budgetrahmens.

Hauptaufgabe dieser Phase ist die umfassende Vorbereitung aller nachfolgenden Aktivitäten.

- **PLAN-Phase**

  Die PLAN Phase beinhaltete insbesondere die

  - Definition des ISMS Scopes
  - Durchführung einer GAP-Analyse zur Feststellung des Status Quo
  - Erstellung der Security Policy
  - Festlegung und Definition der anzuwendenden Risk Assessment (RA)-Methodik
  - Durchführung einer ersten Risiko Analyse auf Basis der festgelegten RA-Methodik
  - Erstellung eines Risk Treatment Plans auf Basis der durchgeführten RA
  - Erstellung des sogenannten Statement of Applicability.

- **DO-Phase**

Ziel dieser Phase war die Umsetzung der Planung; sie beinhaltete die Implementierung der Sicherheitspolitik, die Umsetzung von Kontrollmechanismen sowie die Integration von Prozessen und Abläufen zur Steuerung des ISMS.

- **CHECK/ACT-Phase**

Die Check/ACT-Phase diente der Bewertung der ISMS-Prozessperformance (Self Assessments) und der erreichten Fortschritte durch Anwendung des ISMS.

Sie sollte sicher stellen, dass frühzeitig Verbesserungsbedarf erkannt würde und geeignete Maßnahmen ergriffen und im Rahmen der ACT Phase umgesetzt würden.

- **Projektabschluss**

Diese Phase diente dazu, die ISMS Aufbau- und Implementierungsphase abzuschließen und das ISMS in den „Wirkbetrieb“ zu überführen. In dieser Phase erfolgte die Durchführung des durch den Standard vorgeschriebenen, eigenständigen Self Assessments. Dem Management wurden Projektergebnisse und –bewertung vorgelegt.

Zum Abschluss jeder Projektphase wurde ein **Meilenstein** definiert, der die Projektfortschritte dokumentieren sollten. Die Meilensteine M2 und M3 waren dabei von besonderer Bedeutung, da diese Meilensteine ebenfalls dazu dienten zu beurteilen, ob in Abhängigkeit von den bisherigen Projektergebnissen die weitere Projektfortsetzung sinnvoll waren oder nicht. Hätte beispielsweise die Risiko-Analyse ergeben, dass die zu etablierenden Sicherheitsmaßnahmen nicht im geplanten Zeit- und Kostenrahmen hätten umgesetzt werden können, hätte dies eine Verschiebung der Zertifizierung zur Folge gehabt. Diese „Rückzugsmöglichkeiten“ wurden durchweg als positiv bewertet, da zu Projektbeginn nicht die gesamten Auswirkungen des Projekts belastbar prognostiziert werden konnten und man bestrebt war, keine unrealistischen Ziele anzustreben.

Im Laufe des Projektes zeigte sich, dass eine strikte Einhaltung dieser Phasen nicht zwingend erforderlich war. Vielmehr wurde innerhalb jeder einzelnen Phase das beschriebene PDCA-Model „im Kleinen“ angewendet und iterativ wiederholt. Dadurch konnte schon sehr frühzeitig dokumentiert werden, dass die einzelnen ISMS Prozesse auch tatsächlich als solche gelebt wurden. Ein Vorteil, der beim späteren Zertifizierungs-Audit zum Tragen kam.

3.2 Anforderungen des BS7799-2

Der Standard BS 7799-2 stellt konkrete Anforderungen, die zu erfüllen sind, damit eine Zertifizierung erfolgreich durchlaufen werden kann.

Primäres Ziel des BS 7799-2 ist die Etablierung eines *dokumentierten* Information Security Management Systems, in dem alle relevanten Strukturen, Prozesse und Abläufe für Planung, Steuerung und Kontrolle des ISMS beschrieben und schriftlich fixiert sind.

Benötigte Dokumente

Der Standard nennt eine Reihe von Dokumenten, deren Erstellung im Rahmen der Etablierung des ISMS notwendig ist:

- Security Policy
- ISMS-Scope
- Risk Assessment Report
- Risk Treatment Plan

- Dokumentierte Prozesse zur Sicherstellung einer effektiven Planung, Steuerung und Kontrolle der Information Security Prozesse
- Aufzeichnungen
- Statement of Applicability.

Zu Art, Umfang, Ausgestaltung und Form der Dokumentation macht BS 7799-2 keine Vorschriften. Diese Merkmale orientieren sich in der Praxis einzig an den Gegebenheiten und Notwendigkeiten der Sicherheitsanforderungen für den betrachteten Anwendungsbereich.

Dem **Risk Assessment** kommt dabei innerhalb von BS 7799-2 eine zentrale und entscheidende Bedeutung zu. Das ganze Information Security Management System basiert letztlich auf der Anwendung geeigneter Risk Management Methoden, die auf die Identifizierung von Bedrohungen und Schwachstellen, die Auswahl angemessener Maßnahmen und somit die Reduzierung der Gefährdungen auf ein akzeptables Restrisiko zielen. Welche Risk Management Methoden angewendet werden sollen, schreibt der Standard allerdings nicht vor.

Der **Verantwortung des Managements** für Etablierung, Implementierung, Betrieb, sowie für Monitoring, Review und die Verbesserung des ISMS wird ebenfalls ein hoher Stellenwert beigemessen. Bei einer angestrebten Zertifizierung muss *plausibel* und *nachvollziehbar* dargelegt werden können, wie das Management dieser Verantwortung konkret nachkommt.

Es muss ein **regelmäßiges Review** des ISMS erfolgen, um die Tauglichkeit, Angemessenheit und Effizienz des ISMS sicherzustellen. Planung, Durchführung, Input und Ergebnisse der Reviews müssen *plausibel* und *nachvollziehbar* dargestellt werden.

Die **kontinuierliche Verbesserung** des ISMS ist ein wesentliches Qualitätsmerkmal von BS 7799-2 und soll durch die konsequente Umsetzung der Security Policy, der Maßnahmen, der Resultate aus Audits, der Analyse der Monitoring-Ereignisse sowie der Ergebnisse aus dem Management Review erreicht werden.

Im Rahmen der Zertifizierung muss nachgewiesen werden, dass diese Prozesse etabliert sind und gelebt werden. Es ist also nicht ausreichend, dass entsprechende Prozessbeschreibungen (Workflows und Berechtigungen) existieren. Es muss nachvollziehbar dargestellt werden können, dass und wie diese Prozesse funktionieren und ineinander greifen.

Annex A von BS 7799-2 verweist auf die **Control objectives und Controls** von ISO 17799. Die Umsetzung dieser Controls ist verpflichtend und im Statement of Applicability zu dokumentieren; ein ebenfalls zu dokumentierender Ausschluss darf nur durch eine entsprechende Untermauerung mit einer Risiko Analyse erfolgen.

3.3 Die Umsetzung

Im Rahmen der Projektinitialisierung wurden, neben der Etablierung des Projektteams, auch grundlegende Strukturentscheidungen getroffen. Eine Besonderheit des Projektes bestand darin, dass zeitgleich die POET als auch ein Kunde der POET die Zertifizierung anstrebte. Hier zeigte sich, dass zwei unterschiedliche Ebenen/Betrachtungsweisen berücksichtigt werden mussten.

3.3.1 Dokumentenmanagement

Für den Kunden von POET, der Firma PhonoNet, war wichtig, insbesondere die Anforderungen an den sicheren Betrieb (sowohl aus Prozess- als auch aus Requirementssicht) zu definieren. Die Festlegung und Umsetzung konkreter Maßnahmen und die Etablierung der Sicherheitsprozesse war dann Aufgabe des Dienstleisters.

Der Dienstleister wiederum musste neben den Anforderungen seiner externen Kunden auch auf die internen Strukturen Rücksicht nehmen und diese geeignet in sein ISMS integrieren. Hieraus ergab sich die folgende Dokumenten-Hierarchie:

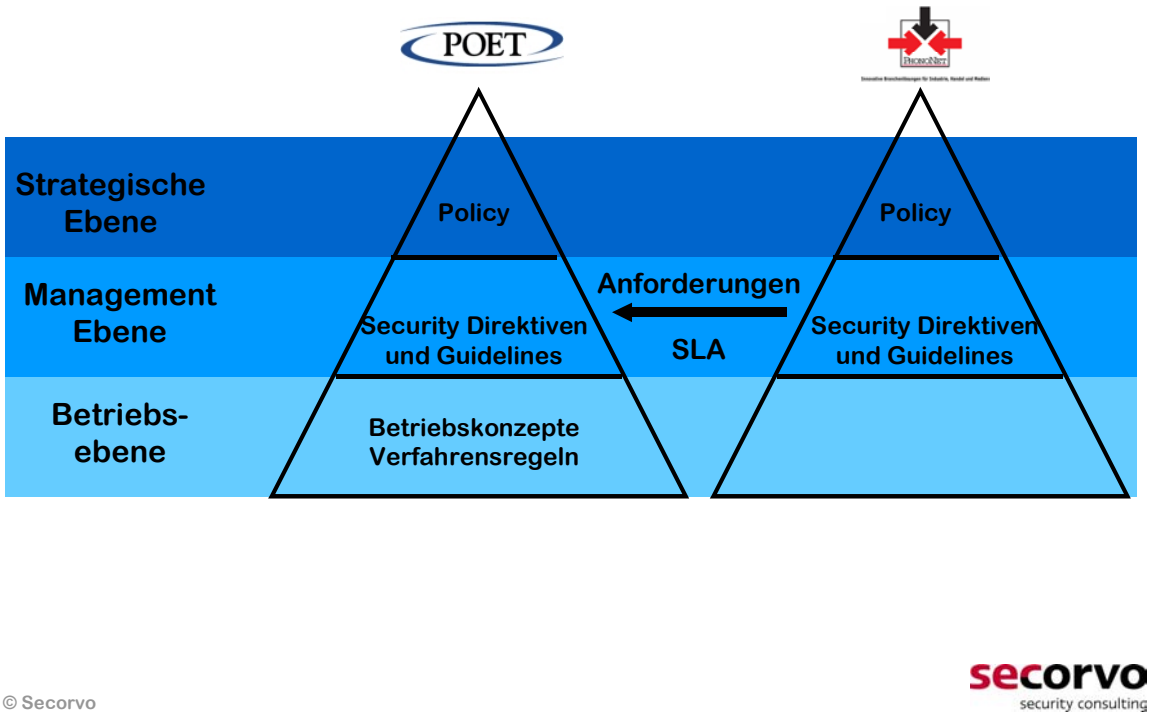


Abbildung 3: Dokumenten-Hierarchie

- **Strategische Ebene**

Auf der strategischen Ebene wurden im wesentlichen die allgemeine **Sicherheitsstrategie** und deren **Ziele** formuliert, Verantwortlichkeiten geregelt und die Verbindlichkeit der Vorgaben fixiert.

- **Management Ebene**

Die Security Directives und Guidelines dienten primär dazu, zu definieren, *WAS* zu tun ist, um die auf strategischer Ebene festgelegten Ziele zu erreichen. Im wesentlichen orientierte sich die Ausgestaltung der Directives an der Gliederung der Managementgebiete zu ISO 17799:2005. Für PhonoNet stand hier vor allem im Vordergrund, die Anforderungen an den sicheren Betrieb des Systems aus Sicht des System-Owners zu definieren (z.B. Verschlüsselung auf Transportebene, Anforderungen an die Authentifizierung der Teilnehmer, Festlegung von Logging- und Reportinganforderungen etc). Diese Anforderungen sollten sich dann in den entsprechenden SLA-Vereinbarungen wiederfinden.

- **Betriebsebene:**

In den Betriebskonzepten und Verfahrensregeln ist dann zu dokumentieren, *WIE* die Anforderungen nun konkret (technisch oder organisatorisch) umgesetzt werden (z.B. Sicherung der Transportebene durch Einsatz von TLS/SSL etc.). Aus Sicht des Kunden von POET kann die Betriebsebene entfallen, denn hier werden die Details zur Erfüllung der Vorgaben der Security Directives dokumentiert. Da der Kunde i.d.R. keinen direkten Einfluss auf den Betrieb hat, ist dies Sache des Dienstleisters. Aus Sicht des Kunden ist dann aber wichtig, dass ein angemessenes Reporting System vorhanden ist, über das die entsprechend zu

vereinbarenden Kennzahlen (Key Performance Indicators, KPI) zur Leistungsüberprüfung zeitnah abgefragt werden können.

Neben Struktur, Inhalten und Zuständigkeiten für die Dokumente spielt auch deren „Verwaltung“ ein wichtige Rolle im Rahmen von BS 7799-2. Denn es muss sichergestellt werden, dass jeder Nutzer zu jeder Zeit die aktuell gültige Version eines Dokumentes zu Rate zieht und dass obsolete Dokumente zuverlässig als solche gekennzeichnet und aus dem Verkehr gezogen werden. Wie können Bearbeitungsworkflows effizient und nachvollziehbar gestaltet werden? Dies sind nur einige der Aspekte und Fragen, die im Rahmen des Dokumentenmanagements zu beantworten, aber auch technisch zu unterstützen waren. Die organisatorischen Rahmenbedingungen wurden deshalb in einem entsprechenden Dokument „Dokumentenmanagement“ fixiert. Hierin wurde geregelt,

- welche Dokumenten-Templates für welche Dokumentengruppe (Direktive, Betriebsverfahren, etc.) zu verwenden sind
- wie die Dokumente zu benennen und inhaltlich zu „versionieren“ sind
- wer berechtigt (und verpflichtet) ist, nach einem Review vorgeschlagene Änderungen einzuarbeiten und zu übernehmen
- welchen Status ein Dokument in seinem Lebenszyklus einnehmen kann (von in Bearbeitung über Freigabe bis obsolet)
- wie die Freigabe und Ablage von Dokumenten zu erfolgen hat.

Wie viele kleinere und mittelständische Unternehmen verfügte auch POET nicht über ein eigenständiges Dokumentenmanagement System, das geeignet gewesen wäre, die organisatorischen Anforderungen auch technisch zu unterstützen. Aus diesem Grund wurde auf Basis eines Open Source Content Management Systems (CMS) eine ISMS Plattform geschaffen, die sowohl für die Projektgruppe als auch für die Mitarbeiter der POET als Informationszentrale genutzt werden konnte. Analog wurde eine fast identische Plattform bei PhonoNet aufgebaut.

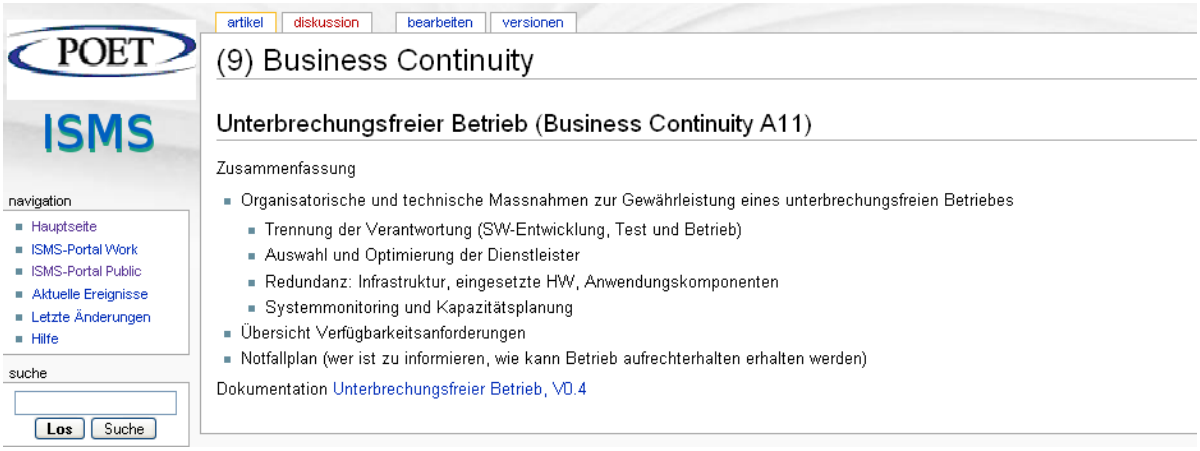


Abbildung 4: ISMS-Content Management System (Wiki)

Die Verwendung eines Content-Management-Systems bot u.a. folgende Vorteile

- Einfache Bereitstellung aller relevanten Informationen
- Schutz vor Veränderung durch Rechte-Profil
- Statistische Informationen direkt verfügbar (Änderungshistorie, wer hat die letzte Änderung eingespielt, frühere Fassungen etc.)
- Integrierte Suchfunktion erleichtert das Auffinden bestimmter Dokumente und Begriffe

Der Einsatz des CMS stellte sich als einfache, effektive und kostensparende Lösung heraus, die im weiteren Projektverlauf um Funktionen zur Ablagen von Schulungsinformationen, Protokollen und Nachweisen für durchgeführte Awarenessmaßnahmen u. ä. erweitert wurde.

3.3.2 ISMS Scope

Durch die große Flexibilität in der Handhabung des Standards ist dessen Anwendung für Unternehmen aller Größe und Branchen gleichermaßen möglich. Dies erfordert allerdings, dass das ISMS auf die jeweiligen unternehmens- bzw. bereichsbezogene Gegebenheiten angepasst wird.

Diese konkrete Ausgestaltung des ISMS, der sogenannte **Scope**, ist ebenfalls zu dokumentieren. Hier wird detailliert beschrieben, für welchen Regelungsbereich (einzelne Abteilung, Rechenzentrum, ganzes Unternehmen) das ISMS zuständig ist. Im Scope sollte ebenfalls die Abgrenzung des ISMS zu anderen Bereichen detailliert beschrieben sein, sowie welche Ausschlüsse es gibt, wie die Schnittstellen zu anderen Bereichen aussehen und wo bei diesen der Verantwortungsbereich des ISMS endet.

In konkreten Fall von POET waren folgende, stellvertretend für eine Reihe ähnlicher Fragen von Relevanz:

- Wie sieht der Verantwortungsbereich der POET aus, wenn der Kunde seine Systeme selbst administriert?
- Wo und abhängig von welchen Bedingungen endet die Verantwortlichkeit der POET auf Client-Seite?
- Ist die Softwareentwicklung Bestandteil des Scopes?
- Wie ist die Erbringung interne IT-Leistungen abzugrenzen?

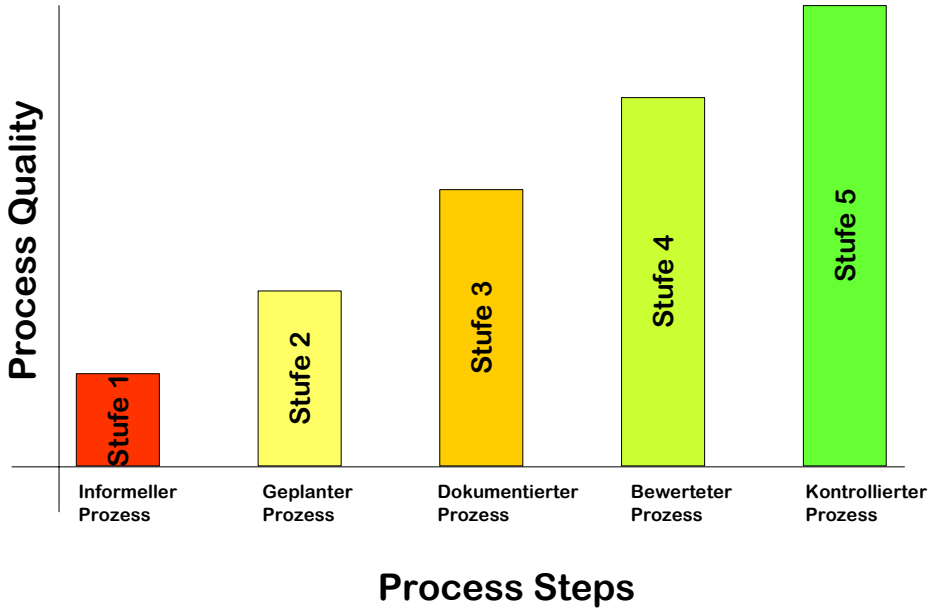
Der Scope sollte so detailliert wie möglich Antworten auf diese Fragen liefern, sodass bei einer späteren Zertifizierung die Auditoren auch eine passende und angemessene Prüfung vornehmen konnten.

3.3.3 Bestimmung des Status Quo

Der nächste große Projektschritt bestand darin, eine GAP-Analyse durchzuführen. Diese GAP-Analyse diente dazu festzustellen, welche ISMS relevanten Regelungen, Prozesse und Dokumentationen bereits vorhanden waren und in welcher „**Güte**“ diese vorlagen.

Schon während der Initialisierungsphase zeigte sich, das eine „einfache“ Beantwortung der BS 7799-2 Anforderungen („vorhanden“-„nicht vorhanden“/ „erfüllt“-„nicht erfüllt“) der Wirklichkeit bei POET (und wahrscheinlich der meisten anderen Firmen) nicht gerecht wurde.

Aus diesem Grund wurde beschlossen, in Anlehnung an SSE-CMM (System Security Engineering Capability Maturity Model [5]) und COBIT (Control Objectives for Information and related Technology [6]) sowohl für die zu etablierenden Prozesse als auch für die umzusetzenden Maßnahmen ein mehrstufiges Qualitätsschema zu verwenden. Diese Stufen sollten den aktuellen Umsetzungsgrad widerspiegeln und gleichzeitig dazu dienen, ISMS-Verbesserungen bereits während der Projektdurchführung zu dokumentieren.



Als vorteilhaft erwies sich, dass POET bereits etliche Betriebsprozesse in Analogie zu ITIL etabliert hatte (z.B. Configuration Management, Change Management, Incident Management). Weniger vorteilhaft war, dass diese Prozesse zwar gelebt wurden, aber leider nicht ausreichend dokumentiert vorlagen. Ein Missstand, der bis zur angestrebten Zertifizierung zu beheben war und dadurch auch Mehraufwand verursachte.

Die GAP-Analyse brachte auch einen Umstand zu Tage, der zwar als solcher schon in den Köpfen der Verantwortlichen schlummerte, aber bis dahin nicht offensiv angegangen worden war: Die Durchsicht einiger ASP-Verträge mit Kunden zeigte Schwächen in SLA (Service Level Agreement) Definitionen auf, die nun bereits zu einem sehr frühen Projektzeitpunkt identifiziert und behoben werden konnten.

Exemplarisch hierfür waren die Backup-Verfahren im Fehlerfall: Die SLAs enthielten zwar Regelungen zur Durchführungen von regelmäßigen Backups; wie aber vorgegangen werden sollte, falls das reguläre Backup (warum auch immer) nicht zur vereinbarten Zeit durchgeführt werden konnte, dazu fand sich keine Regelung. Sollte das Backup dann nach Feststellung des Problems (i. d. R. in den betreuten Betriebszeiten) durchgeführt werden, oder das Backup für den Zeitraum komplett ausfallen? Welche Auswirkungen auf den Produktionsbetrieb des Kunden könnte es haben, falls das Backup dann zu den betreuten Betriebszeiten ausgeführt wird? Muss eventuell mit Kapazitätsengpässen gerechnet werden?

Diese und weitere Fragen bedurften der Klärung und Fixierung in entsprechenden SLAs.

3.3.4 Risiko Management

Der BS 7799-2 basiert auf der Anwendung eines geeigneten Risk Assessments. Wie sehr viele dieser Standards krankt auch der BS 7799-2 an der Tatsache, dass der Standard zwar sagt, was getan werden muss, aber nicht wie. So verhält es sich auch in Bezug auf das Risiko Management: Der Standard fordert zwar einen systematischen Risiko Management Prozess und nennt auch einige Punkte, die in einer formalen Risiko Analyse zu berücksich-

tigen sind; wie dieser aber konkret auszusehen hat und zu implementieren ist, gibt der Standard jedoch nicht vor.

Das Risk Management dient dabei nicht nur der Vermeidung von Risiken; es sollte auch helfen, Risiken frühzeitig zu identifizieren, das damit verbundene Risikopotenzial zu evaluieren, frühzeitig korrigierende Maßnahmen zu ergreifen sowie die Entwicklung von Risiken zu kontrollieren.

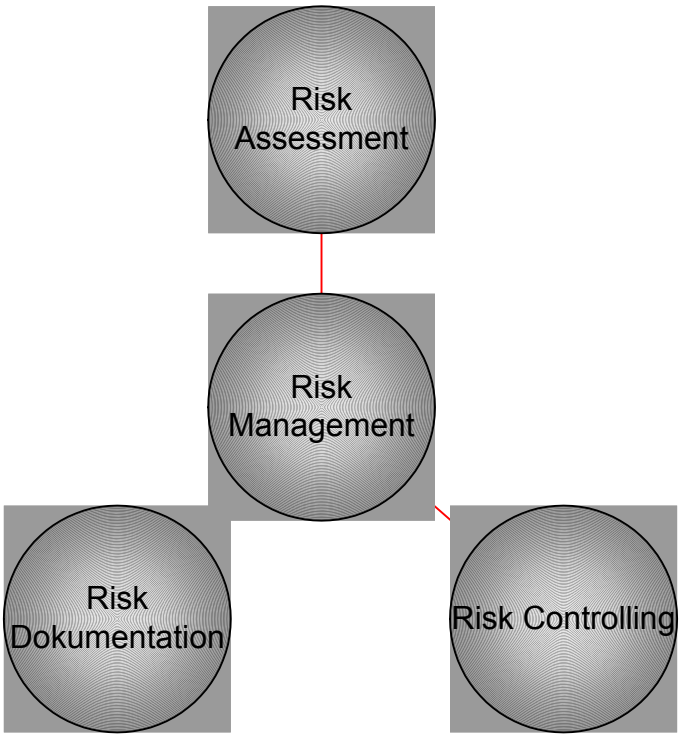


Abbildung 5: Risk Management Model

Das Risk Management basiert dabei auf der Durchführung einer auf die wichtigsten Geschäftsprozesse des Bereichs RZ fokussierten Business Impact Analyse (BIA). Die BIA dient dazu, den Schutzbedarf (Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität) der untersuchten Geschäftsprozesse zu ermitteln, die Abhängigkeiten von IT-Systemen aufzuzeigen und anschließend das Risikopotential zu bestimmen. Die BIA verfolgt dabei einen „top-down“ Ansatz, d.h. von den identifizierten Geschäftsprozessen zu den involvierten Anwendungen, Ressourcen und IT-Systemen. Ziel der Business Impact Analyse ist dabei die

- Erfassung der Geschäftsprozesse und Beurteilung ihrer Kritikalität,
- Darstellung der Abhängigkeiten der kritischen Geschäftsprozesse und der diese unterstützenden Anwendungen, Ressourcen und IT-Systeme,
- Erstellung einer Übersicht der jeweiligen Sicherheitsanforderungen (Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität),
- Festlegung des Schutzniveaus der kritischen Systeme (inklusive einer Beurteilung, ob Grundschutz gemäß des IT-Grundschutzhandbuchs des BSI ausreichend ist oder weitergehende Sicherheitsmaßnahmen ergriffen werden müssen), und
- Priorisierung der zu ergreifenden Maßnahmen nach ihrer jeweiligen Bedeutung und Dringlichkeit.

Abbildung 6 illustriert die generelle Vorgehensweise bei der Durchführung der Risiko Analysen.

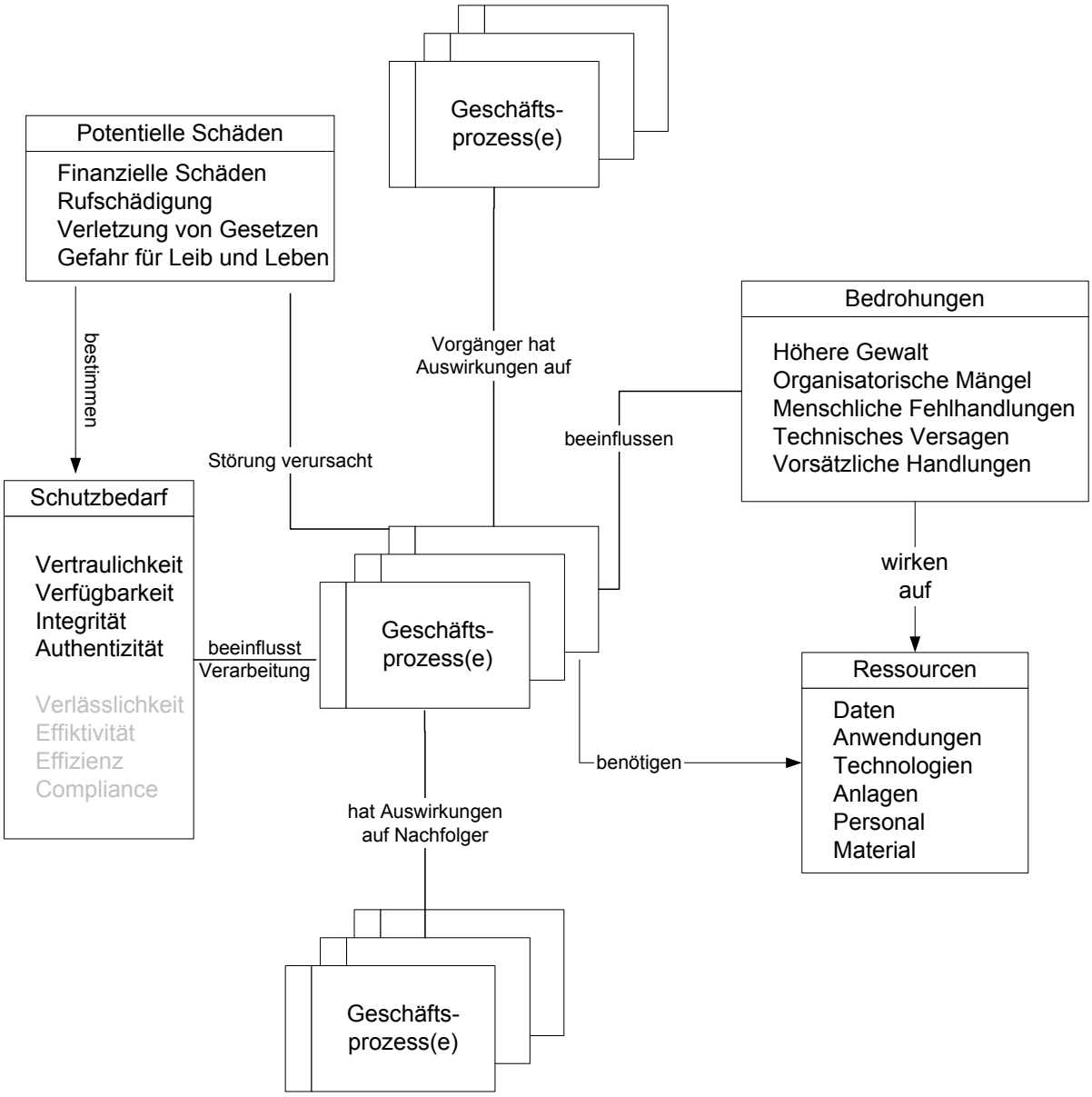


Abbildung 6: Prozessübersicht Risikoanalyse

Risikobestimmung, Maßnahmenauswahl und Kontrolle der Umsetzung erfolgte mit Hilfe eines Excel-Tools „ISMS_Risiko-Analyse“. In diesem Tool wurden erfasst:

- die Geschäftsprozesse
- die notwendigen Ressourcen
- die Anwendungen
- die IT-Systeme

Pro Ressource, Anwendung und IT-System kann für den Geschäftsprozess die grundlegende Kritikalität bestimmt werden. Des Weiteren ist es möglich, bereits bestehende risikominimierende Maßnahmen bei der Bewertung der Kritikalität zu berücksichtigen.

Hier zeigt sich, dass dem **Asset Management** im Rahmen von BS 7799-2 eine besondere Bedeutung beigemessen werden muss. Nur wenn die Assets, die Unternehmenswerte, vollständig bekannt sind, können diese auch angemessen im Rahmen einer Risiko Analyse be-

rücksichtigt werden. Aus Sicht des Autors ist deshalb die Erfüllung der Anforderung „A.5 Asset classificatio and control“ von BS 7799-2 (Managementgebiet 7 „Asset Management“ in ISO 17799:2005) eine unabdingbare Grundvoraussetzung. Dabei beschränkt sich die Definition von Asset nicht nur auf Hardware und Software, sondern umfasst alle relevanten Unternehmenswerte, bspw. auch Prozesse.

Abbildung 7 illustriert die Prozessschritte bei der Durchführung der Risiko Analyse.

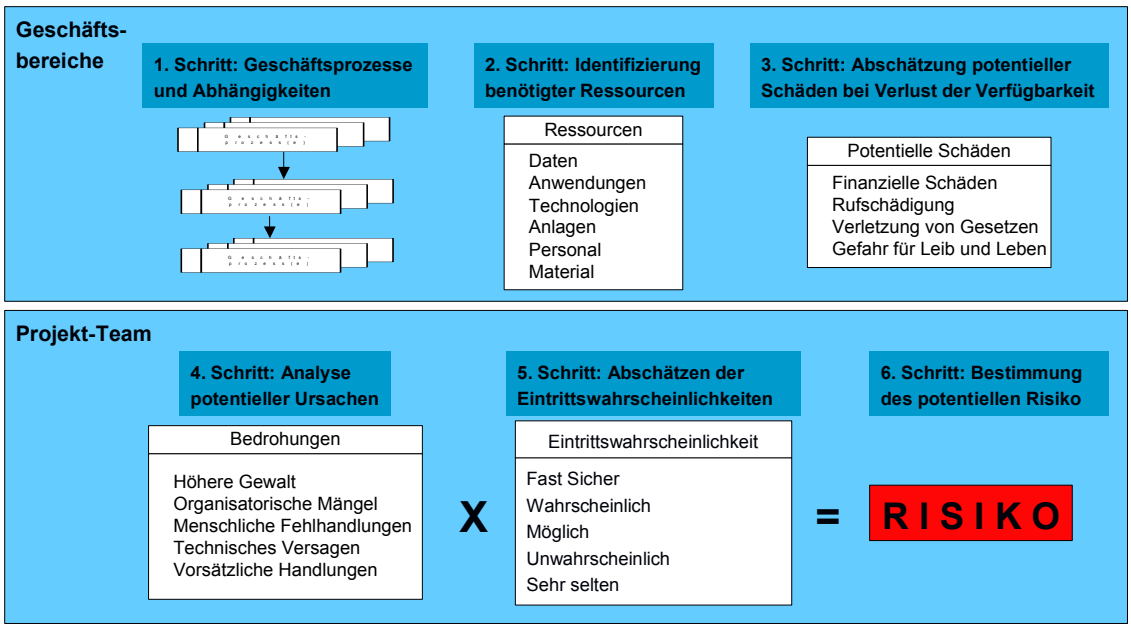


Abbildung 7: Methodik der Risko Analyse

- **Erfassung der Geschäftsprozesse**

Es wurden die relevanten Geschäftsprozesse erfasst, sowie deren Abhängigkeiten von vor- und nachgelagerten Prozessen. Dies diente zur Erkennung der Auswirkungen von Störungen innerhalb einer Prozesskette.

- **Identifizierung benötigter Ressourcen**

  Für jeden relevanten Geschäftsprozess wurden die benötigten Ressourcen identifiziert. Zu diesen können zählen:

  - Daten
  - Anwendungen
  - besondere Technologien
  - besondere Anlagen
  - Personal
  - Material

- **Festlegung der Auswirkungen**

Die Bedeutung der Geschäftsprozesse wurde anhand relevanter Schadensarten (z.B. finanzielle Schäden, Rufschäden, Vertrauensverlust, Verletzung von Datenschutzbestimmungen) in Abhängigkeit vom Schadenswert ermittelt. Hierbei wurde die folgende Tabelle herangezogen:

Wirkung	Definition
Unbedeutend	Es ist nicht zu erwarten, dass Störungen zu Schäden für das Unternehmen führen
Gering	Selbst mehrere Schäden dieser Art können vom Unternehmen gut verkraftet werden. Erst sehr viele solcher Schäden könnten die Existenz des Unternehmens bedrohen
Mittel	Mehrere Schäden dieser Art bedrohen die Existenz des Unternehmens
Groß	Ein Schaden in dieser Kategorie bedroht die Existenz des Unternehmens
Katastrophal	Ein Schaden dieser Kategorie führt zum Zusammenbruch des Unternehmens

- **Festlegung der Eintrittswahrscheinlichkeiten**

In Zusammenarbeit mit den Mitarbeitern des Bereichs wurden wesentliche, charakteristische Störfall- und Bedrohungsszenarien für die Prozesse identifiziert, die zur Beurteilung der Schadenshäufigkeit herangezogen wurden. Hierzu wurden relevante Lücken identifiziert, die zu Bedrohungsszenarien führen können.

Die Häufigkeit der Schäden wurden anhand der erarbeiteten Szenarien geschätzt. Um eine Vergleichbarkeit zwischen den Prozessen zu erreichen, erfolgte die Abschätzung der Häufigkeiten anhand einer Häufigkeitstabelle. Die folgende Tabelle wurde verwendet:

Eintrittswahrscheinlichkeit	Häufigkeit
Fast sicher	öfter als einmal pro Woche
Wahrscheinlich	öfter als einmal pro Monat
Möglich	öfter als einmal pro Jahr
Selten	öfter als einmal innerhalb von zehn Jahren
Sehr selten	seltener als einmal innerhalb von zehn Jahren

- **Risikobestimmung**

Das Risiko (Kritikalität) wird aus den Schadenswerten und Eintrittswahrscheinlichkeit abgeleitet. Hierzu wurde die folgende Risikomatrix angewendet:

Nach Festlegung der primären Kritikalität wurde, unter Berücksichtigung bereits bestehender Sicherheitsmaßnahmen, eine weitere Einstufung vorgenommen, die die Grundlage für die zu treffenden Entscheidungen bildete.

		Wirkung				
		Unbe-deutend	**Gering**	**Mittel**	**Groß**	**Katas-trophal**
Eintrittswahr-scheinlichkeit	**Fast sicher**	Mittel	Bedeutend	Hoch	Hoch	Hoch
	Wahrschein-lich	Mittel	Bedeutend	Bedeutend	Hoch	Hoch
	Möglich	Gering	Mittel	Bedeutend	Hoch	Hoch
	Selten	Gering	Mittel	Mittel	Bedeutend	Hoch
	Sehr selten	Gering	Gering	Mittel	Bedeutend	Bedeutend

- **Risikobehandlung**

Abschließend wurde festgelegt, welche Risiken als tragbar und welche als untragbar einzustufen sind. Hierbei wurde dokumentiert, durch wen und wann die Einstufung vorgenommen wurde. Sofern Maßnahmen zur Risikobehandlung ergriffen wurden, wurde dokumentiert, um welche Maßnahme es sich dabei handelte, wer für die Bearbeitung verantwortlich war, welchen Status die Umsetzung der Maßnahme hatte und wann die nächste Überprüfung der Umsetzung erfolgen würde.

Ziel der Risikobehandlung war es, alle identifizierten Risiken auf die Risikostufen „gering“ bis „mittel“ senken zu können. Hierzu waren in jedem Falle geeignete Maßnahmen aufzuzeigen und umzusetzen. Abweichend von dieser Regelung durften Risiken nur akzeptiert werden, wenn die zu ergreifenden Maßnahmen in einem extrem ungünstigen Kostenverhältnis stehen, so dass der potentielle Sicherheitsgewinn dadurch neutralisiert würde. Eine solche Entscheidung musste schriftlich durch das Management fixiert werden.

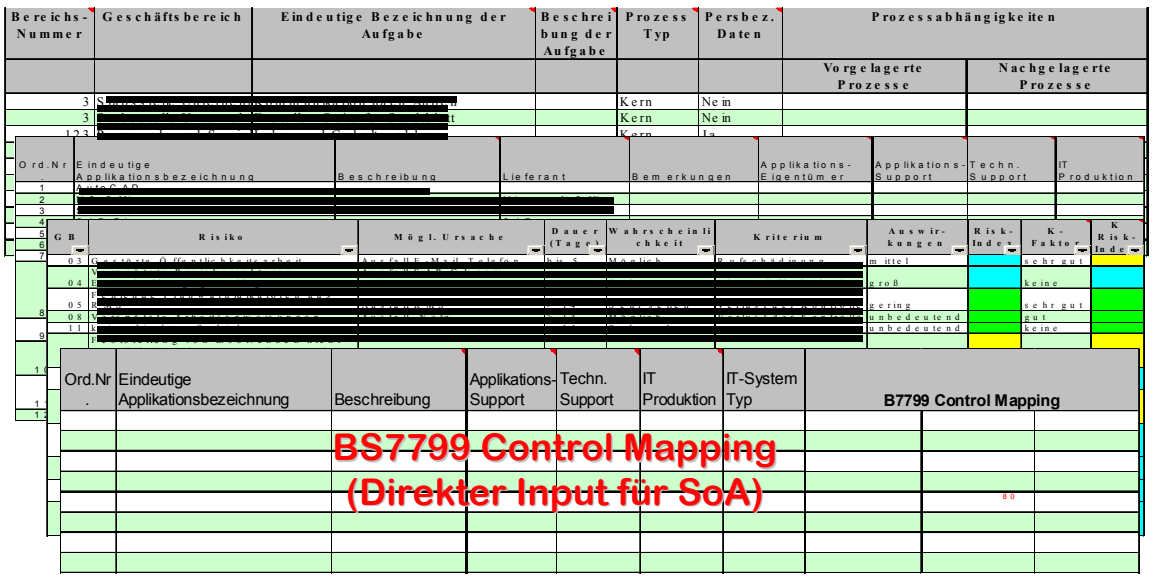


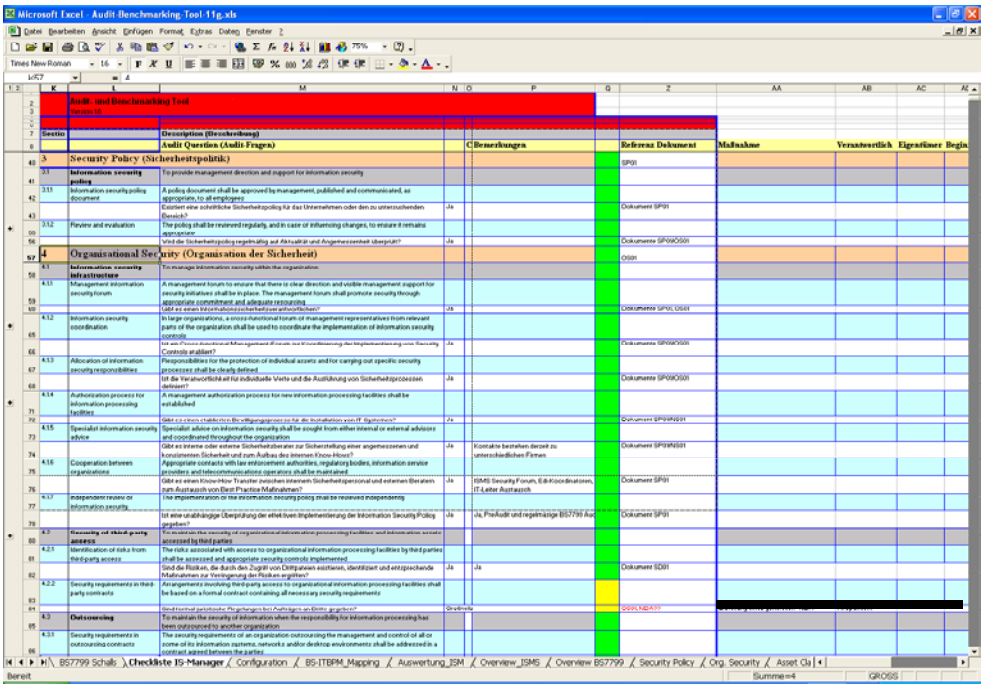
Abbildung 8: Risiko Management Tool

- **Risiko Management Prozess**

Es wurde definiert, von wem, wann und wie die Risikoanalysen durchzuführen sind, wie die Risiko-Reports auszusehen haben und wer die Risikobehandlung festzulegen hat. Des Weiteren wurde definiert, wie diese Analysen und der daraus resultierende Risk Treatment Plan zu dokumentieren und zu archivieren sind, damit auch bei späteren Kontrollen die Nachvollziehbarkeit von Entscheidungen, sowie die Verdeutlichung der Verbesserungen ersichtlich wird.

3.3.5 Statement of Applicability

Die Maßnahmenziele und Maßnahmen aus Annex A von BS 7799-2 sowie die Gründe für deren Auswahl oder deren Ausschluss mussten in einem sogenannten „Statement of Applicability“ (SoA) dokumentiert werden. Zur Erleichterung der Kontrolle der Auditoren im Rahmen der Zertifizierung ist es empfehlenswert darzulegen, in welchen Dokumenten die entsprechenden Regelungen fixiert sind, bzw. wo in der Risiko-Analyse festgestellt wurde, warum die Maßnahme nicht umgesetzt werden muss. Weitere Hinweise können zudem das Verständnis erleichtern.



© Secorvo

Im Rahmen des Projektes war es nicht möglich, alle erforderlichen Maßnahmen bis zum Zertifizierungstermin zu 100% umzusetzen. Aus Sicht des Autors war und ist dies auch nicht zwingend erforderlich, sofern plausibel und nachvollziehbar dargelegt werden kann, warum einzelne Maßnahmen noch nicht vollständig umgesetzt werden konnten (z.B. weil bevorstehende technische Änderungen der Infrastruktur erst abgewartet werden sollen) und dass die Umsetzung der Maßnahmen bereits geplant und im Tracking durch die Verantwortlichen ist. Dann steht einer erfolgreichen Zertifizierung nichts im Wege. Allerdings sollte man dann auch für das im folgenden Jahr anstehende Nachaudit entsprechend präpariert sein und die Umsetzung der geplanten Maßnahmen auch planungsgemäß vorangeschritten sein.

3.3.6 Tool Unterstützung

Im Vorfeld des Projektes wurde die Frage eingehend diskutiert, ob für die angestrebte Zertifizierung der Erwerb eines entsprechenden Software-Tools notwendig ist. Die Vorteile eines solchen Tools wurden insbesondere gesehen in:

- Unterstützung der Prozess- und Dokumenten-Workflows
- Unterstützung des Risk Managements
- Verwaltung der Assets
- Schnellerer Aufbau und effizientere Verwaltung des ISMS.

Aus diesem Grund wurden einige Tools auf ihre prinzipielle Eignung geprüft. Sehr schnell zeigte sich aber, dass im vorliegenden Fall der Einsatz einer entsprechenden Software sowohl aus finanzieller als auch organisatorische Sicht nicht uneingeschränkt zu befürworten war. Einige der Tools weisen eine recht „starre“ Vorgehensweise auf, die so nicht oder nur mit größeren Kompromissen einsetzbar gewesen wären.

Wie bereits geschildert wurde sowohl zur Dokumentenverwaltung als auch zur Publizierung der Dokumente, der internen Darstellung und Wissensvermittlung zum und über das ISMS, sowie der Dokumentation durchgeführter Trainings und Awarenessmaßnahmen ein Content Management System auf Open Source Basis genutzt. Die Wahl fiel dabei auf MediaWiki (http://www.mediawiki.org).

Die Risiko-Analyse wurde auf Basis eines Excel-Tools von Secorvo durchgeführt. Das Tool, das in ähnlicher Form bereits mehrfach für Risikoanalysen bei Kunden zum Einsatz kam, wurde dafür an die spez. Anforderungen von POET angepasst.

So war es bsplw. möglich, die Ergebnisse direkt als Reporting für das Management zu nutzen, sowie ein Tracking der anzugehenden Maßnahmen durchzuführen.

Auch die Verwendung dieses Tools wurde den allgemeinen Anforderungen an das Dokumentenmanagement unterstellt. So konnte auch später die Risiko-Entwicklung in der Historie analysiert werden. Allerdings zeigten sich hier erste Schwächen des Tools, denn dies konnte nicht durchgängig automatisiert erfolgen.

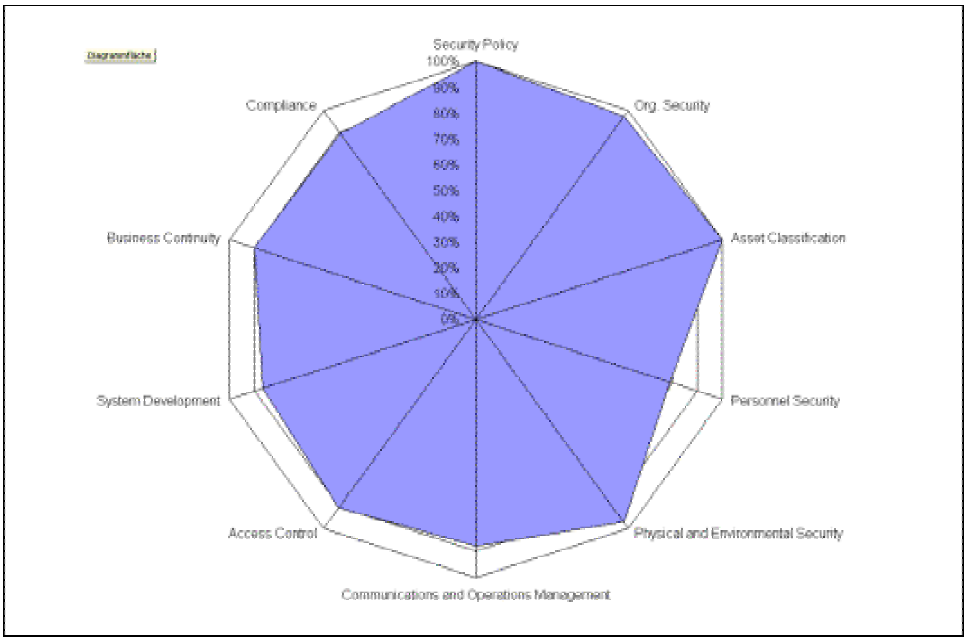


Abbildung 9: Übersicht Umsetzungsstatus Annex A

Die Durchführung der BS 7799-2 Self-Assessments erfolgten ebenfalls auf Basis von Excel Tools (siehe Abbildung 9), die von Secorvo zur Verfügung gestellt wurden. Neben der Möglichkeit, die Prozessqualität darzustellen, bot auch dieses Tool die Option, ein Tracking der anzugehenden Maßnahmen durchzuführen.

Die Verwendung dieser recht „einfachen" Tools wurden im Verlauf des Projekts durchgängig sehr positiv bewertet. Sie waren schnell und problemlos einzusetzen und von allen Mitarbeitern ohne Einarbeitung zu nutzen.

Einen Nachteil haben diese Tools allerdings: Nachdem BS 7799-2 durch den ISO 27001 Standard „abgelöst" wurde, müssen diese Tools entsprechend überarbeitet werden, was mit relativ viel Aufwand verbunden ist. Mit einem kommerziellen Produkt hätte sich dieser Aufwand vermeiden lassen.

3.3.7 Von BS 7799-2 nach ISO 27001

Bereits vor der Zertifizierung war abzusehen, dass zum Ende des Jahres der BS 7799-2 in einen ISO Standard überführt werden sollte. Um sicherzustellen, dass spätestens zum ersten Nachaudit nach einem Jahr die Umstellung auf ein ISO-Zertifikat möglich war, wurden bereits im Vorfeld verschiedene Vorkehrungen getroffen:

- die Definition des Scopes enthielt bereits eine entsprechende Abgrenzung und die Beschreibung von Schnittstellen sowie die Festlegung der entsprechenden Verantwortlichkeiten an diesen Schnittstellen;
- die Security Directives wurden analog zu ISO 17799:2005 erstellt;
- da entscheidende Prozesse bereits ITIL-konform aufgebaut waren, existierte bereits ein etablierter Incident Management Prozess;
- mit der Einführung und Messung von Qualitätsstufen für Prozesse und Maßnahmen wurde frühzeitig den Anforderungen des ISO 27001 an die Messbarkeit der Prozessperformance Rechnung getragen.

Die frühzeitige Berücksichtigung dieser Aspekte dürfte die Nachzertifizierung nach ISO 27001 um ein Vielfaches erleichtern.

4 Lessons Learned

Auch wenn dem BS 7799-2 gelegentlich vorgeworfen wird, ähnlich wie ISO 9000 sehr „dokumentenlastig" zu sein (und somit die Gefahr besteht, nur „Schrankware" zu produzieren), zeigt sich in der Praxis, dass man durch den Aufbau eines ISMS nach BS 7799-2 (ISO 27001) den unterschiedlichen Interessen und Anforderungen aller Verantwortlichen und Beteiligten in hervorragender Weise gerecht werden kann:

- Das Management
  benötigt standardisierte und dokumentierte Prozesse, sowie, wenn möglich, entsprechende Metriken zur Messung der Betriebs- und Projektperformance sowie zur Beurteilung der Effektivität und Angemessenheit von Informationssicherheit im Unternehmen
- Die Mitarbeiter
  benötigen im täglichen Betrieb konkrete Vorgaben, Anleitungen, HowTo's und Regelungen zu Sonderfällen zur Aufrechterhaltung eines kontinuierlichen Betriebs mit gleichbleibender Qualität

- Marketing und Vertrieb
  kann komplexe IS-Prozesse, -Regelungen und -Maßnahmen einfach darstellen und den Mehrwert für den Kunden verständlich und überzeugend aufzeigen
- Der Kunde
  hat die Gewissheit, dass Informationssicherheit nicht nur als Marketing-Floskel existiert. Prozesse, Regelungen und Umsetzung von Maßnahmen sind kontrollier-, prüf- und messbar. Die Definition entsprechender Service Level Agreements ist aufgrund standardisierter Prozesse einfacher möglich, Schnittstellen können klarer abgrenzt und entsprechende Verantwortlichkeiten konkreter festgelegt werden.

Bei der Implementierung von BS 7799-2 bzw. ISO 27001 muss immer die Angemessenheit der Umsetzung im Vordergrund stehen. Der Standard stellt zwar einerseits konkrete Anforderungen, die zu erfüllen sind, lässt aber andererseits die flexible Anpassung und Integration in bestehende Strukturen, Prozesse und Abläufe zu. Nicht die wortgetreue Umsetzung sollte im Vordergrund beim Aufbau eines ISMS stehen, sondern die Etablierung eines praxisnahen und praktikablen Lenkungsinstruments zur effizienten und effektiven Planung, Steuerung und Kontrolle angemessener Informationssicherheit im Unternehmen.

5 Literatur

[1] BS 7799-2:2002, Information security management — Part 2: Specification for information security management systems

[2] ISO/IEC 17799:2005, Information technology -- Code of practice for information security management, http://www.iso.ch

[3] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements , http://www.iso.ch

[4] Völker, Jörg: BS7799 Von Best Practice zum Standard, Secorvo Whitepaper, September 2005, http://www.secorvo.de/whitepapers/secorvo-wp10.pdf

[5] Systems Security Engineering Capability Maturity Model® SSE-CMM®, Model Description Document, Version 3.0, June 15, 2003 http://www.sse-cmm.org/index.html

[6] COBIT 4.0, Control Objectives Management Guidelines Maturity Models, IT Governance Institute