Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Bachelorarbeit

Daniel Conta

Leitfaden eines mandantenunabhängigen Identity Access Management

Fakultät Technik und Informatik
Studiendepartment Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Daniel Conta

Leitfaden eines mandantenunabhängigen Identity Access Management

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung

im Studiengang Bachelor of Science Wirtschaftsinformatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Rüdiger Weißbach
Zweitgutachter: Prof. Dr. Klaus-Peter Kossakowski

Eingereicht am: 13. Februar 2017

Daniel Conta

Thema der Arbeit
Leitfaden eines mandantenunabhängigen Identity Access Management

Stichworte
Identitätsmanagement, BDSG, Berechtigungssteuerung, GoBD, ISO 20000, ISO 27000, ISO 31000, IT-Compliance, IT-Governance, IT-Grundschutz, KonTraG, Rechteverwaltung, Rollenmodell, Zugriffskontrolle, Zugriffsrechte

Kurzzusammenfassung
Die immer zur Verfügung stehende Möglichkeit, fast überall auf der Welt Informationen zugänglich zu machen, konfrontiert Unternehmen damit, ihre sensiblen Informationen sowohl nach innen als auch nach außen abzuschirmen. Die Arbeit zeigt auf, mit welchen Methoden und Werkzeugen ein Identity Access Management den generellen Zugang zu Informationen unterbindet und gleichzeitig zu der unternehmensweiten Compliance beiträgt.
Daniel Conta

Title of the paper
Guide about an Identity Access Management

Keywords
Access control, access control list, access management, COBIT, ITIL, ITIL Service Operation, RBAC model, role based, SOX, access right, authorisation, identity management, role model

Abstract
The permament opportunity to share useful information around the world is the reason why companies around the world need to expand their internal and external safety. This bachelor thesis illustrates which methods and tools can be applied in the context of Identity Access Management to prevent uncontrollable data access and simultaneously help to strengthen Corporate Compliance.

Erklärung über die selbständige Abfassung der schriftlichen Arbeit

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, 13. Februar 2017 Daniel Conta

Inhaltsverzeichnis

1 Einleitung

In der heutigen Zeit wächst der Einfluss der Informationstechnologie oder Informationstechnik (IT) auf die Gesellschaft und auf Unternehmen, die unter den unterschiedlichsten Rechtsformen firmieren. Es besteht zu jeder Zeit die Möglichkeit, über den elektronischen Weg in Interaktion zu treten, beispielsweise durch Textnachrichten, Sprachmitteilungen und visuelle Momentaufnahmen wie Bilder und Videos. Die IT ist in vielen Haushalten zu einem festen Bestandteil des Alltags geworden. Der Verzicht auf Smartphones, Notebooks, Personal Computer (PC), Fernseher und Radios, ist für den Autor dieser Arbeit ein unwirklicher Gedanke. Es ist daher nur ein konsequenter gedanklicher Schritt, sich die Frage zu stellen: "*Wer nimmt an den weltweiten Interaktionen teil?*" und "*Gibt es einen Mechanismus zum Schutz von Informationen?*"
Die immer zur Verfügung stehende Möglichkeit, fast überall auf der Welt Informationen zugänglich zu machen, ob visuell oder auditiv, ist der Garant für das Wachstum und die Verdichtung der weltweiten Globalisierung. Ein international agierendes Unternehmen kann in der heutigen Zeit kaum auf eine IT-Infrastruktur verzichten. Die Produkte und Dienstleistungen werden immer vielfältiger und komplexer und die Anzahl an Wettbewerbern immer größer. Täglich entsteht eine Vielzahl an innovativen Ideen und Lösungen, unabhängig von der Motivation der Entwickler und Investoren. Es ist daher nur eine logische Konsequenz, dass Unternehmer und Vorstände mit der Problematik konfrontiert werden, sensible Informationen ihrer Unternehmenssubstitutionen sowohl nach innen als auch nach außen abzuschirmen. Das Identity Access Management (IAM) setzt an dem Punkt an, ab dem der unkontrollierte Informationsfluss und der generelle Zugang zu Informationen unterbunden werden muss und nur kontrolliert erteilt werden darf.
Daher stehen im Kapitel *Anforderungen, Gesetze und Normen* die Beweggründe für ein IAM im Fokus. Ein naheliegender Schluss aufgrund sicherheitsrelevanter Aspekte ist, dass zentrale Gesetze Vorgaben für ein IAM enthalten und im Detail eine Umsetzung vorgeben. Daraus folgt die...

Erste Zielsetzung:
Es gilt zu zeigen, dass ein Identity Access Management durch eine Vielzahl direkter und indirekter Forderungen aus Gesetzen, Normen und Regularien geprägt wird.

Im weiteren Verlauf der gegenständlichen Arbeit soll ein Grundverständnis geschaffen werden, das *grundlegende Elemente* des IAMs erläutert und in Verbindung zu den Forderungen setzt.

Zweite Zielsetzung:
Es gilt zu zeigen, welche Elemente des Identity Access Managements zur Erfüllung der Forderungen beitragen.

Der weitere Teil konzentriert sich auf die prozessuale Anwendung des IAMs in der Unternehmenslandschaft und verdeutlicht den Einfluss von ITIL, der Information Technology Infrastructure Library. Weiter wird der Teil durch die Erfahrungen des Autors der gegenständlichen Arbeit ergänzt, die im Rahmen des Projekteinsatzes bei Wincor Nixdorf Global IT Operation GmbH im Access Management gewonnen wurden.

Dritte Zielsetzung:
Die Erarbeitung eines konzeptuellen Vorgehenmodells zur Implementierung eines Identity Access Managements, an das beliebige Kunden und Dienstleister angebunden werden können und damit mandantenunabhängig zur Verfügung steht.

Zum Abschluss erfolgt die Erarbeitung einer Fragestellung, mit welcher der Autor die Arbeit als Anregung für wissenschaftliche Aufbereitungen rund um die IAM-Thematik stehen lassen wird.

2 Anforderungen, Gesetze und Normen

Der vorliegende Teil dieser Arbeit erläutert die grundlegende Forderung nach Gesetzes- und Anforderungskonformität an Unternehmen. Dazu ist zu Beginn die Begriffseinführung von Corporate Governance und -Compliance notwendig. Sowohl Abgrenzung und Zusammenspiel werden erörtert und ermöglichen damit den Einstieg in die Explikationen der wichtigsten Gesetze und Verordnungen für die IT-Governance und IT-Compliance. Gleichermaßen wichtig ist darauf aufbauend die Bezugnahme, welche gesetzlichen Forderungen ein Identity Access Management zu erfüllen hat und welche Gesetze dies erforderlich machen.

2.1 Corporate Governance und -Compliance

Nach[1]*S.3* wird Corporate Governance als rechtlicher und faktischer Ordnungsrahmen für die Leitung und Überwachung des Unternehmens als Kurzform zusammengefasst. Im Ordnungsrahmen lässt sich unterscheiden zwischen der Unternehmensverfassung, die primär die Binnenordnung des Unternehmens beschreibt und rechtlichen Vorgaben wie Gesetze und Verordnungen. Bei der Betrachtung von Corporate Governance Aspekten nach[1]*S.4* wird in interne und externe Governance-Perspektiven unterschieden. Die Innensicht befasst sich mit den Rollen, Kompetenzen, Funktionsweisen und regelt das Zusammenwirken der Unternehmenssubstitutionen wie Vorstand, Aufsichtsrat und Hauptversammlung. In der Außensicht steht das Verhältnis zwischen dem Topmanagement und dem Teilhaberkreis des Unternehmens, wie z.B. den Aktionären oder Investoren, im Mittelpunkt. Unter dem Begriff Corporate Governance kann demzufolge die Bündelung aller internationaler und nationaler Gesetze, Vorschriften, Werte und Grundsätze verstanden werden, die im Unternehmensalltag gelten und diesen bestimmen, sowie darüber hinaus die Mechanismen, die die Einführung, Anwendung und kontinuierliche Überwachung regeln. Aus[1]*S.18* können folgende Prinzipien, in Abbildung 2.1 aufbereitet, in den Mittelpunkt der Corporate Governance gestellt werden:

- **Transparenz**
  Verringerung von Informationssymmetrien zwischen den Unternehmenssubstitu-

tionen. Durch transparente Austauschprozesse kann die Integrität der Unternehmensleitung und das Vertrauen in das Unternehmen gegenüber dem Teilhaberkreis gestärkt werden.

- **Gewaltenteilung**
  Verteilung der Verfügungsrechte auf verschiedene Akteure, sodass Machtmonopole verhindert werden. Darüber hinaus formelle und transparente Verfahren zur Benennung und Wahl von Kontrollgremien und Aufsichtsratsmitgliedern.
- **Eindämmung von Interessenkonflikten**
  Besonders hohe Gefahr besteht bei den Trägern von Verfügungsrechten wie dem Top-Management. Hier soll ein transparenter Umgang mit Konfliktlagen einem Interessenkonflikt entgegenwirken, wie beispielsweise einem Konflikt zwischen den Abschlussprüfern und Aufsichtsratsmitgliedern, deren Interessen gegensätzlich sein können. Weiterhin gilt die transparente Ausrichtung von Managemententscheidungen auf die langfristige Wertschöpfungskette als weitere Möglichkeit zur Eindämmung von Animositäten.
- **Unabhängigkeit der Unternehmensorgane**
  Dies betrifft die Forderung nach Unabhängigkeit und Fokussierung auf das übergeordnete Unternehmenswohl und den angemessenen Umgang mit Risiken.

Abbildung 2.1: Gewaltenteilung und Unabhängigkeit der Unternehmensorgane

Zusammengefasst: Im Rahmen dieser Arbeit wird folglich für Corporate Governance festgehalten[1]*S.33*: *"Corporate Governance ist der Prozess der Steuerung des Unternehmens zur Sicherstellung eines Interessensausgleichs zwischen den Anspruchsgruppen durch transparente Regeln und Kontrollmechanismen in unternehmerischen Abläufen und Entscheidungen. Der Prozess dient der Sicherstellung des Fortbestands des Unternehmens und unterliegt externer Prüfung."*
Corporate Governance ist damit ein Prozess, der das Unternehmen steuert und einen Interessenausgleich schafft zwischen den Unternehmensorganen. Dieser sichert damit den Fortbestand des Unternehmens und wird von außen geprüft.

Corporate Compliance

Die Begriffsauffassung der Corporate Compliance umfasst in erster Linie Handlungen und Entscheidungen im Einklang mit geltenden Gesetzen, Regularien und Normen. Dies gilt für natürliche und juristische Personen und resultiert unter anderem aus dem deutschen Aktiengesetz[2]*§1 Wesen einer Aktiengesellschaft für Aktiengesellschaften* und aus dem deutschen Gesetz betreffend die Gesellschaften mit beschränkter Haftung[3] *§13 Abs. 1-3.* Die Unternehmensführung ist dazu verpflichtet, durch das Gesetz über Ordnungswidrigkeiten[4], gegenüber den Verwaltungsbehörden des Bundes, der Länder und der Gemeinden sowie anderen Körperschaften und Anstalten des öffentlichen Rechts, dafür Sorge zu tragen, dass aus dem Unternehmen heraus keine Gesetzesverstöße erfolgen. Neben der Einhaltung von Gesetzen und Normen im Alltag des Unternehmens sind selbst auferlegte Verfassungen, Richtlinien, Vereinbarungen oder ein geltender Kodex einzuhalten. Folgende Definition von Compliance umfasst die wichtigsten Punkte[5]*S.50*: *"Der Begriff Compliance steht für die Einhaltung von gesetzlichen Bestimmungen, regulatorischer Standards und Erfüllung weiterer, wesentlicher und in der Regel vom Unternehmen selbst gesetzter ethischer Standards und Anforderungen."*
Damit stellt Corporate Compliance einen Unternehmensstatus dar, der sich auf die Erfüllung gesetzlicher und selbst auferlegter Anforderungen bezieht. Im Rahmen dieser Arbeit soll die Begriffsauffassung der Corporate Compliance erweitert werden, unter Berücksichtigung der Aspekte aus[6]*S.34*:
[7]*:"Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance)."*
Damit trägt der Vorstand die Verantwortung hinsichtlich Compliance oder Non-Compliance.

[8]*S.73: "Handlungsweisen, die entweder dem Unternehmen verbindlich vorgegeben oder durch das Unternehmen selbst eingefordert werden, um die angestrebte Normkonformität zu sichern und nachzuweisen."*
Compliance besteht also erst, wenn Anforderungskonformität nachgewiesen und dokumentiert worden ist.

[9]*S.2: " (...) bedeutet in etwa: Einhaltung, Befolgung, Übereinstimmung, Einhaltung bestimmter Gebote. Damit verlangt Compliance zunächst nur, dass sich Unternehmen und Organe im Einklang mit geltendem Recht bewegen müssen."*
Damit ist Compliance für Unternehmen ein verbindlicher Status, der zu jeder Zeit erfüllt sein muss.

[10]*S.2: "Compliance steht (...) für die Einhaltung von gesetzlichen Bestimmungen, regulatorischen Standards und die Erfüllung weiterer wesentlicher Anforderungen der Stakeholder."*
Somit wird die Konformität um die Anforderungen aus dem Teilhaberkreis eines Unternehmens erweitert.

[11]*S.4: "Gesetze, Verordnungen, Reglemente, Rundschreiben und Standesregeln sowie allgemein anerkannte bzw. anerkennungswürdige Geschäftsgrundsätze müssen von der Unternehmung, vom Management und von allen Mitarbeitenden eingehalten werden."*
Damit gilt der Grundsatz der Anforderungskonformität für alle Unternehmensbeteiligten.

[12]*S.646: "Compliance umfasst die Gesamtheit aller Maßnahmen, um das rechtmäßige Verhalten aller Unternehmen, ihrer Organmitglieder, ihrer nahen Angehörigen und der Mitarbeiter im Blick auf alle gesetzlichen Gebote und Verbote zu gewährleisten."*
An dieser Stelle wird die Konformität jeder Maßnahme, die zur Compliance beiträgt, verbindlich.
In Anlehnung an[6]*S.34-35* ist die Erweiterung der Begriffsauffassung von Corporate Compliance ein konsequenter Schluss, da die Handlungen des Unternehmens auf verschiedenen Compliance-Arten beruhen:

1. Gesetzliche Compliance in Bezug auf internationale und nationale Gesetze, sowie Normen und branchenspezifische Verschärfungen. In Abschnitt 2.6 verdeutlicht.

2. Kommerzielle Compliance bezüglich vertraglicher Pflichten gegenüber den Vertragspartnern und Vereinbarungen in Kooperationsverträgen.

3. Organisatorische Compliance in puncto selbst auferlegter Qualitäts- und Wertmaßstäbe des Unternehmens, erweitert um Normen und Vorschriften.

Aus der zuvor getroffenen Differenzierung wird die Begriffsauffassung wie folgt erweitert: [6]*S.35 "Corporate Compliance bezeichnet die Auswahl und Bewertung der für das jeweilige Unternehmen relevanten Anforderungen und den Zustand der Anforderungskonformität unter Berücksichtigung verschiedener Anspruchsgruppen des Unternehmens."*

Zusammengefasst: Compliance, aufbereitet in Abb. 2.2, beinhaltet alle relevanten Anforderungen verschiedener Anspruchsgruppen mit dem Ziel einer unternehmensweiten Erfüllung durch Transparenz und Kontrollen.

Abbildung 2.2: Anforderungen und Ziele an die Compliance-Konformität

Abgrenzung Governance und Compliance

Corporate Governance wird in dieser Arbeit als Prozess zur Steuerung betrachtet mit dem Ziel eines Interessenausgleichs zwischen den Teilhabern und Unternehmenssubstitutionen. Dabei stehen transparente Regeln und Kontrollen der Geschäftsprozesse im Vordergrund. Corporate Compliance dagegen wird in dieser Arbeit als die Sicherstellung von Gesetzes- und Anforderungskonformität betrachtet und stellt damit einen Unternehmenszustand dar, in Bezug auf die Einhaltung oder Verletzung geltender Gesetze und unternehmensinterner Richtlinien. In der Bekanntmachung vom 24. Juni 2014[13] des Deutschen Corporate Governance Kodex (DCGK) und BMJV ordnet dieser dem Vorstand die Verantwortung der Aufrechterhaltung der Corporate Compliance, folglich eine Gesetzeskonformität, eindeutig zu. In[6]*S.35-36* erfolgt daraus, dass Corporate Governance ein in der gesamten Unternehmensweite verankerter Prozess ist und damit eine Vielzahl von Maßnahmen etabliert. Das Ziel dieser Maßnahmenbündelung ist die Anforderungserfüllung und Gesetzestreue, d.h. das Erreichen von Corporate Compliance. Siehe grafische Darstellung 2.3.

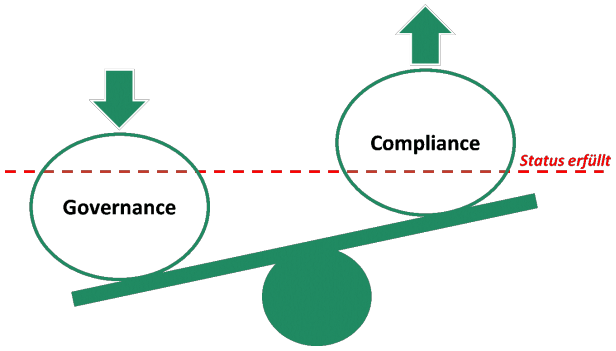

Abbildung 2.3: Governance Prozess zur Compliance-Konformität

2.2 IT-Governance und -Compliance

In[6]*S.35-36* wird von einer Unschärfe in der wissenschaftlichen Literatur gesprochen in puncto IT-Governance und IT-Compliance. An dieser Stelle der Arbeit sollen Corporate-Governance und Compliance weiter spezifiziert und konkretisiert werden, in Hinblick auf die im Unternehmen eingesetzte Informationstechnologie oder Informationstechnik (IT).
"IT-Governance ist ein Prozess der verantwortungsvollen Steuerung von IT, der durch transparente Regeln und Kontrollmechanismen die optimale Unterstützung der Geschäftsprozesse durch IT sicherstellt. IT-Governance befasst sich mit dem (1) Wertbeitrag der IT, dem (2) IT-Risikomanagement und der (3) IT-Compliance." [6]S.37
Aus diesem Zitat erfolgt der Rückschluss, dass IT-Governance jene Prozesse umfasst,

die sich vorrangig mit der Steuerung der IT im Unternehmen befassen.

"IT-Compliance bezeichnet den Zustand der Anforderungskonformität der IT selbst und die Umsetzung von Anforderungskonformität mit IT-Unterstützung." [6]S.37
Hiermit ist der Bezug zur Konformität hergestellt, welche sich auf die Erfüllung von Anforderungen an die IT bezieht.

Zusammengefasst: Das in den Zitaten entwickelte Verständnis macht deutlich, dass IT-Compliance durch einen in der gesamten Unternehmensweite etablierten IT-Governance-Prozess erreicht werden kann. Im näheren Fokus der IT-Governance steht das IT-Risikomanagement, welches im weiteren Verlauf der Arbeit noch aufgegriffen wird.

Referenzframework COBIT

Control Objectives for Information and Related Technology (COBIT) ist ein Governancemodell für die Implementierung des Prozess mit Maßnahmen und Vorgehensweisen[14]. Im Mittelpunkt stehen dabei Steuerungsvorgaben, Kontrollziele und das daraus resultierende IKS (Internes Kontrollsystem). COBIT unterstützt die Einführung und Aufrechterhaltung einer Ordnung innerhalb der Prozesse der IT-Landschaft im gesamten Unternehmen[15]*S.255-232*. Damit kann COBIT speziell als Referenzframework für die IT-Governance verstanden werden, um IT-Compliance im Unternehmen zu erreichen[16]*S.1-13*. Die fünf Prinzipien aus der Version COBIT5 vom April 2012[14]*S.15*, liefern einen strukturellen Überblick:

- Einbindung aller Unternehmensbeteiligten und Anforderungen
- Schutz des Unternehmens
- Integration und Anwendung eines einheitlichen Frameworks
- Anwendung eines einheitlichen Ansatzes
- Trennung von Governance und Management

Ergänzend die sieben Enabler-Kategorien nach[14], die als Faktoren und Ressourcen zur Realisierung der Unternehmensziele verstanden werden:

- Prinzipien, Richtlinien und Rahmenwerke
- Prozesse
- Organisationsstrukturen
- Kultur, Ethik und Verhalten
- Informationen

- Services, Infrastruktur und Anwendungen
- Mitarbeiter, Fähigkeiten und Kompetenzen

Das Framework wurde 1996 von einem Verband internationaler IT-Prüfer[17], der Information Systems Audit and Control Association (ISACA), entwickelt. Es diente vorrangig als Werkzeug der Prüfer zur Auditierung von Unternehmen und entwickelte sich erst mit der Zeit zu einem Werkzeug des Unternehmens zur Erfüllung der IT-Compliance.

Referenzframework ITIL

Parallel zu dem unter 2.1 aufgeführten Referenzframework COBIT kommt der "De-Facto-Standard" Information Technology Infrastructure Library (ITIL) zum Einsatz. Dieses Referenzframework bietet spezielle "Best-Practices" für das IT-Service-Management. Im Abschnitt 2.5.2, analog zur ISO 20000-Serie, wird ITIL näher erläutert.

2.3 Motivationsgründe für das IAM

Die Analyse der Anforderungen, Gesetze und Normen ergab, dass in wenigen Passagen, in Bezug auf ein "allumfassendes" IAM, direkte Forderungen zu finden sind. Wird der Fokus auf die grundlegenden Elemente gerichtet, lassen sich deutlich mehr konkrete Anforderungen und Vorgaben ermitteln, die von dem Autor als indirekte Forderungen im Rahmen der Arbeit aufgefasst werden. Im nachfolgenden Abschnitt erfolgt die Auflistung der Impulse für ein IAM. Die Analyse und Nachweiserbringung der Fundstellen ist in den Abschnitten 2.4-2.7 zu finden.

- **SOX/EuroSox aus Abschnitt 2.4.1:**
  - *direkt*: Berechtigungsvergabe, Transaktions-Monitoring, Funktionstrennung
  - *indirekt*: IT-Kontrollen, Dokumentationspflicht

  Die grundsätzliche Forderung der Berechtigungsvergabe in Sarbanes Oxley Act (SOX) und EuroSOX, verschärft durch die indirekten Forderungen, macht die Einführung und Anwendung der Berechtigungssteuerung und Zugriffskontrolle erforderlich. Kontrollen und Dokumentationen sind erst möglich, wenn Aufgaben, Rollen und Berechtigungen eindeutig definiert sind.
- **KonTraG aus Abschnitt 2.4.2:**
  - *direkt*: keine
  - *indirekt*: Angemessenes Enterprise Risk Management (ERM), Erhöhung der Transparenz

Das Gesetz zur Kontrolle und Transparenz (KonTraG) fordert ein angemessenes ERM neben dem internen Kontrollsystem (IKS) und Transparenz über die Verteilung von Verantwortung und Aufgaben. Unbehelligter Zugriff auf sensible und sicherheitsrelevante Informationen würde im Enterprise Risk Management (ERM) als Risiko identifiziert werden. Eine daraus entstehende Maßnahme wäre demzufolge die Einführung einer Zugriffskontrolle und Berechtigungssteuerung. Diese Möglichkeit wird als indirekte Forderung verstanden.

- **GoBD aus Abschnitt 2.4.3:**
  - *direkt*: Zugriffskontrolle und Berechtigungskonzepte im Rahmen des IKS für transparente und nachvollziehbare Bewegung und Veränderungen von Informationen
  - *indirekt*: Definition von Verantwortlichkeiten und ein etabliertes IDM

  Durch die GoBD entsteht, mit den Vorgaben zum IKS, betreffend der Zugriffskontrolle auf Basis von Berechtigungskonzepten, eine direkte Forderung ein IAM zu etablieren. Ebenfalls entsteht indirekt der Bedarf nach einem Identitätsmanagement (IDM) durch die Vorgabe, dass die Veränderungen von Daten einem Benutzer eindeutig zugeordnet werden müssen.
- **BDSG aus Abschnitt 2.4.4:**
  - *direkt*: Zutritt- und Zugangskontrolle, Zugriff- und Weitergabekontrolle, Eingabekontrolle und Funktionstrennung
  - *indirekt*: Berechtigungskonzepte

  Das Bundesdatenschutzgesetz (BDSG)[18] gibt vor, dass personenbezogene Daten in IT-Systemen, Geschäftsprozessen und bei der Auftragsverarbeitung vor Missbrauch geschützt und zweckgebunden verarbeitet werden müssen. Damit setzt das BDSG in Deutschland direkte Forderungen, ein IAM zu integrieren.
- **IT-Grundschutz aus Abschnitt 2.7.4:**
  - *direkt*: Baustein[19]*B 1.18* Identitäts- und Berechtigungsmanagement
  - *indirekt*: Grundschutzkatalog: Software und Kommunikation sowie Organisation und Personal. Hinzukommend generierte Anforderungen aus der Schutzbedarfsfeststellung.

  Der IT-Grundschutz soll kostengünstig gegen elementare Gefährdungen schützen. Dazu bietet dieser standardisierte Schutzbedarfsfeststellungen und Risikoanalysen. Wird während der Sicherheitsanalysen der Baustein[19]*B 1.18* als notwendig eingestuft, ist eine Akkreditierung nur noch nach dessen Implementierung und

Integration möglich. Damit entsteht an dieser Stelle eine direkte Forderung nach einem IAM.

- **ISO 9000-Serie aus Abschnitt 2.5.1:**
  - *direkt*: keine
  - *indirekt*: Einbeziehung beteiligter Personen, prozessorientierter Ansatz und Leistungsverbesserung

  Eine Leistungsverbesserung kann erzielt werden, wenn alle beteiligten Personen vollständig eingebunden sind. Mit der Definition und Zuweisung von Verantwortung, Zuständigkeit und Geschäftsrollen wird sichergestellt, dass relevante Personen einbezogen werden und damit eine Leistungsverbesserung ermöglicht wird. Das IAM setzt die getroffenen Definitionen und Zuweisungen durch Berechtigungskonzepte und Zugriffssteuerung organisatorisch um und schafft damit den Rahmen zur Erfüllung der Anforderungen.
- **ISO 20000-Serie aus Abschnitt 2.5.2:**
  - *direkt*: Festlegung von Rollen und Verantwortlichkeiten
  - *indirekt*: Konstante Kontrollelemente, Steuerungsprozesse, Plan-Do-Check-Act-Zyklus (PCDA-Zyklus) und Kontinuierlicher Verbesserungsprozess (KVP)

  Das IAM setzt festgelegte Rollen und Verantwortlichkeiten in den System- und Netzwerkumgebungen um. In Bezug auf die Zugriffskontrolle stellt dieses ein wichtiges Kontrollelement dar und strukturiert den Umgang mit Geschäftsrollen durch deren Abbildung in der virtuellen Umgebung. Aufgrund dieser Schnittstelle werden Rollen im Unternehmen kontrolliert, hinterfragt, angepasst und fördern damit indirekt den KVP.
- **ISO 27000-Serie aus Abschnitt 2.5.3:**
  - *direkt*: Einführung und Anforderungen eines Information Security Management System (ISMS), Verfolgung eines risikobasierten Ansatzes
  - *indirekt*: Berücksichtigung von Risiken innerhalb der Organisation, Kontrollmechanismen für die Informationssicherheit (IS)

  Ein Bindeglied zur IS ist das IAM, da an dieser Stelle der Zugriff auf Informationen erteilt wird. Identifizierte Risiken können bereits durch eine konsequente Berechtigungssteuerung kontrolliert werden. Die ISO 27002:*9 Access control* enthält Vorgaben und Empfehlungen für die Einführung eines IAMs. Demnach entsteht an dieser Stelle eine direkte Forderung.
- **Basel II-III aus Abschnitt 2.6.1:**
  - *direkt*: keine

  - *indirekt*: Erhöhung der Qualität, Konsistenz und Transparenz der Eigenkapitalbasis

  Mit einem Identitätsmanagement und einer Berechtigungssteuerung werden die Werte der Organisation vor unbefugtem Zugriff in der virtuellen Umgebung geschützt. Folglich wird dadurch eine qualitative Eigenkapitalbasis gefördert, die durch die Werte und Güter des Unternehmens erzeugt wird. Das IAM hat einen erheblichen Anteil an der "Grundsicherheit" der Organisation.
- **BaFin aus Abschnitt 2.6.2:**
  - *direkt*: keine
  - *indirekt*: Treibende Kraft zur Gesetzeskonformität u.a. Gesetz über das Kreditwesen (KWG), Versicherungsaufsichtsgesetzes (VAG), Wertpapierhandelsgesetz (WpHG) und Liquiditätsverordnung (LiqV)

  Da die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) bei Gesetzesverstößen dazu berechtigt ist, Sanktionen zu verhängen, wird Gesetzeskonformität für Finanzdienstleister ein essentieller Bestandteil aller Unternehmensorgane. Ein IAM erleichtert diese Konformität, sobald kritische Werte und Güter, speziell vor Zugriffen, geschützt werden müssen.

Zusammengefasst: Folgende Vorgaben an die Unternehmensorgane werden aus der Summe der erläuterten Forderungen abgeleitet:

- Verwaltung von Identitäten durch rollenbasierte Authentifikationsprozesse
- Zweckgebundener und kontrollierter Informationsgehalt und -verarbeitung
- Kontrollierte und zweckgebundene Befugnisse
- Risikominimierung
- Interne Kontrollen
- Transparenz
- Flexibilität

Somit ist ein IAM ein Teilprozess der unternehmensweiten IT-Governance mit dem Ziel einer kontinuierlichen und nachweislichen IT-Compliance. Die zentralen Elemente[20]*S.155* des IAM umfassen die Benutzerverwaltung und die Zugriffs- und Berechtigungssteuerung. Diese sind folglich eine der tragenden Säulen zur gesetzlichen, kommerziellen und organisatorischen Compliance, das durch[21]*S.41*,[22]*S.308*,[23]*S.3* untermauert wird. Mit dem Abschnitt 2.3 wurde gezeigt, dass das IAM durch eine Vielzahl direkter und

Fundstelle	**Forderung**	
	direkt	*indirekt*
SOX EuroSOX	✓	✓
KonTraG	*keine*	✓
GoBD	✓	✓
BDSG	✓	✓
IT-Grundschutz	✓	✓
ISO 9000-Serie	*keine*	✓
ISO 20000-Serie	✓	✓
ISO 27000-Serie	✓	✓
Basel II-III	*keine*	✓
BaFin	*keine*	✓

Tabelle 2.1: Fundstellen der direkten und indirekten IAM-Forderungen

indirekter Forderungen aus Gesetzen, Normen und Regularien geprägt wird. Tabelle 2.3 zeigt, zur Erfüllung der ersten Zielsetzung, die Fundstellen der Forderungen auf.

2.4 Gesetzliche Vorgaben

Bis zu diesem Abschnitt stand die Bildung eines grundsätzlichen Verständnisses im Vordergrund, wie die Forderungen nach Gesetzes- und Anforderungskonformität durch verschiedene Interessengruppen geprägt werden kann und ein unternehmensweiter Governance-Prozess die Einhaltung des Status gewährleisten soll. Weiterhin wurden direkte und indirekte Forderungen ausfindig gemacht, die einen IAM-Prozess erforderlich machen.

Im nachfolgenden Abschnitt werden die Fundstellen der in Tabelle 2.3 aufgeführten Forderungen erläutert und mit den Elementen des IAMs in Verbindung gesetzt.

2.4.1 SOX und EuroSOX

Der Sarbanes Oxley Act (SOX) nach[24]*S.283-285* trat am 30.07.2002 in den USA in Kraft. Das US-Bundesgesetz sollte die Verlässlichkeit der Berichtserstattung von Unternehmen verbessern, die am US-Kapitalmarkt tätig sind. Es ist ein Instrument zum Finanz-Reporting für internationale und nationale Buchhalter, Prüfer, Chief Financial Officer (CFO) und für alle beteiligten Personen in den Unternehmensbereichen der Rechnungslegung und des Bilanzabschluss. Hauptaugenmerk des Gesetzes ist die Verschärfung der Vorschriften zur Rechnungslegung. SOX fordert Definition und Festlegung von Unternehmensprozessen für Kontrollverfahren. Das Ziel dabei ist, das Risiko einer falschen Bilanz zu minimieren. SOX fordert deshalb ein Internes Kontrollsystem (IKS), welches sich auf alle Unternehmensbereiche zur regelmäßigen Finanzberichtserstattung erstreckt. Zusätzlich muss das IKS in operativen Abläufen und im jährlich wiederkehrenden Regelbetrieb verankert werden. In der IT sind die Aufgaben der Datensicherheit, Backups, die Archivierungspflicht sämtlicher elektronischer Kommunikation und die Erfüllung der Compliance-Anforderungen betroffen. Die Prüfung und Bewertung des IKS selbst findet jährlich durch externe Prüfer statt, mit anschließender Offenlegung bestehender Fehler gegenüber dem Management. Die Korrektheit und Vollständigkeit der Ergebnisse ist durch eine eidesstattliche Versicherung der Chief Executive Officer (CEO) und CFO zu garantieren. In Bezug auf IT-Security und Informationssicherheit fordert SOX:

- Allgemeine IT-Kontrollen
- Dokumentationspflicht
- Berechtigungsvergabe und ein Transaktions-Monitoring
- Funktionstrennung
- Schnittstellenüberwachung
- Auswertungs- und Berichtsfunktionen

Die Gültigkeit von SOX erstreckt sich auf:

- US-börsengeführte Unternehmen
- Ausländische Unternehmen, die an der US-Börse oder der National Association of Securities Dealers Automated Quotations (NASDAQ) notiert sind

- Ausländische Töchter von US-Gesellschaften

Überwacht wird SOX durch:

- Die US-Börsenaufsicht Securities and Exchange Commission (SEC)
- Dem Public Company Accounting Oversight Board Public Company Accounting Oversight Board (PCAOB), eine aufgrund SOX gegründete privatrechtlich organisierte Aufsicht für Wirtschaftsprüfer.

Die EuroSOX adaptierte die geltenden Regelungen und führte 2006 zur Einführung der EU-Richtlinie 2006/43/EG. Darin wird die Regelung von Abschlussprüfungen, Jahresabschlüssen und konsolidierten Abschlüssen getroffen. Die Richtlinie verpflichtet die EU-Mitgliedsstaaten zur Einhaltung und Anwendung und erstreckt sich auf:

- Börsennotierte Unternehmen
- Banken und Versicherungen
- Zusätzlich die Monopolunternehmen z.B. Energieversorger, Deutsche Post oder Deutsche Bahn

Die EU-Richtlinie fordert einen Prüfungsausschuss (Audit-Committee) der gemeinsam mit den Wirtschaftsprüfern arbeitet. Das Committee wird von dem Abschlussprüfer über die Schwachstellen des internen Kontrollsystems informiert.

Zusammengefasst: SOX und die EU-Richtlinie 2006/43/EG, auch EuroSOX genannt, schreiben ein IKS in der gesamten Unternehmensweite vor. Hauptaugenmerk liegt dabei auf der Rechnungslegung. Durch die Verschärfung der Finanzberichtserstattung soll das Risiko einer falschen Unternehmensbilanz minimiert werden. Die Forderungen allgemeiner IT-Kontrollen, einer Berechtigungsvergabe und der Funktionstrennung können direkt mit einem IAM in Verbindung gebracht werden.

2.4.2 KonTraG

Der weitere Ansatz ein umfangreiches IKS zu etablieren, ist das Gesetz zur Kontrolle und Transparenz (KonTraG). Es trat im 1. Mai 1998 in Kraft und war der Beitrag der damaligen Bundesregierung zum Corporate Governance. Folgende Ziele nach[24]*S.285-286* standen dabei im Mittelpunkt:

- Verbesserung der Arbeit des Aufsichtsrats

- Erhöhung der Transparenz
- Stärkung der Kontrolle durch die Hauptversammlung
- Abbau von Stimmenrechtsdifferenzierungen
- Zulassung moderner Finanzierungs- und Vergütungsinstrumente
- Verbesserung der Zusammenarbeit von Abschlussprüfer und Aufsichtsrat und der Abschlussprüfung selbst
- Kritische Prüfung des Beteiligungsbesitzes von Kreditinstituten

Weiterhin wird in[24]*S.285-286* aufgeführt, dass der Vorstand börsennotierter Unternehmen dafür Sorge zu tragen hat, dass ein angemessenes Enterprise Risk Management (ERM) neben dem IKS im Unternehmen vorhanden ist und gelebt wird[2]*§91 Abs. II.* Der Vorstand hat im Falle einer Krise den Nachweis, dass Maßnahmen zur Früherkennung und Abwehr von Risiken getroffen wurden und diese objektiv als auch subjektiv pflichtgemäß angewandt wurden, zu erbringen. Diese Forderung setzt ein Risikohandbuch oder eine schriftliche Richtlinie zur Dokumentation des ERMs voraus. Die Identifizierung, Analyse und Bewertung von Risiken ist in den genannten Dokumenten festzuhalten. Die pflichtgemäße Anwendung und Einhaltung kann nur durch die Zuordnung von Verantwortlich- und Zuständigkeiten im ERM-Prozess gewährleistet werden. KonTraG schreibt jedoch nicht vor, wie das ERM-System im Detail auszugestalten ist. Lediglich wird das Vorhandensein und die individuelle Anpassung an die Wirtschaftsbranche, Größe und Struktur des Unternehmens gefordert. Die Früherkennungsmaßnahmen müssen in Bezug auf bestandsgefährdete Entwicklungen und einem Risikoeintritt so rechtzeitig greifen, dass Zeit für Gegenmaßnahmen bleibt. Das gilt nach[24],[2] für:

- Risikobehaftete Geschäfte
- Verstöße gegen gesetzliche Vorschriften
- Nicht korrekte Rechnungslegung, mit Auswirkung auf die Vermögens-, Finanz- und Ertragslage des Unternehmens.

Zusammengefasst: Neben der Forderung nach einem IKS, besteht in KonTraG die Forderung, dass der Vorstand für ein etabliertes ERM Sorge zu tragen hat.
Eine direkte Forderung eines IAMs durch KonTraG kann an dieser Stelle nicht abgeleitet werden. Dessen ungeachtet hat die Forderung eines ERMs indirekten Einfluss auf das IAM. Die Berechtigungssteuerung und Zugriffskontrolle eines IAMs begünstigt den bewussten Umgang mit Risiken und minimiert diese.

2.4.3 GoBD

Mit den "Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)" legt das Bundesfinanzministerium allgemeingültige Prinzipien, die IT-gestützten Prozessen zugrunde liegen, dar. Die GoBD wurden am 14. November 2014 veröffentlicht und traten am 1. Januar 2015 in Kraft. Nach[25]*S.10* setzt GoBD erforderliche Modernisierungen um, die eine Überarbeitung der Vorgaben aufgrund vorausgegangener Entwicklungen beinhaltete und von der Wirtschaft gefordert wurde.
Die GoBD lösen die (GoBS) Grundsätze ordnungsgemäßer datenverarbeitende gestützte Buchführungssysteme und die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) ab. Demnach geben die Grundsätze auf der einen Seite die bestehende Rechtslage wieder, während auf der anderen Seite die Anforderungen eine Fortentwicklung bestehender Regelungen erfahren haben. Gemäß[25]*S.16* wird den Unternehmen empfohlen, die GoBD für eine eingehende Auditierung ihrer Prozesse zu nutzen, um diese der aktuellen Rechtslage anzupassen und parallel dazu eine Optimierung ihrer Abläufe anzustreben. Die etablierten Kern-Anforderungen, die wiederholt in verschiedenen Abschnitten zur Ausführung der Prozesse und Abläufe der Unternehms-IT zu finden sind, werden in[25]*S.17* in ein "Vier-Säulen-Modell zur Umsetzung der GoBD", siehe Abb.2.4 überführt. Die Tabelle 2.2 gibt einen Überblick zu den Ausprägungen der jeweiligen Kern-Anforderung.

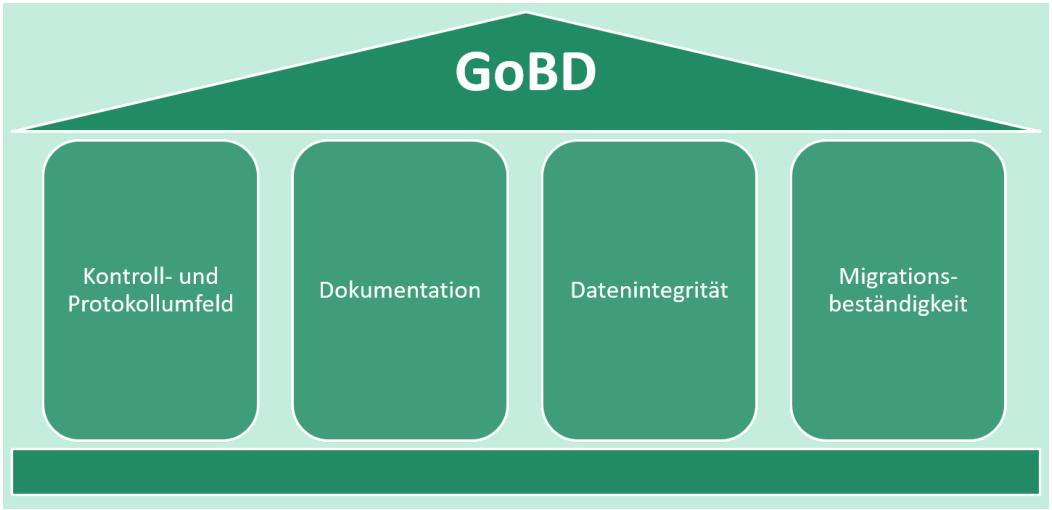

Abbildung 2.4: GoBD Vier-Säulen-Modell, adaptierte Grafik[25]*S.17*

Tabelle 2.2: GoBD Kern-Anforderungen und Ausprägungen, adaptierte Tabelle[25]*S.18*

Säule	**Ausprägungen der Anforderung**
Kontroll- und Protokollumfeld	Internes Kontrollsystem
	Grundsätze der Nachvollziehbarkeit, Nachprüfbarkeit
	Wahrheit, Klarheit und fortlaufenden Aufzeichnung
	Progressive und retrograde Prüfbarkeit
	Anforderung an die Vollständigkeit
	Anforderung an Richtigkeit, Zeitgerechtheit
	Definition von Verantwortlichkeiten
Dokumentation	Nachvollziehbarkeit für einen sachverständigen Dritten
	Anforderung an die Erstellung einer Verfahrensdokumentation
	Ordnung und Indexierung
	Protokollierungsanforderungen
Datenintegrität	Anforderungen an Unveränderbarkeit und Sicherheit der Daten
	Historisierungsanforderungen
	Lesbarmachung
	Verknüpfung von Buchung und Beleg
Migrationsbeständigkeit	Auswertungsmöglichkeiten über den Zeitraum der Aufbewahrung
	Datenmigration beim Austausch von IT-Systemen
	Auslagerung von Daten in Archivsysteme
	Inhouse-Formate und Konvertierungsvorgaben
	Entschlüsselung von verschlüsselten Daten
	Strukturbeschreibungen von steuerrelevanten Daten

Mitgeldende Vorgaben

In GoBD fließen allgemeine Vorgaben aus dem Handelsgesetzbuch (HGB)[26] über die Ordnungsmäßigkeit von elektronischen Bücher und sonst erforderlichen elektronischen Aufzeichnungen und Verfahren, in denen ein DV-System eingesetzt wird, mit ein, sowie die Bereiche des DV-Systems selbst. Folgende Anforderungen sind gemäß[27]*S.8* zu beachten:

- Grundsatz der Nachvollziehbarkeit und Nachprüfbarkeit *(§ 145 Absatz 1 Anordnung (AO),§ 238 Absatz 1 Satz 2 und Satz 3 [26]HGB)*
- Grundsätze der Wahrheit, Klarheit und fortlaufender Aufzeichnung:
  - Vollständigkeit *(§ 146 Absatz 1 AO, § 239 Absatz 2 [26]HGB)*
  - Richtigkeit *(§ 146 Absatz 1 AO, § 239 Absatz 2 [26]HGB)*
  - Zeitgerechte Buchungen und Aufzeichnungen *(§ 146 Absatz 1 AO, § 239 Absatz 2 [26]HGB)*
  - Ordnung *(§ 146 Absatz 1 AO, § 239 Absatz 2 [26]HGB)*
  - Unveränderbarkeit *(§ 146 Absatz 4 AO, § 239 Absatz 3 [26]HGB)*

Zusammenlegung von GoBS und GDPdU

In GoBD fließen folgende Grundsätze aus den genannten Regelwerken mit ein:

- **GoBS**
  Die GoBS umfassen Dokumentation, Prüfung und Datensicherheit. Diese Verordnung räumte der elektronischen Buchführung bzw. der EDV Elektronische Datenverarbeitung den gleichen Stellenwert gegenüber der manuellen Buchführung ein, unter Beachtung der oben aufgeführten Vorgaben aus dem HGB[26]. Parallel dazu wurde das IKS gefordert, mit Schwerpunkt auf Sicherung und Schutz von vorhandenen Vermögen und Informationen.
- **GDPdU**
  Die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen enthielten Vorschriften zur Aufbewahrung digitaler Dokumente und Informationen und ordneten den Unternehmen eine Mitwirkungspflicht bei Betriebsprüfungen ein. Die Mitwirkungspflicht betraf unter anderem, dass Datenzugriff für den prüfenden Dritten gewährleistet wird.

GoBD Vorgaben zum IKS

Bei der Betrachtung der aufgeführten Anforderungen und zugehörigen Ausprägungen lassen sich die nachfolgenden Vorgaben[25]*S.17* zum IKS direkt dem IAM zuordnen:

- Zugangs- und Zugriffskontrolle auf Basis der Berechtigungskonzepte
- Funktionstrennungen
- Erfassungskontrolle
- Schutzmaßnahmen gegen beabsichtigte und unbeabsichtigte Verfälschung von Programmen, Daten und Dokumenten

Die Ausgestaltung ist nach GoBD von der Komplexität des Geschäftsfelds, der Organisationsstruktur und den eingesetzten IT-Systemen im Unternehmen abhängig. Um die Einhaltung der Vorschriften zu gewährleisten, sind Kontrollen einzurichten, auszuüben und zu protokollieren. Insbesondere stehen im Kontrollumfeld des IAMs die Nachvollziehbarkeit von Veränderungen betreffend Einfügen, Ändern und Löschen der Daten im Mittelpunkt:

- Zugangs- und Zugriffsberechtigungskontrollen
- Erfassungs- und Eingabekontrollen
- Verarbeitungs- und Abstimmungskontrollen

Nach[25]*S.25* müssen die Kontrollen so ausgestaltet sein, dass die Identität eines Benutzers festgestellt werden kann und erkennbar ist, dass nicht autorisierte Zugriffsversuche abgewiesen wurden. Zusätzlich wird in[25] darauf verwiesen, dass die Zugriffskontrollen so auszugestalten sind, dass diese den Festlegungen der Sicherheitskonzepte entsprechen und zu der im Unternehmen gelebten Berechtigungsverwaltung passen.

Zusammengefasst: Das in[25] entwickelte "Vier-Säulen-Modell" unterteilt die GoBD in Kern-Anforderungen mit Ausprägungen rund um Kontroll- und Protokollumfeld, Dokumentation, Datenintegrität und Migrationsbeständigkeit, siehe Tabelle 2.2. Die oben aufgeführten Vorgaben zum IKS können direkt dem IAM zugeordnet werden. Damit fördert das IAM den Compliance-Status in Bezug auf die Erfüllung der in GoBD getroffenen Vorgaben und Kontrollen.

2.4.4 Bundesdatenschutzgesetz

Das BDSG fordert in Deutschland den Schutz von personenbezogenen Daten. Dies gilt sowohl für die Daten der Mitarbeiter eines Unternehmens als auch für die Kundendaten, die im Zuge der Auftragsverarbeitung genutzt werden. Die Anlage zu *§9 Satz 1*BDSG verlangt unter anderem:

Zutrittskontrolle

"Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren." 1.Absatz §9 Satz 1 [28],[18]

Realisierung: Bei der Zutrittskontrolle steht der physische Zutritt und Zugang zu datenschutzrechtlich relevanten Daten im Vordergrund. Diese Vorschrift schreibt eine physische Sicherung vor, sodass nur berechtigte Personen Zutritt zu den Daten erhalten.

Zugangskontrolle

"Zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können." 2.Absatz §9 Satz 1 [28],[18]

Realisierung: Damit rückt die Kontrolle des Zugangs zu datenverarbeitenden Systemen in den Vordergrund. Diese schützt vor unbefugtem Zugang und verhindert damit, dass Manipulationen vorgenommen werden können. Aus der Vorgabe wird an dieser Stelle abgeleitet, dass ein Identitätsmanagement (IDM) im Unternehmen vorhanden sein muss.

Zugriffskontrolle

"Zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können." 3.Absatz §9 Satz 1 [28],[18]

Realisierung: Erteilte Zugriffe sind nur über eine zentrale Berechtigungssteuerung, die somit im Unternehmen geführt werden muss, kontrollierbar. Erteilte Berechtigungen sind in einem Berechtigungskonzept zu dokumentieren und Zugriffsversuche auf personenbezogenen Daten auf allen Systemen zu protokollieren. Bei der Vergabe von Berechtigungen darf der Mitarbeiter nur jene Daten erhalten, die für den Verarbeitungszweck notwendig sind (Need-to-know-Prinzip).

Weitergabekontrolle

"Zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist." 4.Absatz §9 Satz 1 [28],[18]

Realisierung: Nachvollziehbare Protokollierung der Bewegungen personenbezogener Daten (Quelle, Ziel und durchführende Identität). Dies gilt sowohl in der physischen als auch in der nicht-realen bzw. virtuellen Umgebung. Die Weitergabekontrolle wird an dieser Stelle als direkte Forderung nach einer Berechtigungssteuerung verstanden.

Eingabekontrolle

"Zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind." 5.Absatz §9 Satz 1 [28],[18]

Realisierung: Es erfolgt die Erfassung und Dokumentation, welche Person einen Vorgang mit datenschutzrelevanten Daten angestoßen hat und welche Handlungen daraus resultiert sind. Demnach muss nachträglich prüfbar sein, ob und von wem Veränderungen im System vorgenommen worden sind. Diese Vorgabe macht ein IDM erforderlich.

Auftragskontrolle

"Zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können." 6.Absatz §9 Satz 1 [28],[18]

Realisierung: Weisungen und regelmäßige Kontrollen des Arbeitnehmers, dass datenschutzrechtliche Pflichten eingehalten werden, resultieren aus dieser Vorgabe. Ein unternehmensweites Rollenmodell, analog zu den Anforderungen innerhalb der Verarbeitungsschritte, ist ein wichtiger Teil der Auftragskontrolle.

Verfügbarkeitskontrolle

"Zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind." 7.Absatz §9 Satz 1 [28],[18]

Realisierung: Schutz der Daten durch Datensicherungs- und Notfallkonzepte vor unbeabsichtigter und vorsätzlicher Manipulation oder Verlust. Die Verfügbarkeitskontrolle impliziert den Schutz der IT-Infrastruktur vor physischen und virtuellen Einwirkungen. Daraus kann ebenfalls eine direkte Forderung nach der Zugriffs- und Berechtigungssteuerung abgeleitet werden.

Funktionstrennung

"Zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können." 8.Absatz §9 Satz 1 [28],[18]

Realisierung: Personenbezogene Daten dürfen nur zweckgebunden genutzt werden, daran gebunden ist auch der Umfang der Datennutzung. Ein Identitätsmanagement und die Schaffung von festen Funktionsbereichen, in Form von Geschäftsrollen, wird aus dieser Forderung abgeleitet. Die Funktionstrennung hat ein Berechtigungskonzept zur Folge, in dem definiert wird, welche Geschäftsrollen im Rahmen der Anforderungen zur Verarbeitung berechtigt sind.

Absätze 1 bis 8 werden verschärft durch: *"Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind."* weiter heißt es *"Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren." §9 Satz 1* [28],[18]

Realisierung: Daraus resultiert die Notwendigkeit eines technischen Sicherheitskonzepts, die technische Umsetzung und die dauerhafte Anwendung der oben aufgeführten Punkte.

Zusammengefasst: Das BDSG hat nach *§1 Satz 1* [28],[18] zum Zweck *"... den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird."*
Das Gesetz konkretisiert den Umgang durch Vorgaben zur Kontrolle über Zutritt, Zugang, Zugriff, Weitergabe, Eingabe, Auftragsverarbeitung und Verfügbarkeit. Weiter fordert das BDSG Funktionstrennung und Anpassung der Unternehmensabläufe an das BDSG, sobald datenschutzrelevante Inhalte betroffen sind. Diese Forderungen können als direkte Vorgaben für das IAM verstanden werden und machen dieses zum Pflichtbestandteil eines jeden Unternehmens, welches mit Daten in Berührung kommt, die gemäß BDSG zu schützen sind.

2.5 ISO/IEC Reihen

Mehrfach wurde Bezug auf ISO/IEC-Reihen genommen. Die Internationale Organisation für Normung (ISO) und International Electrotechnical Commission (IEC) sorgen für internationale Normen und Satzungen. Die IEC tut dies speziell im Bereich der Elektrotechnik. Das Ziel internationaler Normen besteht unter anderem in der Schaffung eines

gemeinsamen Verständnisses einer produkt- und prozessorientierten Vorgehensweise. Einheitlichkeit, Zuverlässigkeit, Qualität, Transparenz und Gesetzeskonformität - kurz gefasst: Vertrauen und Verständigung ist, der Auffassung des Autors zufolge, der Kern von Normen und Satzungen.

2.5.1 ISO 9000-Serie

Die ISO 9000-Serie stellt die wichtigsten Normen für das Qualitätsmanagement dar und fordert Unternehmen zur bereichsübergreifenden Organisation der Prozesse auf. Im Mittelpunkt stehen die Beachtung der Kundenanforderungen an Produkte und Dienstleistungen. Die Erfüllung soll in den Phasen der Entwicklung, Produktion, Einführung und Betreuung nachvollziehbar sein. Durch Strukturen und systematische Leitung soll die ständige Leistungsverbesserung vorangetrieben werden. Analog die acht Grundsätze des Qualitätsmanagements der ISO 9000:2000[29]:

- Kundenorientierung
- Verantwortlichkeit der Führung
- Einbeziehung der beteiligten Personen
- Prozessorientierter Ansatz
- Systemorientierter Managementansatz
- Kontinuierliche Verbesserung
- Sachbezogener Entscheidungsfindungsansatz
- Lieferantenbeziehungen zum gegenseitigen Nutzen

Damit ist die ISO 9000-Serie einer der grundlegenden Normen und nahezu in jedem Unternehmen, das am globalen Markt tätig ist, durch ein zertifiziertes Qualitätsmanagement etabliert.

2.5.2 ISO 20000-Serie

Die Serie bildet einen Standard, der sich mit dem IT-Service-Management befasst[30]*S.9*. Im Vordergrund steht dabei die Organisation der IT-Abteilung durch die Abgrenzung von Aufgabenbereichen, Ansprechpartnern und Eskalationsstufen. Die ISO-Reihe aus dem Jahr 2005 ist unterteilt in Spezifikation (Teil 1) und einem Leitfaden (Teil 2) mit einer integrierten prozessorientierten Vorgehensweise für das IT-Service-Management. Der erste Teil spezifiziert Anforderungen für einen qualitativen IT-Service. Dazu werden folgende Prozessgruppen vorgegeben[22]*S.59-62*:

- Service Delivery Prozesse
- Release Prozesse
- Resolution Prozesse
- Beziehungsmanagement-Prozesse
- Steuerungsprozesse

In den genannten Prozessgruppen wird grundsätzlich der PCDA-Zyklus integriert, um eine gleichbleibende Servicequalität zu gewährleisten und der KVP (Kontinuierlicher Verbesserungsprozess) gelebt werden kann. Weitere wichtige Forderungen aus der ISO 20000-Serie:

- Kommunikationspolitik durch das Management, in der alle relevanten Personen und auch Kunden informiert und auf dem aktuellen Sachstand sind
- Geeignete Kontrollelemente zur Dokumentation
- Aufzeichnung sicherheitsrelevanter Ereignisse durch das Incident-Management
- Erfassung, Klassifizierung und Dokumentation sämtlicher IT-Elemente als Asset mit der Zuordnung zum jeweiligen Asset-Eigner und dem Schutzbedarf
- Regelmäßige dokumentierte Bewertung von Sicherheitsrisiken nach den Kriterien Art der Bedrohung, Eintrittswahrscheinlichkeit und mögliche Folgen
- Festlegung von Rollen und Verantwortlichkeiten
- Gleichbleibende integrierte Kontrollelemente

In Verbindung mit der ISO 20000 steht der "De-Facto-Standard" (ITIL) Information Technology Infrastructure Library. Es handelt sich dabei um eine Sammlung von Best-Practices-Werken und ist damit ein IT-Framework zur Verbesserung der IT-Service Qualität[20]*S.1,4*, das kann als Weg zur ISO/IEC 20000 IT-Service-Management Zertifizierung betrachtet werden. Das Framework etabliert mit der dritten Version aus dem Jahr 2007 einen Service-Lifecycle und hat damit einen Wechsel vollzogen. ITIL ist ab der genannten Version lebenszyklusbasiert und hat sich damit von dem Schwerpunkt der Prozessorientierung entfernt[22]*S.61-63*. Der Lebenszyklus besteht aus den Phasen:

- Service Design
- Service Transition
- Service Operation
- Der im Mittelpunkt stehenden Service Strategie

Als weiterer kurzer Auszug zu ITIL soll an dieser Stelle die Unterscheidung von Störung und Problem dienen:
Bei einer Störung *im engl. incident* liegt eine kurzfristige Unterbrechung oder Minderung des Betriebsablaufes vor[20]*S.14,23*. Ist die Ursache einer Störung unbekannt, wird von einem Problem *im engl. problem* gesprochen[20]*S.28*. Weitere Kriterien zur Einstufung kann das wiederholte Eintreten der Störung sein oder wenn eine grundlegende Änderung im Betriebsablauf notwendig wird. Die Differenzierung von Incidents und Problems soll reaktive und präventive Schwerpunkte setzen. Im Falle eines Incidents ist eine schnelle und wirksame Lösung (reaktiv) erforderlich, während die Maßnahmen bei Problemen langfristige Auswirkungen (präventiv) berücksichtigen müssen. Weiterhin werden, wie in den Anforderungen aus der ISO 20000-Serie, Elemente und Ressourcen des Unternehmens als Asset verbucht, in einer Datenbank klassifiziert und einem Eigner zugeordnet.
Mit den genannten Methoden und Werkzeugen werden die vorgegebenen Prozessgruppen ausgestattet. Im Laufe dieser Arbeit wird ITIL erneut im Kontext des IAMs aufgegriffen.

2.5.3 ISO 27000-Serie

Dies ist ein abgestimmter ISO 20000 Standard speziell für die Informationssicherheit[30]*S.9-10* und dem zugehörigen ISMS. Die ISO 27001 enthält die Anforderungen für ein in der gesamten Unternehmensweite etabliertes ISMS unter Berücksichtigung der IT-Risiken innerhalb der Organisation[30]. In die ISO-Serie flossen im Jahr 2005 der British Standard (BS) 7799-1 und BS 7799-2 mit ein. Die BS 7799-Serie wurde mit dem Ziel entwickelt, den Unternehmen ein Modell und konkrete Spezifikationen bereitzustellen, betreffend der Einführung eines effektiven ISMS. Dies erleichtert die Abstimmung zwischen der Unternehmensstrategie und den Geschäftszielen. Da die BS 7799 zur Prüfung und Akkreditierung von Unternehmen verwendet wird, basieren viele Teile der ISO 27000-Serie auf dem British Standard.
Die Norm erstreckt sich auf sämtliche Organisationen, unabhängig unter welchen Namen und welcher Rechtsform diese firmieren. Eine Zertifizierung kann direkt nach ISO/IEC 27001 erfolgen oder auf Basis des IT-Grundschutzes. An dieser Stelle ein kurzer Überblick über die ISO 27000-Serie[22]*S.49-51*:

- ISO/IEC 27000: Begriffe und Definitionen
- ISO/IEC 27001: Anforderungen an ein ISMS
- ISO/IEC 27002: Empfehlungen für diverse Kontrollmechanismen für die IS
- ISO/IEC 27003: Leitfaden zur Umsetzung der ISO/IEC 27001

- ISO/IEC 27004: Leitlinie zum Design, Implementierung und Definition von Kennzahlen zur Kontrolle eines ISMS
- ISO/IEC 27005: Management von Informationssicherheitsrisiken
- ISO/IEC 27012: Richtlinien für Finanzdienstleister
- ISO/IEC 27014: Leitfaden für Governance in der Informationssicherheit

Der Standard ISO/IEC 27014 definiert sechs Grundsätze[31]:

- Eine unternehmensweite Informationssicherheit (IS)
- Verfolgung eines risikobasierten Ansatzes
- Richtungsentscheidungen für Investitionsentscheidungen
- Konformität mit internen und externen Anforderungen
- Fördern eines positiven Sicherheitsumfelds
- Bewertung der Kosten und des Nutzens der Informationssicherheit in Bezug auf die Geschäftsergebnisse

Die Erfüllung der Grundsätze zur Verfolgung eines risikobasierten Ansatzes, Konformität mit internen und externen Anforderungen und Förderung eines positiven Sicherheitsumfeldes stehen im engen Zusammenhang mit dem IAM. Die ISO 27002:*9 Access control* spezifiziert Vorgaben und Empfehlungen unterteilt in *business requirements of access control* und *user access management*. Nach einem Vergleich[32]*S.11* ist dieser Teil im IT-Grundschutz im Maßnahmenkatalog[33]*M 2.585 S.2890* und im Baustein[33]*B 1.18 S.67* wiederzufinden. Gleichermaßen fordern ISO 27002 und der IT-Grundschutz die Implementierung und Integration eines IAMs.

Zertifizierung nach ISO 27000/IT-Grundschutz

Eine Akkreditierung eines Unternehmens für die ISO 27000-Serie kann sich, wie im oberen Abschnitt bereits angesprochen, unterscheiden:

- **Zertifizierung nach 27001**
  Erfordert die Einführung eines angemessenen Risikomanagementsystems und Sicherheitsmaßnahmen, die aus dem Unternehmensumfeld abzuleiten sind. Angewendet wird das ERM in allen Substitutionen des Unternehmens bis in die Geschäftsprozesse hinein[30]*S.11*.
- **Zertifizierung nach 27001 auf Basis IT-Grundschutz**
  Eine Zertifizierung auf Basis des IT-Grundschutzes durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einen ausgeprägten Schwerpunkt auf die IT-Sicherheit und geht damit über die Anforderungen der ISO 27001

hinaus[30]*S.7-11*. Es erfolgt zusätzlich eine Modellierung der Sicherheitslage herunter gebrochen auf einzelne IT-Anwendungen. Zusätzlich ist die Durchführung einer Schutzbedarfsanalyse für IT-Hardware und Software eine weitere Anforderung für diese Akkreditierung[33].

2.5.4 ISO 31000-Serie

Die ISO-Serie beinhaltet Prinzipien, Richtlinien und einen Leitfaden für den Aufbau und die Integration eines Enterprise Risk Management (ERM)-Prozess im Unternehmen. Zweck der ISO-Reihe ist die abgestimmte Etablierung von universellen Paradigmen und Kriterien, auf die Ziele des Unternehmens[34]:

- Identifikation und Beschreibung der Risiken nach Art, Ursache und Auswirkung
- Analyse der Eintrittswahrscheinlichkeit
- Schaffung und Bewertung einer Risiko-Akzeptanz unter vorgegebenen Kriterien
- Risikobewältigung und -Beherrschung durch Maßnahmen, die Gefahren oder Eintritt reduzieren und die Folgen beherrschbar machen
- Risikoüberwachung, um Indikatoren aufzuzeigen durch Kontrolleinheiten in den Organisationseinheiten
- Aufzeichnungen und Dokumentation der Risiko-Sachverhalte

Ein Risikomanagement mit Wertbezogenheit wird zu einem systematischen, strukturierten, zeitgerechten, angepassten und dynamischen Unternehmensprozess, der durch die iterative Anwendung im Unternehmen, den KVP fördert. Die gezielte Behandlung von Risiken mit allen verfügbaren Informationen, unter der Berücksichtigung von sozialen und kulturellen Faktoren, trägt zu einer nachhaltigen Entscheidungsfindung bei.

Zusammengefasst

Eine Zertifizierung nach einer der genannten ISO-Reihen bedeutet, dass die Unternehmen nach einem vorgegebenen Ablauf unter Verwendung einheitlicher Werkzeuge und Methoden produzieren oder eine Dienstleistung erbringen. Für den Kunden resultiert daraus, dass seine Anforderungen unter der Verwendung von bewährten Mitteln qualitativ hochwertig oder zumindest annehmbar erfüllt werden.

2.6 Schärfung der Vorgaben in der Finanzdienstleistung

Der Abschnitt 2.1 weitete die gesetzliche Compliance auf branchenspezifische Verschärfungen aus, die nun am Beispiel der Finanzdienstleistung verdeutlicht werden.

2.6.1 Basel II-III

In[24]*S.294* wird Basel II als nicht-rechtsverbindliches Konvolut von Regeln zur Beaufsichtigung von Banken bezeichnet. Es handelt sich dabei um ein Übereinkommen der Zentralbankgouverneure und Bankenaufsichtsbehörden der G10-Staaten. Die Namensgebung wurde dadurch geprägt, dass die Erarbeitung im Rahmen des Baseler Ausschusses für Bankenaufsicht stattfand. Im Mittelpunkt stehen Eigenkapitalvorschriften der Finanzdienstleistungsinstitute. Die Anwendung in Deutschland wird durch das Gesetz über das Kreditwesen (KWG), die Solvabilitätsverordnung (SolvV) und die Mindestanforderungen an das Risikomanagement (MaRisk) seit Januar 2007 getrieben. Basel III löste 2013 schrittweise die Vorläuferregeln aus Basel II ab, um die Schwächen der Vorschriften zu reformieren. Dies entstand als Konsequenz aus der Finanzkrise 2007. Die Reform[35] umfasste u.a:

- Höhere Eigenkapitalquoten
- Schärfere Konsolidierungspflicht von Tochterunternehmen
- Erhöhung der Qualität, Konsistenz und Transparenz der Eigenkapitalbasis
- Verbesserung der Risikodeckung durch höhere Kapitalanforderungen und stärkere Offenlegung
- Einführung einer Verschuldungsgrenze (Leverage Ratio)

Ziel dieser Reform war die Schaffung einer Balance zwischen einem stabilen Finanzsystem und einer Vermeidung von Kapitalverknappung. Ein weiterer wichtiger Aspekt war nach[35] die Begrenzung und Reduzierung der Haftung durch die öffentliche Hand und den Steuerzahler.

2.6.2 BaFin

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ist dem Bundesministerium der Finanzen unterstellt und wurde am 1. Mai 2002 gegründet. Die BaFin beaufsichtigt und kontrolliert die Gesetzeskonformität von Banken und Versicherungen, die am Finanzmarkt tätig sind. Ziel der ist die Sicherstellung von Integrität, Stabilität und der Erhalt der Funktionsfähigkeit des deutschen Finanzsystems.

Damit ist die BaFin eine staatliche Kontrollinstanz der zugrundeliegenden Gesetze: KWG, dem VAG, dem WpHG, der SolvV und LiqV. Darüber hinaus ist die BaFin dazu berechtigt, bei Verstößen und Missachtungen Sanktionen zu verhängen. Demnach ist diese die treibende Kraft zur Gesetzeskonformität der Banken und Versicherungen.

Zusammengefasst

Basel II-III ist ein beispielhaftes Konvolut von Regeln zur Beaufsichtigung von Banken, das einerseits nicht rechtsverbindlich ist, andererseits durch KWG, SolvV und MaRisk getrieben und deren Umsetzung durch die BaFin geprüft wird. Der Auffassung des Autors zufolge ist dies ein Beleg für die notwendige Betrachtungsweise der Corporate Compliance aus gesetzlichen, kommerziellen und organisatorischen Blickwinkeln heraus. Für das IAM lassen sich indirekte Forderungen ableiten, da eine qualitative Eigenkapitalbasis von einem soliden IT-Grundschutz gefördert wird, an dem das IAM maßgeblich beteiligt ist gemäß Abschnitt 2.7.4.

2.7 Informations- und Risikomanagement

KonTraG fordert ein angemessenes Enterprise Risk Management (ERM). Bevor in diesem Abschnitt der daraus resultierende Einfluss auf das IAM aufgezeigt wird, sind ein Überblick und eine Abgrenzung grundlegender Begrifflichkeiten, wie IT-Sicherheit und IS, notwendig.

2.7.1 Sicherheit

- **IT-Sicherheit**
  Wird nach[36] als der Schutz von IT-Systemen in der nicht realen bzw. virtuellen Umgebung definiert. Im Fokus stehen Angriffe ausgehend von IT-Systemen auf andere IT-Systeme. Die klassische Definition, die sich auf Schutz von Vertraulichkeit, Integrität und die Sicherstellung von Verfügbarkeit konzentriert, lässt sich erweitern auf den Schutz von Authentizität, Daten und rechtlichen Vorgaben. Im Fokus stehen z.B. Hardware, Firmware, Software und Speicher sowie der darauf befindlichen Daten[36].
- **Informationssicherheit**
  Konzentriert sich auf den Schutz von Informationen in der physischen und virtuellen

Umgebung mit konzeptuellem Schwerpunkt. Dabei ist es unbedeutend, in welchem Dateiformat oder in welcher physischen Beschaffenheit diese vorliegen[36].

- **Cyber-Sicherheit**
  Das BSI definiert Cyber-Sicherheit als Ausweitung des klassischen Aktionsfelds der IT-Sicherheit auf sämtliche mit dem Internet und vergleichbaren Netze verbundene Informationstechnologie oder Informationstechnik (IT). Der darauf aufbauende Austausch von Kommunikation, Anwendungen und Prozessen etc. steht dabei im Mittelpunkt[37].
  In[36] wird Cyber-Sicherheit erweitert auf den Schutz der Gesellschaft vor Angriffen auf sensible Informationen, die im öffentlichen Interesse stehen.

Zusammengefasst: Im Rahmen der vorliegenden Arbeit wird festgehalten, dass IT-Sicherheit sich auf den Schutz der IT-Systeme konzentriert und mögliche Angriffsszenarien berücksichtigt. Bei der IS stehen Umgang und Schutz von Informationen in beliebiger Form im Mittelpunkt. Die Cyber-Sicherheit erweitert hingegen dieses Bewusstsein auf den Schutz aller Informationen im öffentlichen Interesse, auf beliebig verbundener IT. Dieses nun geprägte Bewusstsein erzwingt die grundsätzliche Auseinandersetzung mit bestehenden Risiken.

2.7.2 Informationen

Die Verwaltung von Informationen umfasst die Aufgaben des Aufbaus und der Aufrechterhaltung einer unternehmensweiten Informationsstruktur, die sowohl technologisch als auch organisatorisch die Unternehmensprozesse unterstützt. Die Begriffsauffassung nach[38]*S.27* fasst das Informationsmanagement als *"das Management im Unternehmen in Bezug auf Information und Kommunikation"* zusammen. Damit bestehen Schnittstellen und Abhängigkeiten zur IS und ein daraus resultierendes enges Verhältnis zur IT-Sicherheit.

2.7.3 Risiko

Dies ist der zentrale Aspekt im ERM und wird in[38]*S.28* kurz und prägnant definiert als: *"Risikomanagement ist die systematische Anwendung der Managementpolitik, der Verfahren und Maßnahmen zur Analyse, Bewertung und Beherrschung des Risikos."*
Die Geschäftsführung ist für die Etablierung und Aufrechterhaltung eines zentralen Risikomanagements (ERM) verantwortlich. In diesem erfolgt die Bündelung der Risk

Management Prozesse der einzelnen Unternehmenssubstitutionen, wie beispielsweise Finanzen, Produktion, Vertrieb und der IT. Die Erfassung der Risikorelevanz und das spätere prüfen von Handlungsalternativen stehen im Mittelpunkt. Mögliche Handlungen werden gekapselt und unter den Begriffen vermeiden, vermindern, begrenzen, überwälzen, selbst tragen oder outsourcen[38]*S.28* betrachtet.

2.7.4 IT-Grundschutz

Der IT-Grundschutz ist ein wichtiger Baustein für eine funktionierende IT und enthält konkrete Maßnahmen für die verschiedenen Organisationseinheiten zum Zwecke einer soliden Absicherung[33]. Aus der Umstrukturierung des IT-Grundschutzhandbuchs im Jahr 2006 durch das BSI entwickelte sich dieser[39]. Hintergrund der Entwicklung war gemäß[36] die Verhältnismäßigkeit herzustellen zwischen dem Wert der Güter und deren Schutzmaßnahmen[40]. Ziel ist demnach, die Kosten von Schutzmaßnahmen in Einklang zu bringen mit dem zur Verfügung stehenden Budget. Der Hauptfokus liegt auf vorgegebenen Prozessen, die durch Bausteine aus dem IT-Grundschutzkatalog vor allem technische Maßnahmen zur Verfügung stellen. Ebenfalls im Fokus stehen Gefährdungskataloge, die gängige Bedrohungen auflisten und eine konkrete Vorgehensweise für Risikoanalysen bieten. Dabei zu beachten ist, dass nach[36] der IT-Grundschutz gegen elementare Gefährdungen und Bedrohungen ausgerichtet ist. Um die Sicherheit auch in erhöhten Risikoszenarien zu gewährleisten, müssen von dem Informations- und Risikomanagement weitere Maßnahmen identifiziert und ergriffen werden.

Struktur des IT-Grundschutzes

- Grundschutzkatalog mit Bausteinen für:
  - Infrastruktur und Notfallvorsorge
  - Organisation und Personal
  - Hardware, Software und Kommunikation

- Gefährdungskatalog mit Risikoanalysen für:
  - Elementare Gefährdungen und höhere Gewalt
  - Organisatorische Mängel und Fehlhandlungen
  - Technische Mängel und Versagen

Vorgehensweise des IT-Grundschutzes

An dieser Stelle folgt ein kurzer Überblick zur standardisierten Absicherung der IT.

- Strukturanalyse:
  - Beschreibung des IT-Verbunds
- Sicherheitsanforderungen:
  - Schutzbedarfsfeststellung
- Modellierung der Grundschutzmaßnahmen:
  - Auswahl der Bausteine aus dem Grundschutzkatalog
- Basis-Sicherheitscheck:
  - Organisationsinstrument zur Feststellung des Umsetzungsgrades der ausgewählten Bausteine
- Weiterführende Sicherheitsmaßnahmen:
  - Für Zielobjekte mit hohem bis sehr hohem Schutzbedarf
- Implementierung:
  - Umsetzung der IT-Grundschutzmaßnahmen
- Sicherheitsrevision:
  - Abschließende Prüfung des Umsetzungsgrad der ausgewählten Bausteine

Zusammengefasst: Diese standardisierte Vorgehensweise zur Auswahl von vorgefertigten Bausteinen, Gefährdungslagen und Risikoanalysen ermöglicht die direkte Anwendung im Unternehmen, ohne dass zuvor umfangreiche Anforderungen, Analysen, Vorgehensweisen und Strategien ausgearbeitet werden müssen. Der Maßnahmenkatalog[19]*M 2.585 S.2890* und die Bausteine[19]*B 1.18 S.67* beschäftigen sich mit der Konzeption eines Identitäts- und Berechtigungsmanagements *(in dieser Arbeit als IAM bezeichnet)* und den Folgen einer mangelhaften Durchführung.
Ein Unternehmen, das die aufgeführte Vorgehensweise vollständig durchgeführt und die jeweils relevanten Bausteine implementiert hat, kann durch ein Audit die Zertifizierung nach ISO 27001 auf Basis des IT-Grundschutzes erhalten. Neben SOX und EuroSOX enthält der IT-Grundschutz direkte Forderungen, ein IAM im Unternehmensalltag zu integrieren.

2.7.5 MaRisk

Eine Grundlage für ein ERM ist die Einhaltung der Mindestanforderungen an das Risikomanagement (MaRisk), eine Sammlung die das KWG[41]*§25* konkretisiert. Darin erfolgt die Zuordnung der Gesamtverantwortung für alle Risk Management Prozesse bei der Geschäftsführung. Ein weiteres internes Kontrollsystem soll die Aufbau- und Ablauf-

organisation überwachen und steuern, durch die Einrichtung entsprechender Prozesse. Weitere Anforderungen werden gestellt an Organisationsrichtlinien, Dokumentationen und die technische und organisatorische IT-Sicherheit. Zusätzlich wird das Arbeiten nach Standards im Unternehmensalltag auferlegt, wie beispielsweise die ISO 27001. Darüber hinaus regelt MaRisk in puncto Outsourcing, wie Risiken und Verantwortlichkeiten zu berücksichtigen sind.
Zur Nachweiserbringung wird die Durchführung von Tests gefordert und eine dokumentierte Abnahme über die Einhaltung von Standards. Als Nachweis über die Behandlung von Risikoaspekten ist ein Notfallkonzept vorzuhalten.
Es wird in MaRisk für Banken und Finanzinstitute (MaRisk BA) und MaRisk für Versicherungsunternehmen (MaRisk VA) unterschieden. Erlassen wurde MaRisk BA von der BaFin im Dezember 2005[24]*S.295*.
MaRisk konkretisiert den[41]*§25* des KWGs und regelt damit die Umsetzung, der rein qualitativen Anforderungen aus Basel II-III im Risikocontrolling.

2.7.6 Wirken eines Informations- und Risikomanagements

Die zuvor definierten Begrifflichkeiten lassen sich für das Verständnis eines Informations- und Risikomanagements zusammenfassen und werden in dieser Arbeit in nachfolgende Bestandteile gruppiert:

1. Risiko und Sicherheit
   Das Zusammenwirken eines ERM und der IT-Sicherheit bedarf einer gesonderten Abstimmung, da die IT-Sicherheit den Schutz von IT-Systemen und die Abwehr von Angriffen in den Mittelpunkt rückt. Dabei sind konkrete Verfahren und Maßnahmen zur Analyse, Bewertung und Beherrschung von Risiken mit dem ERM zu erarbeiten. Umgekehrt müssen alle IT-Systeme im ERM bekannt sein, um diese vollständig berücksichtigen zu können.

2. Informationen
   Die Informationssicherheit (IS) konzentriert sich auf den Schutz von Informationen, sowohl innerhalb als auch außerhalb des Unternehmens. Dafür ist eine Abstimmung zu allen Fachbereichen notwendig, um den Schutzumfang und den allgemeinen Umgang mit Informationen festzulegen.

3. Gesellschaftliche Interessen
   Informationen und IT-Systeme, die im besonderen öffentlichen Interesse stehen

und darauf Einfluss haben, müssen gesetzeskonform und im Einklang mit dem Interesse behandelt werden.

Nachfolgende Abbildung 2.5 veranschaulicht die vorgenommene Bündelung. Anzumerken ist, dass eine Zusammenarbeit und Abstimmung aller Komponenten untereinander erforderlich ist und erheblichen Einfluss auf das Wirken des Informations- und Risikomanagements hat.

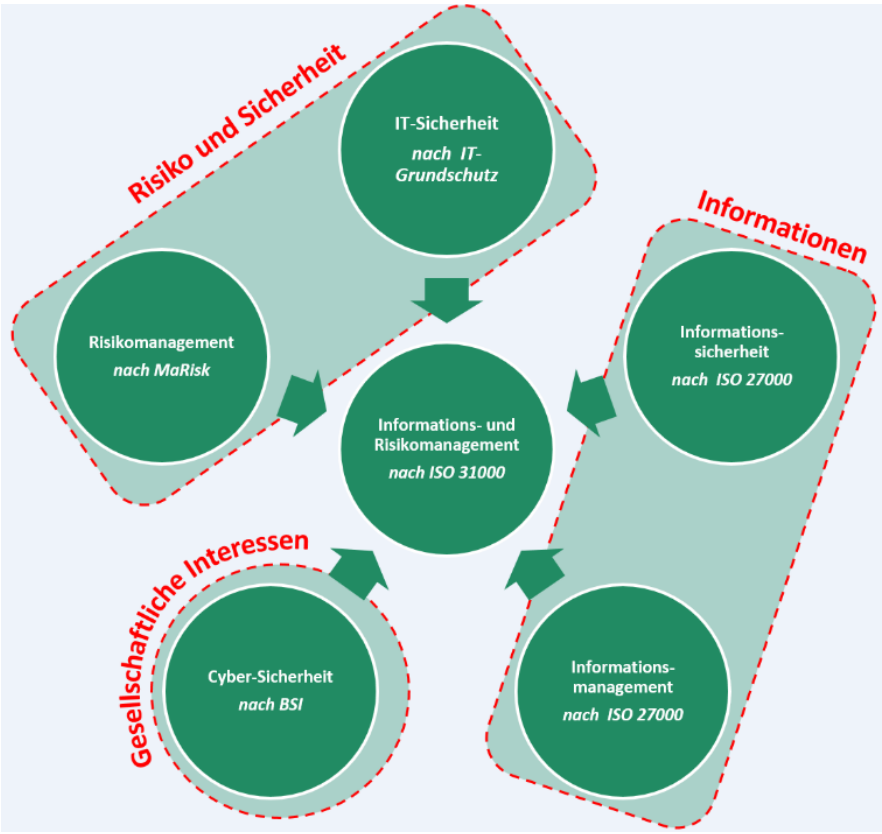

Abbildung 2.5: Komponenten und Wirkung eines Informations- und Risikomanagements

2.8 Rechtsfolgen einer Non-Compliance

In der gegenständlichen Arbeit sollen die Rechtsfolgen aus[24]*S.296* einer Non-Compliance als weitere Motivation für Gesetzeskonformität aufgefasst werden.

- **Gesetzliche Folgen**

  - Bundesdatenschutzgesetz: Bei Verletzungen drohen nach[28],[18]*§6,7* Auskunfts-, Berichtigungs-, Sperrungs-, Löschungs-, Unterlassungs- und Schadensersatzansprüche.
  - EuroSOX: Eine Verletzung hat zur Folge, dass die Erstellung des Testats durch den Wirtschaftsprüfer nach[26]*§322* HGB ausbleibt. Es folgt nach[2]*§120* Aktiengesetz (AktG) keine Entlastung des Vorstandes. Darüber hinaus bestehen die Möglichkeiten, Bußgelder zu verhängen oder der Entzug der Börsenzulassung.
  - KonTraG: Verschärft die unter EuroSOX aufgeführten Folgen um die Möglichkeit, den Vorstand in persönliche Haftung zu nehmen bei grober Fahrlässigkeit.
- **Sanktionen**
  - Basel II-III: Droht dem Kreditgeber bei Verletzungen mit Bußgeldern und Testatsverweigerung durch Wirtschaftsprüfer. Bei fehlendem Testat ist die Entlastung des Aufsichtsrates ausgeschlossen.
  - BaFin: Kann die Nachbesserung der Verträge nach[41]*§6 Abs.3* KWG fordern und ist nach[41]*§56 Abs.2 Nr.4* KWG zum Verhängen von Bußgeldern berechtigt. Darüber hinaus ist der Entzug der Bankenerlaubnis nach[41]*§35 Abs.2 Nr.6* KWG und sogar die Abberufung des Geschäftsführers nach[41]*§36 Abs.1,2* KWG möglich.
- **Verweigerungen im Vergabeverfahren**
  Nachweiserbringungen und Eigenerklärungen können im Verfahren unberücksichtigt bleiben. Dies hat zur Folge, dass der Compliance Status nicht nachgewiesen werden kann und damit die Konformität gebrochen wird.
  Bußgelder, Sanktionen und negative Vergabeverfahren ausgehend von staatlichen oder anderen anerkannten Organen können schwere Imageschäden nach sich ziehen. Dies kann zum Vertrauensverlust des Kunden führen und darüber hinaus den Versicherungsschutz gefährden, da Standards und Vorgaben eingehalten werden müssen. Bei ausbleibenden Aufträgen oder der Entziehung der Zulassung drohen Insolvenz, Aufgabe von Geschäftsfeldern oder die Unternehmensauflösung.

3 Definition grundlegender Elemente

Abbildung 3.1: Elemente des IAMs

Das folgende Kapitel dieser Arbeit wird sich mit den grundlegenden Elementen des IAMs beschäftigen. Die Abb. 3.1 zeigt vier Teilgebiete, nach denen die Elemente gruppiert werden.
Im Abschnitt Identitätsmanagement wird die Auffassung und der Umgang mit Identitäten in der realen und virtuellen Umgebung erläutert.
Der Bereich Zugriffskontrolle beschäftigt sich mit der Unterscheidung des physischen Zutritts und dem Zugriff in einer nicht-realen bzw. virtuellen Umgebung.
Die Ausführungen zur Berechtigungssteuerung sollen ein Verständnis schaffen, rund um die Erteilung von Befugnissen auf zu schützende Objekte.
Der Abschnitt Role Based Access Control (RBAC) erläutert das konzeptuelle Zusammenspiel der Elemente.

Erfüllung der Zielsetzung

Die Tabelle 3 fasst zusammen, welche der Elemente Wirkung auf die jeweiligen Anforderungen, Gesetze und Normen haben und erfüllt die zweite Zielsetzung der Arbeit. Die Nachweise folgen im Anschluss in den Definitionen.

Element	Betroffene Forderung	Fundstelle
Identitätsträger und -arten	Identitätsmanagement	ISO 27000-Serie, IT-Grundschutz
	Verantwortlichkeiten	ISO 20000-Serie
	Erhöhung der Transparenz	KonTraG
Rollen	Funktionstrennung	SOX/EuroSOX, BDSG
	Festlegung von Rollen	ISO 20000-Serie
Berechtigungen	Berechtigungsvergabe	SOX/EuroSOX
	Zugriffskontrolle	BDSG, GoBD
	Berechtigungsmanagement	ISO 27000-Serie, IT-Grundschutz
Ressourcen	Zugangskontrolle	BDSG
	Schutzbedarfsfeststellung, Sicherheitsanalysen	IT-Grundschutz
	Berücksichtigung von Risiken	ISO 27000-Serie, IT-Grundschutz
Lebenszyklusphasen	PCDA-Zyklus, KVP	ISO 20000-Serie, ISO 9000-Serie
RBAC, als Elemente in Kombination verstanden	Weitergabekontrolle	BDSG
	Konstante Kontrollelemente, Steuerungsprozesse	ISO 20000-Serie
	Erhöhung der Transparenz	KonTraG
	IT-Kontrollen,Transaktions-Monitoring, Dokumentationspflicht	SOX/EuroSOX
	Erhöhung Qualität, Konsistenz und Transparenz der Eigenkapitalbasis	Basel II-III

Tabelle 3.1: Wirkung grundlegender Elemente zur Erfüllung der Forderungen

3.1 Identitätsmanagement

Der Begriff der Identität steht nach[24] in der Informatik für die statische und einzigartige Zuordnung eines Objekts zu bestimmten Eigenschaften. Das Objekt muss physisch, kontextuell oder logisch existent sein. Eine Identität wird zusätzlich durch eine Rolle, die definiert in welcher Weise das Objekt agiert und interagiert, beschrieben. Es erfolgt demnach eine Differenzierung zwischen passiven Merkmalen (Eigenschaften) und der aktiven Interaktion (Rolle). Dargestellt in Abb.3.2. Bei Identitäten mit gemeinsamen Eigenschaften erfolgt eine Bündelung in Gruppen, sodass eine Identität als Bezeichner für eine wohldefinierte Kombination aus Eigenschaften, Rollen und der Zugehörigkeit einer Gruppe aufgefasst werden kann. Rollen dürfen von beliebig vielen Identitäten gelebt werden, während eine Identität nur durch ein Subjekt repräsentiert werden darf[24]*S.21-23*. Rollen werden im Verlauf des Kapitels noch näher erläutert und in Beziehung zu Berechtigungen gesetzt, vorerst werden Rollen vereinfacht als Bündelung für Funktionen und Aufgaben betrachtet.

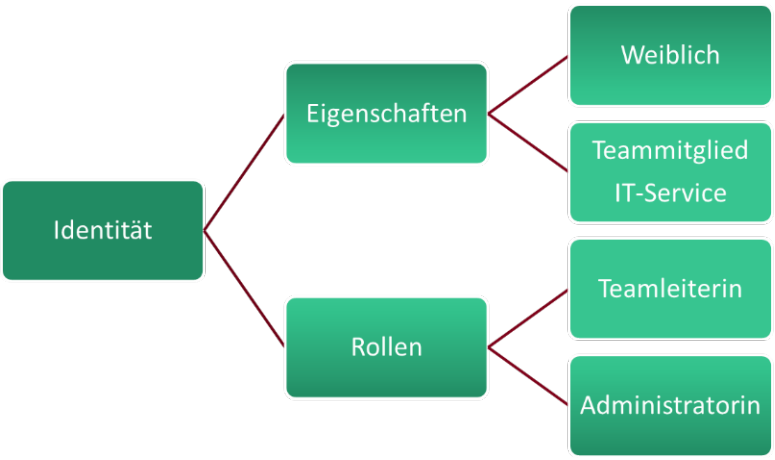

Abbildung 3.2: Merkmale und Ausprägungen einer Identität

3.1.1 Identitätsarten

Physische Identität

Die einfachste Form der Identität ist nach[24]*S.23* die physische oder die personelle Identität. Eine Person mit körperlichen und charakteristischen Eigenschaften, die entweder angeboren, vererbt, erworben oder sozialisiert worden sind und verschiedene Rollen leben kann. Die personelle Identität stellt aus Sicht des Unternehmens eine unveränderliche Größe dar und ist der Ausgangspunkt der Anforderungen auf denen Aufgaben, Funktionen, Rollen und spätere Berechtigungen zur Ausübung aufbauen.

Beispiel: Max Mustermann

Gelebte Identität

Das aktiv werden einer personellen Identität zum Zwecke Erfüllung vorgegebener Anforderungen durch Rollen und Funktionen, wird als gelebte Identität bezeichnet[24]*S.24*. Diese kann somit genutzt werden, um eine Rolle oder eine Kombination von Rollen zu kapseln und im Anschluss einer personellen Identität zuzuordnen.

Beispiele: Einkäufer, Verkäufer, Abteilungsleiter

Kontextuelle Identität

Die Identität wird in einen Kontext gesetzt, sodass entscheidend ist, in welcher Beziehung oder in welchem Zusammenhang die Identität betrachtet wird. Bezeichnend dabei ist, dass nur der direkte Bezug relevant ist und übrige Umstände vernachlässigt werden[24]*S.24*. Aufgrunddessen kann eine kontextuelle Identität von mehreren personellen Identitäten gleichzeitig, die synonym zur Rolle stehen, gelebt werden.

Beispiele: Brandschutzbeauftragter oder Krisenmanager

Logische Identität

Erfolgt eine Abbildung einer personellen oder kontextuellen Identität in eine nicht-reale oder virtuelle Umgebung, wird dies als logische Identität bezeichnet. Diese Identitäten existieren auf einer erzeugten, berechneten und logischen Ebene und werden von physischen Identitäten aus der realen Welt gesteuert. Aus Sicht der IT repräsentiert die logische Identität überwiegend personelle Identitäten in einem System oder innerhalb einer Anwendung. In diesem Bezug wird dann von einer technischen Identität gesprochen[24]*S.24*. Die Verwaltung der technischen Identitäten erfolgt seitens des IT-Systems durch Konten, *im engl. accounts*. Wird dieses Konto ausschließlich von einer personellen Identität gesteuert, wird von einem Benutzerkonto, *im engl. user account*, gesprochen.

Beispiele: Max.Mustermann@beispielAG, human.resource@beispielAG oder sekretariat@beispielAG

3.1.2 Identifizierung von Identitäten

Die rechtlichen Vorgaben aus Abschnitt 2.4 geben vor, dass Konzepte zur Zugriffskontrolle und Berechtigungssteuerung Mechanismen enthalten müssen, die aufzeigen können, welche Accounts von welchen Identitätsträgern innerhalb der IT-Landschaft gelebt werden. Aus Sicht eines Unternehmens bedeutet dies, dass jederzeit ersichtlich sein muss, welcher Mitarbeiter oder Benutzer welche Befugnisse bzw. Berechtigungen besitzt und

für welche Objekte diese Gültigkeit haben[24]*S.25*. Berechtigungen werden im Kapitel 3.3.2 erläutert und daher vorerst vereinfacht als Befugnisse oder Autorisierung betrachtet. Nachfolgend die wichtigsten Identitätsträger gebündelt nach Art der Identität[24]*S.25-29*.

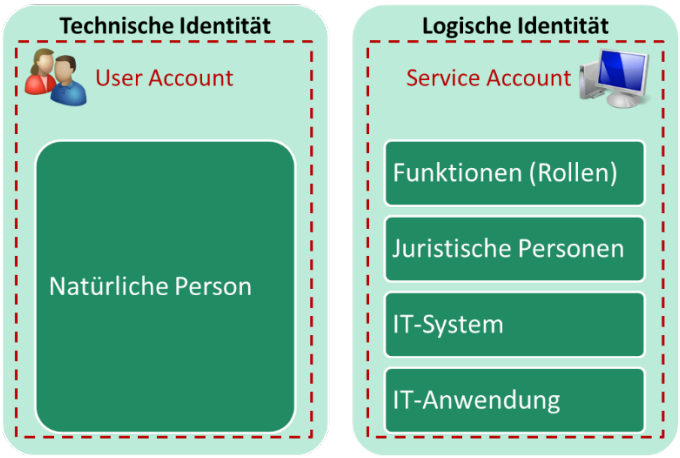

Abbildung 3.3: Unterscheidung von Identitäten

Technische Identität

- **Natürliche Person**
  Einem User Account kann direkt eine Person bzw. ein Mitarbeiter zugeordnet werden.

Logische Identität

- **Funktionen (Rollen)**
  Im Rahmen einer Funktion nimmt ein Mitarbeiter eine Rolle ein und erhält folglich für diese Befugnisse. Die Rolle ist somit ein Bindeglied zwischen personeller Identität und notwendigen Berechtigungen[24].
- **Juristische Personen oder Organisationseinheit**
  Die Erteilung von Befugnissen kann sowohl für juristische Personen (einem Unternehmen), für eine gesamte Organisationseinheit, einem Fachbereich oder einer ganzen Abteilung erfolgen[24].
- **IT-System**
  Ein Server oder Client kann in einer definierten Umgebung eine eigenständige Identität annehmen, um Daten und Informationen verarbeiten oder übertragen zu können[24].

- **IT-Anwendung**
  Analog zu einem IT-System kann Software eine eigenständige Identität darstellen, um automatisierte Schritte im Hintergrund durchführen zu können. Hier ist eine Unterscheidung in zwei Berechtigungsebenen gemäß[24] notwendig. Die erste bezieht sich darauf, welche Funktionen auf dem System oder im Netzwerk erlaubt sind, die zweite Ebene definiert einen Berechtigungsrahmen innerhalb der Anwendung. Wenn eine logische Identität z.B. eine Organisationseinheit, ein IT-System oder eine IT-Anwendung, durch einen Account repräsentiert wird, dann wird in dieser Arbeit von einem technischen Dienstkonto gesprochen und die engl. Bezeichnung Service Account zukünftig verwendet.

Zusammengefasst

Die Grafik 3.3 fasst die genannten Identitäten und deren Träger zusammen. Mit dem IDM wird der Grundstein für Transparenz gelegt, um Aktivitäten einer Identität zuordnen zu können innerhalb eines IT-Umfeldes. Der logischen Identität können beliebig viele Identitätsträger zugeordnet werden, weshalb die Wichtigkeit der Transparenz- und Dokumentationspflicht aus z.B. KonTraG, Grundsätze ordnungsgemäßer datenverarbeitende gestützte Buchführungssysteme (GoBS), BDSG oder SOX und EuroSOX *(Kapitel 2.4 bis 2.7)* an dieser Stelle besonders deutlich wird.

3.2 Zugriffskontrolle

3.2.1 Authentifizierung

Die Zugriffskontrolle durch Authentifizierung[24]*S.127* prüft, während einer Aktivität, identitätsbezogene Informationen der Identität um diese zu bestätigen, durch:

- Preisgabe von Wissen:
  - Benutzername
  - Passwort
  - PIN
- Benutzung eines Besitzes:
  - Ausweis
  - Schlüssel
  - Token, der ein Code oder Passwort generiert
- Benutzung des eigenen Subjekts:

- Fingerabdruck
- Scan der Iris oder Retina
- Stimmendiagramm

Mit der Wiedergabe, Aushändigung oder Nennung identitätsbezogener Informationen, wird die Identität des Subjekts und ebenfalls die Einzigartigkeit dieser bestätigt.

3.2.2 Autorisierung

Die Zugriffskontrolle durch Autorisierung nach[24]*S.159* prüft, ob eine Identität, die eine Aktivität vornehmen möchte dazu berechtigt ist. Beispiel aus[24]*S.159/160*:
"*Der Sachverhalt der Autorisierung auf einem IT-System verhält sich ähnlich der Autorisierung bei einer Kreditkartenzahlung. Eine Karteninhaberin möchte z.B. eine Zahlung bei einem Kauf ausführen. Dazu wird ihre Kreditkarte durch das Lesegerät im Geschäft gezogen, und die Daten werden an die Kreditkartenfirma übertragen. (...) Nachdem die Überprüfung stattgefunden hat, und die von der Kreditkartenfirma in ihrem EDV-System vorliegenden Regeln die Transaktion erlauben würden, kann der mittels Kreditkarte gewünschte Kauf stattfinden.*"
Der Autorisierungsvorgang im IT-Umfeld besteht folglich aus mehreren Stufen[24]*S.159/160*:
"*Nachdem ich nunmehr Ihre Identität kenne und weiß wer Sie sind, lassen Sie mich nachschauen ob ich Ihnen erlauben werde zu tun, was Sie gerne möchten.*" Ablauf dargestellt in Abb.3.4.

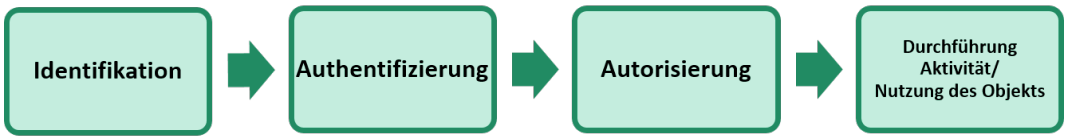

Abbildung 3.4: Schritte eines Autorisierungsvorgangs nach[24]*S.159*

3.2.3 Zutrittskontrolle

Ein naheliegender Rückschluss kann die Annahme sein, dass die Zutrittskontrolle im IAM untergebracht werden kann, da dort Identitäten, deren Rollen und Berechtigungen im Unternehmen administriert werden. Die Zutrittsausweise parallel zu der Verwaltung von Accounts auszuführen erscheint in[42] als eine logische und pragmatische Konsequenz. Im

Rahmen dieser Arbeit werden daher die Begrifflichkeiten Zugriff und Zutritt spezifiziert, unter der Berücksichtigung eines Kontextes, um eine Abgrenzung vorzunehmen.

- **Physischer Zutritt**
  Bei dem physischen Zutritt geht es um Räume und Objekte in der Realität. Dieser beginnt am Gebäudeeingang, über den Empfangsbereich, die Stockwerke, Flure, Büroräume bis hin zum Lager, Abstellkammern oder zuvor definierten Bereichen die Räumlichkeiten umfassen. Weiterer physischer Zugriff kann die Benutzung von Werkzeugen, Fahrzeugen, Schränken, Kassen oder der Zutritt zum Safe sein. Der physische Zutritt ist folglich mit der Zutrittskontrolle durch Authentifizierung umzusetzen, unter dem Einsatz von Zutrittsausweisen.
- **Virtueller Zugriff IT-Betrieb**
  Der virtuelle Zugriff im IT-Betrieb bezieht sich auf alle virtuellen Zugriffe einschließlich der dazu notwendigen Betriebsmittel. Notebooks, Fat- und Thin- Clients, Desktop Computer, Server, Applikationen, Laufwerke, Ordner oder einzelne Dateien. Der physische Zutritt zu Computern oder Terminals ist demnach Aufgabe der Zugangskontrolle, die in ITIL[43] dem Facilities Management zugeordnet ist.

In den nachfolgenden Kapiteln steht der virtuelle Zugriff im IT-Betrieb im Vordergrund, der vereinzelnd mit dem physischen Zutritt in Verbindung gebracht wird.

3.3 Berechtigungssteuerung

Die Berechtigungssteuerung befasst sich mit der konzeptuellen Struktur, wie Berechtigungen erteilt werden. Dabei erhalten Rollen, im Rahmen bestimmter Vorgaben, abgestimmte Berechtigungen auf notwendige Ressourcen und unterliegen einem Lebenszyklus, dessen Nachweiserbringung im Abschnitt 3.9 zu finden ist.

3.3.1 Rollen

Eine Rolle stellt eine Instanz zwischen einem Subjekt dar, dass mit einem Objekt interagiert. Daraus folgend ist die Rolle ein Werkzeug zum abstrahieren eines allgemeinen Handlungsrahmens. Dieses formale Beschreibungskonzept[44] wurde im Jahr 1969 auf der American Federation of Information Processing Societies (AFIPS) Spring Conference vorgestellt. Eine Rolle stellt damit eine Subjekt-Objekt Beziehung dar und kann im mathematischen Sinne als Relation beschrieben werden[45]*S.19.* Abbildung 3.5 verdeutlicht die Subjekt-Objekt Relation und deutet, durch die schraffierte Hinterlegung, den

Handlungsrahmen an. Die Betrachtung einer Rolle steht immer im festen Zusammenhang eines Kontextes.

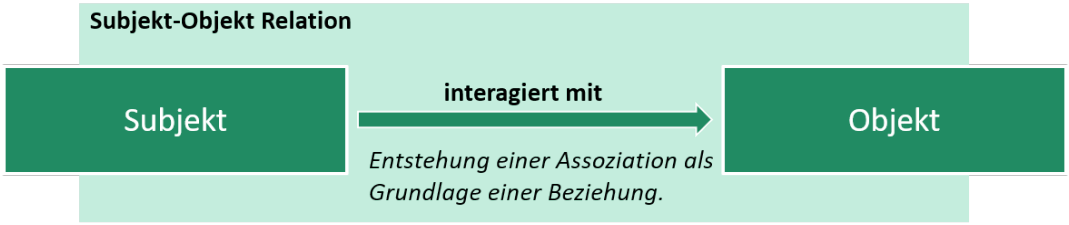

Abbildung 3.5: Subjekt interagiert mit Objekt

- **Organisatorisch**
  Im organisatorischen Sinne stellt die Rolle eine Funktion, die ein Subjekt innerhalb eines Unternehmens lebt dar und wird als Unternehmens- oder Geschäftsrolle nach[45]*S.3* bezeichnet *(engl. business or enterprise role)*.
  Beispiele: Sachbearbeiter, Entwickler, Abteilungsleiter
- **Technisch**
  Unter dem technischen Aspekt beschreibt eine Rolle die Interaktion eines Subjekts mit einem zu schützenden Objekt. Näher spezifiziert fasst die Rolle den Umfang der Befugnisse auf das Objekt zusammen[24]*S.12*. Folglich wird von einer IT-Rolle gesprochen. *Im engl. It or system role*[45]*S.3*.
  Beispiel: Befugnisse eines Benutzers zum Start eines Programms und welche Teile der Anwendung genutzt werden dürfen.

Unternehmensrolle

Ausgehend von Geschäftsprozessen dienen Unternehmensrollen als Einheiten für die Beschreibung von Anforderungen, Aufgaben und Verantwortlichkeiten innerhalb der Organisation. Diese sind unterschiedlich orientiert[24]*S.10*:

- **Funktionsorientiert**
  Hier wird die Rolle nach der Funktionsart gebildet: Mitarbeiter, Teamleiter, Abteilungsleiter oder Projektleiter.
- **Zuständigkeitsorientiert**
  Diese Rollen sind analog zur Aufbauorganisation abgeleitet: IT-Sicherheit, Risiko Management, Facility Management, Human Ressource oder Controlling.
- **Funktionsträgerorientiert**
  Ebendiese richten sich nach der Benennung des Trägers einer Funktion: Leiter Personal, Leiter Finanzen oder Sachbearbeiter Kredit.

- **Geschäftsprozessorientiert**
  Hinzukommend ist die Ausrichtung der Rollen an den Geschäftsprozessen möglich. Das ist der Fall, wenn die Mitarbeiter im Kontext der zugeteilten Prozessrolle tätig werden: Datenschutzaudit, Produktionsüberwachung und Qualitätssicherung.

Weitere Unterscheidungen zwischen Rollen erfolgt zum Zwecke Bündelung oder hierarchischer Strukturierung[24]*S.11*:

- **Abstrakte Rollen**
  Stellen ein Werkzeug zur Bildung einer Hierarchie im Rollenkonzept dar. Diese bündeln und beschreiben abstrakte Funktionen oder Funktionsbereiche: Auftragsprüfung oder Lager und Versand.
- **Operative Rollen**
  Gewährleisten eine Konkretisierung von abstrakten Rollen. Es wird ein konkreter Bezug zur einzelnen Tätigkeit hergestellt der nicht weiter spezifiziert werden muss: Auftragsprüfung Annahme oder Auftragsprüfung Freigabe.
- **Primärrollen**
  Geschäftsrollen mit Einfluss auf die Wertschöpfungskette werden als Primärrollen eingestuft. Haben diese eine Abhängigkeit und direkten Bezug zur Geschäftstätigkeit wird auch von operativen Rollen gesprochen.
- **Sekundärrollen** Diese Rollen unterstützen mit ihren Tätigkeiten und Aufgabenfeldern die Primärrollen. Deshalb wird an dieser Stelle von unterstützenden Rollen gesprochen (Support-Rollen). Es besteht ein indirekter Einfluss auf die Geschäftstätigkeit und demzufolge eine geringe Berührung der Wertschöpfungskette.

IT-Rolle

Im Fokus stehen die zu berechtigenden Objekte für eine noch unbestimmte Identität. Die technischen Rollen sind auf die Funktionalität innerhalb einer Anwendung oder einem System ausgerichtet und sollen diese beschreiben. Die IT-Rolle wird damit nicht an der Identität, sondern in Anlehnung am Objekt ausgerichtet[24]*S.12*. Als Beispiel für IT-Rollen eignen sich die unterschiedlichen Berechtigungen auf einem System: Administrator, Benutzer oder Gast. Die Zuordnung zwischen der IT-Rolle und einer Identität erfolgt gemäß[24]*S.12*, durch die Anmeldung mit einem Benutzerkonto, welches dann eine technische Rolle, ausgehend von dem System zugeordnet bekommt.

Zusammengefasst

Gemäß[24]*S.10* ermöglichen Rollen (im Rahmen dieser Arbeit auch Rollengruppen genannt) eine Entkopplung von Berechtigungen und Identitäten. Damit wirken diese auf die Funktionstrennung aus SOX/EuroSOX, BDSG ein und ermöglichen die Festlegung von Rollen, die z.B. in der ISO 20000-Serie gefordert wird.
Geschäftsrollen dienen dazu Aufgabenfelder zu benennen, in denen Mitarbeiter aktiv sind. Die IT-Rollen beziehen sich auf den Handlungsrahmen innerhalb des IT-Umfelds und werden von unterschiedlichen Geschäftsrollen genutzt.

3.3.2 Berechtigungen

Interagiert ein anfragendes Subjekt mit einem zu schützenden Objekt muss dieses dazu berechtigt worden sein. Eine Berechtigung stellt eine Befugnis auf das Objekt dar und ist ein zentrales Gestaltungselement zum Schutz von Objekten. Auf der einen Seite steht das Objekt, auf der anderen Seite eine angeforderte Operation[24]*S.1-2*. Grafisch dargestellt in Abb.3.6. Berechtigungen können physischer Natur sein oder sich auf die virtuelle Umgebung beziehen.

- Zutrittsberechtigungen:
  - Steht für die Art des physischen Zutritts in ein reales Objekt
- Nutzungsberechtigungen:
  - Regeln die physische Nutzung eines Objekts
- Zugriffsberechtigungen:
  - Bezeichnet den Sachstand wenn Funktionen und Inhalte in der IT-Umgebung betroffen sind und somit Zugriff in einer virtuellen Umgebung erfolgt[24]*S.1.*
- Ausführungsberechtigungen:
  - Bezeichnet die Nutzung einer bestimmten IT-Funktion[24]*S.1*, beispielsweise das Starten von einem Schreibprogramm

Berechtigungspunkt

Die Stelle an der, z.B. während eines Arbeitsvorgangs, eine Berechtigungsprüfung erfolgt wird in[24]*S.2* als Berechtigungspunkt bezeichnet. Nach erfolgreicher Prüfung verfügt das anfragende Subjekt über die Berechtigung zu einer Operation auf das Objekt. Diese Abfrage kann bereits kurz vor dem Start einer Anwendung erfolgen oder direkt während des Zugriffsversuchs auf das Objekt. Die Abbildung 3.6 zeigt die Instanzen eines anfragenden Subjektes auf ein Objekt.

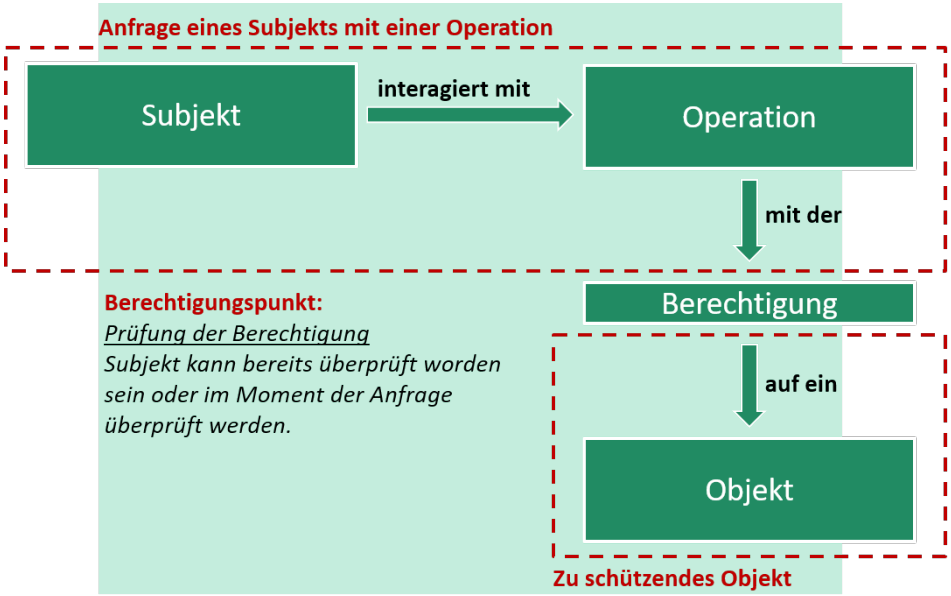

Abbildung 3.6: Ein Subjekt interagiert mit einer Operation auf ein Objekt, dazwischen steht die Berechtigung

Operationen

Aktionen mit Objekten im IT-Umfeld werden als Operation bezeichnet. Ein Subjekt kann für bestimmte Operationen zur Durchführung berechtigt werden. Der folgende Abschnitt stellt die grundlegenden Operationen vor gemäß[24]*S.3-5*:

- **Entdecken** *(im engl. Detect)*
  Ermöglicht, dass die Existenz eines Objekts festgestellt werden kann. Zu beachten ist, dass das Objekt dennoch verborgen bleibt. Es ist möglich, dass 23 Dateien in einem Verzeichnis vorhanden, jedoch nur 21 Dateien sichtbar sind.
- **Suchen** *(im engl. Search)*
  Diese Operation ermöglicht die Suche nach einem Objekt und schließt die Detect-Operation mit ein. Die Suche ist unabhängig davon, ob der Name des Objekts bekannt ist. Enthält das Objekt einen Teil der gesuchten Zeichenkette, wird es in den Suchergebnissen angezeigt.
- **Vergleichen** *(im engl. Compare)*
  Ermöglicht das Vergleichen des ausgewählten Objekts mit anderen. Die Detect-Operation muss eingeschlossen sein, um die Existenz des Objekts feststellen zu können.

- **Darstellen oder Anzeigen** *(im engl. Show)*
  Mit dieser Operation wird das Objekt gegenüber einer Identität sichtbar. Eingeschlossen sind die Search- und Compare-Berechtigungen, die die Detect-Operation enthalten.
- **Lesen** *(im engl. Read)*
  Gestattet ein Objekt inhaltlich zu betrachten und setzt die Show-Operation voraus. Ausgeschlossen ist eine Veränderung des Objekts. Ebenfalls gestattet ist der Zugriff auf die Eigenschaften des Objekts.
- **Hinzufügen** *(im engl. Add)*
  Schafft die Möglichkeit zum Hinzufügen von neuen Objekten und Inhalten. Zu beachten ist, dass nur die Detect-Berechtigung mit eingeschlossen ist. Die Vergabe der Add-Berechtigung hat daher immer einen Bezug zur IT-Security, da diese einem Angreifer bösartiges Verhalten ermöglicht.
- **Ändern** *(im engl. Change or Modify)*
  Die Operation, zum Ändern von Objekten und deren Inhalte ist die erste kritische Operation. Diese ermöglicht das Manipulieren und Zerstören des Objekts und schließt die Read-Operation ein. Es gibt eine erweiterte Form des Schreibens *(im engl. Write)*. Die Write-Operation autorisiert zur Löschung, da die Delete-Operation enthalten ist. Damit ist diese Operation noch mächtiger und ebenfalls im IT-Security Aspekt zu betrachten.
- **Löschen** *(im engl. Delete)* Mit der Delete-Operation kann ein Objekt vollständig gelöscht werden und enthält die Detect-Operation.
- **Ausführen** *(im engl. Execute)*
  Die Execute-Operation ermöglicht das Starten von ausführbaren Objekten, wie z.B. Programme, Skripte oder Dienste. Folglich sind die Detect und Show mit eingeschlossen. Es besteht die Möglichkeit, die Show-Operation auszuschließen, wenn im Hintergrund automatisierte Prozesse tätig sind.

Die formale Genauigkeit unterscheidet zwischen einer zur Verfügung stehenden Operation und der Autorisierung die Operation ausführen zu dürfen. Zur Vereinfachung wird im übrigen Teil dieser Arbeit eine autorisierte Operation auf ein Objekt als Berechtigung zusammengefasst.

Berechtigungsstufen

Einige der vorgestellten Berechtigungen implizierten weitere Berechtigungen und stellen damit eine erste Bündelung dar. Berechtigungsstufen setzten an diesem Punkt an

und umfassen Sammlungen von Berechtigungen. Siehe Abb.3.7. Dies ermöglicht eine schnelle und übersichtliche Vergabe von Berechtigungen auf Objekte. Ein weiteres optionales Merkmal von Berechtigungsstufen ist, dass Funktionen und Inhalte einfließen können[24]*S.8-9.*

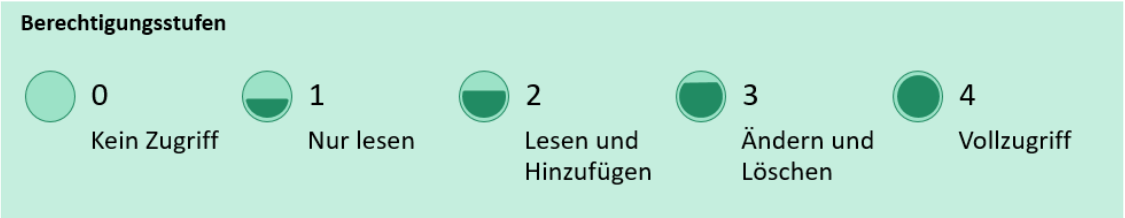

Abbildung 3.7: Zeigt fünf Berechtigungsstufen, adaptiert aus[24]*S.8* die aufeinander aufbauen

- **Stufe 0**
  Ein anfragendes Subjekt erhält keinerlei Zugriff auf ein zu schützendes Objekt. Ob trotzdem die Detect-, Search-, Compare-, oder Show-Berechtigung bestehen, steht in Abhängigkeit zum Schutzbedarf des Objekts.
- **Stufe 1**
  Es wird Lesezugriff auf ein Objekt gewährt. In dieser Stufe werden die Read- und Show-Berechtigungen gemeinsam erteilt. Diese implizieren die Detect-, Search- und Compare-Berechtigungen.
- **Stufe 2**
  Aufbauend auf Stufe 1 ermöglicht diese zusätzlich die Add-Berechtigung. Je nach Schutzanforderungen kann hier bereits die Execute-Berechtigung erteilt werden.
- **Stufe 3**
  Zusätzlich zu allen Berechtigungen der Stufe 2, werden hier die Berechtigungen Modify und Delete hinzugefügt.
- **Stufe 4**
  Auf dieser Berechtigungsstufe gibt es keinerlei Einschränkungen mehr. Diese baut auf den Stufen 1-3 auf und enthält sämtliche Berechtigungen auf die Funktionen, Eigenschaften und Inhalte des Objekts.

Der Abb.3.7 sind die Operationen der Berechtigungsstufen zugeordnet, um die Bündelung zu verdeutlichen.

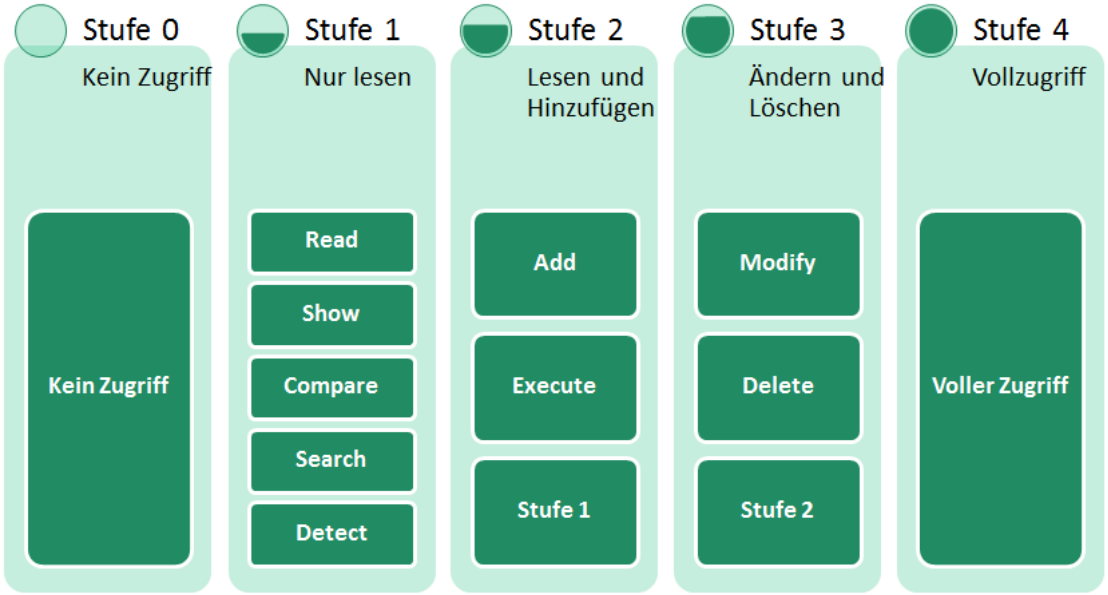

Abbildung 3.8: Berechtigungsstufen mit Operationen

Gestaltung der Berechtigungsstufen

Die bisher vorgestellten Stufen lassen sich beliebig schwach oder stark granulieren und weiter anpassen:

- **Nur lesen und ausführen**
  Dadurch, dass die Execute- und Add-Berechtigungen voneinander unabhängig sind, lässt sich hier eine feinere Abstufung zwischen der Stufe 1 und der Stufe 2 vornehmen.
- **Ändern ohne löschen**
  Diese Verfeinerung wird notwendig, wenn nur bestimmte Identitätsträger die Löschung von Objekten vornehmen sollen. Dies verhindert das versehentliche oder vorsätzliche Entfernen von z.B. Ordnern, Dokumenten oder andere Dateien.
- **Verfeinerung Stufe 3-4**
  Eine Unterscheidung innerhalb der Stufen kann das Erteilen zusätzlicher Operationen durch das Subjekt betreffen. Auf Stufe 3 dürfen nur Lese- und Ausführungsberechtigungen, ab Stufe 4 die Modify- und Delete-Berechtigungen erteilt werden.

Zusammengefasst: Damit wird ersichtlich, wie fein sich Berechtigungsstufen granulieren lassen. Abschließend kann festgehalten werden, dass die Granulierung stark im Kontext des Objekts zu betrachtend ist. Durch die Berechtigungssteuerung sind die Anforderungen z.B. aus der Zugriffs- und Eingabekontrolle des BDSGs und der GoBD umsetzbar. Weiter wirken diese auf die Erfüllung der Berechtigungsvergabe und -Management aus SOX/EuroSOX, ISO 27000-Serie und IT-Grundschutz. Gleichermaßen zu berücksichtigen ist das "Need to know-Prinzip"[33]*S.2890*,[24]*S.9*. Es schreibt vor, dass der Identitätsträger nur jene Berechtigungen erhält, die zur Erfüllung seiner Rolle benötigt werden, analog mit den verbundenen Anforderungen, Aufgaben und Funktionen.

Vergleich zur Zutrittskontrolle

Der Zugriff von Subjekten auf Objekte in einer nicht-realen bzw. virtuellen Umgebung steht in dieser Arbeit im Vordergrund. Die Regelung und Kontrolle der physischen Nutzung eines Objekts oder der Zutritt zu diesem, weißt Parallelen zwischen der Zugriffskontrolle und Berechtigungssteuerung auf.

- **Subjekt und Objekt**
  Ein Subjekt ist in diesem Fall eine Person z.B. in der Rolle eines Mitarbeiters oder eines externen Dienstleisters. Ein Objekt kann in diesem Fall ein Gebäude, Flur, Raum oder eine Kammer sein.
- **Zutritts- und Zugriffsberechtigung**
  Statt virtuelle Operationen stehen physische Aktionen im Mittelpunkt.
- **Nutzungs- und Ausführungsberechtigungen**
  Betreffen Handlungen, die innerhalb eines Raumes vorgenommen werden dürfen.

Neue Ansätze, wie[42] beschreibt, vereinen physische Zutritts- und virtuelle Zugriffsverwaltung. Der Auffassung des Autors zufolge, ein interessanter Gedanke der weiter verfolgt werden kann, da auf diese Weise Zutritts- und Berechtigungsprofile in einer organisatorischen Hand und zentral im Fokus des Informations- und Risikomanagements liegen.

3.3.3 Ressourcen

Bisher standen die Interaktionen von Subjekten im Vordergrund. Ressourcen stellen diesen Inhalte und Funktionen zur Verfügung und werden nach[24]*S.2* unterschieden in:

- Funktionsressourcen:

  - Repräsentieren funktionale Aktivitäten
  - Bsp.: Administrationstool oder Messenger-Dienst
- Inhaltsressourcen:
  - Ermöglichen Zugriff auf Inhalte:
  - Bsp.: Dokumentenverzeichnisse oder Kundendaten
- Funktions- und Inhaltsressourcen:
  - Gewähren Veränderungen von Inhalten
  - Bsp.: Bedienungsoberfläche der Kundendatenbank oder ein Mailprogramm

Obendrein wird die Umgebung, in der die Ressourcen existieren oder genutzt werden differenziert:

- **Physische Umgebung**
  In diesem Bezug sind die Ressourcen Gegenstände, Räume oder andere Objekte in der realen Welt.
- **Nicht-reale bzw. virtuelle Umgebung**
  Die Ressourcen stehen im Kontext des IT-Umfelds: Desktop Computer, Clients, Server, Betriebssysteme, Programme oder Dienste.

Schutzbedarf der individuellen Ressource

Der Schutzbedarf einer Ressource ist im Kontext mit dem Nutzungszweck und -umfang zu betrachten. Dabei wird der Umfang, die Notwendigkeit des Zugriffes und das damit verbundene Risiko geprüft. Ein Risiko ist nach[36]*1.Foliensatz S.5-7* das Ausmaß einer Bedrohung welches quantitativ oder qualitativ bestimmt werden kann. Zwei Werkzeuge nach[36]*1.Foliensatz S.65-66* zur Bewertung von Risiken sollen an dieser Stelle der Arbeit angeschnitten werden:

- **Technische Sicherheitsanalyse**
  Im Vordergrund stehen technische Sicherheitsmaßnahmen und Schwachstellen die Einfluss auf Bedrohungen und die Ressourcen haben. Individuelle Sicherheitslücken, die in Verbindung mit einer einzelnen Ressource auftreten, sind zu beachten. Während der Durchführung der Analyse wird der Wert der Ressource und die Auswirkungen der Nutzung, sowohl die missbräuchliche als auch die reguläre Nutzung, ermittelt. Gleichermaßen sind mögliche Einschränkungen aufzuspüren, die durch die Sicherheitsmaßnahmen hervorgerufen werden.
- **Bedrohungsanalyse**
  In dieser Analyse wird das Verhältnis zwischen potenziellen Angreifern und den Ressourcen betrachtet. Angreifer, die Bedrohungen ausüben und mögliches Wissen

über vorhandene Schwachstellen haben stehen im Vordergrund. Die Ressourcen können, unabhängig ihres Wertes, bereits genug anreizt für einen Angreifer darstellen. Folglich ist der Einfluss der Ressourcen auf die Bedrohungen zu berücksichtigen. Die Ressourcen können, während eines Angriffes, Ziel und Schwachstelle zugleich sein. Dies ist zum Beispiel der Fall, wenn durch eine Funktionsressource Zugriff auf eine Inhaltsressource erlangt werden kann. Die Motive der Angreifer und die Werte und Abhängigkeiten der Ressourcen haben Einfluss auf die Art und den Umfang von Bedrohungen und den damit verbundenen Sicherheitsmaßnahmen.

Zusammengefasst: Die Mitarbeiter eines Unternehmens benötigen unterschiedliche Ressourcen für die Erfüllung der gestellten Anforderungen an ihr Tätigkeitsfeld. Unter Verwendung der vorgestellten Analysen lassen sich mögliche Bedrohungen und deren Eintrittswahrscheinlichkeit ermitteln und bewerten. Dies ist die Grundlage, zur Gestaltung von Berechtigungen und -Stufen, um den Schutz der Ressourcen angemessen aufrechtzuerhalten gemäß BDSG, ISO 27000-Serie und IT-Grundschutz.

3.3.4 Lebenszyklusphasen

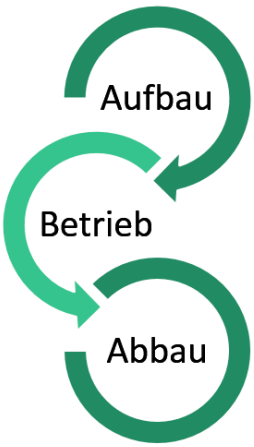

Abbildung 3.9: Lebenszyklus

Die bisher vorgestellten Elemente der Berechtigungssteuerung regeln den Zugriff von verschiedenen Identitätsträgern auf unterschiedliche Ressourcen. Es kann zum Beispiel ein häufiger Wechsel von Identitätsträgern, durch Ein- und Austritt von Mitarbeitern in einem Unternehmen stattfinden. Weiterhin können Umstrukturierungen neue Organisationseinheiten im Unternehmen hervorbringen oder vorhandene verändern. Durch die Einführung neuer Software gelangen weitere Ressourcen in das Unternehmen und alte werden abgebaut. Da Veränderungen in jeden Unternehmensalltag gehören, sind wenige Elemente von dauerhafter und statischer Existenz. Somit kann der Lebenszyklus aus der ISO 31010 IT Risiko Management bei diesen Elementen angewandt werden.

- **Aufbau**
  Konzeption und Definition muss geregelt und definiert sein.
- **Betrieb**
  Die Realisierung und der daraus resultierende dauerhafte Betrieb müssen dokumentiert und überwacht werden. Simultan zählen laufende Anpassungen hinzu, verursacht von neuen bzw. wechselnden Anforderungen oder Regularien.
- **Abbau**
  Wird eines der Elemente nicht mehr benötigt, ist die Aussonderung zu definiere und dokumentieren.

Zusammengefasst: Neue Anforderungen durch Gesetze, Kunden, dem Management oder Geschäftsprozessen erfordern Flexibilität im Unternehmensalltag. Dies bedeutet, dass in der Berechtigungssteuerung der Aufbau, Betrieb und Abbau der aufgeführten Elemente organisiert sein muss. Analog dazu stehen die zu erfüllenden Vorgaben der ISO 20000-Serie Kapitel 2.5.2, die den PCDA-Zyklus integrieren und für eine gleichbleibende Servicequalität Sorge tragen. Dadurch kann zusätzlich eine Wirkung auf den KVP abgeleitet werden, der in der ISO 9000-Serie verankert ist.

3.4 Role Based Access Control

Im bisherigen Verlauf dieser Arbeit wurde die Subjekt-Objekt Relation konkretisiert und spezifiziert. Hinter jedem Subjekt verbirgt sich eine einzigartige Identität, welche durch einen Account in der nicht-realen bzw. virtuellen Umgebung repräsentiert wird. Weitere Kapselung der Interaktion zwischen Subjekt und Objekt sind die technisch und organisatorisch ausgerichteten Rollen, denen Berechtigungsprofile zugeordnet werden. Die Berechtigungen auf ein Objekt repräsentiert zusammengefasst eine Ressource. Die Abbildung 3.10 gibt einen Überblick über die fortwirkende Kapselung und Spezifizierung der Interaktion eines anfragenden Subjekts auf ein zu schützendes Objekt. Diese Elemente der Berechtigungsvergabe sind wiederzufinden im Entwurf aus dem Jahr 2000 für einen Standard der rollenbasierten Zugriffskontrolle, auch Role Based Access Control (RBAC) genannt. Im Februar 2004 wurde dieser vom American National Standards Institute (ANSI) zum *(ANSI INCITS 359-2004)* erklärt. Gemäß[24]*S.69* ist im Standard ein Beitrag von David Ferraiolo und Richard Kuhn[46] enthalten, ebenso floss das an der Goerge University in Fairfox entwickelte Framework[47] zur Zugriffskontrolle von

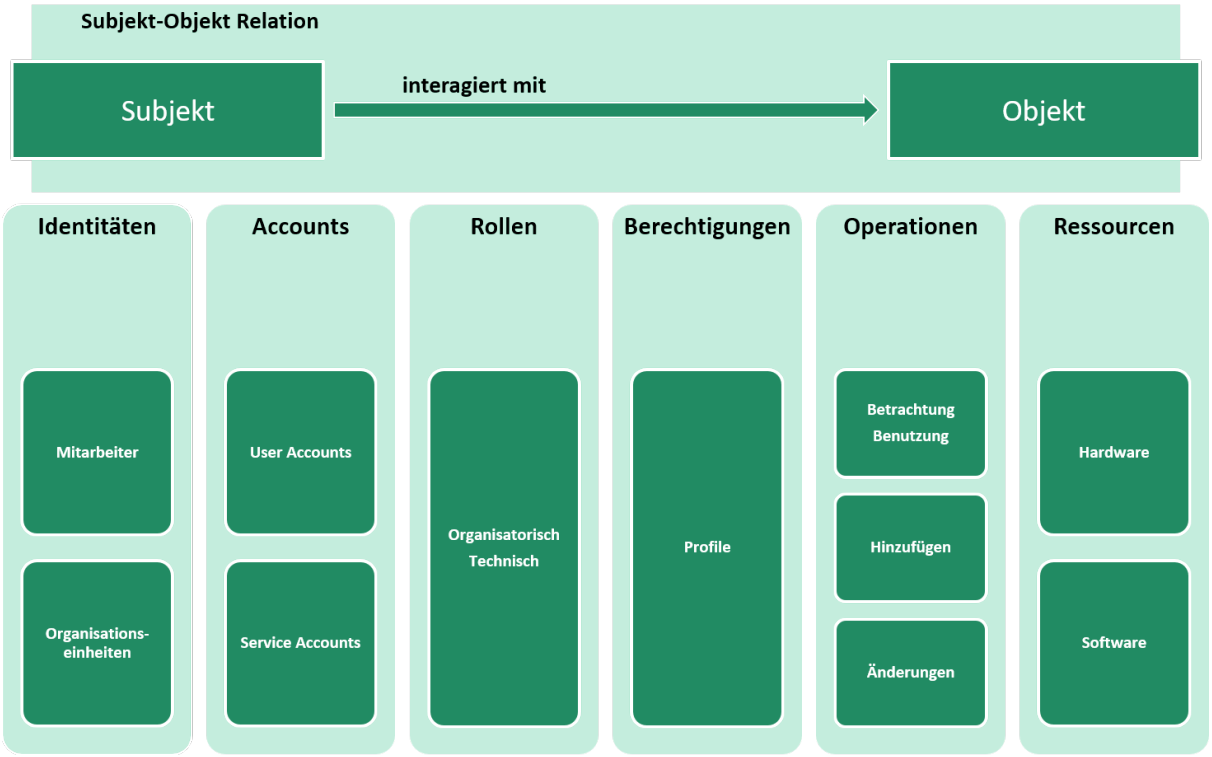

Abbildung 3.10: Subjekt-Objekt Interaktionsstruktur

Ravi Sandhu mit ein. Der Beitrag[46] mit dem Titel "Role-Based Access Control" beschäftigt sich mit der grundlegenden Systematik der Berechtigungsvergabe durch Rollen und der damit notwendigen Trennung einzelner Funktionen. Das Modell, welches auf dem RBAC-Standard basiert, hat drei unterschiedliche, aufeinander aufbauende Ausprägungen[24]*S.69*:

- Core RBAC
- Hierarchical RBAC
- Constrained RBAC

In jeder Ausprägung des Modells wird unterschieden zwischen:

- **RBAC Referenzmodell**
  Es erfolgt die Beschreibung der im Modell verwendeten Elemente. Dazu wird aufgezeigt, wie die Elemente in Beziehung zueinander stehen und diese zusammen wirken.

- **RBAC Funktionale Spezifikation**
  In die Spezifikation fließen die Definitionen von Funktionalitäten der RBAC-fähigen Systeme ein, die zur Verwendung vorgesehen sind. Diese setzen später die Modellausprägung um und ermöglichen damit die Verwaltung.

3.4.1 Core RBAC

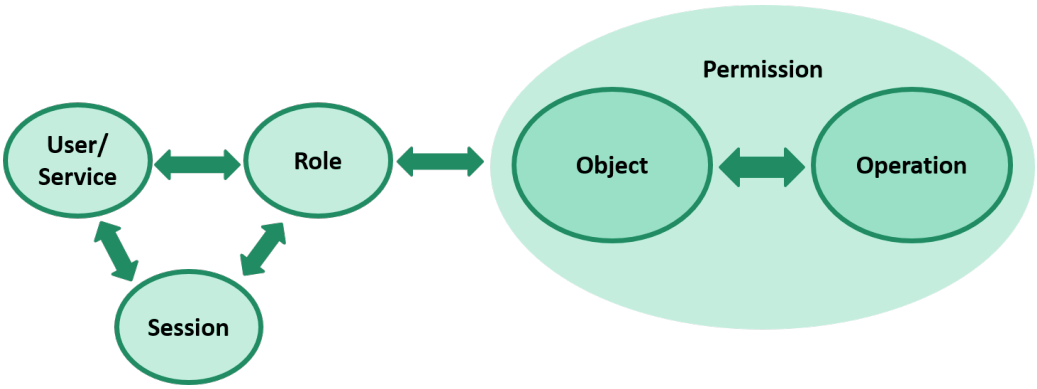

Abbildung 3.11: Core RBAC, adaptierte Grafik aus[24]*S.71*

Dies bildet den Kern des rollenbasierten Berechtigungsansatzes. Siehe Abb.3.11. Grundlegende Komponenten nach[24] sind:

- Benutzer *(engl. User)*:
  - Repräsentiert die in Abschnitt 3.1.1 vorgestellten Identitätensarten.
- Rolle oder Rollengruppe (engl. Role or role group):
  - Stellt die in Kapitel 3.3.1 definierten Rollen dar.
- Benutzersitzung *(engl. User session)*:
  - Ist eine zeitlich begrenzte Verknüpfung, die den Benutzer und die Rolle zur Laufzeit des Zugriffes verbindet. Siehe ergänzend Abb.3.6.
- Objekt *(engl. Object)*:
  - Ist das zu schützende Element im Modell wie z.B. Hardware, Software oder Informationen wie Dateien und Ordner. Siehe Kapitel 3.3.3
- Berechtigung *(engl. Permission)*:
  - Stellt mögliche Aktivitäten dar, wie in Abschnitt 3.3.2 erläutert
- Operation *(engl. Operation)*:

– Repräsentiert die Art einer Aktivitäten mit einem Objekt, wie in Abschnitt 3.3.2 erläutert

Wie in Kapitel 3.3.3 definiert, wird im Rahmen der Arbeit eine gewährte Operationen als Berechtigung oder -Stufe verstanden. Hinzukommend wird nun eine Berechtigung auf ein Objekt als Ressource zusammengefasst. Grafische Darstellung in Abb. 3.12, 3.13. Daraus folgt, dass z.B. für den Administrations- und Anwenderzugriff auf einen Server je eine separate Ressource konzeptuell angelegt wird. Dieser Schritt ermöglicht es, die in Kapitel 4.2 aufgeführte Access Control List zu erweitern.

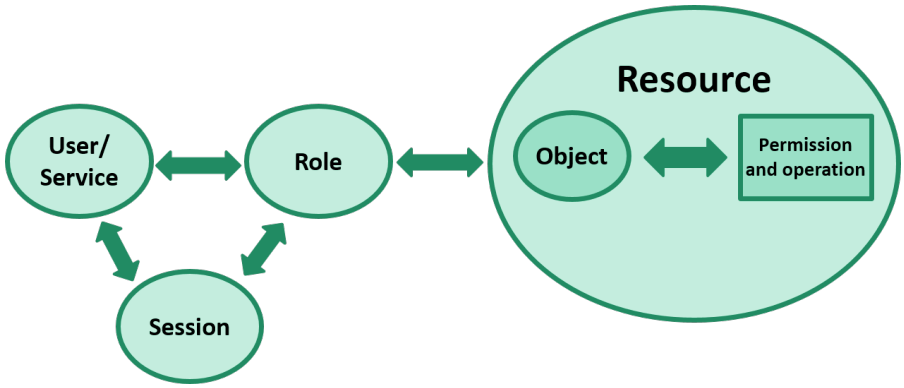

Abbildung 3.12: Zusammenfassung von Object, Operation und Permission

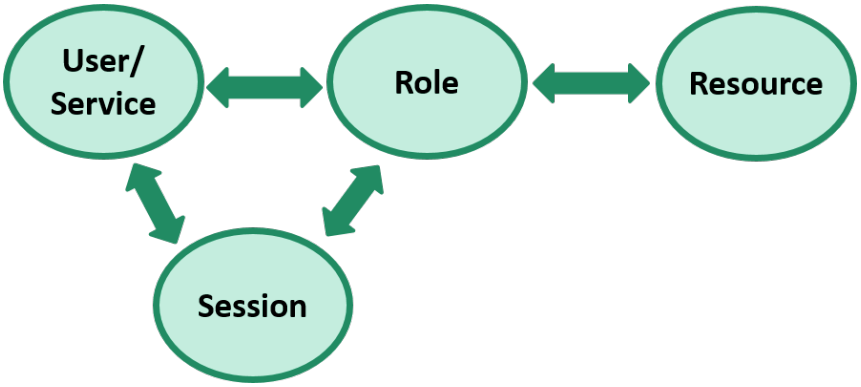

Abbildung 3.13: Vereinfachung Abbildung 3.12

3.4.2 Hierarchical RBAC

Dies folgt der Struktur aus dem Core RBAC und erweitert das Modell um eine hierarchische Ordnung der Rollen. Das Modell ermöglicht zwei Arten von Hierarchien[24]*S.75.*

General Hierarchical RBAC

Dies ermöglicht die freie Gestaltung der Rollen-Hierarchie. Rollen können mehrere übergeordnete und untergeordnete Rollen besitzen *(im engl. multiple inheritance)* und damit weitere Befugnisse vererbt bekommen oder weiter vererben. Flexibilität und schnelle Anpassung werden dadurch ermöglicht. Dies kann auf Kosten der Übersicht geschehen.

Limited Hierarchical RBAC

In manchen Fällen kann es sinnvoll sein, eine Limitierung in die Hierarchie einzuführen. Dies führt zu einer festen Struktur innerhalb der Rollen und verhindert, dass untereinander zu viele Abhängigkeiten entstehen. Ein weiteres Kriterium zur Anwendung des Limited Hierarchica1 RBAC kann das System selbst darstellen. Nicht alle Betriebssysteme, Firmwares oder Anwendungen ermöglichen eine multiple inheritance. Folgende Vererbungshierarchien sind möglich:

- **1:n Verhältnis**
  Eine Rolle darf beliebig viele untergeordnete Rollen enthalten, jedoch nur eine übergeordnete Rolle zugeordnet bekommen. Somit können Berechtigungen an mehrere Rollen weitergegeben werden, aber jede Rolle empfängt weitere Befugnisse von nur einer übergeordneten.
- **n:1 Verhältnis**
  Eine einzige untergeordnete Rolle ist gestattet, jedoch eine Vielzahl an übergeordneten. Dies ermöglicht eine Baumstruktur und sorgt dafür, dass Berechtigungen von unterschiedlichen Rollen geerbt werden können und nur an eine einzige Rolle weitergegeben werden dürfen.

Bei der Wahl eines Limited Hierarchical RBAC-Models muss beachtet werden, dass eine nachträgliche Änderung der Struktur nur unter Einhaltung des 1:n oder n:1 Verhältnisses möglich ist. Dies geht zu Lasten der Flexibilität und zu Gunsten der Ordnung und Übersicht.

3.4.3 Constrained RBAC

Mit dieser Erweiterung des RBAC-Modells wird die Funktionstrennung eingeführt. Der Ansatz verhindert gemäß[24]*S.77*, dass ein Benutzer *Antragsteller* zusätzlich zu der Rolle *Genehmiger* ausführt. Erfolgt diese Funktionstrennung nicht, kann es unter Umständen möglich sein, dass sich eine Person die eigenen Anträge genehmigt, z.B. die Budgetplanung des eigenen Teams gegenüber der Finanzabteilung. Zwei verschiedene Modi bietet das Constrained-RBAC:

- **Statische Funktionstrennung** *(engl. Static Separation of Duty, SSD)*
  Bereits während des Anlegens der Rollenzuordnung wird geprüft, ob diese Kombination innerhalb der Hierarchie unzulässig ist. Dabei werden bereits zugeordnete Rollen berücksichtigt.
- **Dynamische Funktionstrennung** *(Dynamic Separation of Duty, DSD)*
  Erst während der Benutzersitzung erfolgt die Prüfung, ob zwei Sitzungsrollen eine unzulässige Kombination bilden.

Das passende Beispiel aus[24]*S.79* verdeutlicht den Unterschied zwischen der statischen und dynamischen Funktionstrennung:
"*Nehmen wir die beiden Rollen Handy-Telefonierer und Autofahrer. Die statische Funktionstrennung würde sagen: Wenn du bereits die Rolle Autofahrer besitzt, verweigere ich die Zuordnung der Rolle Handy-Telefonierer und umgekehrt. Das bedeutet: Als Autofahrer bekomme ich erst gar kein Handy.*
Die dynamische Funktionstrennung sagt: Du kannst mit dem Auto fahren. Du kannst mit dem Handy telefonieren. Während des Autofahrens darfst du aber nicht mit dem Handy telefonieren, also beides nicht gleichzeitig tun."

Zusammengefasst

Die unterschiedlichen RBAC Ausprägungen vereinen die in Kapitel 3.3 vorgestellten Elemente und ermöglichen Rollenhierarchie und Funktionstrennung. Damit stellen die RBAC-Modelle einen wichtigen Bestandteil dar, um Anforderungen, Gesetze und Normen aus Kapitel 2.3 zu erfüllen. Dabei ist zu beachten, dass die rollenbasierte Berechtigungsvergabe ein IDM voraussetzt und davon getrennt steht.
Abgeleitet aus[46],[24] stellt RBAC die Frage: "Welche Identität wird *wie* berechtigt?", während das IDM die Frage: "Welche Identitäten dürfen oder müssen *existieren*?" in den Mittelpunkt rückt. Die konzeptuelle Schnittstelle ist nach[24] das Berechtigungskonzept,

das Rollen und Berechtigungen zuordnet und begründet. Zusätzlich wird definiert welche Identitäten existent sind und welche Rollen von den Identitäten gelebt werden. Im späteren Kapitel 4.2 der gegenständlichen Arbeit wird diese Thematik aufgegriffen.

4 Einfluss praktischer Begebenheiten

Dieses Kapitel schafft den Übergang, ausgehend von den Anforderungen und Vorgaben, über die grundlegenden Elemente hin zu einer ITIL geprägten Anwendung des IAMs im Unternehmensalltag. Der Autor der gegenständlichen Arbeit ergänzt den Einfluss praktischer Begebenheiten, die das ITIL Framework um Erfahrungswerte und Best-Practices erweitern.

4.1 Access Management gemäß ITIL

Prozess *Access Management* (*auch Berechtigungs-Management oder Identity or Rights Management[20]S.155,[21]S.88 genannt*) wurde in ITIL-V3 2007, nachdem Aspekte der Informationssicherheit (IS) zu der Aufnahme drängten[43], integriert und wird in diesem Abschnitt mit ERM- und IS-Bezug betrachtet. Einer der Hauptaspekte ist die Sicherstellung, dass nur autorisierten Usern die Nutzung von Ressourcen wie z.B. IT-Systemen, Software oder Hardware gestattet wird. Deshalb wird im Rahmen dieser Arbeit die Bezeichnung Identity Access Management (IAM) gemäß[19]*S.170* genutzt, da sowohl Identitäten als auch Rollen und Berechtigungen für den Prozess relevant sind und der Beantragungsweg für Berechtigungen eine Überprüfung der Identität und Autorisierung des Antragsstellers vorsieht. Die daraus resultierenden Vorgaben führten zu der Integration[21]*S.41* des IAMs in die Service Operation und zur Anbindung des Request Fulfilment und Incident Management als weitere Kontrollinstanzen[43]. Die ITIL-Version 2011 etablierte die Schnittstelle zum Event-Management, das sicherstellen soll, dass Zugriffsrechte zurückgenommen werden, wenn einmalige Aktivitäten, z.B. Projekte, Testphasen etc. durchgeführt worden sind.

Einordnung in die Service Operation

Mit den Vorgaben der ITIL Service Operation (Servicebetrieb) wird sichergestellt[20]*S.154*, dass der Tagesbetrieb z.B. IT-Services, Anwender-Anfragen und Betriebsaufgaben, effektiv und effizient erbracht wird. Folglich stehen die Abwicklung und Betreuung der

betrieblichen Aufgaben und Aktivitäten im Mittelpunkt. Folgende Konzepte und Themen sind gemäß[20] dem Servicebetrieb zuzuordnen:

- Service Operation Lebenszyklus
- Prozessgrundlagen
- Prozeduren und Funktionen
- Anwendungsmanagement
- Infrastrukturmanagement
- Betriebsmanagement
- Rollen und Verantwortungen
- Prozesssteuerung
- Arbeitsvorlagen (Templates)
- Methoden, Praktiken und Werkzeuge
- Umsetzung der Service Design Vorgaben
- Skalierbarkeit
- Messung und Steuerung
- Herausforderungen, kritische Erfolgsfaktoren und Risiken
- Bewährte gelebte Praktiken im Unternehmen

Die Einordnung der Service Operation im ITIL-Lifecycle zeigt Abb. 4.1.

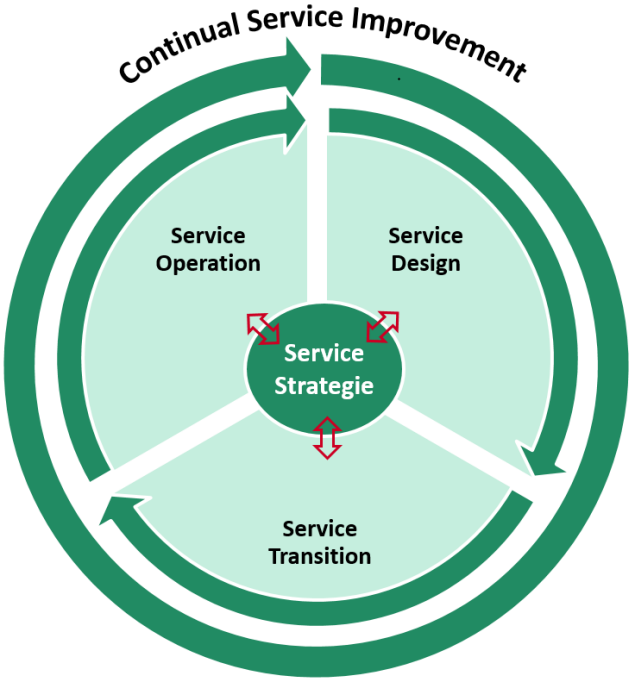

Abbildung 4.1: ITIL Lifecycle adaptierte Grafik aus[20]*S.145*

Gemäß[20]*S.155* und[43] sind die Ziele des IAMs die Unterbindung von unbefugtem Zugriff, Bewilligung und Erteilung von Zugriffsrechten auf vorhandene Ressourcen und die Verwaltung der User- und Service- Accounts. Der Prozess beruht hauptsächlich

auf Vorgaben aus dem Informations- und Risikomanagement (Kap. 2.7). Daraus folgend lassen sich folgende Themen als Submenge der Service Operation für das IAM identifizieren:

- Einhaltung des Lebenszyklus
- Prozeduren und Funktionen
- Betriebsmanagement
- Umsetzung Service Design Vorgaben
- Skalierbarkeit
- Abwendung von Risiken

Handlungsrahmen des IAMs

Das IAM ist effektiv die Ausführung von Availability Management und der Informationssicherheit (IS) in der Form, dass der Prozess das Unternehmen befähigt, die Vertraulichkeit, Verfügbarkeit und Integrität seiner Ressourcen und sensiblen Informationen zu gewährleisten. Der Prozess stellt auf diese Art sicher, dass ein Benutzer die Rechte erhält, um benötigte Ressourcen nutzen zu können[21],[20]. Die Sicherstellung, dass dieser Zugriff dauerhaft in der vereinbarten Zeit zur Verfügung steht, ist die Aufgabe des Availability Management[48]. Das IAM wird in der Regel mit einem Service Request durch den Service Desk initiiert.

ITIL Implementierungsvorgaben

Für die Implementierung eines IAMs gibt es verschiedene Ansätze, die von der Größe des Unternehmens abhängen. ITIL stellt deshalb nur die wichtigsten Aspekte dar, wie z.B. notwendige Schnittstellen zu anderen Prozessen, wichtige Teilprozesse, Artefakte und dass in der IS-Richtlinie Vorgaben und Anforderungen gestellt werden müssen, um die hohen Sicherheitsstandards zu erreichen[43]. Verschiedene Ansätze zur Implementierung sind im IT-Grundschutz und in der ISO 27002:*9 Access control* zu finden. Übersicht siehe Kap. 2.7.4 und 2.5.3.

Zusammengefasst

Das IAM stellt sicher, dass nur autorisierten Usern die Nutzung von Ressourcen der IT-Landschaft gestattet ist und überprüft bereits bei der Beantragung die Autorisierung des Antragsstellers. Damit sind Identitäten ebenso relevant im IAM wie Rollen, Berechtigungen und Ressourcen. Damit unterstützt dieses die Abwicklung und Betreuung der betrieblichen Aktivitäten und ist daher im Servicebetrieb angesiedelt.

4.2 Artefakte und Informationsobjekte

In ITIL werden für das Access Management folgende Artefakte und Informationsobjekte gemäß[43] aufgeführt:

- **Anforderungen für Benutzer-Rollen**
  Erstellung, Anpassung oder Löschung von Rollen, die für den Servicebetrieb notwendig sind.
- **Benutzer-Einrichtungs-Antrag**
  Ein Antrag zur Einrichtung, Änderung oder Löschung einer einzigartigen logischen Identität.
- **Benutzer-Berechtigungs-Antrag**
  Anträge betreffend der Einrichtung und Anpassung von Ressourcen.
- **Benutzer-Rolle**
  Verwaltung und Überprüfung von Rollen bzw. Rollengruppen für die User- und Service-Accounts.
- **User Identity Record**
  Ein Datensatz mit allen Informationen und Attributen rund um einen Account. Es folgt die Zuordnung eines Mitarbeiters und der Abteilung.
- **User Role Access Profile (Berechtigungsprofil)**
  In Form eines Datensatzes wird darin festgehalten, welchen Rollen in den Netzwerk- und Systemumgebungen Zugriff auf Ressourcen gewährt wird.
- **Zugriffsrechte**
  Es werden die Rollenmitgliedschaften der User- und Service-Accounts in Form eines Datensatzes dokumentiert.

Im Rahmen dieser Arbeit werden folgende Artefakte und Informationsobjekte ergänzt:

- **Access Control List**
  Das in[24]*S.168* vorgestellte Werkzeug der Zugriffskontrollliste soll nach einem Vergleich mit der Access Control Matrix[47]*S.37-44* im Rahmen dieser Arbeit erweitert werden. Die Vereinigung von *User Identity Records*, *User Role Access Profile* und *Zugriffsrechte* schafft, den praktischen Erfahrungen des Autors zufolge, eine Matrix mit allen relevanten Informationen der Interaktionsstruktur zwischen Subjekt-Objekt (Kap. 3.4 und Abb. 3.10). Die Liste (Abb. 4.2) lässt sich zur Verdeutlichung als mehrdimensionaler Würfel darstellen (Abb. 4.3). Die erweiterte Access Control List schafft einen *Single Point of Contact*, zu der in Abschnitt 4.5.4

Account	Rolle	Ressource	Team	(...)
Max.Mustermann	Windows-Admin	Domain1-Alle-Server	Active-Directory	
Max.Mustermann	Basis-Rolle	MS-Office365	Active-Directory	
Max.Mustermann	Basis-Rolle	Anmelden-Domain1	Active-Directory	
(...)	(...)	(...)	(...)	

Abbildung 4.2: Tabellarische Access Control List mit Beispieleinträgen. Beliebige Dimensionen können aufgenommen werden.

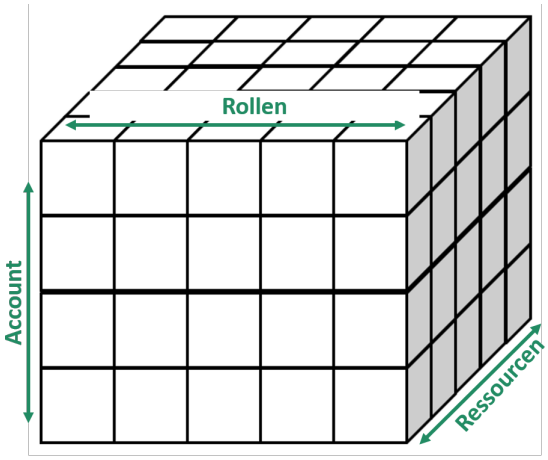

Abbildung 4.3: Erweiterte Access Control List in Form eines mehrdimensionalen Datenwürfels

vorgestellten AC DB und bildet damit die Schnittstelle für den Abgleich zwischen dem technischen Ist-Stand und dem organisatorischen Soll-Stand, der durch die Teilprozesse laufend verändert wird.

- **Richtlinien**
  Gemäß[19]*S.170-173*,[22]*S.308*,[48]*S.246* und den Erfahrungen des Autors enthalten die nachfolgenden Richtlinien zentrale Vorgaben, die im operativen Betrieb eingehalten werden müssen. An erster Stelle stehen die Vorgaben der Compliance (Kap. 2.1).
  - Gesetzliche Compliance
  - Kommerzielle und organisatorische Compliance
  - Security und IS-Richtlinien

    - Regeln Umgang mit Informationen, Risiken, Kennwörtern und Compliance Vorgaben
  - IAM-Richtlinie
    - Spezifiziert die Vorgaben bei der Vergabe von Zugriffsrechten

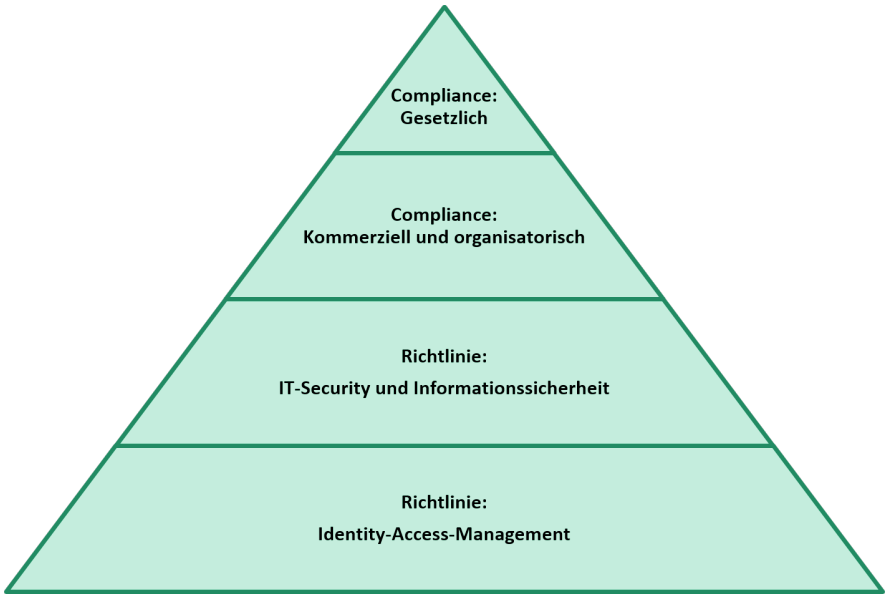

Abbildung 4.4: Abgeleitete Hierarchie der Richtlinien in einem Unternehmen

- **Berechtigungskonzept**
  Es beinhaltet ein Rollen-Rechte Modell[19], die Zugriffskontrollanforderungen der Ressourcen und die unterschiedlichen Account Typen. Die Erstellung und Aktualisierung verantwortet die Fachabteilung wie folgt:
  - Definition von Berechtigungsprofilen, Rollen und Ressourcen
  - Zuordnung Ressourcen und Berechtigungsprofile
  - Zuordnung Rollen und Ressourcen
  - Dokumentation von Administrations-, User- und Service-Accounts
- **Prozessdokumentation**
  Der Prozess IAM muss samt seiner Teilprozesse schriftlich dokumentiert werden, um die Anforderungen aus KonTraG zu erfüllen. Ebenfalls sind die Kontrolleinheiten für das IKS aufzuführen, um die Vorgaben aus Kap. 2.4.1 SOX, EuroSOX und ITIL umzusetzen.
- **Arbeitsanweisungen**
  Anleitungen für die Mitarbeiter der Fachbereiche, die die Beantragungsprozesse

aufzeigen und eine gleichbleibende Servicequalität gewährleisten. Siehe Anforderungen aus Kap. 2.5.2 ISO 20000-Serie. Weitere Arbeitsanweisungen umfassen die Aktivitäten des IAMs, um die Teilprozesse nach Tabelle 4.4 ausführen zu können.

- **Kontrolleinheiten für das IKS**
  Formale Kontrolleinheiten zur Sicherstellung, damit gesetz-, anforderungs- und prozesskonform gearbeitet wird.

4.3 Rollen und Verantwortlichkeiten

Die Ermittlung der Zugriffskontrollanforderungen obliegt nach[49]*S.149-153* dem Fachbereich, während die formale, technische und unternehmensweite Einhaltung dem IAM unterliegt. Eine beratende Aktivität kann dem IAM bei der Ermittlung zugeordnet werden, um die Erfüllung der Vorgaben aus der IS-Richtlinie zu gewährleisten. Folglich werden unterschiedliche Prozessrollen notwendig, die jeweils im IAM und Fachbereich angesiedelt sind.

4.3.1 Access Manager

Dieser bewilligt autorisierten Anwendern und Benutzern das Recht, einen Service zu nutzen und ist eine ITIL-Prozessrolle[43]. Gleichzeitig unterbindet dieser den Zugriff von nicht autorisierten Anwendern durch Ablehnung unberechtigter Anträge. Hauptaufgabe ist die Sicherstellung, dass die Vorgaben aus der IS-Richtlinie eingehalten werden. Dies gilt für Vorgänge innerhalb des IAMs und für Schnittstellentätigkeiten zu anderen Organisationseinheiten. In[48]*S.249* wird der Access Manager wie folgt dargestellt:

- Aufgaben:
  - Überwachung der Zugriffsvergabe
  - Stichprobenkontrolle zur Überprüfung, zwecks Einhaltung der Sicherheitsvorschriften
  - Erstellung von Reports zur Kontrolle des IAMs
- Besetzung:
  - Vorzugsweise durch einen Mitarbeiter aus dem IT-Security-Bereich

Die Erweiterung der Aufgaben, um die Überwachung und Steuerung von Animositäten wirkt der in[49]*S.149-150* beschriebenen Kommunikationslücke zwischen Fach- und IT-Seite entgegen. Dies ermöglicht eine proaktive Handlungsweise des Access Managers in den Teilprozessen, bei auftretenden Problemsituationen.

4.3.2 Access Editor

Die Rolle ist zuständig für die Ausführung der operativen Aufgaben des IAMs und ist keine ITIL-Prozessrolle. Die Adaptierung ist in Anlehnung des *Access Analysts* aus[48]*S.248* gehalten und wird wie folgt beschrieben:

- Aufgaben:
  - Analyse und Verifikation der Aufträge (Service Requests)
  - Umsetzung der Aufträge betreffend Anlegen, Ändern und Löschen für die Benutzer-, Rollen- oder Ressourcenverwaltung
  - Initialisierung und Überwachung von Validierungen
  - Einleitung von Eskalationsmaßnahmen bei Verzögerungen, Fehlern, Sicherheitsverstößen oder Animositäten bei Ausführung der Teilprozesse
- Besetzung:
  - Durch Mitarbeiter aus dem IT-Security-Bereich, wenn kritische Berechtigungen betroffen, oder aus dem Service Desk, wenn unkritische Rechte zu bearbeiten sind

Die Erweiterung um diese Rolle ist für verschiedene Aufgabenschwerpunkte der Prozessrollen sinnvoll. Während der Access Editor auf die operative Umsetzung ausgerichtet ist, ausgehend davon seine Namensgebung erhält und über Detailtiefe verfügt, hat der Access Manager einen regulativen Schwerpunkt, um proaktiv und bereichsübergreifend agieren zu können. Da der Access Editor täglich mit der Umsetzung von Service Requests und dem Ist-Stand vergebener Berechtigungen in Berührung kommt, hat dieser eine fundierte Entscheidungsgrundlage, um regulativen Handlungsbedarf zu erkennen, der dann durch den Access Manager ausgeübt wird.

4.3.3 Schnittstellen zum Fachbereich

Die nachfolgenden Prozessrollen sind in den Fachbereichen der Organisationseinheiten angesiedelt und haben eine Schnittstellenfunktion zum IAM-Prozess. Dazu werden in dieser Arbeit drei Rollen, in Anlehnung des *Access Verifier* aus[48]*S.248*, adaptiert und spezifiziert, um das in Abb. 4.5 verdeutlichte Kommunikationsmodell zwischen IAM und Fachbereich zu ermöglichen. Weiter spezifiziert werden die Prozessrollen durch die praktischen Erfahrungen des Autors.

Access Coordinator *default* (AC default)

Dieser hat zur Hauptaufgabe die Sicherstellung, dass ein Berechtigungskonzept und zwei Access Coordinator-Rollen innerhalb seines Fachbereichs gelebt werden. Neben der Ernennung zweier Mitarbeiter zum AC1 und AC2, hat dieser Zugang zu allen Informationsobjekten, Artefakten und Schulungsunterlagen für diese herzustellen. Im laufenden Betrieb unterstützt der AC-default den Genehmigungsprozess in Vertretung. Welcher Mitarbeiter in den Organisationseinheiten zum AC default ernannt wird, entscheidet sich in Absprache zwischen der IS, dem ERM, dem IAM und der Geschäftsführung. Verankert wird diese Regelung in der IAM-Richtlinie. Es empfiehlt sich den Team- oder Gruppenleiter zum AC-default zu ernennen, da auf diese Art eine "Vorab-Genehmigung" im Handlungsrahmen der Prozessrollen AC1 und AC2 erteilt wird. Demzufolge kann von einer im Prozess delegierten Verantwortung gesprochen werden, die Wartezeiten im Genehmigungsablauf verkürzt. Dies wird in Abschnitt 4.4.1 aufgegriffen.

Access Coordinator *First* (AC1)

Der AC1 ist innerhalb seines Fachbereichs für die Sicherstellung verantwortlich, dass die Zugriffskontrollanforderungen eingehalten werden. Dieser entwirft auf Fachabteilungsebene Zugriffsprofile auf Ressourcen für die Mitarbeiter, die gemäß RBAC (*Kap. 3.4*) in Rollen gekapselt werden (*Rollen und Rechtemodell gemäß[19]*). Hinzukommend betreut dieser die User- und Service-Accounts. Die Beauftragung von Accounts, Rollen und Zugriffsrechten durch Service Requests bei dem IAM obliegt dem AC1. Folglich ist dieser die erste prüfende Instanz im Genehmigungsprozess.

Access Coordinator *Second* (AC2)

Dieser vertritt und unterstützt den AC1 bei der Erfüllung der Aufgaben und ist im Genehmigungsprozess die zweite prüfende Instanz.

Resource owner

Dieser ist Inhaber der Ressourcen, die dem Fachbereich zugeordnet sind und definiert die Zugriffskontrollanforderungen. Für den Genehmigungsprozess bedeutet das, dass bei einer Beantragung von Zugriff auf Ressourcen eines anderen Fachbereichs der verantwortliche Resource owner einzubinden ist. Es empfiehlt sich, den AC1 automatisch zum Resource owner zu ernennen, da auf diese Weise sich Zugriffskontrollanforderungen und das Berechtigungskonzept in einer verantwortlichen Hand befinden. Parallel mindert dieser Ansatz, den Erfahrungen des Autors zufolge, die Anzahl von Ressourcen ohne verantwortlichen Besitzer.

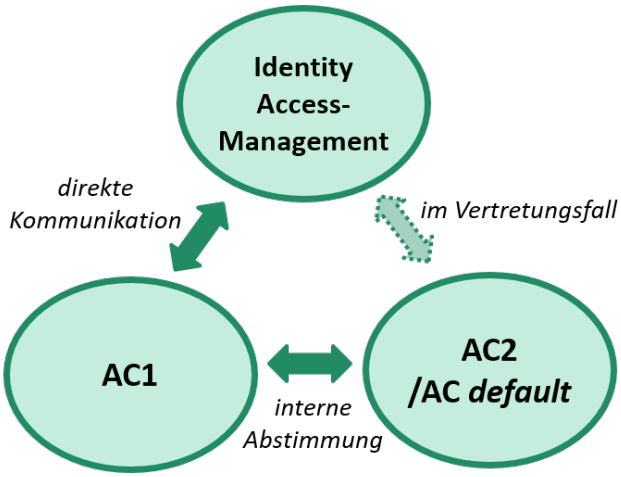

Abbildung 4.5: Kommunikationsmodell zwischen dem IAM und Fachbereich

Zusammenwirken Fachbereich und IAM

Die Rollen AC1 und AC2 bewirken eine Entlastung des Request Fulfilments und Incident Managements bei der Prüfung der Autorisierung des Antragsstellers dahingehend, dass nur autorisierte ACs Anträge stellen dürfen. Folglich verbleibt den genannten Schnittstellen eine Prüfung: Die Ernennung der ACs, die durch den AC default bekanntgegeben worden sind.
Dieses Verfahren ist besonders praktikabel, wenn die Fachbereiche eines Kundens oder externer Dienstleister eingebunden werden müssen, da hier die Autorisierung nur auf Sachstand der vorliegenden Aufbauorganisation geprüft werden kann. Fallbeispiele:

- Einbindung des Kunden:
  - Teile des IAM-Prozess werden durch den Kunden selbst gelebt
  - Die Ausführung von Teilprozessen ist von der Genehmigung des Kunden abhängig
- Einbindung des Dienstleisters:
  - Der Dienstleister verwaltet, unter der Kontrolle des Auftraggebers, seine Mitarbeiter und deren Berechtigungsprofile eigenständig

Zusammengefasst: Die eingeführten Prozessrollen der Fachabteilungen schaffen ein Modell, dass organisatorische und fachliche Verantwortung integriert und Kommunikationsabläufe transparent und eindeutig regelt. Dieses liefert die Grundlage für einen prozessorientierten Genehmigungsablauf, aufgegriffen in Abschnitt 4.4.1, für Benutzer-

und Berechtigungsanträge. Darüber hinaus lassen sich mit dem Modell jederzeit Organisationseinheiten eines Kunden oder Dienstleisters, die sich eigenständig unter Einhaltung der Richtlinien verwalten, einbinden. Dieser Ansatz fördert ein mandantenunabhängiges IAM.

4.4 Teilprozesse

In dieser Arbeit wurde eine strukturelle Sortierung vorgenommen, in der die Teilprozesse analog zum Aufgabenbereich aufgeführt sind, wie Tabelle 4.4 zeigt. Darüber hinaus fließt, in welchen Aktivitäten eine Genehmigung durch die IS oder dem ERM erfolgen muss, in die Tabelle mit ein. Hierdurch wird ersichtlich, dass sobald neue Zugriffsrechte auf Informationen, Systeme, Anwendungen oder andere Ressourcen erteilt werden, zuvor Sicherheitsaspekte berücksichtigt werden, um einen risikobasierten Ansatz zu verfolgen.

Anträge bearbeiten und umsetzen

Bearbeitung und Umsetzung von Anträgen (Service Requests) betreffend der Elemente eines IAMs. Die Anträge sind der Auslöser für die in Tabelle 4.4 aufgeführten Teilprozesse und beinhalten Aktivitäten[19]*S.2893* zum:

- Hinzufügen
- Ändern
- oder Löschen

Vor der Umsetzung wird durch das IAM die Autorisierung des Antragstellers und die Einhaltung des Genehmigungsprozess geprüft, um die in Kapitel 3.2 definierte Zugriffskontrolle umzusetzen. Durch die Teilprozesse wird der in Kapitel 3.3.4 eingeführte Lebenszyklus, gemäß ISO 31010 und[33]*S.2890* gelebt.

4.4.1 Genehmigungsprozess

Bevor neue Rechte durch das IAM erteilt werden, ist eine formale Beantragung, siehe Kapitel 3.2) notwendig. Die Prüfung umfasst:

- Authentifizierung/Autorisierung:
  - Antragsteller
  - Begünstigte Identität, die neue Rechte erhalten soll
- Einbindung weiterer Kontrollinstanzen

Teilprozess	**IS & ERM involviert**
Benutzerverwaltung	
Account anlegen	✓
Account deaktivieren	
Account löschen	
Rollenverwaltung	
Neue Rolle	✓
Rolle löschen	
Ressourcenverwaltung	
Ressource anlegen	✓
Ressource löschen	
Zugriffsverwaltung	
Account eine Rolle zuweisen	
Account eine Rolle entziehen	
Berechtigungsprofile	
Rolle einer Ressource zuordnen	✓
Rolle einer Ressource entziehen	
Validierung	
Benutzer validieren	
Rollen validieren	
Ressourcen validieren	

Tabelle 4.1: Teilprozesse des IAMs analog zum Aufgabengebiet

Der Genehmigungsprozess greift die in Abschnitt 4.2 definierten Anträge zur Einrichtung von Benutzern und der Erteilung von Berechtigungen auf und verhindert damit, dass Mitarbeiter eigenständig Zugriffsrechte erlangen. Weiterhin wirkt, nach[48]*S.245*, der vorgestellte Genehmigungsprozess auf die Erfüllung der Anforderungen aus der IS-Policy ein. Dieser erfüllt damit die in[15]*S.161* gestellten Anforderungen zur Verifikation bevor Zugriffsrechte erteilt werden. Den praktischen Erfahrungen des Autors der gegenständlichen Arbeit zufolge, werden Beantragungswege in Zusammenarbeit mit dem Enterprise Risk Management (ERM), der Informationssicherheit (IS) und der Geschäftsführung gestaltet. Dabei ist zu beachten, dass mehrere eingebundene Kontrollinstanzen Verzögerungen hervorrufen können. Dies ist dann der Fall, wenn leitende Geschäftsrollen in die Genehmigungskette eingebunden sind. Die genannten Rollen sind zeitlich stark ausgelastet, was dazu führen kann, dass Anträge mehrere Arbeitstage zur Genehmigung ausstehen können. Abb. 4.6 zeigt Kontrollinstanzen, die eine Beantragung analog zur

Aufbauorganisation durchläuft. Im Rahmen dieser Arbeit wird die am Prozess ausge-

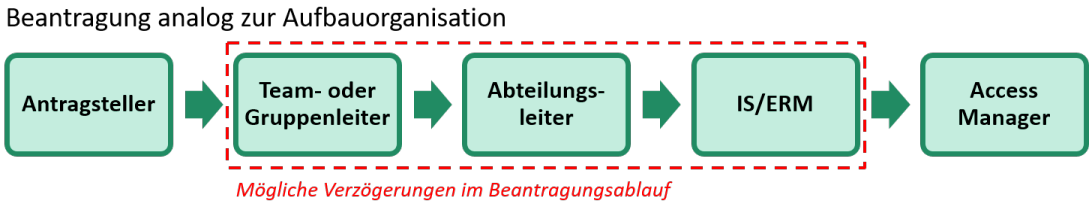

Abbildung 4.6: Kontrollinstanzen die den Antrag genehmigen oder ablehnen.

richtete Beantragung vorgestellt. Den Rückschlüssen des Autors zufolge, wirken die in Abschnitt 4.3 eingeführten Prozessrollen AC1, AC2, AC default und Resource owner Wartezeiten entgegen. Die Abb. 4.7 verdeutlicht den Beantragungsweg.

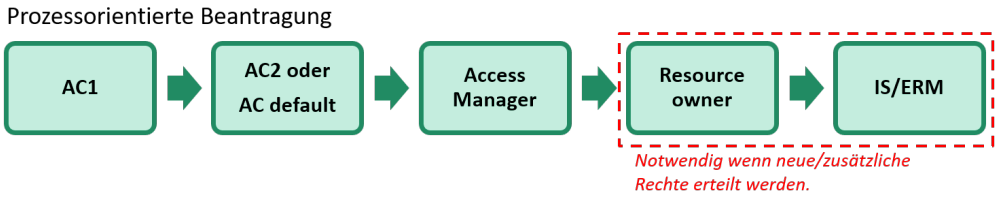

Abbildung 4.7: An den Fachbereich delegierte Verantwortung

Zusammengefasst: Der Vergleich mit Tabelle 4.4, den Abb. 4.6 und 4.7 zeigt, dass IS und ERM in die Beantragung eingebunden werden, wenn neuer Zugriff im Unternehmen erteilt wird. Die Verwaltung von Rollen und Ressourcen und der Entzug von Zugriffsrechten verbleibt in eigenständiger Verantwortung des Fachbereichs. Mit jährlichen Validierungen wird die Ansammlung von Zugriffsrechten verhindert[48]*S.246*. Näheres zu Validierung ist in Abschnitt 4.4.7 zu finden.

4.4.2 Benutzerverwaltung

Dieser Teilprozess regelt die Verwaltung von Accounts und die in[15]*S.161-162* genannte Überwachung des Identitätsstatus der Anwender. Weiter wird in[15] die Abstimmung mit der Personalabteilung aufgeführt zum Zwecke folgender Indikatoren:

- Ein- und Austritte von Mitarbeitern
- Veränderungen von Geschäftsrollen, Funktionen und Verantwortlichkeiten
- Änderungen der Aufbauorganisation
- Disziplinarische Sachstände

In[48]*S.246* werden unterschiedliche Benutzer-IDs, die durch Accounts im System repräsentiert werden, definiert und anhand des Rechte- und Zugriffsumfangs differenziert. Darauf aufbauend und unter Berücksichtigung der Identitätsarten aus Kapitel 3.1.1, werden folgende User und Accounts adaptiert:

- **Hoch priviligierter User (HPU)**
  Administrationskonten für Mitarbeiter innerhalb des Fachbereichs.
- **User Account**
  Ein "normaler Benutzeraccount", gemäß Kapitel 3.1.2, für die Mitarbeiter des Unternehmens, zwecks Erfüllung der täglichen Aufgaben.
- **Service Account**
  Ein Account, gemäß Kapitel 3.1.2, der von mehreren Identitäten, z.B. einer Anwendung oder einem Service, genutzt wird und häufig über Administrationsberechtigungen verfügt. Folglich ist die Einbeziehung von IS und ERM besonders wichtig. Eine gesonderte Dokumentation der Service Accounts, unter Einbeziehung von Risikoaspekten, ist, der Erfahrung des Autors nach, eine übliche Anforderung des ERMs.

4.4.3 Rollenverwaltung

Die organisatorische Verwaltung von Rollen und die Ausarbeitung des Rollen- und Rechtemodells obliegen den Fachbereichen[19]*S.170,1512*, da dort nach[49]*S.149-150* die Verantwortung über die Zugriffskontrollanforderungen liegen. Das IAM wirkt hier beratend und mit der Rolle eines Vermittlers zwischen Fachseite, IS und ERM, um der in[49] benannten Kommunikationslücke entgegenzuwirken.

- **Neue Rolle**
  Erstellung einer neuen Rolle, die auch ohne Account- oder Ressourcenzuordnung bestehen kann. Auf diese Art können Berechtigungsprofile und Rollenmodelle umgesetzt werden, ohne das bereits Zugang auf Ressourcen ermöglicht wird. Leere Rollen können darüber hinaus als Quarantäne genutzt werden, wenn Mitarbeiter länger Abwesend sind, ohne das Unternehmen zu verlassen.

- **Rolle ändern**
  Eine bestehende Rolle dahingehend ändern, dass der Name der Rolle angepasst wird.
- **Rolle löschen**
  Es erfolgt die Entkopplung aller zugewiesenen Accounts und Ressourcen, damit die Rolle gelöscht werden kann.

4.4.4 Ressourcenverwaltung

Dieser Teilprozess umfasst die Zuordnung (Abb. 4.8) von Berechtigungen auf Objekte, gemäß Kap. 3.3.2. Jede Berechtigungsstufe wird mit dem Zielobjekt verknüpft und separat als Ressource abgebildet, wie in Kap. 3.4 festgelegt. Das bedeutet: Sollen vier verschiedene Berechtigungsstufen den Zugriff auf einen Server ermöglichen, werden vier verschiedene Ressourcen mit der jeweiligen Berechtigungsstufe, aber demselben Server angelegt. Dies führt zu folgenden Erleichterungen:

- Weniger Komplexität im Berechtigungskonzept:
  - Berechtigungsprofile werden einmal mit den zugehörigen Operationen definiert und durch die Ressourcen den Objekten zugeordnet
  - Die Namen der Ressourcen werden selbst-sprechend gehalten, um Objekt und Berechtigungen ablesen zu können
  - Keine Auflistung und Zuordnung von Einzelberechtigungen pro Objekt
- Einfache Verfahrensweise:
  - Die Berechtigungen auf Server, Anwendungen etc. lassen sich agiler und feiner abstimmen
  - Ressourcen können in den Teilprozessen schneller geprüft werden

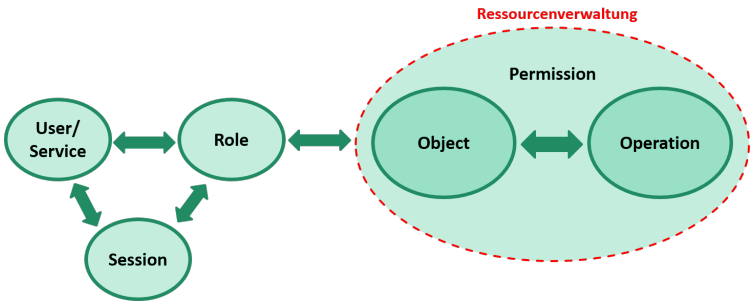

Abbildung 4.8: Zuordnung Ressourcenverwaltung zum RBAC-Model

Folgende Teilprozesse ergeben sich aus der Verwaltung von Ressourcen:

- **Ressource anlegen**
  Die Anlage einer Ressource umfasst die Festlegung des Resource owners und welches Objekt mit welcher Berechtigung verknüpft wird.
- **Ressource löschen**
  Vor der Löschung müssen alle Verknüpfungen mit den Rollen aufgehoben werden.

Grundlegend ist zu beachten, dass Anlage oder Löschung nur durch den Resource owner beauftragt werden dürfen. Abweichende Aufträge müssen abgelehnt werden.

4.4.5 Zugriffsverwaltung

Sicherstellung einer angemessenen Rechtevergabe und der laufenden Anpassung erteilter Zugriffsrechte, deren Häufung insbesondere zu verhindern ist. Die Gefahr der Ansammlung besteht dann, wenn nicht mehr benötigte Berechtigungen nach Aktivitäten erteilt bleiben oder eine unregelmäßige bis seltene Überprüfung aller vergebenen Rechte erfolgt. Die Mitgliedschaft von Accounts in Rollen stehen im Mittelpunkt, siehe Abb.4.9. Nachfolgend ergeben sich Teilprozesse:

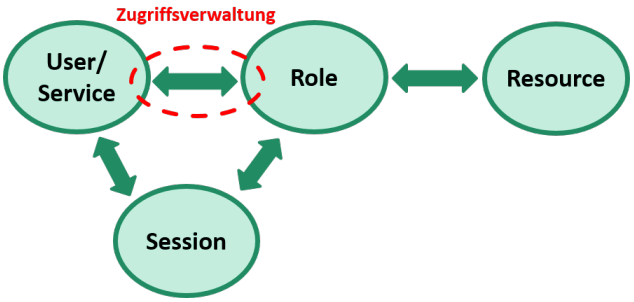

Abbildung 4.9: Zuordnung der Zugriffsverwaltung zum RBAC-Model

- **Account eine Rolle zuweisen**
  Der Account wird zu einem Mitglied der Rolle bzw. Rollengruppe.
- **Account eine Rolle entziehen**
  Diese Aktivität beendet die Mitgliedschaft eines Accounts in der Rollengruppe.

4.4.6 Berechtigungsverwaltung

Dieser Aufgabenbereich umfasst die Zuordnung von Ressourcen und Rollen. Siehe Abb.4.10. Folgende Teilprozesse:

- **Rolle einer Ressource zuordnen**
  Rolle und Ressource werden einander zugewiesen. Ferner können alle Rollenmitglie-

der diese Ressource nutzen. Durch diese Verknüpfung wird Zugriff auf Ressourcen gewährt, weshalb die Einbindung der IS und dem ERM notwendig ist.

- **Rolle einer Ressource entziehen**
  Die Verbindung von Ressource und Rolle wird gelöst. Beide bleiben in ihrer Existenz unberührt.

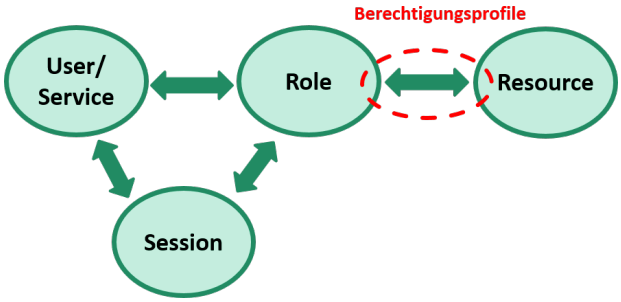

Abbildung 4.10: Zuordnung Berechtigungsprofil zum RBAC-Model

4.4.7 Validierung

Aus den in[48]*S.245-246* gestellten Anforderungen an eine Validierung lassen sich verschiedene Schwerpunkte ableiten. Eine Validierung umfasst sämtliche Systeme, Software, Hardware bzw. Objekte der IT-Landschaft, auf die durch das IAM Zugriff erteilt worden ist.

- **User-Validierung**
  Umfasst die Überprüfung von User Accounts. Dazu müssen alle existierenden Accounts auf sämtlichen Systemen in den Netzwerkumgebungen erfasst werden.
- **Role-Validierung**
  Erfassung und Zuordnung der vergebenen Rollen. Im Anschluss erfolgt die Prüfung der zugeordneten Ressourcen.
- **Resource-Validierung**
  Überprüfung des Resource owners. Die Ressourcen werden hinzukommend auf Aktualität und erteilter Berechtigungen hin geprüft.

Durch die verschiedenen Schwerpunkte ist die stufenartige Erfüllung der Forderungen aus[48]*S.246* möglich:"*Alle Benutzer-IDs mit ihren Rechten müssen einmal jährlich durch den zuständigen Vorgesetzten oder den Verantwortlichen des entsprechenden IT Services validiert werden. (Dies kann eine Vorgabe aus der Security Policy sein).*"

Nach der Durchführung ist das IAM dafür verantwortlich, dass die Ergebnisse der Überprüfung, durch die ACs der Fachabteilungen zur Umsetzung beauftragt werden.

4.5 Provisioning

Das Provisioning ist ein Bestandteil[24] des Servicebetriebs und befasst sich mit der technischen Verwaltung der Benutzer; deren Mitgliedschaften in Rollen, den Ressourcen, der Bereitstellung von Verbindungen; von Hardware, Software, Diensten und Anwendungen. Das Ziel eines Provisioning-Systems ist es, den autorisierten Anwendern die erforderlichen Ressourcen in den vorgesehenen Netzwerk- oder Systemumgebungen zur Verfügung zu stellen. Dazu gehören folgende Aufgaben[24]*S.116*:

- Anlage und Änderung der Accounts
- Bereitstellung der Zugriffsrechte, analog zu den Rollenmitgliedschaften auf die Ressourcen
- Anbindung der Netzwerk- und Systemumgebungen

Damit ist das Provisioning-System für die technische, soweit möglich automatisierte Umsetzung der Vorgaben aus den Teilprozessen zuständig. Nach[24]*S.115* gibt es verschiedene Arten des Provisionings und eine daraus entstehende Architektur. Näheres im nachfolgenden Abschnitt.

4.5.1 Benutzer

Das Benutzer im *engl. User Provisioning* System sorgt für das Einfügen oder Entfernen der User- und Service-Accounts. Damit setzt es die Vorgaben, die im Rahmen der Teilprozesse für die Erstellung, Deaktivierung und Löschung von Identitäten beantragt worden sind, technisch um. Ebenfalls ordnet das User Provisioning die dokumentierten Eigenschaften einer Identität dem zugehörigen Account auf Systemebene zu.

4.5.2 Ressourcen

Das *Resource Provisioning* System, gemäß[24]*S.116*, richtet den Zugriff der Accounts auf die Ressourcen unter Berücksichtigung der Berechtigungsprofile ein und setzt dabei die Schutzanforderungen technisch um.

4.5.3 Server

Server Provisoining definiert nach[24]*S.124* die Serverkonfiguration auf der Basis der Geschäfts- und Schutzanforderungen und des Verwendungszwecks. Darüber hinaus wird der Server über seinen Lebenszyklus hinaus begleitet, dies umfasst:

- Auditierungen
- Prüfung auf gesetzeskonformen Betrieb (Compliance)
- Sicherheitsprüfung auf Schwachstellen und Lücken
- Aktualisierung durch Updates

Das Server Provisoining wird als zweckgebundene Einrichtung und Pflege eines Servers betrachtet, die einem automatisierten System oder der manuellen Administration obliegt.

4.5.4 Architektur

Dem Provisioning-System liegt eine Architektur (siehe Abb. 4.11) zugrunde, die Schnittstellen, Verzeichnisdienste, Netzwerk- und Systemumgebungen verbindet. Im Zentrum ist die Access Datenbank (AC DB) abgebildet, die mit Informationen gespeist wird[24]*S.115-126*:

- Personelle Informationen aus dem Identitätsmanagement (IDM)-System
- Daten über die Aufbauorganisation
- Rollen und Rechte
- Ressourcen durch Verzeichnisdienste

Die Datenbank bündelt sämtliche Informationen über Accounts, Organisationseinheiten, Rollen, Rechte und Ressourcen zu einem technischen Ist-Stand. Dieser wird über die vorgestellten Teilprozesse laufend verändert und validiert, unter Berücksichtigung der geltenden Richtlinien. Damit stehen die AC DB und die in Abschnitt 4.2 vorgestellte Access Control List in Beziehung.
Zu Beginn des Werktags stellt die Access Control List den Ist-Stand aus der AC DB bereit und enthält zum Ende des Arbeitstages den neuen Soll-Stand, der vorzugsweise über Nacht durch das Provisioning-System umgesetzt wird.

Konnektoren

Sorgen nach[24]*S.118* für die technische Umsetzung der Vorgaben aus der AC DB und bilden zu jedem Verzeichnisdienst eine Schnittstelle zur Erstellung von Accounts und Berechtigungsprofilen, um Anwendungen und Dienste anzubinden. Weitere Konnektoren

konzentrieren sich auf die Synchronisation des Berechtigungsstands in die Verzeichnisdienste anderer Netzwerkumgebungen. Je nach Architektur kann es einen zentralen Verzeichnisdienst geben, der auf sämtliche abgebildet wird oder die AC DB wird durch weitere Konnektoren direkt mit anderen Verzeichnisdiensten verbunden.

Zusammengefasst

Das Provisioning-System sorgt für die technische Umsetzung des Benutzers-, Berechtigungs- und Konfigurationsstands gemäß der Vorgaben aus den IAM-Teilprozessen. Es bestehen verschiedene Schwerpunkte, die sich auf User, Ressourcen, Server und Netzwerkumgebungen konzentrieren. Mit den technischen Schnittstellen, genannt Konnektoren, wird die technische Umsetzung in allen Verzeichnisdiensten und Netzwerkdomänen sichergestellt. Auf diese Weise lassen sich unterschiedliche Mandanten und Dienstleister an das IAM anbinden, welches sich damit mandantenunabhängig macht. Der Fokus dieser Arbeit liegt auf der organisatorischen und konzeptuellen Sichtweise, deshalb erfolgt keine technische Vertiefung.

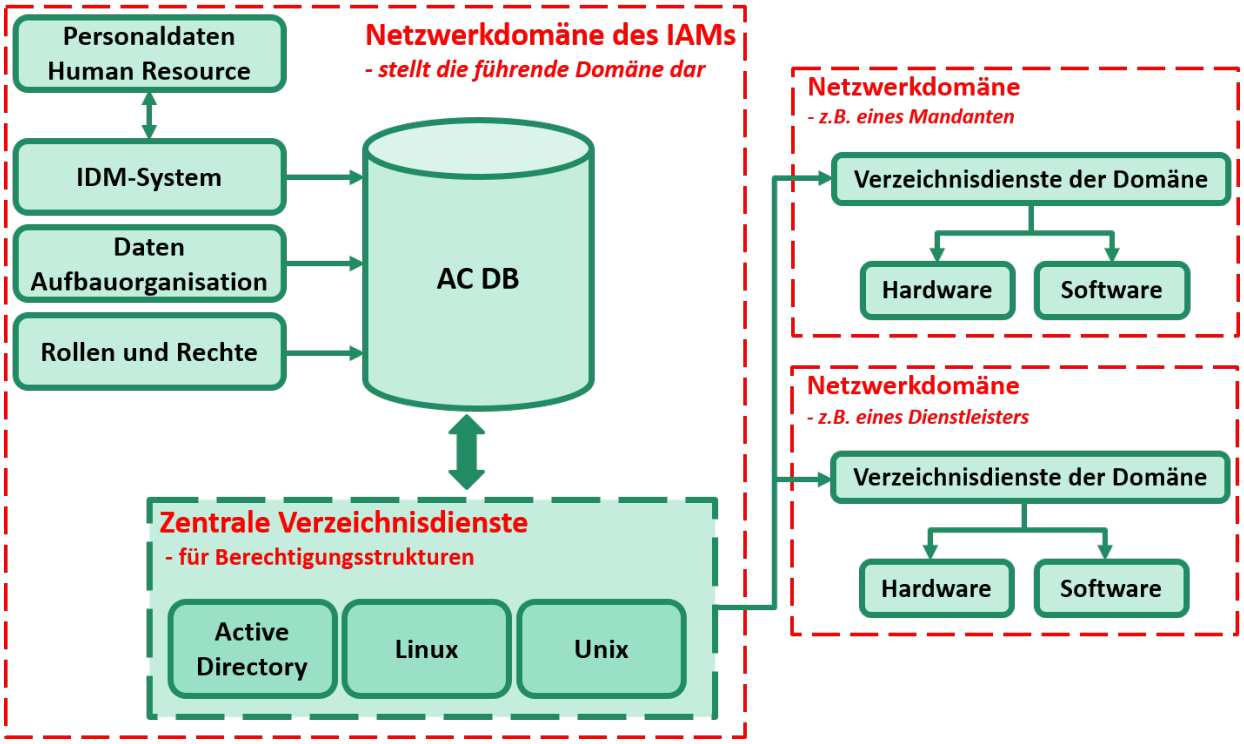

Abbildung 4.11: Architektur eines Provisioning-Systems, adaptiert aus[24]*S.122* und erweitert durch die Erfahrungen des Autors.

5 Schrittweiser Aufbau eines Identity Access Managements

Rahmen und Abgrenzung

Die vorliegenden zehn Schritte für den Aufbau eines IAMs haben einen organisatorisch und ITIL geprägten Schwerpunkt und sind als Impulse für die konzeptuelle Vorgehensweise erdacht. Die Maßnahme *M 2.585 Konzeption eines Identitäts- und Berechtigungsmanagements* nach IT-Grundschutz aus[33]*S.2890* ist zusätzlich in die Schritte eingeflossen. Aufgebaut sind diese aus Best-Practices von Unternehmen[50]*S.28-33*,[23] die sich auf die IAM-Thematik spezialisiert haben und die gewonnen Erfahrungen des Autors, im Rahmen des Arbeitseinsatzes bei der Wincor Nixdorf Global IT Operations GmbH im *Access Management*.

Schritt 1: Analyse der IT-Landschaft

Einbeziehung aller Interessengruppen

Das IAM ist in Kapitel 2.3 als Teilprozess, mit dem Ziel einer kontinuierlichen und nachweislichen Compliance der unternehmensweiten IT-Governance, zugeordnet worden. Für Transparenz, Gewaltenteilung, ein Interessenausgleich und die Unabhängigkeit der Unternehmensorgane sind Kenntnisse über das Unternehmen und die internen Geschäftsprozesse essentiell, um die erforderlichen Informationen über folgende Aspekte zu erlangen: Rollenkonzepte, Genehmigungsprozesse, Erwartungen an das IAM oder die Barrieren zwischen Abteilungen. Das Projektteam muss demnach aus Kompetenzträgern der IT und der Unternehmenssubstitutionen bestehen:

- Human Resource (HR)
- Enterprise Risk Management (ERM)
- Informationssicherheit (IS)
- Vertreter der Fachbereiche

In zeitlich regelmäßigen Abständen sind durch das implementierende Projektteam Kick-Offs, Schulungen und Informationsveranstaltungen für die Unternehmenssubstitutionen zu organisieren. Dies fördert das Verständnis und den bewussten Umgang nach[50]*S.28,31,34* rund um die Zugriffskontrolle und Berechtigungssteuerung. Der Autor empfiehlt an dieser Stelle, die Projektbeteiligten mit den, in Abschnitt 4.3 definierten Prozessrollen vertraut zu machen. Die frühe Benennung der in Abschnitt 4.3.3 definierten Access Coordinators, etabliert frühzeitig das Kommunikationsmodell (Abb. 4.5) und vereinfacht die Zusammenarbeit zwischen Fachbereich und Projektteam.

Erfassung der System-Vielfalt

Die System- und Applikations-Vielfalt in Unternehmen kann sehr unterschiedlich sein. Daher ist die Erfassung aller Systeme, Applikationen und angeschlossener Hardware notwendig. Hinzukommend ist, welches Provisioning-System gemäß Kap. 4.5 im Einsatz ist und in welchem Umfang die Systeme und Netzwerke bereits automatisch oder noch manuell gepflegt werden zu dokumentieren. Zur Erfassung der System-Vielfalt empfiehlt sich die IT-Grundschutz-Vorgehensweise (siehe BSI-Standard 100-2) anzuwenden, um eine vollständige Analyse zu gewährleisten.

Definition eines Ist-Berechtigungsstands

Der derzeitige Stand der erteilten Berechtigungen ist aus allen Systemen- und Netzwerkumgebungen auszulesen und nach Benutzer und Fachbereich aufzuschlüsseln. Aus dem vorliegenden Ist-Stand lassen sich Projektaufwand, -Dauer und -Kosten ableiten. Sofort erkennbare Sicherheitsverstöße und -Risiken sind umgehend dem ERM und IS zu melden. Unter Umständen können Sofortmaßnahmen noch vor der unternehmensweiten IAM-Implementierungen notwendig werden.

Schritt 2: Festlegen von Anforderungen und Ziele

Ziele definieren

Eindeutig definierte Ziele und Aufgabe, sowie ein strukturierter Rahmen zu deren Planung und Überwachung, haben Einfluss auf den Projektverlauf. Dies erfordert eine Zusammenarbeit zwischen erfahrenen Mitarbeitern sowohl im Fachbereich als auch im implementierenden IAM-Projektteam. Da nach[49]*S.149-153* der Ursprung der Zugriffskontrollanforderungen der Ressourcen dem verantwortlichen Fachbereich obliegen, ist sicherzustellen, dass ein Interessenausgleich, analog zum gebildeten Verständnis[1]*S.33* in Kapitel 2.1 zur Corporate Governance, zwischen den Anspruchsgruppen und den

Projektbeteiligten geschaffen wird, bevor die Umsetzung beginnt. Nachträgliche Anpassungen haben Einfluss auf die Projektdauer und die veranschlagten Kosten. Darüber hinaus gilt: "Ziele sind so zu gestalten, dass diese Fakten schaffen und messbare Erfolge hervorbringen."

- Beispielhafte Projektkennzahlen:
  - Anzahl abgebauter Benutzerkonten
  - Anzahl erstellter Rollen und Ressourcen
  - Auflistung identifizierter und behobener Risiken
  - Auflistung manueller Verfahren, die abgelöst wurden

Schrittweise Umsetzung

Ein IAM muss in alle IT-Systeme und Netzwerkumgebungen des Unternehmens integriert werden, um diese im operativen Betrieb steuern und verwalten zu können. Dabei muss die Skalierbarkeit und Agilität im Mittelpunkt stehen. Weder die Anzahl der einzubindenden Benutzer noch die der Systeme und Netzwerkumgebungen dürfen auf ein Maximum beschränkt sein. Eine iterative Vorgehensweise und fein gesteckte Projektziele sorgen für ein stetiges Vorankommen und für regelmäßige Erfolge im Projektverlauf. In [50]*S.35* wird vor einer Komplexitätsfalle gewarnt, die mit dem Anspruchsdenken in Verbindung gebracht wird. Es gilt die Devise: "Nicht alles auf einmal!" Das bedeutet, ein Zielsystem nach dem anderen anzubinden und die Standardfunktionalitäten der Benutzer vorrangig herzustellen[50]*S.32*. Die Feinabstimmung der Rollenmodelle und Berechtigungsstufen wird im Nachgang durchgeführt. Gleiches gilt für Teilprozesse, die vorrangig die am meist frequentierten und störenden Verfahren ablösen, bevor spezielle Gegebenheiten aufgenommen werden.

Standard-Software einsetzen

Statt vermehrt auf Customizing zurückzugreifen, ist der Einsatz von Standardsoftware zu prüfen, der den Implementierungsaufwand und spätere Wartungs- und Betriebskosten langfristig reduzieren kann. In Standardsoftware fließen Erfahrungen aus realisierten Projekten, langjährig erworbenes Wissen und vorkonfigurierte Rahmenbedingungen der IAM-Anbieter nach dem Best-of-Breed-Ansatz ein[50]*S.37*. Das System individuell an die Gegebenheiten des Unternehmens anzupassen muss eine Ausnahme bleiben, denn dies bindet Mitarbeiter, Fachwissen und Flexibilität. Dazu ist der IT-Grundschutzkatalog[33]*M 4.499 Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen, S.4333* zu berücksichtigen.
Leitsatz: "Statt Software, Methoden und Werkzeuge vollständig den internen Prozessen, Terminologien und Verantwortungen anzupassen, ist Flexibilität und Agilität durch

Standardsoftware zu fördern, um auf veränderte Rahmenbedingungen zeitnah reagieren zu können."

Realistisch bleiben

Die Ziele eines IAMs sind: Eine am Geschäftsprozess ausgerichtete und verständliche Sicht auf die Identitäten, den Berechtigungsstand und die Zugriffsrechte im Unternehmen. Dies wird erreicht durch: Eindeutig definierte Ziele und der schrittweisen Umsetzung nach[50]*S.32,34* von realistischen Zwischenzielen. Mit dieser Vorgehensweise wird das IAM zu einem unternehmensweiten Prozess, der die Strategien aus dem Governance-Prozess, dem ERM und der IS erfüllt und damit die Corporate Compliance fördert.

Schritt 3: Definition der Identitätsarten und -träger

Konsolidierung der Benutzerkonten

Der vorliegende Bestand an Benutzerkonten und erteilten Zugriffsrechten kann in unterschiedlichen Qualitäts- und Quantitäts-Stufen vorliegen. Die Gründe dafür sind vielfältig: Umstrukturierungen, Unternehmensfusionen oder Projekttätigkeiten können für ein "historisches Wachstum" der Zugriffsrechte und Benutzeraccounts verantwortlich sein. Folglich ist im ersten Schritt eine gründliche Konsolidierung[50]*S.32* mit der Devise: "Aufräumen!" durchzuführen.

Statt jedes Konto individuell zu prüfen, werden die Fachbereiche dazu aufgefordert, benötigte Benutzerkonten als "aktiv" zu melden und mit einer prägnanten, fachlichen Begründung zu versehen. Accounts, die von keinem Fachbereich beansprucht werden, können zur Sicherheit erst deaktiviert und nach der abgelaufenen Karenzzeit gelöscht werden. Für diese Vorgehensweise eignet sich die Erstellung von Listen, die den Ist-Stand der Benutzeraccounts aufzeigen und soweit möglich die darin enthaltenen Accounts in Abstimmung mit der HR, einem Fachbereich zuordnen. Auf diese Weise werden verwaiste Benutzerkonten aufgespürt und bereinigt.

Schnittstelle zur Human Resource schaffen

Wie in Abschnitt 4.1 aufgeführt, stellt das IAM sicher, dass nur autorisierten Benutzern die Nutzung von Ressourcen gestattet wird und die Vorgaben aus der IS-Richtlinie, siehe Abschnitt 4.3, eingehalten werden. Dazu ist eine Schnittstelle zwischen dem HR-Team und IAM zu definieren. Werden Änderungen der Personalstruktur oder Tätigkeitsbereichen aus der HR nicht weitergeleitet, können Personen Zugang zu Ressourcen erlangen, obwohl sie aufgrund ihrer neuen Geschäftsrolle keine Berechtigungen dazu haben. Verlässt ein Mitarbeiter das Unternehmen, muss das zugehörige Benutzerkonto mit allen

Zugriffsrechten entfernt werden. Ein manueller, nicht automatisierte Informationsfluss und dezentrales Arbeiten trägt dazu bei, dass sich Fehler in den Berechtigungsstrukturen ausbreiten[33]*S.2890*. Folglich ist eine Schnittstelle zwischen HR und IAM zu implementieren, die für eine Automatisierung zwischen beiden Systemen sorgt und einen festen Kommunikationsablauf etabliert zum Zwecke von Sicherheit und Kontrolle.

Aussagekraft durch Datenqualität

Für das IAM ist hohe Datenqualität essentiell, um der Dokumentationspflicht und Erhöhung von Transparenz im Unternehmen aus 2.4.4 *BDSG*, 2.4.3 *GoBD*, 2.4.2 *KonTraG* und 2.4.1 *SOX* gerecht zu werden. Die Verbindung zwischen der logischen Identität (Account) und dem personellen Identitätsträger (Mitarbeiter) ist durch das IAM zu dokumentieren und bildet z.B. für die Bestimmungen des BDSG eine wichtige Grundlage. Dies betrifft u.a. die Zugangs-, Zugriffs- und Eingabekontrolle.

Schritt 4: Bildung eines Rollenmodells

Rollen implementieren

In Kapitel 3.3.1 wurden Rollen als Sammlung einzelner Zugangsrechte, die für eine bestimmte Funktion oder Aufgabe im Unternehmen erforderlich sind, definiert. Das in Kapitel 3.4 vorgestellte RBAC-Modell, mit den dazugehörigen Abbildungen 3.10 und 3.12, greift diese Thematik auf und bündelt Ressourcen mit den zugehörigen Zugriffsrechten in Rollen. Das Bündeln von Zugriffsrechten in technische Rollen verhindert den Administrationsaufwand von direkten Berechtigungen zwischen Benutzern und Ressourcen und ist folglich die Grundlage für eine automatisierte Rechtevergabe durch ein Provisioning-System. Im Rahmen dieser Arbeit wird folgende Vorgehensweise festgehalten:

- Zuordnung der Mitarbeiter nach Fachthema innerhalb der Abteilung
- Erzeugung einer Rolle pro Fachthema
- Zuordnung der erzeugten Rolle zum Fachbereich
- Zusammenstellung der notwendigen Zugriffsrechte, um die technische Systemrolle abzubilden

Diese Vorgehensweise steht analog zu[49]*S.97*:"*Das Modell unterscheidet zwischen zwei verschiedenen Rollentypen: Geschäftsrollen werden durch die Fachabteilung genutzt, deren fachlicher Kontext darin abgebildet ist. Systemrollen werden innerhalb der Anwendungssysteme verwendet, sie sind technischer Natur und werden durch die IT-Abteilung verwaltet.*"

Durch die Zuordnung eines Aufgabenthemas des Mitarbeiters wird der fachliche Kontext erfasst, damit das implementierende Projektteam die Systemrolle definieren kann. Alternativ können folgende Ansätze nach[51],[50]*S.31* zur Rollenbildung in Erwägung gezogen werden:

- **Top-down**
  Ausgehend der Unternehmensstrukturen und Geschäftsfunktionen werden die Geschäftsrollen adaptiert und schrittweise verfeinert.
- **Bottom-up**
  Bildung einer technischen Rolle ausgehend der Zugriffsrechte durch schrittweise Zusammenfassung.
- **Middle-out**
  Steht für einen hybriden Ansatz, der beide Vorgehensweisen kombiniert und ähnelt der oben aufgeführten Vorgehensweise.

Rollenverantwortliche festlegen

Der in Kapitel 3.3.4 und Abbildung 3.9 vorgestellte Lebenszyklus nach ISO 31010 *IT Risiko Management* wurde im genannten Abschnitt auf die IAM Elemente angewendet. Die definierten Rollen können folglich als dynamische Strukturen, die einem ständigen Überwachungs- und Anpassungsprozess unterliegen, betrachtet werden. Deshalb ist die Zuweisung eines Besitzers, der die Verantwortung der sauberen Ausgestaltung dauerhaft übernimmt, notwendig. Daraus folgt das regelmäßige Prüfen, ob aufgrund von Veränderungen in der Organisationsstruktur oder der IT-Landschaft Anpassungen vorzunehmen sind. Die im Abschnitt 4.3.3 behandelten Prozessrollen des AC1, AC2 und AC default eignen sich für die Überwachung und Durchsetzung des Lebenszyklus. Diese eignen sich ideal als Verantwortliche, da auf diese Weise Berechtigungskonzept und Kommunikation zum IAM im gleichen Mitarbeiterkreis verbleiben. Der Empfehlung zu folgen fördert gemäß[49]*S.149-153*, angemessene Zugriffskontrollanforderungen.
Folglich sind für die Erzeugung und Implementierung der Rollen kleine Teilziele, unter Einbeziehung aller relevanten Interessen- und Anspruchsgruppen zu bilden, um Teilerfolge durch wohldefinierte Rollen vorweisen zu können.

Schritt 5: Ressourcen überführen und konsolidieren

Ressourcen erfassen und zuordnen

Ressourcen stellen aus der IAM-Perspektive gemäß Kap. 3.3.3, Inhalte und Funktionen in der zumeist virtuellen Umgebung dar. Durch die vorgestellten Sicherheits- und Bedrohungsanalysen wird der Schutzbedarf der Ressourcen definiert, die in die Zugriffskontrollanforderungen einfließen. Folglich kann dem implementierenden Projektteam eine koordinierende und vermittelnde Rolle zugeordnet werden, um über alle Fachbereiche hinweg die einheitliche Erfassung, Pflege und Dokumentation der Ressourcen im Unternehmen zu erreichen. Analog zur Konsolidierung der Benutzerkonten werden die bisher erfassten Ressourcen durch die Fachabteilungen geprüft und ergänzt. Dazu wird ein Ist-Stand der IAM relevanten Ressourcen für jede physische oder virtuelle Umgebung durch das Projektteam erzeugt und im Anschluss an die Organisationseinheiten weitergeleitet. Verwaiste Ressourcen werden, in Abstimmung mit ERM und IS, abgebaut oder einem Fachbereich zugewiesen. Hier gilt die Devise: “Aufräumen und dokumentieren!”

Zugriffskontrollanforderungen umsetzen

Die dokumentierten und zugeordneten Ressourcen werden, gemäß Abschnitt 3.3.2 mit Berechtigungen (Operationen) oder Berechtigungsstufen, siehe Abbildung 3.8 verknüpft und als zusammengesetzte Ressource (Objekt und Operation) im Berechtigungskonzept hinterlegt. Die technische Umsetzung in den verschiedenen Netzwerkumgebungen wurde gemäß Kapitel 4.5 dem Provisioning zugeordnet. Die Namen der Ressourcen sind so zu gestalten, dass diese selbsterklärend sind mit dem Ziel, die Prüfung im Genehmigungsprozess zu vereinfachen.

Virtuelle Ressourcen aufnehmen

Der Autor dieser Arbeit hat im Laufe seines Arbeitseinsatzes den Ansatz rund um die virtuelle Ressource kennengelernt. Betroffen sind Objekte, wie z.B Server oder Clients, die von dem automatisierten Provisioning-System abgeschnitten sind. Für diese Objekte ist, die in[24]*S.119,171* beschriebene dezentralisierte Verwaltung notwendig. Virtuelle Ressourcen werden analog zu den bestehenden gepflegt, dokumentiert und in der zentralen AC DB hinterlegt. Diese sind durch die Teilprozesse, siehe Kap. 4.4, steuerbar. Durch die Dokumentation, dass es sich um virtuelle Ressourcen handelt, kann das IAM feststellen, dass die Berechtigung durch die Fachabteilung manuell eingerichtet werden muss. Dieses Verfahren hat den Vorteil, dass sämtliche, auch dezentral erteilte Berechtigungen, in der Access Control List einsehbar sind. Verlässt ein Mitarbeiter das Unternehmen und soll laut Auftrag “auf sämtlichen Systemen entfernt werden”, erspart

das Vorhandensein der virtuellen Ressourcen dem IAM das manuelle Durchsuchen der Systeme, auf die der Mitarbeiter Berechtigungen hat. Die Verantwortung, dass der Stand der virtuellen Ressourcen 1:1 auf den Systemen abgebildet ist, obliegt den verantwortlichen Fachabteilungen, die jederzeit den Soll-Stand abrufen können.

Schritt 6: Benutzer und Rollen zuordnen

Berechtigungskonzept gestalten

Das in Kap. 4.2 vorgestellte Berechtigungskonzept ist durch das implementierende Projektteam vorzubereiten, damit die zentralen Vorgaben Berücksichtigung finden und über jeden Fachbereich hinweg eine einheitliche Struktur entsteht. Die Vorlage wird in der Fachabteilung angewandt und durch die Access Coordinators ausgestaltet. Dabei muss dargestellt werden, welche Ressourcen der Fachbereich verantwortet, welche Berechtigungen darauf erteilt sind und durch welche Rollen diese genutzt werden. Bei der Erstellung sind die ACs durch das Projektteam zu koordinieren und zu unterstützen.

Umsetzung des Konzepts

Nach Vollendung erfolgt die Umsetzung im zentralen IAM-System.

- Verknüpfung: Accounts und Rollen
  Die konsolidierten und den Mitarbeitern zugeordneten Accounts werden, den zuvor gebildeten Rollen zugeordnet.
- Verknüpfung: Rollen und Ressourcen
  Es erfolgt die Zuordnung zwischen den im fachlichen Kontext stehenden Ressourcen, die zur Ausübung der Tätigkeiten notwendig sind und der Rollen, die für das Tätigkeitsfeld gebildet wurden.

Access Control List aufbauen

Die gebildeten Verknüpfungen werden in der Access Control List gepflegt, um ein zentrales Informationsobjekt zu schaffen, mit dem jederzeit die erteilten Zugriffsberechtigungen der Benutzer eingesehen werden können. Gleichzeitig liefert diese den Soll-Stand an das IAM-System, welches dann die technische Umsetzung durchführt.

Schritt 7: Umsetzen und einführen

Schnellere Erfolge auf Fachabteilungsebene

Für eine Akzeptanz über alle Unternehmensbereiche hinweg sollten die Anwender bereits im frühen Projektstadium die Teilprozessen evaluieren, die noch mit geringem Aufwand

an die Wünsche und Bedürfnisse der Fachabteilungen angepasst werden können. Bereits verfügbare Abläufe lassen sich im operativen Betrieb anbieten, anstatt die vollständige Lösung zum Projektende in einem Atemzug aktiv zu setzen. Dabei ist zu beachten, dass vorzugsweise bereits im Unternehmen eingesetzte Tools und Verfahren zur internen Beauftragung verwendet werden sollten. Wird ein externer Dienstleister oder ein Kunde eingebunden, so sind Schnittstellen zwischen den internen und externen Tools zu schaffen. Mit diesem Ansatz wird der Nutzen des IAMs im Arbeitsalltag für die Beteiligten schneller sichtbar und dies fördert den Gesamterfolg des Projekts.

Ausarbeitung der Teilprozesse

Die unter 4.4 vorgestellten Teilprozesse sind schematisch so auszuarbeiten, dass diese als Workflows und Arbeitsanweisungen implementiert und zentral hinterlegt werden können. Dazu eignen sich grafische Diagramme, ergänzt durch schriftlichen Ausführungen.
Parallel dazu sind Arbeitsanweisungen für die Mitarbeiter des IAMs zu erstellen, damit diese das IAM-System bedienen und die Verfahrenseinhaltung gewährleisten können. Dabei ist die Maßnahme *M 2.587 Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement* zu berücksichtigen, gemäß[33]*S.2896*.

Technische Umsetzung

Es erfolgt die technische Umsetzung von Datenbereinigungen, Provisioning und Implementierung der Funktionalitäten, wie[50]*S.32* Workflows für Anträge, Genehmigungsabläufe, Eskalationen und die Anbindung der Quell- und Zielsysteme an das IAM-System. Weiter ist ein Verfahren umzusetzen, dass die Access Control List (Kap. 4.2) mit allen Informationen versorgt und an das System koppelt, sodass diese als Grundlage für Artefakte, Informationsobjekte und Teilprozesse genutzt werden kann.

Konsolidierung auf Fachabteilungsebene

Sind Teilprozesse bereit für die Auslieferung in den operativen Betrieb, sollten diese nach der ersten Anwendung durch die Fachbereiche konsolidiert werden. Umständliche oder zeitintensive Verfahren verbreiten schnell Unmut bei den Beteiligten und können für Verzögerungen der Arbeitsabläufe sorgen. Daher sind Schulungen der Beteiligten und Workshops mit Fachabteilungen unerlässlich. Es gilt die Devise: “Ein abgestimmtes Miteinander fördert die Akzeptanz neuer Verfahren und Prozesse.”

Schritt 8: Schaffung von Kontrollmöglichkeiten

Die Gestaltung der Projektziele stehen unter dem Aspekt Fakten zu schaffen und messbare Erfolge hervorzubringen. Dieser Schritt befasst sich mit der Definition von

Kennzahlen, um den langfristigen Erfolg im operativen Betrieb und im ITIL-Lifecycle gemäß Kap. 4.1, messbar zu machen. Dazu stellt der Autor mit seinen praktischen Erfahrungen folgende Kennzahlen und Kontrollen auf:

- IKS-Kontrollen:
  - Prüfung zweier Aufträge wöchentlich, auf Einhaltung des Genehmigungsprozesses
  - Überprüfung eines Benutzer-Löschen-Auftrags wöchentlich, auf vollständige Bereinigung in allen Umgebungen
- Kennzahlen für das IKS und den operativen Betrieb nach[48]*S.249* zur Überwachung des IAMs Tabelle 5:

Kennzahl	Beschreibung	Definition Grün	Definition Gelb	Definition Rot
Aktualität der Validierung	Das Alter der zurückliegenden Validierung der Einträge in der Access Control List kann ins Gesamtverhältnis gesetzt werden	<5% sind älter als 1 Jahr	5-15% sind älter als 1 Jahr	>15% sind alter als 1 Jahr
Einhaltung der Sicherheits-vorgaben	Der Access Manager prüft die Einhaltung von Sicherheits-vorgaben innerhalb der Aufträge zur Berechtigungssteuerung	Alle wurden eingehalten	-	>0 wurden eingehalten
Anzahl durchge-führter Stichproben	Durchgeführte Stichproben, die auf Einhaltung der Sicherheitsvorgaben hin prüfen	>2 Stich-proben pro Woche	>1 Stich-proben pro Woche	= oder <1 Stich-proben pro Woche
Anzahl Aufträge bei der Rechtevergabe	Durchgeführte Aufträge bei Anlage, Änderung oder Löschung von Benutzern, Rollen oder Ressourcen		Informative Kennzahl	
Aufwand Access Manager Rolle	Kumulierter Aufwand in Stunden der ausgeführten Access Manager Rolle			

Tabelle 5.1: Aus[48]*S.249* adaptierte Tabelle zeigt IAM Kennzahlen für die Rapportierungsperiode

Schritt 9: Vollständige Inbetriebnahme abschließen

Nach der Implementierung aller technischen Funktionalitäten und organisatorischen Artefakten und Teilprozessen steht die Überwachung des laufenden IAM-Systems im Vordergrund und ein Coaching der Mitarbeiter, die dauerhaft den Prozess leben, ist durchzuführen. Ziel ist es, die letzten speziellen Gegebenheiten und Abläufe in das IAM zu integrieren, sodass ein einheitlicher Ansatz dauerhaft angewendet wird.

Validieren und Konsolidieren

Es gilt, den neuen Stand von Accounts, Rollen, Ressourcen und Berechtigungen durch die Fachabteilungen validieren zu lassen, unter Anwendung und Einhaltung der eingeführten Teilprozesse. Dabei ist die Durchführung speziell aus Sicht des IAM-Teams zu konsolidieren, sodass letzte Mängel und Schwachstellen optimiert werden können, um die vollständige Inbetriebnahme abzuschließen.

Schritt 10: Kontinuierliche Verbesserung leben

Die ISO 9000-Serie (Kap. 2.5.1) stellt die Phasen der Entwicklung, Produktion, Einführung und Betreuung in den Mittelpunkt, um eine Leistungsverbesserung voranzutreiben. Dies bedeutet, dass im IAM der Aufbau, Betrieb und Abbau der Methoden, Werkzeuge und Artefakte organisiert sein muss. Analog dazu stehen die zu erfüllenden Vorgaben der ISO 20000-Serie (Kap. 2.5.2), die den Plan-Do-Check-Act-Zyklus integrieren und für eine gleichbleibende Servicequalität gemäß KVP, Sorge tragen. Dazu folgende Ansätze, unter diesen die kontinuierliche Verbesserung gefördert wird:

- Weiterentwicklung des Prozesswissens und des fachlichen Know-hows
- Kennzahlen, die realistische Messwerte schaffen, um Zahlen, Daten und Fakten des IAMs abzubilden zum Zwecke Eigenkontrolle und Reporting gegenüber dem Management, IS und ERM
- Verminderung von Ausfallzeiten und Verzögerungen
- Integration von Weiterentwicklungen und Trends
- Regelmäßiges Anpassen der Zugriffskontrollanforderungen durch Sicherheits- und Bedrohungsanalysen gemäß[33]

6 Fazit und Ausblick

Die Bedeutung von Governance zeigt, dass Transparenz und Unabhängigkeit der Unternehmensorgane zur Erfüllung der Compliance essentiell sind. Das IAM wurde als Teilprozess der IT-Governance zu- und untergeordnet. Die Arbeit unterteilt die Explikationen in direkte und indirekte Forderungen.
Die Recherchen des Autors ergaben, dass in der Literatur und IAM-Leitfäden (u.a. [50],[33]*M.2587 S.2890/ M.2.587 S.2896* ISO 27002:*9 Access control*,[45]*S.69-106*,[52],[23]) technische Funktionalitäten und Best-Practices im Mittelpunkt stehen und der Ursprung der Forderungen vernachlässigt wird. Die vielfältigen Vorgaben werden vermehrt als zentrale Compliance-Vorgaben zusammengefasst. Dieser Umstand ist aus Sicht des Autors eine Schwäche, da die nachhaltige und wirksame Erfüllung der Vorgaben nur gelingt, wenn die Vorgaben von der ursprünglichen Quelle ausgehend berücksichtigt werden als Basis der künftigen Handhabung. Für die praktische Umsetzung sind alle Interessengruppen des Unternehmens einzubeziehen und mit einem einheitlichen Verständnis auszustatten. Die Erfüllung der ersten und zweiten Zielsetzung beruht daher auf juristischen Recherchen mit dem Ziel, dass der vorliegende Leitfaden eine Orientierungshilfe zu den Anforderungen, Gesetzen und Normen ist und diese auf die IAM-Elemente zurückführt.
Das Kap. 5 vereint die praktischen Begebenheiten und die Erfahrungen des Autors zu einer ITIL und IT-Grundschutz Katalog geprägten Vorgehensweise. Die Kombination ist ein idealer Ausgleich zwischen organisatorischen und technischen Best-Practices für die Erfüllung der dritten Zielsetzung.

Zentrale Erfolgsfaktoren

- *Einbeziehung aller Interessengruppen ist für ein erfolgreiches IAM entscheidend.*

Die Teilprozesse ermöglichen einen Lebenszyklus der Accounts, Rollen, Ressourcen und Berechtigungen, der in jeder Organisationseinheit angewandt wird. Der Interessenausgleich aller Anspruchsgruppen bewirkt die unternehmensweite Akzeptanz.

- *Customizing ist zu vermeiden, um Flexibilität und Agilität mit Standard-Software zu erreichen.*

Statt Software, Methoden und Werkzeuge vollständig den internen Prozessen, Terminologien und Verantwortungen anzupassen, ist Flexibilität und Agilität durch Standardsoftware zu fördern, um auf veränderte Rahmenbedingungen zeitnah reagieren zu können. Dazu ist die Maßnahme *M 4.499 Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen*[33] zu berücksichtigen.

- *Dezentrale Verantwortung über Zugriffskontrollanforderungen und Berechtigungskonzept in den Fachabteilung fördert eine angemessene Rechtevergabe.*

Die Fachbereiche verfügen über detaillierte Kenntnisse, welche Ressourcen zur Ausübung der Tätigkeiten benötigt werden. Das IAM übt eine beratende Funktion aus, um die Sicherheitsrichtlinien in den Fachbereichen zu integrieren.

- *Virtuelle Ressourcen ermöglichen die Anbindung von Systemen, deren automatisierte Steuerung unmöglich ist.*

Mit dieser Methodik kann jede noch so heterogene System- und Netzwerklandschaft an das zentrale IAM gesteuert werden.

- *Mit informativen und IKS bezogenen Kennzahlen Kontrollmöglichkeiten schaffen.*

Einhaltung und Kontrolle der Teilprozesse sorgen für einen qualitativen und dokumentierten Berechtigungsstand. Mit aussagekräftigen Kennzahlen kann dem Management das positive Wirken des IAMs verdeutlicht werden.

Abschließende Fragestellungen

In Kapitel 2 *Anforderungen, Gesetze und Normen* wurden direkte und indirekte Forderungen auf Fundstellen zurückgeleitet und als Motivationsgründe für das IAM aufgeführt (siehe Tabelle 2.3). Es folgte, dass ein IAM ein Teilprozess der unternehmensweiten IT-Governance mit dem Ziel einer kontinuierlichen und nachweislichen IT-Compliance ist. Die Überlegungen des Autors bewegen sich dahingehend, eine Veränderung der Denkweise anzustoßen. Für ihn erhärtet sich der Verdacht, dass die Implementierung

eines IAMs hauptsächlich durch die gesetzliche Compliance getrieben wird. Dies verkennt oft die deutlich weiter gehenden Möglichkeiten der Implementierung eines IAMs.
Den Erfahrungen des Autors zufolge werden Unternehmenssubstitutionen, die maßgeblich zur Compliance beitragen, häufig einzig und allein als "notwendige Ausgaben ohne Einnahmen" betrachtet. Bei Budgetkürzungen und anderen Sparmaßnahmen rücken diese deshalb häufiger in den Fokus, mit dem Ergebnis: "Konsolidieren, Optimieren und Outsourcen".
So kann eine Kettenreaktion ausgelöst werden, da Abteilungs- und Teamleiter hinsichtlich ihrer Anstellung und dem ihnen zur Verfügung stehenden Budget großem Druck ausgesetzt sind und in einen Rechtfertigungsmodus verfallen. So leidet die Effektivität und Qualität im Arbeitsalltag, es entsteht ein negatives Arbeitsklima.
Folgende Fragen stellen sich:

- Wo wirkt sich das IAM, abseits von Zugriffs- und Berechtigungssteuerung, weiterhin positiv aus?
- Wie lassen sich positive Effekte des IAMs darstellen?
- Was muss dem Management vorgetragen werden, um das Wirken des IAMs als Wertbeitrag betrachten zu können?

Am Ende steht die Frage:

Mit welchen Kennzahlen lässt sich das positive Wirken des Identity Access Managements in Bezug auf Agilität, Skalierbarkeit und dem Beitrag zur Compliance, durch die verbesserte Sicherheit abbilden?

Abkürzungsverzeichnis

AC DB Access Datenbank

AFIPS American Federation of Information Processing Societies

AktG Aktiengesetz

ANSI American National Standards Institute

BaFin Bundesanstalt für Finanzdienstleistungsaufsicht

BDSG Bundesdatenschutzgesetz

BMJV Bundesministerium der Justiz und für Verbraucherschutz

BS British Standard

BSI Bundesamt für Sicherheit in der Informationstechnik

CEO Chief Executive Officer

CFO Chief Financial Officer

COBIT Control Objectives for Information and Related Technology

DCGK Deutschen Corporate Governance Kodex

DV-Systems Datenverarbeitungssystem

EDV Elektronische Datenverarbeitung

ERM Enterprise Risk Management

GDPdU Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen

GoBD Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff

GoBS Grundsätze ordnungsgemäßer datenverarbeitende gestützte Buchführungssysteme

HGB Handelsgesetzbuch

HPU Hoch priviligierter User

HR Human Resource

IAM Identity Access Management

IDM Identitätsmanagement

IDM Identitätsmanagement

IEC International Electrotechnical Commission

IKS Internes Kontrollsystem

IS Informationssicherheit

ISACA Information Systems Audit and Control Association

ISMS Information Security Management System

ISO Internationale Organisation für Normung

IT Informationstechnologie oder Informationstechnik

ITIL Information Technology Infrastructure Library

KonTraG Gesetz zur Kontrolle und Transparenz

KVP Kontinuierlicher Verbesserungsprozess

KWG Gesetz über das Kreditwesen

LiqV Liquiditätsverordnung

MaRisk BA MaRisk für Banken und Finanzinstitute

MaRisk VA MaRisk für Versicherungsunternehmen

MaRisk Mindestanforderungen an das Risikomanagement

NASDAQ National Association of Securities Dealers Automated Quotations

PC Personal Computer

PCAOB Public Company Accounting Oversight Board

PCDA-Zyklus Plan-Do-Check-Act-Zyklus

RBAC Role Based Access Control

SEC Securities and Exchange Commission

SolvV Solvabilitätsverordnung

SOX Sarbanes Oxley Act

VAG Versicherungsaufsichtsgesetzes

WpHG Wertpapierhandelsgesetz

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[1] A. Werder. *Führungsorganisation: Grundlagen der Corporate Governance, Spitzen- und Leitungsorganisation*. Springer Fachmedien Wiesbaden, 2015.

[2] BMJV. Aktiengesetz. http://www.gesetze-im-internet.de/aktg/, 11 2016.

[3] BMJV. Gesetz betreffend die Gesellschaften mit beschränkter Haftung. http://www.gesetze-im-internet.de/gmbhg/, 11 2016.

[4] BMJV. Gesetz über Ordnungswidrigkeiten. http://www.gesetze-im-internet.de/owig_1968/, 11 2016.

[5] Eberhard Krügler. Compliance - ein Thema mit vielen Facetten. *Umwelt Magazin Heft 7/8 2011*, 2011.

[6] M. Falk. *IT-Compliance in der Corporate Governance: Anforderungen und Umsetzung*. SpringerLink : Bücher. Gabler Verlag, 2012.

[7] Regierungskommission Deutscher Corporate Governance Kodex (Hrsg.). Deutscher Corporate Governance Kodex (in der Fassung vom 26. Mai 2010). 05 2010.

[8] R.T. Grünendahl, A.F. Steinbacher, and P.H.L. Will. *Das IT-Gesetz: Compliance in der IT-Sicherheit: Leitfaden für ein Regelwerk zur IT-Sicherheit im Unternehmen*. Vieweg+Teubner Verlag, 2012.

[9] C.E. Hauschka and P. Buck-Heeb. *Corporate Compliance: Handbuch der Haftungsvermeidung im Unternehmen*. Beck, 2007.

[10] C. Menzies. *Sarbanes-Oxley Act: professionelles Management interner Kontrollen*. Schäffer-Poeschel, 2004.

[11] M. Roth. *Compliance, Integrität und Regulierung: ein wirtschaftsethischer Ansatz in 10 Thesen*. Schulthess, 2005.

[12] Dr. iur. Uwe H. Schneider. Compliance als Aufgabe der Unternehmensleitung. *Zeit für Wirtschaftsrecht - ZIP 2003, 645*, 2003.

[13] BMJV. Bekanntmachung des deutschen corporate governance kodex (in der fassung vom 24. juni 2014), 2014. Amtlicher Teil.

[14] ISACA. *COBIT 5: Enabling Information.* Cobit 5. Information Systems Audit and Control Association, 2013.

[15] M. Beims. *IT-Service-Management in der Praxis mit ITIL 3: Zielfindung, Methoden, Realisierung.* Hanser Verlag, 2010.

[16] W. Goltsche. *COBIT kompakt und verständlich: Der Standard zur IT Governance - So gewinnen Sie Kontrolle über Ihre IT - So steuern Sie Ihre IT und erreichen Ihre Ziele.* Vieweg+Teubner Verlag, 2007.

[17] ISACA. Information Systems Audit and Control Association: Offizieller Webauftritt. http://www.isaca.de/, 12 2016.

[18] BMJV. Bundesdatenschutzgesetz. https://www.gesetze-im-internet.de/bdsg_1990/, 11 2016.

[19] BSI. It-grundschutz online. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_n 12 2016.

[20] A. Olbrich. *ITIL kompakt und verständlich: effizientes IT-Service-Management - den Standard für IT-Prozesse kennenlernen, verstehen und erfolgreich in der Praxis umsetzen.* Aus dem Bereich IT erfolgreich lernen. Vieweg+Teubner Verlag, 4., erweiterte und verbesserte Auflage edition, 2008.

[21] R. Buchsein, F. Victor, H. Günther, and V. Machmeier. *IT-Management mit ITIL® V3: Strategien, Kennzahlen, Umsetzung.* Edition CIO. Vieweg+Teubner Verlag, 2008.

[22] K.R. Müller. *IT-Sicherheit mit System.* Vieweg+Teubner Verlag, 4., neu bearbeitete und erweiterte auflage edition, 2011.

[23] Ernst & Young. *Identity and access management Beyond compliance.* Insights on governance, risk and compliance, 2013.

[24] A. Tsolkas and K. Schmidt. *Rollen und Berechtigungskonzepte: Ansätze Für Das Identity- und Access Management Im Unternehmen.* Edition kes. Vieweg+Teubner Verlag, 2010.

[25] Wolfgang Heinrich Stefan Groß, Thorsten Brand. *Die GoBD in der Praxis - Ein Leitfaden für die Unternehmenspraxis.* Peters, Schönberger & Partner mbB, 2017.

[26] BMJV. Handelsgesetzbuch. https://www.gesetze-im-internet.de/hgb/, 11 2016.

[27] Bundesministerium der Finanzen. *Bekanntmachung GoBD.* 2014.

[28] BMJV. *Bundesdatenschutzgesetz - (BDSG 2006) ; Textausgabe ; deutsch/englisch.* Datakontext., 2006.

[29] ISO 9000:2000-12. DIN EN ISO 9000:2000-12, Abschnitt 0.2.

[30] H. Kersten, J. Reuter, K.D. Wolfenstetter, and K.W. Schröder. *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz: Der Weg zur Zertifizierung.* Edition kes. Springer Fachmedien Wiesbaden, 2013.

[31] ISO 27014. ISO/IEC 27014 grundsätze: Offizieller Webauftritt, 12 2016.

[32] BSI. *Vergleich ISO 27000 und IT-Grundschutz.* Stand 15. ergÃ¤nzungslieferung edition, 2016.

[33] BSI. *IT-Grundschutz.* 2016.

[34] ISO 31000. Risk management: Offizieller Webauftritt, 12 2016.

[35] Basel Committee on Banking Supervision. *Basel III: International framework for liquidity risk measurement, standards and monitoring.* Bank for International Settlements, 2010.

[36] Prof. Dr. Klaus-Peter Kossakowski. IT Security Risk Management - Vorlesungsscript, 10 2015.

[37] BSI. Cyber-Sicherheit. https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html, 11 2016.

[38] MBA Dipl. Ing. Dr. Manfred Stallinger. *IT-Governance im Kontext Risikomanagement Dissertation am Institut für Wirtschaftsinformatik.* PhD thesis, Institut für Wirtschaftsinformatik, 05 2007.

[39] BSI. IT-Grundschutz Modernisierung, 11 2016.

[40] BSI. IT-Grundschutz Standards, 11 2016.

[41] BMJV. Gesetz über das Kreditwesen. http://www.gesetze-im-internet.de/kredwg/, 11 2016.

[42] Bernd Schöne. Verheiratung zweier Welten. *PROTECTOR Special Zutrittskontrolle 2012*, 2012.

[43] Dipl. Ing. Stefan Kempter und Dr. Andrea Kempter. ITIL Process maps: ITIL Access Management: Offizieller Webauftritt. IT Process Maps GbR, 2016 12.

[44] B. W. Lampson. Dynamic Protection Structures. In *Proceedings of the November 18-20, 1969, Fall Joint Computer Conference*, AFIPS '69 (Fall), pages 27–38, New York, NY, USA, 1969. ACM.

[45] Korbinian Molitorisz. Rollenmodelle für die Zugriffskontrolle in Unternehmen. Diplomarbeit, Universität Karlsruhe (TH) Institut für Telematik, 11 2008.

[46] David Ferraiolo und Richard Kuhn. Role-Based Access Controls. *15th National Computer Security Conference (1992), Baltimore MD pp. 554 - 563*, 1992.

[47] D. Ferraiolo, D.R. Kuhn, and R. Chandramouli. *Role-based Access Control*. Artech House Computing Library. Artech House, 2007.

[48] F. Kleiner. *IT Service Management: Aus der Praxis für die Praxis*. Springer Fachmedien Wiesbaden, 2013.

[49] H. Klarl. *Zugriffskontrolle in Geschäftsprozessen: Ein modellgetriebener Ansatz*. Vieweg+Teubner Verlag, 2011.

[50] deron services GmbH. *Leitfaden Identity & Access Management ... über Funktionsbausteine, Vorteile und Good Practice in IDM-Projekten*. 2015.

[51] Sangrae Cho Seunghun Jin Dongwan Shin, Gail-Joon Ahn. *A role-based infrastructure management system: design and implementation*. John Wiley & Sons Ltd, 2004.

[52] Daniel Reisacher. *Ganzheitliches Identity & Access Management (IAM)*. ipg ag, information process group, 2011.