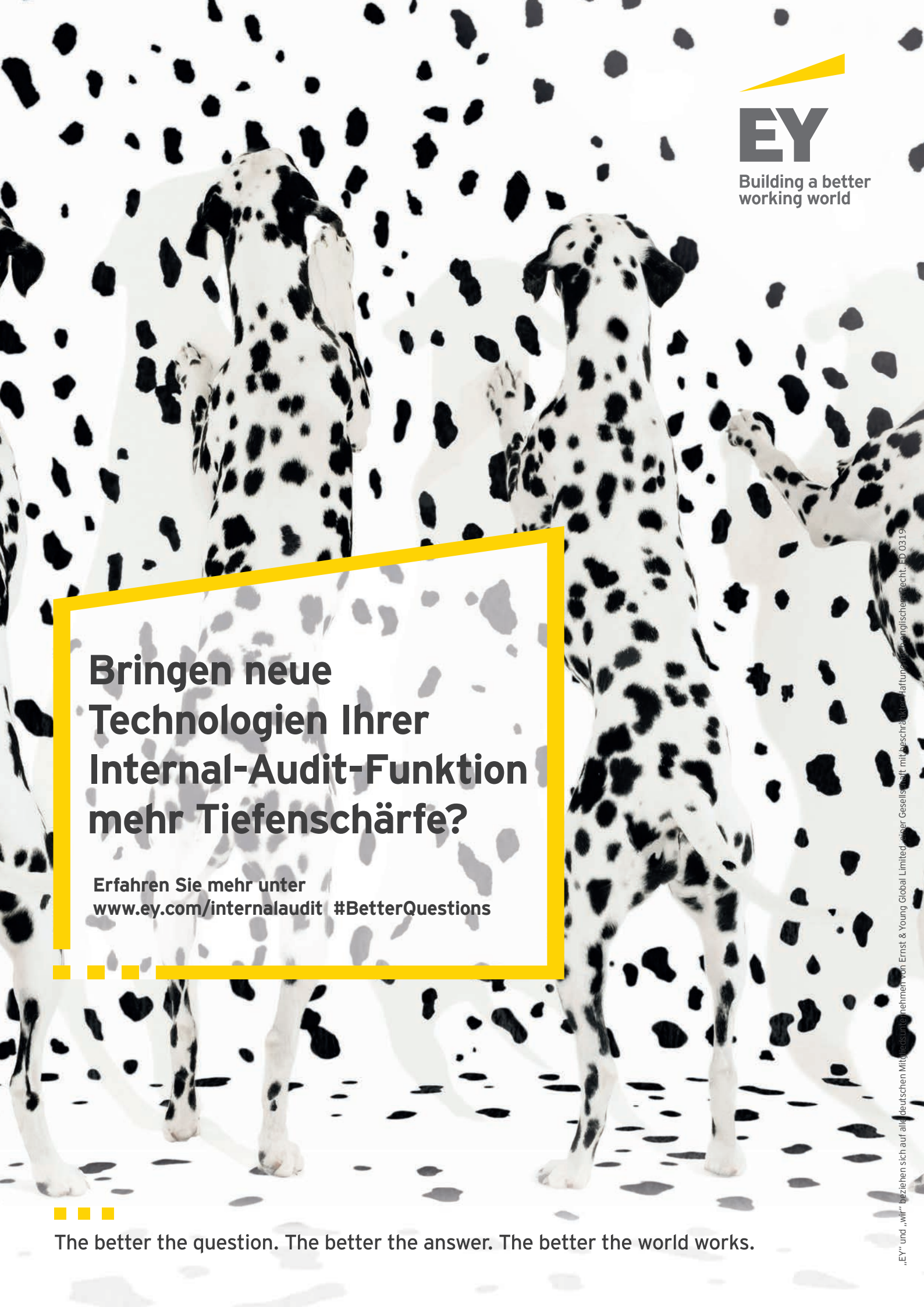
2017

# Jahrbuch

INSTITUT FÜR
INTERNE REVISION
ÖSTERREICH

IIA AUSTRIA



# Inhaltsverzeichnis

# Vorwort

## Liebe Kolleginnen und Kollegen,

es ist wieder soweit – wir dürfen Ihnen das zweite Jahrbuch des Institutes für Interne Revision Österreich überreichen. Es wurde mit Spannung erwartet und spiegelt ein weiteres Jahr in der Weiterentwicklung unseres Institutes wider.

Dabei könnte man meinen, dass ein Jahrbuch dem anderen gleichen müsste, da sich ja nur die Berichtsjahre ändern und Interne Revision immer Interne Revision ist und bleibt. Dem ist jedoch nicht so! Die Aufgabenstellung und das Umfeld der Internen Revision entwickeln sich rasant weiter und auch das Berufsbild und die Anforderungen an „den Revisor" steigen ständig und machen das Berufsbild so interessant und abwechslungsreich.

Beim Durchblättern unseres Jahrbuchs werden Sie feststellen, dass sich wieder eine Reihe von Kollegen und Kolleginnen bereit erklärt haben, für Sie interessante Themenstellungen darzustellen und zu beleuchten. An dieser Stelle ein herzliches Dankeschön an die Autorinnen und Autoren für ihre Mühen und Unterstützung.

Sie werden feststellen, dass wir dieses Jahrbuch um eine Reihe von Fakten und Zahlen ergänzt haben, die Sie im Anhang finden.

Blättern Sie in diesem Jahrbuch, studieren Sie unsere Homepage, und Sie werden sehen in welchem flexiblen und dynamischen Umfeld wir als Revisorinnen und Revisoren arbeiten welches wir gemeinsam mit Ihnen gestalten können.

Wir wollen Ihr Wissen – wir brauchen Ihre Unterstützung! Bieten Sie uns ein interessantes Thema an als Vortrag für unseren „Erfahrungsaustausch", nützen Sie auch die Arbeitskreise des Institutes zum Networking, zum Austausch mit Kolleginnen und Kollegen zur Wissenserweiterung. Wir freuen uns auf Ihre Wünsche und Anregungen.

Unser Institut war auch im Jahr 2017 international aktiv. Angela Witzany war von Mitte 2016 bis Mitte 2017 als Chairman of the Board of the IIA Global tätig. Wir waren weiters bei den europäischen CEO – Meetings, den GELT Meetings, der ECIIA General Assembly und der ECIIA Konferenz in Basel im Herbst 2017 präsent.

Seitens der Akademie der Internen Revision können wir von einem sehr erfreulichen Jahr 2017 berichten. 505 Kolleginnen und Kollegen nutzten das Seminarangebot der Akademie. In diesem Jahr konnten wir auch einige neue Seminare erfolgreich erstmals durchführen, darunter – unverzichtbar – ein Spezialseminar zur DSGVO.

Auch die Veranstaltungen und Konferenzen, die die Akademie gemeinsam mit und für das Institut durchgeführt hat, erfreuten sich großen Zuspruchs. Unsere Jahrestagung fand mit Unterstützung der Casinos Austria im Studio 44 statt und stand unter dem Thema „Auditor's Empowerment". Auch 2017 wurde die CIA Tagung im Parkhotel Pörtschach abgehalten.

Im Jahr 2017 wurden drei ERFA's organisiert. Im Frühjahr zu dem Thema „Prüfung der Wirkungsorientierung". Herzlichen Dank an dieser Stelle an den Arbeitskreis WIFO und speziell an Ines Schubiger und Hannes Schuh für die perfekte Vorbereitung.

Der Herbst – ERFA wurde vom Arbeitskreis GRC organisiert, dem ebenfalls unser Dank gebührt, hier speziell Stephan Pichler für die Vorbereitung.

Und dann war da noch die DSGVO. Aufgrund zahlreicher Anfragen von Mitgliedern organisierten wir am Freitag, den 15. Dezember 2017 nachmittags einen Sonder – ERFA zu diesem Thema. Die Vorbereitung erfolgte gemeinsam vom Arbeitskreis WIFO und WIKRI und unser Dank geht an Gabriele Herbsthofer und Matthias Kopetzky. Bei allen ERFA's konnten wir aufgrund der begrenzten Saalkapazität im Don-Bosco-Haus leider nicht alle Anmeldungen berücksichtigen.

Mit Unterstützung durch den Programmausschuss und der ISACA begannen wir bereits im Sommer 2017 mit der Planung der Audit Competence, die mit etwa 300 Teilnehmerinnen und Teilnehmern im Jänner 2018 im eleganten Ambiente des Hotel Savoyen in Wien stattfand. In drei parallelen Vortragsreihen wurden IT – Themen, aktuelle Trends in der Internen Revision und Soft Skills präsentiert. Key Note Speaker waren Dr. Udo Birkner, Vorstandsdirektor der Hypo Bank Niederösterreich („Aufsichtsrat, Vorstand und Interne Revision"), Georg Beham von Grant Thornton („DSGVO") und Andreas Kamm von Zeppelin GmbH („Grafen ziehen Grafen an").

Zum Zeitpunkt der Drucklegung dieses Jahrbuches fand bereits der Frühjahrs – ERFA 2018 statt. Unter dem Titel „Heiße Eisen, dünnes Eis" berichteten Kolleginnen und Kollegen über heikle und selten geprüfte Gebiete. Dieser ERFA fand erstmals im Kardinal–König–Haus in Wien statt.

Als Ergebnis unserer Kooperation mit INARA, der Plattform für Compliance and Governance, konnte am 15. Mai 2018 eine Podiumsdiskussion in der Wiener Börse organisiert werden. Es diskutierten Aufsichtsräte, Vorstände und Revisionsleiterinnen und -leiter über „Aufsichtsrat und Interne Revision – eine neue Allianz?".

In Planung ist bereits die CIA Tagung in Pörtschach am 14. und 15. Juni 2018 (Thema: „Audit & Fraud – Challenge oder Dilemma") und die Jahrestagung, die uns in diesem Jahr am 13. und 14. September 2018 nach Salzburg führen wird. Das Generalthema der Jahrestagung ist die Digitalisierung. Spannende Referentinnen und Referenten werden diese Themen unter verschiedenen Gesichtspunkten beleuchten.

Erstmals werden wir auch eine gemeinsame Veranstaltung gemeinsam mit dem Rechnungshof organisieren. Dieser „Wissensgipfel" am 12.Juni 2018 wird gemeinsame und unterschiedliche Ansätze bei der „Prüfung der Qualität der Leistungserbringung" beleuchten.

Last but not least wird unser Herbst – ERFA wieder die DSGVO zum Thema haben.

Wir, der Gesamtvorstand des IIRÖ sowie die Geschäftsführung der AIR möchten auch den Mitarbeiterinnen ein ganz besonderes Dankeschön aussprechen, ohne deren unermüdliche Unterstützung wäre ein reibungsloser Ablauf der Betreuung unserer Mitglieder, der Seminare und der Veranstaltungen nicht möglich.

Ihnen allen viel Spaß bei der Lektüre!

Ihr Gesamtvorstand des IIRÖ sowie Ihr Geschäftsführer der AIR

# In welchen Bereichen beeinflusst die Interne Revision die Qualität (Reifegrad) des ERM-Systems?

**Michael Brandstätter und Walter S.A. Schwaiger**
Institut für Managementwissenschaften an der Technische Universität Wien,
Theresianumgasse 27, 1040 Wien, Österreich, walter.schwaiger@tuwien.ac.at

## Vorbemerkungen

Die Interne Revision (IR) unterstützt die Geschäftsführung sowie gegebenenfalls die Aufsichtsorgane beratend bei der Ausgestaltung bzw. Verbesserung des unternehmensweiten Risikomanagements (Enterprise Risk Management: ERM) und prüft zumeist die im Unternehmen implementierten ERM-Systeme. In der am Institut für Managementwissenschaften (TU Wien) durchgeführten ERMMA-Studie 2017 [1] wird die Qualität der ERM-Systeme von österreichischen Unternehmen anhand von fünf Reifegraden gemessen. Dabei zeigt sich, dass der ERM-System-Reifegrad signifikant von der Dauer der IR-Tätigkeit abhängig ist. In diesem Beitrag wird die Analyse vertieft, um zu eruieren, in welchen Bereichen der ERM-System-Ausgestaltung die IR-Tätigkeitsdauer die größten Wirkungen zeigt. Für Unternehmen, welche an der Verbesserung ihres ERM-Systems arbeiten, liefert der dabei festgestellte Befund interessante Hinweise für konkrete Verbesserungsmöglichkeiten.

## Inhalt

# 1. Einleitung

*In carrying out their responsibilities, internal auditors assist management and the board of directors or audit committee by examining, evaluating, reporting on, and recommending improvements to the adequacy and effectiveness of the entity's enterprise risk management.( COSO-ERM-Framework, Seite 88 [2]).*

Die Interne Revision (IR) unterstützt die Geschäftsführung sowie gegebenenfalls die Aufsichtsorgane beratend bei der Ausgestaltung bzw. Verbesserung des unternehmensweiten Risikomanagements (Enterprise Risk Management: ERM) und prüft zumeist die im Unternehmen implementierten ERM-Systeme. In Ausübung ihrer Beraterrolle [3] kann die IR dabei helfen ein ERM-System einzurichten, der Geschäftsführung (Aufsichtsorgane) Vorschläge zur (Weiter-)Entwicklung der Risikostrategie unterbreiten, ERM-Aktivitäten im Unternehmen koordinieren und die Kommunikation von Risikoinformationen verbessern. Um hinsichtlich der Ausgestaltung von ERM-Systemen beratend tätig werden zu können, müssen Revisoren die Anforderungen der Geschäftsführung ans ERM-System kennen, analytische Fähigkeiten besitzen und in der Lage sein unterstützend einzugreifen. Wichtig bei einer intensiven Beratungstätigkeit seitens der IR ist es jedoch, stets die Objektivität und Unabhängigkeit zu bewahren. Die letztendliche Verantwortung für die konkrete Ausgestaltung des ERM-Systems liegt immer bei der Geschäftsführung.

Für die Ausübung der Prüferrolle bedarf die IR der gleichen Kompetenzen wie für die Ausübung der Beraterrolle. Durch die Übernahme von Prüfungstätigkeiten wirkt die IR allerdings nicht mehr nur beratend bei der ERM-System-Ausgestaltung mit, sondern übernimmt einen aktiven Part in der Funktionsweise des im Unternehmen eingerichteten ERM-Systems. Die Prüferrolle der IR wird im 3-Lines of Defense-/3-LoD-Modell [4], welches in leicht modifizierter Form in Abb. 1 abgebildet ist, in der 3. Säule angesiedelt. Insofern ist die IR für die unabhängige Prüfung des in den ersten beiden Säulen eingerichteten ERM-System zuständig. Konzeptionell betrachtet liefert die 2. Säule die für das Risikomanagement benötigten (Risiko-)Informationen, welche in den verschiedenen Managementsystemen der 1. Säule für die Planung und Steuerung auf den jeweiligen Managementebenen eingesetzt werden. Folglich kann die 2. Säule als Provider von Risikoinformationen und die 3. Säule als User der entsprechenden Risikoinformation interpretiert werden.

Der Vorteil dieser informationalen Provider/User-Perspektive liegt in der Offenlegung der verschiedenen Risikotypen [5], welche auf den 3 verschiedenen Managementebenen zu unterscheiden sind. Auf der Prozessebene sind es vermeidbare Risiken (preventable risks), mit welchen keine Chancen verknüpft sind und sie deshalb vollständig zu eliminieren sind. Mit den Risiken auf der Geschäftsebene (strategy execution risks) sind Chancen verknüpft, weshalb sie nicht zu eliminieren, sondern vielmehr in einem ausgewogenen Chancen/Risiko-Profil auszusteuern sind. Mit den externen Risiken (external risks) auf der strategischen Ebene gehen ebenfalls Chancen einher. Im Unterschied zu den Geschäftsrisiken sind sie allerdings nicht steuerbar. Folglich gilt es z.B. im Sinne eines Business Continuity bzw. Resilience Managements auf den möglichen Eintritt von externen Risiken vorzubereitet zu sein.

Um das in Abb. 1 konzeptionell dargestellte 3-LoD-Modell umfassend zu verstehen, bedarf es einer hohen fachlichen ERM-System-Kompetenz (Qualität) seitens der Revisoren. Zur Erlangung dieses umfassenden Verständnisses braucht es sicherlich Zeit. Folglich ist davon auszugehen, dass die Dauer, welche die IR im Unternehmen tätig ist, einen soliden Indikator für die ERM-System-Expertise der IR darstellt. In diesem Sinne ist zu erwarten, dass sich mit zunehmender IR-Tätigkeitsdauer auch die Qualität der Ausgestaltung des ERM-Systems verbessert.

Aus wissenschaftlicher Perspektive zeigt sich hinter dieser Überlegung eine Hypothese, u.z. dass die Qualität (Reifegrad) des ERM-Systems positiv mit der Qualität (IR-Tätigkeitsdauer) der IR zusammenhängt. Zur statistischen Überprüfung dieser Hypothese wird auf das Datenmaterial der am Institut für Managementwissenschaften (TU Wien) durchgeführten ERMMA-Studie 2017 [1] zurückgegriffen. In dieser Studie wurde zur Klassifizierung der ERM-System-Qualitäten das ERMMA-Klassifikationsschema verwendet, wobei das ERM-System über 3 Dimensionen und dessen Qualität anhand von 5 Reifegraden definiert werden. Die Auswertung der Daten bestätigt nicht nur diese Hypothese, sondern gibt darüber hinaus auch noch konkrete Einblicke in die Gestaltungsbereiche, welche durch eine langjährige IR-Tätigkeit signifikant verbessert werden.

Dieser Artikel ist wie folgt aufgebaut: Im nachfolgenden Kapitel wird das zur Messung der ERM-System-Qualitäten verwendete ERMMA-Klassifikationsschema vorgestellt. Ein klares Verständnis dieses Schemas ist wichtig, um zu verstehen, wie das ERM-System konkret definiert ist und wie dessen Qualität gemessen wird. Daran anschließend werden die für diesen Beitrag wichtigen Ergebnisse der ERMMA-Studie 2017 vorgestellt. Diese Ergebnisse beinhalten das ERMMA-Profil, die Dim.Scores und den Gesamt-Score für alle an der Studie teilgenommenen Unternehmen. Diese Informationen bilden den Referenzpunkt (Benchmark), um die Auswirkungen unterschiedlicher IR-Tätigkeitsdauern beurteilen zu können. Diese Auswirkungen werden in einem eigenen Kapitel vorgestellt. Dabei wird der Einfluss der IR-Tätigkeitsdauer auf den Gesamt-Score, die Dim.Scores, das ERMMA-Profil, die Zufriedenheit und die im ERM-System berücksichtigten Risiken und Chancen analysiert. Abschließend werden die Ergebnisse konkludiert und ein Ausblick auf die ERMMA-Studie 2018 gegeben.


**ABB. 1: 3-LINES OF DEFENSE (3-LOD)-MODELL (INKL. STRATEGISCHES MANAGEMENT)**

## 2. ERM-System-Klassifikation: Dimensionen und Reifegrade

Die ERMMA-Studie 2017 basiert auf einem von der Funk-Stiftung (Hamburg) geförderten Wissenschaftsprojekt, wobei zur Messung der Qualitäten (Reifegrade) von ERM-Systemen ein 2-dimensionales Klassifikationsschema und darauf aufbauend ein intelligenter Online-Fragebogen entwickelt wurde. Das dabei entwickelte ERMMA-Klassifikationsschema ist in Abb. 2 zu sehen.

Mit diesem Schema werden zwei Spezifikationsprobleme zugleich adressiert:

1. ERM-System-Definition: Das nicht direkt beobachtbare ERM-System-Konstrukt wird anhand der 3 Dimensionen, u.z. A) ERM-Governance, B) RM-System und C) Risiko(basierte) Planungs- und Steuerungssysteme, definiert. Diese drei Dimensionen sind die Überschriften der Elemente in der zweiten Spalte der in Abb. 2 dargestellten Klassifikationsmatrix. Weiters enthält jede der 3 Dimensionen noch jeweils 3 Sub-Dimensionen, sodass das ERM-System anhand von insgesamt 9 Sub-Dimensionen gemessen wird. Die drei Dimensionen lassen sich im Lichte der Provider/User-Perspektive des 3-LoD-Modells folgendermaßen interpretieren: Beim RM-System (B-Dimension) handelt es sich um den Provider der Risikoinformationen (2. Säule) und die Risiko(basierten) Planungs- und Steuerungssysteme (C-Dimension) sind die User der Risikoinformationen. Die ERM-Governance (A-Dimension) stellt sozusagen das Dach dar, welches auf den beiden Säulen B (Provider) und C (User) aufgesetzt ist. Sie beinhaltet den wohldurchdachten ERM-Plan, nach dem die Säulen B und C ausgestaltet werden.

2. Definition der ERM-System-Qualitäten (Reifegrade): Die ebenfalls nicht direkt beobachtbaren Qualitäten der ERM-System-Ausgestaltungen werden in den letzten fünf Spalten der Klassifikationsmatrix definiert. Bei dieser Definition ist es wichtig zu sehen, dass in allen drei Dimensionen des ERM-Systems die Inhalte der jeweils dargestellten Konstrukte von links nach rechts zunehmen (progressiv zunehmende Inhalte). Beispielsweise wird die in der ERM-Governance ursprünglich angesprochene Silo-Perspektive (Reifegrad 1: RG 1) in der nachfolgenden Spalte (RG 2) erweitert, indem der Prozess zudem geprüft und gemanagt wird. Diese Erweiterung entspricht im ISO 31000-Risikomanagement-Standard [6] der Unterscheidung von Risikomanagement-Prozess und Risikomanagement-Framework. Im nächsten Schritt erfolgt der Übergang zur unternehmensweiten Perspektive (RG 3) sowie zur gesamtunternehmensbezogenen Perspektive (RG 4). Die höchste Reifegradstufe (RG 5) setzt in allen 3 Dimensionen voraus, dass die Geschäftsführung die jeweiligen Konzepte (Konstrukte) interaktiv [7] forciert. D.h., die Geschäftsführung hinterfragt permanent die Sinnhaftigkeit der jeweiligen Konzepte und diskutiert mit den jeweils Verantwortlichen mögliche Verbesserungen.

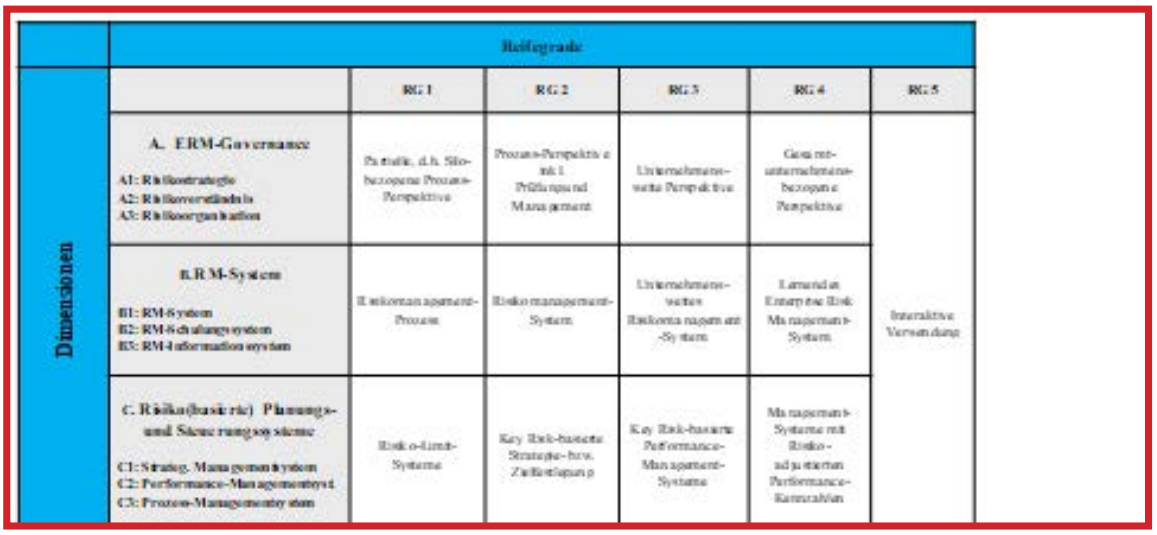



**ABB. 2: ERMMA-KLASSIFIKATIONSSCHEMA – KONZEPTIONELLES MODELL**

Wissenschaftstheoretisch basiert dieser 2-dimensionale Klassifikationsansatz auf dem Vorausschauenden Validierungs-Framework (Predictive Validity Framework [8]). Dabei stellt das ERMMA-Klassifikationsschema die konzeptionelle a priori Spezifikation des zu messenden Konstrukts dar. Dieses wird sodann anhand von inhaltlich progressiv zunehmenden Attributen konkretisiert und somit messbar gemacht. Zur fragebogenmäßigen Messung der Attribute werden schließlich Fragen spezifiziert. Durch die Vorgabe der Attribute kann dabei sichergestellt werden, dass die Fragen sowohl gültig (valid), d.h. inhaltlich richtig messend, als auch zuverlässig (reliable), d.h. interpersonell richtig messend, sind. Diese zweifache Sicherstellung begründet die vorausschauende Eigenschaft des Validierungs-Frameworks.

Der aktive Part der IR-Prüferrolle in der Funktionsweise des im Unternehmen eingerichteten ERM-Systems zeigt sich in den Dimensionen A (ERM-Governance) und B (RM-System) des ERMMA-Klassifikationsschemas ab den Reifegraden 2, wo die Prüfung seitens der IR als definitorisches Attribut erstmals in Erscheinung tritt. D.h., Unternehmen erhalten in diesen Dimensionen bzw. den jeweiligen Sub-Dimensionen nur dann einen Reifegrad von 2, wenn u.a. ihre ERM-Governance bzw. ihr RM-System seitens der IR geprüft wird. Diese Prüfanforderung erstreckt sich auch auf die höheren Reifegrade. Der Unterschied zum Reifegrad 2 liegt nur darin, dass bei höheren Reifegraden sukzessive umfassendere Konstrukte der IR-Prüfung unterliegen.

## 3. ERMMA-Studie 2017: Profil und Scores zum Benchmarking

An der ERMMA-Studie 2017 nahmen 71 österreichische Unternehmen teil, wovon 91,55 % Kapitalgesellschaften sind und 85,92 % durch einen Wirtschaftsprüfer geprüft werden. Aufgrund dieser Teilnehmerschaft gibt die Studie Einblicke in die Qualitäten (Reifegrade) der ERM-Systeme von extern geprüften Kapitalgesellschaften. Durch den Umstand, dass seitens der Wirtschaftsprüfung bei einem Mandat zur Prüfung des ERM-Systems vielfach das RM-System im Vordergrund steht, ist zu erwarten, dass bei den Studienteilnehmern die B1-Sub-Dimension RM-System gut abschneidet.

Abb. 3 zeigt im linken oberen Bild die Verteilung der Reifegrade in Form von Boxplots aller Sub-Dimensionen, der drei Dim-Scores sowie den Gesamt-Score. Der jeweils fett eingezeichnete Strich kennzeichnet den Median der Reifegrad-Verteilung. Der Median ist der (mittlere) Wert, welche die Stichprobe in zwei gleich große Teile teilt. Bei Betrachtung der Mediane für die 9 Sub-Dimensionen (A1 bis C3) fällt auf, dass dieser immer bei 1 liegt außer bei der B1-Sub-Dimension (RM-System). Dies bestätigt die kürzlich gebildete Erwartung, dass bei den Studienteilnehmern diese Sub-Dimension aufgrund der diesbezüglichen Fokussierung der Wirtschaftsprüfer gut abschneidet.

Üblicherweise sind im Boxplot ober- und unterhalb des Medians noch Flächen markiert, welche das 25%- und das 75%-Quantil der Verteilung anzeigen. Bei der B1-Sub-Dimension reichen diese Flächen z.B. bis zum Reifegrad 3 und 1. Dies besagt, dass 25 % der Unternehmen einen Reifegrad bis zu 1, 50 % einen Reifegrad bis zu 2 und 75 % einen Reifegrad bis zu 3 haben. In den Fällen, wo der untere Balken bei 0 ist (wie z.B. in A3), haben mindestens 25 % der Unternehmen einen Reifegrad von 0. In den Fällen, wo der untere Balken ident mit dem Median ist (wie z.B. in A1), haben weniger als 25 % der Unternehmen einen Reifegrad von 0. Schließlich sei noch angemerkt, dass unterschiedliche Größen der über und unter dem Median liegenden Flächen Hinweise auf die Asymmetrie der Verteilung geben. Besonders auffällig ist diese Asymmetrie bei den C-Sub-Dimensionen. In diesen Fällen streuen die Reifegrade der oberhalb des Medians liegenden Unternehmen stärker als die von den unterhalb liegenden Unternehmen.

Die Quantilswerte der Boxplots für die 3 Dim-Scores und den Gesamt-Score unterscheidet sich von denen der Sub-Dimensionen. Der Grund liegt darin, dass durch die gleichgewichtete Durchschnittsbildung der Reifegrade der Sub-Dimensionen die Dim- und

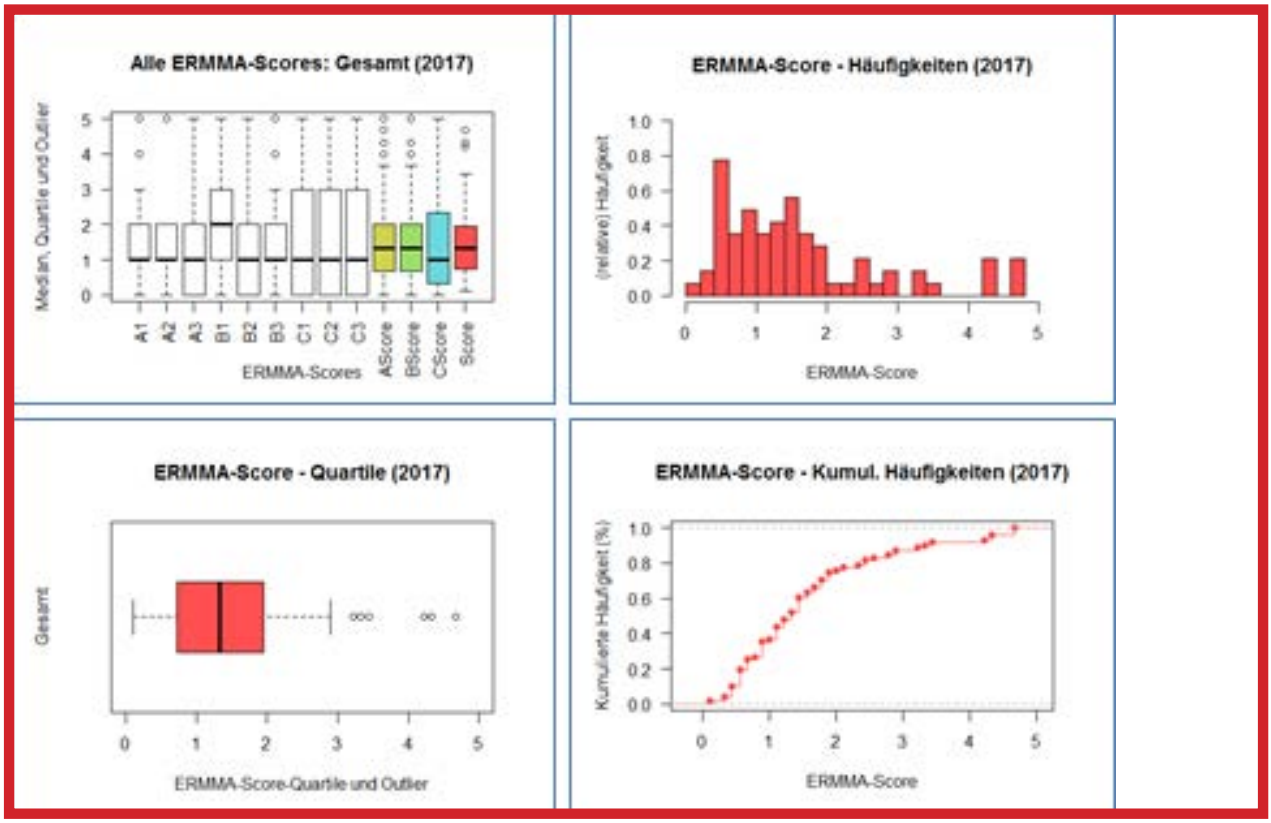



**ABB. 3: AUSGESTALTUNG DES ERM-SYSTEMS – VERTEILUNG DER REIFEGRADE**

Gesamt-Scores nicht mehr ganzzahlig sein müssen. Dies zeigt sich auch in den letzten vier Boxplots, welche sich auf diese Scores beziehen.

Der ganz rechts angesiedelte Boxplot bezieht sich auf den Gesamt-Score. Die im oberen Bereich zu sehenden Punkte zeigen sogenannte Ausreißer an, welche außerhalb der strichlierten Begrenzungslinie liegen. Im rechten oberen Bild von Abb. 3 sind diese Ausreißer am rechten Rand bei den hohen Reifegraden zu sehen. Diese Darstellung zeigt die Verteilung der relativen Häufigkeiten der Gesamt-Scores der an der Studie teilgenommenen Unternehmen. Zur Interpretation ist es wichtig, dass es sich dabei um relative Häufigkeiten und nicht um Wahrscheinlichkeiten handelt. Analog zu Dichten werden die Wahrscheinlichkeiten errechnet, indem die relativen Häufigkeiten mit den Intervallbreiten multipliziert werden. Der höchste Balken von etwa 0,8 ist somit durch 5 zu dividieren, um die entsprechende Wahrscheinlichkeit zu berechnen.

Die relativen Häufigkeiten eignen sich gut, um die Quantilswerte in den Boxplots besser zu verstehen. Die Quantile zeigen sich durch Gruppierung von nebeneinander liegenden Balken. Durch die Gruppierung der ersten 4 Balken ergibt sich approximativ das 25%-Quantil bei einem Reifegrad von 0,8 (0,725 bei exakter Berechnung). Durch die zusätzliche Gruppierung der nächsten 3 Balken ergibt sich das 50%-Quantil (Median) von 1,4 (1,33). Durch die zusätzliche Gruppierung von weiteren 3 Balken ergibt sich das 75%-Quantil von 2 (1,945). Diese 25%-, 50%- und 75%-Quantile, welche auch als Quartile bezeichnet werden, sind im linken unteren Bild von Abb. 3 gut zu erkennen. Das rechte untere Bild der Abbildung zeigt die kumulierten Wahrscheinlichkeiten des Gesamt-Scores über die 5 Reifegrade. Dazu werden die relativen Häufigkeiten mit der jeweiligen Intervallbreite multipliziert und sukzessive addiert.

# 4. Qualität der IR: Auswirkungen auf ERM-System-Qualität?

Nun sind alle Ingredienzien vorhanden, um die eingangs postulierte Hypothese eines positiven Einflusses einer hohen Qualität der IR auf die über den Reifegrad gemessene Qualität der ERM-System-Ausgestaltung empirisch zu testen. Zu diesem Zweck wird das in der ERMMA-Studie 2017 erhobene Datenmaterial nach der IR-Tätigkeitsdauer in zwei Klassen eingeteilt, u.z. in die Unternehmen mit einer kürzer als 5-jähriger IR-Tätigkeitsdauer – IR<5J-Unternehmen (37 an der Zahl) – und solche mit einer zumindest 5-jährigen Tätigkeitsdauer – IR>5J-Unternehmen (34 Unternehmen). Durch die annähernd gleich großen Klassengrößen und den über 30 Beobachtungen liegenden Stichprobenumfang sind die Ergebnisse statistisch fundiert.

## 4.1. IR-Tätigkeitsdauer: Einfluss auf ERMMA-Gesamt-Score

Abb. 4 enthält die sich in der ERMMA-Studie 2017 ergebenen Mittelwerte der Gesamt-Scores für unterschiedlich zusammengestellte Stichproben. Der linke Balken mit einem Wert von 1,618 ist der durchschnittliche Gesamt-Score (Österreich Durch.) aller 71 an der Studie teilnehmenden Unternehmen. Der drittletzte Balken auf der rechten Seite hat einen Wert von 2,225 und bezieht sich auf die IR>5J-Unternehmen. Die Qualität der ERM-Systeme derartiger Unternehmen liegt somit um 0,607 Einheiten höher als der österreichische Durchschnitt. Zumal die Klasse der IR<5J-Unternehmen annähernd groß wie die IR>5J-Klasse ist, liegt ihr durchschnittlicher Reifegradum etwa 0,607 Einheiten unter dem österreichischen Durchschnitt und beläuft sich somit auf einen Wert von 1,011.

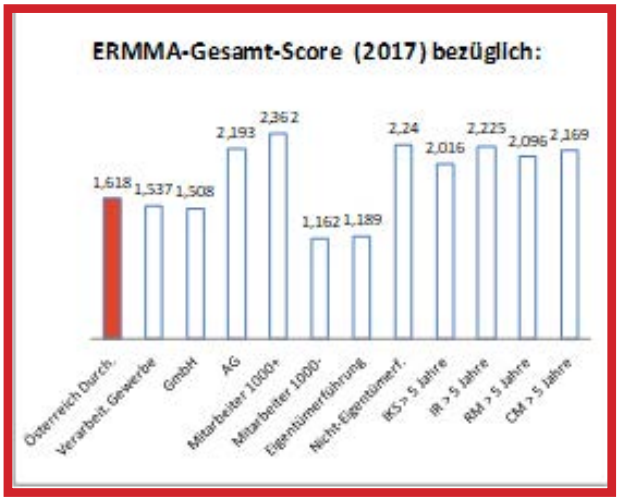



**ABB. 4: ERMMA-GESAMT-SCORE – BESTIMMUNGSFAKTOREN**

Der erste empirische Befund lautet, dass dieser große Unterschied zwischen den IR>5J- und den IR<5J-Unternehmen statistisch signifikant ist. Dieses Ergebnis ist bereits aus der ERMMA-Studie 2017 bekannt.

## 4.2. IR-Tätigkeitsdauer: Einfluss auf ERMMA-Dim-Scores und -Profil

Zur Vertiefung der Analyse werden nunmehr die 3 hinter dem Gesamt-Score stehenden Dim.Scores für die beiden Unternehmensklassen ermittelt und gegenübergestellt. Das diesbezügliche Ergebnis ist in Abb. 5 zu sehen. Die A-, B- und C-Scores sind in beiden Grafiken auf der rechten Seite zu sehen, wobei sich das linke (rechte) Bild auf die IR<5J-Unternehmen (IR>5J-Unternehmen) bezieht. Die Boxplots der IR>5J-Unternehmen haben jeweils höhere Mediane und deutlich höhere 75%-Quantile. Alle drei Reifegradverbesserungen sind auch wieder statistisch signifikant.

Neben den statistisch signifikant besseren Reifegraden in allen 3 Dimensionen des ERM-Systems gibt Abb. 5 auch Einblicke in die unterschiedlichen ERMMA-Profile der beiden Unternehmensklassen. Durch die vornehmlich aus extern geprüften Kapitalgesellschaften bestehende Stichprobe ist wiederum zu erwarten, dass die B1-Sub-Dimension in beiden Klassen passable Werte annimmt. Diese Erwartung wird bestätigt, zumal 50 % der Unternehmen mindestens einen Reifegrad von 1 (IR<5J) bzw. von 3 (IR>5J) haben.

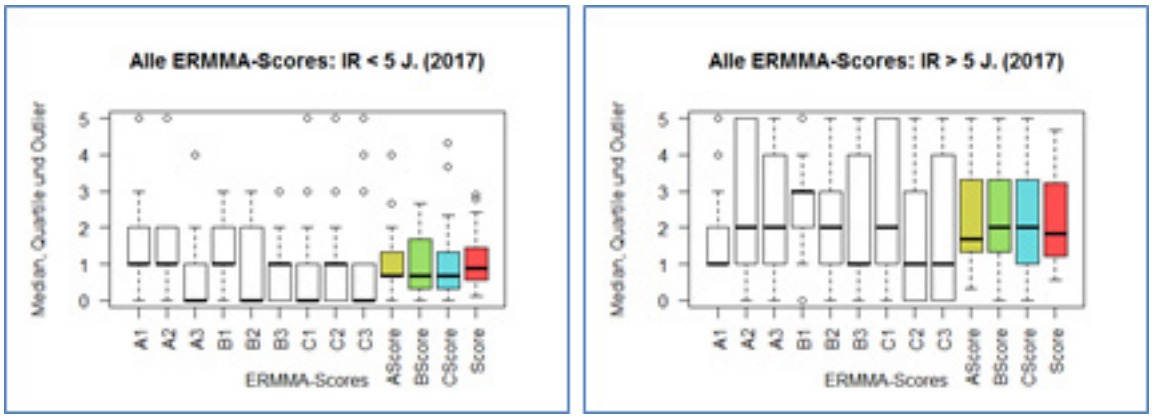



**ABB. 5: ERMMA-PROFIL, DIM- UND GESAMT-SCORE**

Besonders interessant sind aber auch die Sub-Dimensionen bei den IR<5J-Unternehmen, wo der Median den Wert von 0 annimmt. In diesem Fall haben zumindest 50 % der Unternehmen einen Reifegrad von 0. Dies trifft auf 4 Sub-Dimensionen zu, u.z. auf A3 (Risikoorganisation), B2 (RM-Schulungssystem), C1 (strategisches Management) und C3 (Prozess-Management). Diese Bereiche des ERM-Systems betreffen alle drei ERM-Dimensionen und sie stellen die großen Schwachstellen dar, welche bei Abwesenheit einer zumindest 5-jährigen IR-Tätigkeitsdauer, d.h. bei einer niedrigen IR-Qualität zutage treten. Ein Vergleich mit dem rechten Bild in Abb. 5 zeigt, dass diese Schwachstellen bei einer hohen IR-Qualität drastisch verbessert werden. Aus statistischer Sicht sind diese Verbesserungen wieder signifikant.

## 4.3. IR-Tätigkeitsdauer: Einfluss auf Zufriedenheit mit RM-System

Aus dem Datenmaterial der ERMMA-Studie 2017 (?) lassen sich auch noch zwei weitere Unterschiede zwischen den beiden Unternehmensklassen bestimmen.

Der erste Unterschied bezieht sich auf die Zufriedenheit der Eigentümer bzw. Aufsichtsorgane hinsichtlich des Umfanges und der Qualität der Risikoinformationen, welche ihnen zur Entscheidungsfindung durch das RM-System verfügbar gemacht werden. Auf der linken Seite von Abb. 6 ist die Zufriedenheit der Eigentümer bzw. Aufsichtsorgane bei den IR<5J-Unternehmen zu sehen. Die Zufriedenheit wird zumeist mit Gut und Befriedigend eingestuft. Bei den IR>5J-Unternehmen zeigt sich eine deutliche Verbesserung der Zufriedenheit, wo – wie in der rechten Grafik angezeigt – die Zufriedenheit fast ausschließlich mit Sehr gut und Gut eingestuft wird.

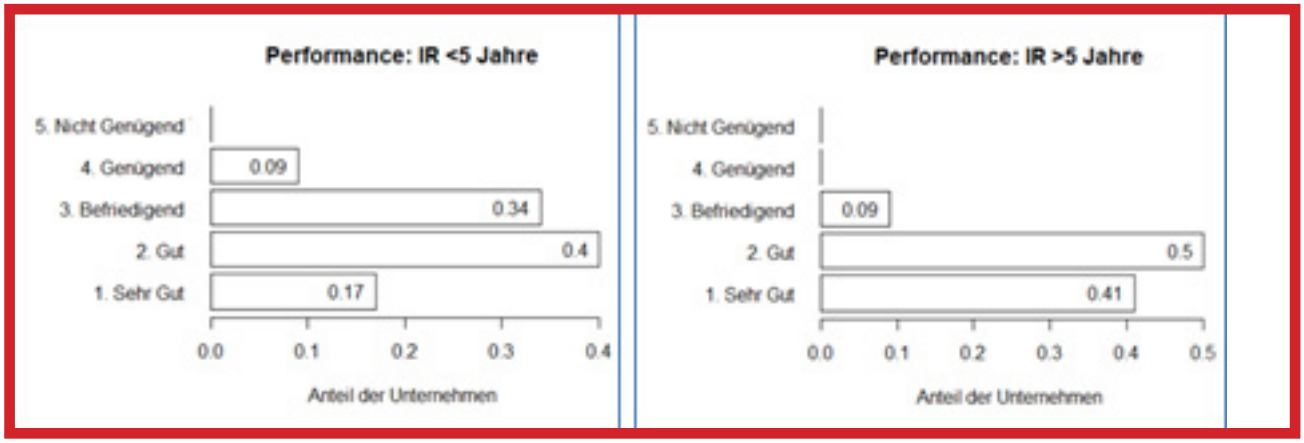



**ABB. 6: EIGENTÜMER/AUFSICHTSORGANE – ZUFRIEDENHEIT MIT RISIKOINFORMATIONEN**

## 4.4. IR-Tätigkeitsdauer: Einfluss auf adressierte Risiken und Chancen

Der zweite Unterschied zwischen den beiden Unternehmensklassen bezieht sich auf die Risiken bzw. Chancen, welche im ERM-System Berücksichtigung finden. Diesbezügliche Unterschiede sind wichtig, zumal sich – wie im in Abb. 1 konzeptionell dargestellten 3-LoD-Modell gezeigt wird – die Planungs- und Steuerungssysteme der verschiedenen Managementebenen auf unterschiedliche Risikotypen ausgelegt sind.

Abb. 7 beinhaltet die auf der strategischen Managementebene berücksichtigten Risiken und Chancen. Ein Vergleich der beiden Grafiken zeigt bei den IR>5J-Unternehmen eine deutlich erhöhte Relevanz jener Risiken, welche über operationale und existenzgefährdende Risiken hinausgehen. Ähnlich ist auch das Bild bei den berücksichtigten Chancen. Dort werden in den IR>5J-Unternehmen operationale Chance sogar weniger häufiger adressiert, wohingegen die Berücksichtigung der anderen Chancen an Bedeutung zunimmt.

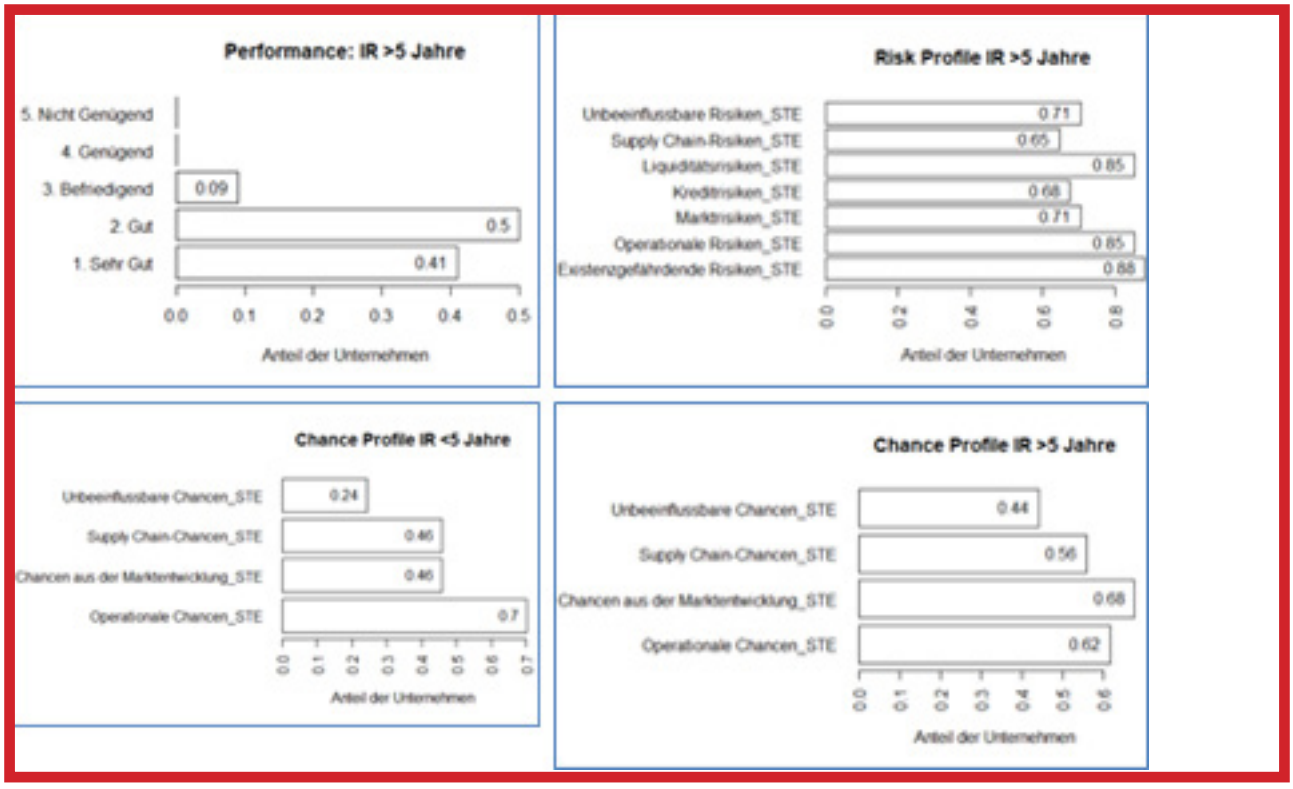



**ABB. 7: STRATEGISCHE EBENE (STE) – BERÜCKSICHTIGTE RISIKEN UND CHANCEN**

## 5. Konklusion und Ausblick

In diesem Beitrag wird erstmals anhand des Datenmaterials der ERMMA-Studie 2017 ein empirischer Befund geliefert, dass die durch die IR-Tätigkeitsdauer gemessene IR-Qualität maßgeblichen Einfluss auf die Qualität (Reifegrad) der in österreichischen Unternehmen implementierten ERM-Systeme hat. Eine langjährige IR-Tätigkeitsdauer sichert somit nicht nur die ERM-System-Qualität, sondern erhöht auch die Zufriedenheit der Eigentümer bzw. Aufsichtsorgane hinsichtlich der Ihnen zur Entscheidungsfindung verfügbar gemachten Risiko- und Chancen-Informationen.

Von großer praktischer Bedeutung sind die in diesem Beitrag aufgezeigten Schwachstellen hinsichtlich der Risikoorganisation, dem Schulungssystem und der Nutzung von Risikoinformationen im strategischen und Prozess-Management, welche durch

eine gute IR-Qualität beseitigt werden. Die Kenntnis des Vorliegens dieser Schwachstellen und deren Beseitigungsmöglichkeiten sollten v.a. für jene Unternehmen interessant sein, welche mit der Konzeptionierung und Implementierung von ERM-Systemen erst am Anfang stehen. Darüber hinaus sollten die insbesondere von den extern geprüften Kapitalgesellschaften gewonnenen Einblicke auch gute Anhaltspunkte für kleinere Unternehmen bieten.

Abschließend sei noch angemerkt, dass die ERMMA-Studie kein einmaliges Unterfangen ist. Vielmehr wird Sie jährlich immer wieder neu durchgeführt. Möglich macht dies die ERMMA-Online-Plattform, welche eine permanente Durchführung der Befragung erlaubt. Seit Beginn des Jahres 2018 ist die kostenlose Teilnahme wieder möglich. Falls Sie bereits im letzten Jahr teilgenommen haben, möchten wir uns dafür an dieser Stelle bedanken und hoffen, dass Sie sich für das ERMMA-Monitoring entscheiden und auch heuer wieder teilnehmen. Falls Sie noch nicht teilgenommen haben und Interesse daran haben, können Sie gerne an der Befragung 2018 teilnehmen. Zu diesem Zweck müssten Sie einfach:

Eine Registrierung auf unserer Homepage http://ermma.imw.tuwien.ac.at durchführen. Dazu benötigen Sie lediglich eine E-Mail Adresse und ein Passwort.

Anschließend wird Ihnen ein automatisch erstellter Benutzernamen an die von Ihnen genannte E-Mail Adresse zugesandt.

Mit Ihrem Benutzernamen und Ihrem Passwort können Sie sich auf unserer Homepage anmelden, die Befragung durchführen und das Ergebnis einsehen.

Für Fragen und Rückmeldungen jeglicher Art steht Ihnen das ERMMA-Team der TU Wien gerne unter ermma@imw.tuwien.ac.at zur Verfügung.

## 6. Literaturverzeichnis

[1] Schwaiger W S A 2017 ERMMA-Studie 2017 – Messung und Analyse der ERM-Reifegrade von österreichischen Unternehmen

[2] Committee of Sponsoring Organizations of the Treadway Commission 2004 Enterprise risk management-integrated framework

[3] The Institute of Internal Auditors 2004 The Role of Internal Auditing in Enterprisewide Risk Management 1–17

[4] The Institute of Internal Auditors 2013 IIA Position Paper : THE THREE LINES OF DEFENSE IN EFFECTIVE RISK MANAGEMENT AND CONTROL 1–7

[5] Mikes A and Kaplan R R S 2013 Towards a Contingency Theory of Enterprise Risk Management Harvard Bus. Sch. 1–47

[6] DIN/ISO (31000) 2011 DIN ISO 31000 Risk Management Standard

[7] Simons R 1995 Levers of Control Harvard Bus. Sch. Press 7–8

[8] Bisbe J, Batista-Foguet J M and Chenhall R 2007 Defining management accounting constructs: A methodological note on the risks of conceptual misspecification Accounting, Organ. Soc. 32 789–820

# Interne Revision und Whistleblowing

**Prof. Mag. Dr. Dr. habil. Peter Hauser**
IIA Certification in Risk Management Assurance (CRMA)
ist Lehrbeauftragter mit dem Schwerpunkt Interne Revision an der University of Applied Sciences FH Campus Wien. Er war Direktor des Konzernbereichs Revision der UNIQA Versicherungsgruppe sowie Vorsitzender des Komitees für Interne Revision und Kontrolle im Verband der Versicherungsunternehmen Österreichs und gehörte mehreren Vorständen und Aufsichtsräten an

## Inhalt

## Stille Beobachterin, Teil des Prozesses, Nutznießerin, Opfer oder Täterin eines an Bedeutung gewinnenden Prozesses.

In jüngster Zeit hat das nicht neue Phänomen „*Whistleblowing*“ an Bekanntheit und Bedeutung gewonnen, wozu auch bekannt gewordenen *Whistleblower*wie *Edward Snowden*,*Bradley/ChelseaManning, Antoine Deltour* ebenso ihren Beitrag geleistet haben, wie die „Enthüllungsplattform“ *WikiLeaks* oder der Anonymus der *Panama Papers.* Öffentliche Normengeber, Verwaltungsorgane und Gerichte auf nationaler und internationaler Ebene sind zwischen dem Bedürfnis der Öffentlichkeit, der Verwaltungen und Organisationen und der Gesellschaft nach Information, Transparenz und Aufdeckung unethischer oder krimineller Machenschaften auf der einen Seite und den Bedürfnissen des Einzelnen sowie der privatwirtschaftlichen Organisationen und öffentlichen Institutionen nach Datenschutz, Schutz der Persönlichkeitsrechte und Schutz von Geschäfts- und Staatsgeheimnissen auf der anderen Seite hin und her gerissen. Der Wunsch sich der Informationen von *Whistleblowern* zu bedienen, besteht für Medien, Parlamentarier, Verwaltungsorgane, Strafverfolgungsbehörden und Organisationsverantwortliche gleichermaßen, woraus Maßnahmen zur Ermunterung und zum Schutz der *Whistleblower* resultieren, die sich beispielweise in Kronzeugenregelungen und sogar Belohnungsprogrammen finden, die allerdings ethisch problematisch anzusehen sind. Das Bedürfnis Vertrauliches vertraulich zu erhalten und die Verpflichtung die Rechte von Beschuldigten und Unbeteiligten zu schützen sowie die Notwendigkeit Staats- und Geschäftsgeheimnisse als solche zu erhalten stehen durchaus in einem Spannungsverhältnis. *Whistleblowing* spielt in und für Organisationen eine immer größere Rolle, gleichgültig ob konkrete Meldesysteme und Prozedere vorhanden oder noch einzurichten sind. Daraus resultiert, dass die Interne Revision zwangsläufig mit diesem Phänomen konfrontiert ist und im Umgang damit verschiedene Rollen übernehmen kann oder zugwiesen bekommt. Sie kann unbeteiligter Dritte oder in den *Whisteblowing* Prozess eingebunden, ja sogar als Anlaufstelle definiert sein. Sie ist nahezu immer in irgendeiner Form Nutznießerin von *Whistleblower* Botschaften, sie kann auch zum Opfer von *Whistleblowing* werden. Letztendlich kann sich für die Interne Revision sogar die Frage stellen, ob eigenes *Whistleblowing* - sei es intern oder extern - eine notwendige und vor allem alternativlose Vorgangsweise in außergewöhnlichen Situationen wäre.

## 1. Einleitung und Definitionen

Einen ersten Eindruck vom Begriff *Whistleblowing* bietet die Übersetzung aus dem Englischen. „To blow the whistle“ kann mit „pfeifen“ übersetzt werden, „to blow the whistle on somebody/something“ mit „über jemandem /etwas auspacken“ oder auch „vor jemandem warnen“ oder letztendlich umgangssprachlich mit „jemandem verpfeifen“.[1] Die Synonyme für „verpfeifen“ können in den Bedeutungsgruppen „ausplaudern, verraten, bespitzeln und anzeigen“ zusammengefasst werden.[2] Beim Gedanken an *Whistleblowing* schwingt somit der Aspekt des Vernaderns, Verpetzens und Ankreidens mit.[3] Diese im allgemei-

[1] Dict.cc Wörterbuch, Deutsch – Englisch Übersetzung für to blow the whistle, 2002 – 2017, Paul Hemetsberger, https://www,dicr.cc/englisch-deutsch/to+blow+the+whistle.html download 08.12.2017

[2] Vgl.Wokikon/Synonyme/Deutsch/V/verpfeifen,http://synonyme.woxikon.de/synonyme/verpfeifen/php,download 03.12.2017

[3] Vgl. Mertinz Anna, Whistleblowing Österreich – Arbeitsrecht und Datenschutz, Fachartikel 27,04.2015, https://www.hrweb.at/2015/04/whistleblowing downlooad 04.12.2017

nen Sprachgebrauch durchaus nachvollziehbare negative Komponente findet sich auch in Zitaten mehr oder weniger Prominenter. Äsop (lat. Aesopus, eingedeutscht Aesop), antiker griechischer Dichter aus dem 6. Jhd. v. Chr, schreibt; „Den Verrat benutzt man wohl, aber den Verräter liebt man trotzdem nicht."[4] Von *Julius Caesar*, römischer Imperator rund 58 v. Chr. stammt der Satz „ich liebe den Verrat, aber den Verräter liebe ich nicht."[5] Ausgesprochen deftig fällt die Formulierung des deutschen Germanisten und Universitätsprofessors *August Heinrich Hoffmann von Fallersleben*(1798 – 1847) aus der meint; „Der größte Lump im ganzen Land ist und bleibt der Denunziant".[6] In diesen Zitaten schwingt auch die aus der Sicht des Verfassers nachvollziehbare Sorge mit, dass eine Person, die einmal zum Verräter wurde oder zumindest Interna ausgeplaudert hat, dieses Verhalten wiederholen könnte und sich die Indiskretion diesmal gegen den Autor richten könnte. In einer vom Verfasser durchgeführten Untersuchung im Jahr 2007 in der österreichischen Versicherungswirtschaft[8], die sich in erster Linie mit Interner Revision, aber auch *Whistleblowing* befasst hatordneten die Teilnehmer *Whistleblowern* folgende Eigenschaften zu. 86,7% "korrekt", 83,8 % „verantwortungsbewusst, 82,2 % „mutig", 47,5 % „sendungsbewusst", 39,7 % „geltungssüchtig", 37,5% „gefährlich", 27,5% „rachsüchtig" und 27,4 % „entbehrlich" (27,4%)[9] Aus der wörtlichen Übersetzung mit „die Pfeife blasen" oder „Alarm schlagen" kann auch bildhaft der Schiedsrichter oder der Polizist abgeleitet werden, der in seine Pfeife bläst um eine unerlaubte Tätigkeit anzuzeigen.[10] Die US-amerikanischen *Whistleblowing* Forscherinnen *Marcia Miceli* und *Janet Near* verweisen darauf, dass Arbeitnehmer die „*organizational wrongdoing*" (*illegal, imoral and ilegitimate practices*) bekannt gemacht haben, oftmals für „*news*" in den Medien sorgten. In den Jahren zwischen 1989 und 1995 haben 35 bedeutende Zeitungen über 1.000 Artikel über die Aufdeckung von Fehlverhalten in Organisationen veröffentlicht und seither ist die Zahl bedeutend gestiegen. Sie verweisen darauf, dass ungeheure Kosten durch Fehlverhalten in den Organisationen entstanden sind, nach einer Schätzung der Weltbank aus 2004[11] als Folge von Korruption 1 Trillion USD.[12]

In diesem Beitrag wird über verschiedene Formen von *Whistelblowing* und verschiedene *Whistleblower* berichtet, die den Kriterien der Begriffsdefinitionen mehr oder weniger entsprechen. Manche können eher unter den Begriff der Aufdecker oder Informanten eingeordnet werden, einige sind Personen, die einfach ihre Pflicht erfüllt haben und als Verräter behandelt wurden, wie dies bei *Andreas Georgiou* der Fall ist. Es ist allgemein bekannt, dass sich Griechenland den Eintritt in den Euro schlicht mit falschen Zahlen erschlichen hat.[13] *Georgiou*, ein Grieche, der in Amerika eine tadellose Karriere absolviert hatte, wurde auf Drängen des *IMF (International Monitary Fund)* mitten in der Wirtschaftskrise 2010 mit dem Aufbau eines effizienten und unabhängigen Statistikamtes in Griechenland *(Elstat*) beauftragt und er kam dieser Aufgabe hervorragend nach. Das gefälscht dargestellte Staatsdefizit wurde unter seiner Leitung auf den wahren – höheren - Wert korrigiert und veröffentlicht. Nicht jene, die die gefälschten Daten erzeugt hatten und das eigene Land und die europäische Gemeinschaft belogen hatten, sondern *Georgiou* wird von der griechischen Regierung und Justiz unerbittlich und zu Unrecht verfolgt. Auffällig ist, dass die europäischen Institutionen dazu schweigen, obwohl sie in ihrer Verpflichtung den europäischen Steuerzahlern gegenüber alles Erdenkliche tun

[4] Vgl. https://de.wikipedia.org/wiki/Äsop, download 03.12.2017

[5] Caesar Gaius Julius, De Bello Gallico, zitiert in www.aphorismen ,de /zitat/150829 download 03.12.2017

[6] https://www.zitate.eu/autor/hoffmann-von-fallersleben-heinrich/zitate download 03.12.2017

[7] Es wurden alle Mitglieder der Vorstände und Aufsichtsräte, Prokuristen und MitarbeiterInnen der Internen Revision aller österreichischer Versicherungsunternehmen, die Geschäftsführer derer Tochtergesellschaften, sowie die Wirtschaftprüfer und Prüfungsassistenten die Versicherungsbilanzen testierten angeschrieben insgesamt 1.276 Personen. Die Rücklaufquote betrug 21,4%.

[8] Hauser Peter, Die Stellung der Internen Revision in der österreichischen Versicherungswirtschaft und ihre Zukunftstendenzen einschließlich der Rolle im Whistleblowingprozess, Institut für Interne Revision Österreich – IIA Austria, Wien 2008 S 92 ff

[9] Hauser s. FN 82008 S 149

[10] Vgl. Mertinz 2015 s.FN 3

[11] World Bank 2004, The costs of corruption, web.worldbank.org

[12] Vgl. Miceli Marcia P./ Near Janet P./ Dworking Terry Morehead, Whistleblowing in Organizations, Routeledge New York2008 S 1 ff

[13] Vgl. Buchter Heide / Lisa Nienhaus, Andreas Georgiou: War dieser Mann zu ehrlich ? Zeit online, 8. August 2017, www.zeit.de/2017/33

müssten um die Statistiktricksereien von Staaten, die umfangreiche Zuwendungen zur Rettung ihrer Staatsfinanzen von diesen Steuerzahlern erhalten, hintanzuhalten und all jene zu unterstützen und schützen, die die Wahrheit offenbaren. *Josef Urschitz* bezeichnet dieses Schweigen der europäischen Institutionen als europäischen „Justizskandal".[14] In Anbetracht der Rolle, die der derzeitige Kommissionspräsident im *LuxiLeaks* Skandal gespielt hat, ist dieses Verhalten nicht wirklich überraschend, lassen sich die europäischen Werte im Falle der Unabsetzbarkeit eines polnischen Bezirksrichters bedeutend überzeugender vertreten.

Eine gängige Definition von *Whistleblowing* stammt von *Near/Miceli* aus dem Jahre 1985. *Whistleblowing* ist die Aufdeckung von ungesetzlichem *(illegal),* unmoralischem *(immoral*) oder unrechtmäßigem Verhalten (*illegimate practices*) unter der Verantwortung (*control*) ihres Arbeitgebers durch derzeitige oder ehemalige Mitglieder der Organisation an Personen oder Institutionen, die in der Lage sein könnten Maßnahmen zu setzen (*effect actions*).[15] „*Transparency International*" hat diese Definition dahingehend ausgeweitet, dass *Whistleblowing* als die Aufdeckung von Informationen über wahrgenommenes oder befürchtetes *(risk of wrongdoing)* Fehlverhalten in Organisationen gegenüber Personen oder Einrichtungen, von denen angenommen wird, dass sie Maßnahmen setzen können, zu sehen ist.[16] Diese erweiterte Definition beschränkt sich nicht nur auf ehemalige oder derzeitige Arbeitnehmer der Organisation (des Unternehmens), sondern bezieht alle Personen ein, die in der Lage sind oder sein können Fehlverhalten oder das Risiko für die Organisation aufzuzeigen. Nach dem „*Chartered Institute of Internal Auditors*"[17] liegt *Whistleblowing* dann vor, wenn sich ein Arbeitnehmer, ein Vertragspartner oder ein Lieferant außerhalb der üblichen Managementinformationskanäle begibt um vermutetes Fehlverhalten bei der Arbeit zu melden und die Meldung vertraulich erfolgt.[18] *Bendel* führt aus, dass beim Whistleblowing Hinweise auf Missstände in Unternehmen, Hochschulen, Verwaltungen etc. gegeben werden, wobei ein Whistleblower meist ein etablierter oder ehemaliger Mitarbeiter oder Kunde ist, der aus eigener Erfahrung berichtet und Mittler, Medien oder die Öffentlichkeit informiert und dabei Stelle, Karriere oder Ruf riskiert beziehungsweise mit Disziplinarmaßnahmen rechnen muss, was eine Beziehung zu Zivilcourage darstellt.[19] In der Untersuchung des Verfassers aus 2007, wurde folgender Ansatz gewählt: „Wenn ein Mitarbeiter eines Unternehmens oder einer sonstigen Organisation in seinem beruflichen Umfeld gesetzwidriges, ordnungswidriges oder unethisches Verhalten entdeckt oder zumindest glaubhaft vermutet und darüber eine Autoritätsinstanz informiert, spricht man von *Whistleblowing*".[20]

Unter *internem Whistleblowing* wird das Aufzeigen von Missständen innerhalb des Unternehmens verstanden, *externes Whistleblowing* ist das Herantreten an externe Adressaten außerhalb des Unternehmens beziehungsweise das Herantreten an die Öffentlichkeit.[21] In der zitierten Untersuchung aus 2007 wurden folgende Anlaufstellen als „ausnahmslos möglich" oder „zusätzlich möglich" gewertet. Die Anlaufstellen des *internen Whistleblowings* führten eindeutig die Reihung an. 84,2% unmittelbarer Vorgesetzter, 74,7% nächsthöherer Vorgesetzter, 67,8% Interne Revision, 63,7% zuständiges Vorstandsmitglied und 50,4% Vorstandsvorsitzender. Als Zwischenstufe zwischen i*nternem* und *externem Whistleblowing* wurden der Betriebsrat (31,8%) und der Vorsitzende des Auf-

[14] Vgl Urschitz Josef, Wenn Justizia die Wahrheit blind verfolgt, Economist, Die Presse Wien 29.Dezember 2017 S 15

[15] Vgl. Near Janet P., Miceli Marcia P., Organizational dissidence: The case of whistleblowing in: Journal of Business Ethics 4 / 1985, Springer Wien/New York S 1 – 16

[16] Transparency International, Recommended draft principles for whistleblowing legislation, 2009, www.tranperency.org

[17] Das „Chartered Institute of Internal Auditors" ist nach eigenen Angaben die einzige Berufsvereinigung von Internen Revisoren im United Kingdom of Great Britain and Northern Ireland, Chartered Institute of Internal Auditors, about the Chartered Institute of Internal Auditors, https://www.iia.org.uk/about-us

[18] Vgl. Chartered Institute of Internal Auditors, Position Paper: Internal Audit and Whistleblowing, Policy Paper in format of a briefing document, What do we mean by whistleblowing, 6 July 2017https://www.iia.org.uk/resources/ethics-values-and-culture/whistleblowing

[19] Vgl. Bendel Oliver, Whistleblowing in Gabler Wirtschaftslexikon, http://wirtschaftslexikon.gabler.de/definition/whistleblowing.htmldownload 02.12.2017

[20] Hauser 2008 s. FN 8 S 133

[21] Vgl. Aschauer Paula, Whistleblowing im Arbeitsrecht, Linde Wien, 2012 S 34

sichtsrates (20,9%) angesehen. Deutlich geringere Zustimmung fand *externes Whistleblowing.* 12,6% Wirtschaftsprüfer, 7,6% Aufsichtsbehörde und Öffentlichkeit 3,5%. Nur in Ausnahmefällen können sich 29,1% eine Information des Wirtschaftsprüfers, 9,8% der Aufsichtsbehörde und nur 3,3% der Öffentlichkeit vorstellen.[22] In der Untersuchung wurde auch abgefragt welche Eigenschaften *Whistleblowern* zugeordnet werden. 86,7% „korrekt", 83,6% „verantwortungsbewusst", 82,2% „mutig", 47,5% „sendungsbewusst", 39,7% „geltungssüchtig", 37,5% „gefährlich", 27.5% „rachsüchtig" und immerhin 24,4 5% sahen Whistleblower als „entbehrlich" an.[23]

## 2. Beispiele für Whistleblowing

*Whistleblowing* ist ein uraltes Phänomen, das, wenn auch nicht unter dieser Bezeichnung, bis in die griechische Mythologie verfolgbar ist wie die Fabel vom schönen weißen Vogel und dem Gott *Apollo* beweist. Die von *Apollo* mit *Aselepius* schwangere, je nach Darstellung Königstochter oder Elfe *Coronis*, betrog *Apollo* während seiner Abwesenheit. Ein schöner weißer Singvogel (ein Rabe), der an sich auf *Coronis* achten sollte verhinderte diesen Seitensprung nicht, berichtete aber Apollo nach dessen Rückkehr. Dieser ließ die Ungetreue durch seine Schwester *Artemis* töten und das Ungeborene durch *Hermes* aus dem Mutterleib schneiden. Den Raben verwandelte er in ein krächzendes schwarzes Geschöpf.[24] *Martin Luther* kann als historisch bedeutender *externer Whistleblower* angesehen werden. Er war Insider der Kirche (Augustiner Mönch) und kritisierte ein Fehlverhalten innerhalb seiner Organisation (Ablasshandel) gegenüber der Öffentlichkeit. Der Überlieferung nach veröffentlichte er vor etwa 500 Jahren seine 95 Thesen durch Anschlag an der Schlosskirche zu Wittenberg. Die Veröffentlichung leitete er mit den Worten „aus Liebe zur Wahrheit und im Bestreben diese zu ergründen soll in Wittenberg unter Vorsitz des ehrwürdigen Vaters Martin Luther über die folgenden Sätze diskutiert werden". Diese Thesen enthalten durchaus starken Tobak, etwa heißt es in der These 42: „Auf Grund eines Ablassbriefes das Heil zu erwarten ist eitel, auch wenn der Ablass - Kommissär ja selbst der Papst selbst ihre Seelen dafür verpfänden". These 21 führt aus: "Deshalb irren jene Ablassprediger die sagen, dass durch Ablässe des Pabstes die Menschen von jeder Strafe frei und los seien."

Zu Beginn dieses Jahrtausends wurden drei Frauen zu *Whistleblowern* und vom *Time Magazine* zu „*Persons of the Year 2002*" gewählt.[25] *Sherron Watkins* informierte die Unternehmensleitung von *ENRON* über „*malpractice*" in der Buchhaltung, *Coleen Rowley* deckte Fehlverhalten des FBI im Vorfeld von 9/11 gegenüber dem FBI Direktor auf und *Cynthia Cooper* wurde als Leiterin der Internen Revision von WorldCom zur *Whstleblowerin*.[26] Bemerkenswerter ist die Geschichte von Kathryn Bolkovac.[27] Die ehemalige Polizistin aus Nebraska arbeitete bei der „*International Police Task Force" (IPTF)* in Bosnien. Die Beteiligung der USA an dieser internationalen Polizeitruppe unter der Aufsicht der UNO, war an die das private Sicherheitsunternehmen *DynCorp* ausgelagert, das Mitarbeiter nach dem Vertragsrecht Großbritanniens anstellte. Bolkovac entdeckte, dass Mitarbeiter der IPTF am internationalem Mädchenhandel beteiligt waren. Sie informierte die Vorgesetzten in UNO, IPTF und DynCorp, die nicht nur nichts unternahmen sondern sie aus fadenscheinigen Gründen entfernten. Sie klagte DynCorp nach dem UK

[22] Vgl Hauser 2008 s. FN 8 S 252

[23] Vgl. Hauser 2008 s. FN 8 S 149

[24] Vgl. Raven Vincent, Mythologie des Raben, www.vincent.raven.ch/index.php?id=7

[25] Lacayo Richard, Ripley Amanda, Persons of the Year 2002, The Whistleblowers, Time Magazine, December 30, 2002, www.time.com

[26] Siehe Abschnit 6.7.

[27] Vgl. Bolkovac Kathryn, Lynn Cari, The Whistleblower. Sex trafficking, military contractors and one woman's fight for justice, Mac Millan Edition New York 2011

[28] Parliament of the United Kingdom: An Act to protect individuals who make certain disclosures of information in the public interest, to allow such individuals to bring action in respect of victimisation; and for connected purposes, chapter c 23 July 2 nd 1998, in force July 2nd1999, Public Interest Disclosure Act - PIDA

„*Public Interest Disclosure Act*“ *(PIDA)*[28] und bekam auch Recht und eine Entschädigung zugesprochen.[29]

Am 13.11.1974, etwa ein Monat bevor *Bradley* (später *Chelsea) Manning* in *Cresent, Ohio* geboren wurde, starb dort *Karen Silkwood* bei einem Verkehrsunfall, der bis heute nicht aufgeklärt ist. Sie war zu einem Treffen mit einem Journalisten der *New York Times* unterwegs um ihm eine Mappe mit Unterlagen zu übergeben, die die von ihr davor erhobenen Anschuldigungen gegen *Kerr Mc Gee*, jenem Unternehmen, das in *Cresent* das Werk *Cimaron* betrieb, untermauern sollten. Diese Mappe wurde nach dem tödlichen Unfall nie mehr gefunden.[30] Im Werk *Cimaron* wurden Plutonium enthaltende Brennstäbe für Atomreaktoren hergestellt. *Silkwood,* die Laborantin und Vertreterin der Belegschaft war, hatte gegenüber der US - amerikanischen Atombehörde und dem Dachverband der Gewerkschaften darauf hingewiesen, dass in diesem Werk Sicherheitsvorschriften nicht eingehalten würden und eine Gefährdung der Belegschaft gegeben wäre. Kurz vor ihrem Tod stellte sich heraus, dass sie selbst verstrahlt war. Der Fabrikbetreiber beschuldigte sie auch nach ihrem Tod noch, Plutonium gestohlen zu haben und daher an der Verstrahlung selbst Schuld zu sein. Ihr Vater klagte *Kerr Mc Gee* sowohl auf Schadenersatz für seine tote Tochter als auch auf Widerruf der Rufschädigung und bekam von einem Gericht in Oklahoma US$ 10 Mio. zugesprochen. Ein Urteil das vom *Court of Appeals of the 10th Circuite of West Oklahoma* aufgehoben wurde. Dieses aufhebende Urteil wurde dann in letzter Instanz vom *US Supreme Court* seinerseits aufgehoben.[31] Es darf angenommen werden, dass *Manning* die Geschichte von *Silkwood* kannte, ist er doch in *Cresent* aufgewachsen, wo sie damals allgegenwärtig war. Er wurde in der Schule, wahrscheinlich auch wegen seiner homosexuellen Neigungen, gemobbt und brachte sein Leben nicht wirklich auf die Reihe. Auf Anraten des Vaters trat er in die *US Army* ein, um zu einem College Abschluss zu kommen. Da er Computerkenntnisse hatte, wurde er zum Nachrichtenanalytiker ausgebildet und im Irak eingesetzt. Trotz seines niedrigen Ranges eines vergleichbaren Stabsgefreiten erlangte er Zugang zu zwei streng geheimen Nachrichtensystemen der US Regierung. Eines war das weitgehend vom Verteidigungsministerium genutzte *Secret Internet Protocol Router Network (SIPRN)* und das andere häufig vom Außenministerium zur Übermittlung vertraulicher Nachrichten genutzte *Joint Worldwide Intelligence System Network (JWISN).* Zur generellen Datensicherheit beider Netze sind Zweifel durchaus angebracht, waren im Jahr 2010 auf SIPRN 2,5 Mio. Personen zugriffsberechtigt und auf WISN immerhin noch 850.000. Bei der Einsicht in die vertraulichen Daten dieser Netzwerke war *Manning* über die Durchlässigkeit der Netzte entsetzt, wurde aber von seinen Vorgesetzten nicht ernst genommen.[32] *Manning* kam mit *Julian Assange* in Kontakt, der in *WIKILeaks* u.a. ein von *Manning* zugespieltes Video über einen US Luftangriff auf Zivilisten oder geheime Korrespondenz von US Botschaften mit dem *State Department* veröffentlichte. *Manning* wurde wahrscheinlich von einem Hacker namens *Adrian Lamo*, der sich das Vertrauen *Mannings* verschafft hatte, verraten, verhaftet und zu 35 Jahren Haft verurteilt. In der Haft machte er eine Geschlechtsumwandlung mit und wurde zu *Chelsea Manning.* Sie wurde vom scheidenden US Präsidenten *Obama* begnadigt und 2017 nach 7 Jahren auf freien Fuß gesetzt. *Manning* hatte in *WIKILeaks* eine Plattform gefunden mit deren Hilfe anonym vertrauliche Dokumente ins Netz gestellt werden konnten. Der Begriff *WIKILeaks* verbindet das hawaianische „wiki = schnell“ mit dem englischen „leak=leck,undicht“. Es ist eine Enthüllungsplattform, auf der Dokumente anonym veröffentlicht werden, die durch Geheimhaltung, Verschlusssache, Vertraulichkeit oder Zensur in ihrer Zugänglichkeit beschränkt sind. Der Domänenname wurde von *John Young* 2006 registriert, der seit 1996 eine *website* mit ähnlicher Zielsetzung betrieben hat. *Julian Assange* stieg in das Projekt mit seiner Gruppe ein und *Young* bald aus. Es hat eine Weile gedauert bis *WIKILeaks* richtig durchstartete. und sich weiterentwickelte. Es sieht sich als eine Seite im Internet,

[29] Vgl. Employment Tribunal South Hampton, Bolkovac v DynCorp Aerospace Operations UK, ET, Case No 3102729/01 in Bowers John et al, Whistleblowing. Law and Practice, Oxford/New York 2007 Appendix 9 548 f

[30] Gorig Karsten / Nord Kathrin, Julian Assange. Der Mann der die Welt verändert, Scorpio Verlag, Berlin München 2011

[31] Richardson Anette, Karen Silkwood, Encyclopedia Britannica, https://britannica.com

[32] Vgl. Hardig Luke / Wigh David, WIKI Leaks. Julian Assanges Krieg gegen Geheimhaltung,1. Auflage, Edition Weltkiosk, London / Berlin 2013 S 30f

die unangreifbar und trotzdem für alle zugänglich ist. Laut eigenen Angaben ist *WIKILeaks* von „Dissidenten, Spezialisten und Mathematikern" aus den USA, Europa, Taiwan, Australien und Südafrika geschaffen worden. Es ist aber neben *Assange* nur noch der Name *Daniel Domscheit-Berg* bekannt geworden, der jahrelang Sprecher von WIKILeaks war und der sich von *Assange* mittlerweile getrennt hat.[33] *Julian Assange* wurde in Australien geboren und im Hacker - Untergrund von Melbourne bekannt. Die Melbourne Hacker wurden bekannt, als sie einen Computerwurm in der website der *NASA,* der US Raumfahrtbehörde, setzten. 1994 ließ die Polizei von Melbourne die Gruppe auffliegen und *Assange* wurde verurteilt.[34] 2010 wurde *Assange* von zwei Frauen in Schweden der Vergewaltigung bezichtigt und flüchtete in die Botschaft von *Ecuador* in London, wo er sich noch immer aufhält, obwohl das Verfahren in Schweden eingestellt wurde. Er fürchtet die Verhaftung und Auslieferung an die USA, wo er wegen des Verrats von Staatsgeheimnissen gesucht wird.

*Eward Snowden* ist einer der bekanntesten *Whistleblower* unserer Zeit. Er wurde 1983 in North Carolina USA geboren. Bis 2013 arbeitete er für das Beratungsunternehmen *Boz Allen Hamilton,* das im *Kunia Regional SIGINT (Signals Intelligence) Operations Center* für die die NSA (National Security Agency) tätig war, Er bekam Zugang zu streng vertraulichen Informationen, u.a. zu US amerikanischen Programmen zur Überwachung der weltweiten Internetkontakte wie *PRISM* (Prisma) und zum britischen *(Tempora),* Codename eines geheimen Projektes von *GCQ (Government Communicaton Headquaters)* zur Überwachung von internationaler Telekommunikation und Internetkommunikation.[35] Im Dezember 2012 nahm *Snowden* unter dem Pseudonym „Cincinatus"[36] Kontakt zu dem Journalisten des *Guardian Glenn Greenwald* und zur Filmemacherin *Laura Poitras* auf. Snowden übermittelte seine Botschaften unter Verwendung des Verschlüssellungsprogramm *PCP (Pretty Good Privacy)*. Die angebotenen Dokumente, die sich mit PRISM (deutsch Prisma) befassten, das es der NSA ermöglicht privat Kommunikationsdaten von den großen Internetkonzernen wie Facebook, Yahoo, Google und Skype abzurufen, war von Snowden schon davor der *Washington Post* angeboten worden, die sich nach umfangreicher rechtlicher Prüfung schlussendlich nicht zur Veröffentlichung entschließen konnte. Bei einem Treffen von *Greenwald* und *Poitras* mit *Snowden* in Hongkong, wohin er zu diesem Zeitpunkt bereits geflüchtet war, erklärte er sein Motiv als den Wunsch die Öffentlichkeit darüber zu informieren, „was in ihrem Namen getan und gegen sie eingesetzt wird."[37] Im Jahr 2013 haben *Greenwald* und *Poitras* einen Teil dieser Informationen ohne Angabe der Quelle veröffentlicht. *Snowden* selbst outete sich von Hongkong aus. Das FBI eröffnete ein Verfahren und es erging ein Haftbefehl. *Snowden* flog nach Moskau und verbrachte einige Zeit auf dem dortigen internationalen Flughafen, ehe er provisorisch Asyl erhielt und nunmehr über eine befristete Aufenthaltsgenehmigung für Russland verfügt.

*Luxemburg Leaks (LuxLeaks*) ist ein Finanzskandal aus Ende 2014. In zwei Phasen wurden 548 Dokumente mit einem Umfang von 28.000 Seiten öffentlich gemacht. Es handelte sich dabei um verbindliche Vorbescheide (Advance Tax Rulings) der luxemburgischen Steuerbehörde. Die Affäre ist von besonderer Brisanz, weil Jean Paul Junker in Luxemburg zu dieser Zeit Regierungschef und Finanzminister war. Die Behauptung, es habe sich um legale Vorgangsweisen gehandelt ist noch nicht widerlegt, die moralische Seite der Angelegenheit sollte aber keineswegs abgetan sein. Es ist unbestritten, dass „LuxLeaks" nicht zur Glaubwürdigkeit und Vertrauenswürdigkeit der Europäischen Kommission und ihres Präsidenten beiträgt.[38] Dass „LuxLeaks" an die Öffent-

[33] Gorig /Nord s. FN 30 S 47 f

[34] Gorig / Nord s.FN 30 S 32 ff

[35] Vgl. o.V: Edward Snowden, Wikipedia, http://de.wikipedia.org/wiki/Edward.snoden

[36] *Cincinatus* war ein Bauer der im 5. Jhd. in Rom zu Diktator bestellt wurde um die Stadt zu verteidigen. Nach seinem Sieg legte er sein Amt unverzüglich und freiwillig zurück. Er gilt seither als Symbol für den Einsatz politischer Macht des Einzelnen ausschließlich im Sinne des Gemeinwohls und für die Beschränkung der politischen Macht des Einzelnen zugunsten der Allgemeinheit

[37] Vgl. Greenwald Glenn, Die globale Überwachung, Droemer Verlag, München 2014 S 17 - 54

[38] Vgl. Mussler Werner, Neue Vorwürfe gegen Juncker wegen Luxemburger Zeit, Frankfurter Allgemeine, Wirtschaft, 2.1.2017, http://www.faz.net/aktuell/wirtschaft/wirtschaftspolitik/luxleaks

lichkeit gelangte, ist *Antoine Deltour* zu verdanken. Er wurde 1985 in Frankreich geboren und arbeitete bei Price Waterhouse Coopers (PWC) in Luxemburg. Dazu ist zu bemerken, dass *„the big four"*, das sind die weltweit größten Wirtschaftsprüfungsgesellschaften (PWC, Ernst & Young, KPMG und Deloite), in Luxemburg zu den größten Arbeitgebern zählen. Laut einer OECD Studie sind in Luxemburg mehr als 3.000 Investmentfonds beheimatet, die ein Vermöge von 3 Bio € managen. *Deltour* stieß bei seiner Arbeit darauf, dass die untersuchten Unternehmen keine Steuern bezahlten. Er ließ sich von den PWC Kollegen des Steuerbereichs über besondere Tricks aus Luxemburg aufklären. Einer der Tricks ist der „Kredittrick." Demnach gründet ein Unternehmen aus einem anderen Land in Luxemburg eine Tochterfirma und nimmt bei ihr ein Darlehen auf. Dafür zahlt es Zinsen nach Luxemburg, die von der Steuer im eigenen Land absetzbar sind und den Gewinn reduzieren bis marginalisieren, in Luxemburg allerdings auf Grund nationaler Gesetzgebung nahezu nicht besteuert werden. *Deltour* stellte fest, dass die meisten der von ihm geprüften Firmen Briefkastenfirmen waren, deren Gründung einfach war und auf deren Gründung sich lokale Firmen spezialisiert hatten und die die auch die Firmenadressen zur Verfügung stellten, an einem Standort waren mehr als 1.000 internationale Konzerne registriert. *Deltour* kamen immer größere moralische Zweifel und er entfernte sich immer mehr von seinem Arbeitgeber. Er kam mit dem französischen Journalisten *Edouard Perrin* vom Fernsehsender *France 2* in Kontakt und übergab ihm die Unterlagen mit der Auflage, die Namen seiner Klienten nicht zu nennen. *Perrin* brachte 2012 eine Reportage auf France 2, doch die Sendung blieb vorerst ohne Folgen. 2014 publizierte ein in Washington DC ansässiges Journalistenkonsortium namens *„International Consortium of Investigative Journalists (ICIJ)"* die Story nochmals und löste ein internationales Erdbeben aus. Weder ein Untersuchungsausschuss des Europäischen Parlaments ergab Wesentliches noch sind die mühevollen Gespräche über Harmonisierungen im europäischen Steuerrecht bisher wirklich erfolgreich gewesen.[39] *Deltour* verlor seinen Job und wurde 2016 von einem Gericht in Luxemburg zu einer moderaten Strafe mit 9 Monaten auf Bewährung und einer Geldbuße von € 1.500 verurteilt. Der Journalist *Perrin* wurde freigesprochen. Das Urteil löste allgemeine Empörung in Europa aus.[40]

Mit der Kontaktaufnahme eines anonymen Informanten, der sich *„John Doe"*nannte mit der Süddeutschen Zeitung (SZ) begann die Aufdeckung eines weltweiten Skandals. John Doe[42] stellte Dokumente der in Panama situierten Anwaltskanzlei *Mossack – Fontensa* zur Verfügung, die die Verwicklung prominenter Personen aus Politik, Wirtschaft, Kunst und Sport in milliardenschweren Steuerbetrug bewiesen. Diese Dokumente wurden als *Panama Papers* bekannt.[42] Die Reporter der SZ arbeiteten gemeinsam mit dem bereits bekannten *International Consortium of Investigative Journalists (ICIJ)* an der Aufarbeitung und Veröffentlichung der Unterlagen. Das *ICIJ* wurde mit dem Pullitzerpreis ausgezeichnet, der Skandal kostete etwa dem isländischen Premierminister den Job. Am 6. Mai 2016 wandte sich *John Doe* im Wege der SZ wieder an die Öffentlichkeit.[43] Er stellt klar, dass er weder für eine Regierung noch für einen Geheimdienst arbeitet. Er begrüßt es, dass die Veröffentlichung der Panama Papers eine weltweite Debatte ausgelöst hat, die Anlass zur Hoffnung gibt, dass „die Höflichkeitsrhetorik der vergangenen Jahre, die das Fehlverhalten der Reichen und Mächtigen sorgsam ausgeklammert hatte", endgültig vorbei sei. Die aktuelle Medienberichterstattung sei allerdings darauf konzentriert darauf zu verweisen „was skandalöserweise innerhalb des Systems legal und erlaubt ist. Die Panama Papers könnten tausende Anzeigen nach sich ziehen. *ICIJ* und *SZ* haben sich geweigert

[39] Vgl. Szietvari Andras, Whistleblower Deltour: Der Preis der Wahrheit, derStandard.at, 3.Jänner 2016, http://derstandardat/2000028347186/Whistleblower-Antoine-Detour

[40] Vgl. Szietvari Andras, Schuldspruch für Lux-Leaks - Whistleblower, derstandard.at 29. Juni 2016, http://derstandard.at/2000040078966/Bewaehrungsstrafen-gegen-zwei-whistleblower

[41] John Doe ist ein englischer Platzname für eine fiktive oder nicht identifizierte Person

[42] Vgl. Obermayer Bastian / Obermayer Frederik, Panama Papers. Die >geschichte einer weltweiten Enthüllung, Kopenhauer & Witsch, Köln 1. Aufl. 2016 S 17 ff

[43] SZ.de/Politik/Panama Papers/Um eines klarzustellen: Ich arbeite nicht für irgendeine Regierung oder irgendeinen Geheimdienst

die Dokumente an Ermittlungsbehörden weiterzugeben,[44] was *Joe Doe* zwar grundsätzlich verständlich findet, er selbst habe sich aber zur Zusammenarbeit mit den Behörden bereit erklärt. Er fordert von der EU Kommission, dem US Kongress und auch vom UK Parlament mehr Whistleblowerschutz und die Aufhebung des Bankgeheimnisses in den britischen Überseegebieten. Er schließt seinen Apell mit der Behauptung, dass „solange gewählte Politiker gerade diejenigen um Geld bitten, die im Vergleich zu anderen Bevölkerungsschichten das größte Interesse haben Steuern zu vermeiden, kann die Steuerhinterziehung unmöglich ernsthaft angegangen werden".

# 3. Europäische und internationale Entwicklungen

Mit dem *Sarbanes Oxley Act (SOX) 2002* [45] wurde u.a. ein neues Kapitel des vermeintlich effektiven *Whistleblower* Schutzes und des *Whistleblower* Prozedere (*Whistleblower* Hotline) eröffnet, der im *Dodd Frank Wallstreet Reform Act 2010* [46] in Richtung von *Whistleblower* Prämien ausgeweitet wurde. Der *UK Public Interrest Disclosure Act PIDA* kann noch heute als Vorbild für *Whistleblower* Schutz herangezogen werden. In Europa herrscht eine gewisse Skepsis in Richtung des Datenschutzes und des Schutzes der Rechte der durch Whistleblowing angeschwärzten oder auch „verpfiffenen" Personen. Neuere Initiativen der Vereinten Nationen, der Parlamentarischen Versammlung des Europarates, des Europäischen Parlaments oder der Europäischen Kommission haben im Zusammenhang mit einer bemerkenswerten jüngeren Rechtssprechung des Europäischen Gerichtshofes für Menschenrechte eine neue Diskussion zu diesem Thema eingeleitet.

## 3.1. UK Public Interest Disclosure Act

Der *UK Public Interest Disclosure Act* ist älter als die US-amerikanischen Regeln. Er enthält einen arbeitsrechtlichen Schutz für *Whistleblower*, allerdings nur dann, wenn im Wesentlichen drei Voraussetzungen gegeben sind: Es muss eine geschützte Information (*protected disclosure)* vorliegen, sie muss von einer geschützten Person *(protected person)* aufgedeckt werden und dabei ist ein vorgegebenes Prozedere einzuhalten. Geschützt sind Informationen über Fehlverhalten von Personen und Organisationen, Gesetzesübertretungen, Gefährdungen von Gesundheit und Umwelt und des Staates. Es muss ein zumindest glaubhafter Verdacht vorliegen. Hauptsächlich ist *Whistleblowing* durch derzeitige und ehemalige Mitarbeiter der Organisation geschützt, sowie von Personen in einem beruflichen Naheverhältnis zu der Organisation. Die *Whistleblower* müssen vor allem im guten Glauben handeln und nicht aus persönlichen Motiven. Whistleblowing ist nur geschützt, wenn dabei auch prozedurale Regeln eingehalten werden. Vorerst ist die Information der Vorgesetzten vorgesehen. Nur wenn diese nicht reagieren oder wenn die Gefahr besteht, dass diese nicht geeignet sind das Fehlverhalten abzustellen oder selbst in Verdacht stehen, ist ein externes *Whistleblowing* zulässig. Ist eine *Whistleblower* Hotline eingerichtet, ist diese zu nutzen. Die externen Stellen die zur Entgegennahmen von *Whistleblower* Botschaften geeignet sind,

[44] Der deutsche Bundesrat hat in einer Resolution die Herausgabe der Domumente an die Finanzbehörden verlangt, was SZ und ICJI ablehnen, SZ.de 12.4.2016 – Bundesrat fordert die Herausgabe der Panama Papers

[45] 107th Congress of the United States of America, Second Session January 23rd 2002: An Act to protect investors by improving the accurancy and realibility of corporate disclosures made pursuant to the securities laws and for other purposes – Sarbanes Oxley Act 2001 H.R. 3763

[46] 111th Congress of the United States of America at Second Session January 5th, 2010. An Act to promote the financial stability of the United Sates by improving accountability and transparency in the financial systems, to end "to big to fail", to protect the American taxpayers by ending bailouts, to protect consumers from abusive financial services practices, and for other purpose. Dodd Frank Wallstreet Reform and Consumer ProtectionAct 2010, H.R. 4173

werden durch Verordnung festgesetzt.[47] PIDA ist allerdings nicht auf die Mitglieder des *Secret Service* oder der Armee anzuwenden und das Aufdecken von Staatsgeheimnissen ist nicht geschützt. Gewisse Daten dürfen unter dem Schutz von PIDA nicht aufgedeckt werden. Dieser *Whistleblowerschutz,* der eine vor allem ausgelobte finanzielle Belohnung für Whistleblowing ausschließt, da es nicht aus dem Streben nach einem persönlichen Vorteil ausgeführt werden darf, scheint beispielhaft, wenngleich der Aspekt des Schutzes des Beschuldigten auszubauen wäre.

## 3.2. US Entwicklung: Vom Schutz im Regierungsbereich zur Belohnung

Mit dem *Civil Service Reform Act 1978 (CSRA)*[48] wurde das *Office of Special Counsel (CSRA)* eingerichtet um u.a. Bedienstete von Bundesbehörden von Repressalien zu beschützen damit sie sich frei fühlen, Betrug, Verschwendung oder anderes Fehlverhalten aufzuzeigen. Es wurde ein eignes gerichtsartiges Gremium für Auseinandersetzungen der Behörden und ihrer *Whistleblower*, der *Merit Systems Protection Board (MSPB)* geschaffen. Entgegen den Absichten des Gesetzgebers war dieses System nicht ausreichend effektiv.[49] Es wurde daher der „*Whistleblower Protection Act 1989*“[50] geschaffen, um eine Verbesserung herbeizuführen. Abgesehen von diesem nunmehr verbesserten Schutz schützte das verfassungsmäßige Recht der freien Meinungsäußerung Regierungsangestellte, die zu *Whistelblowern* wurden. 2006 wurde dieses spezielle Recht auf freie Meinungsäußerung für Regierungsangestellte durch eine Entscheidung des *Supreme Court* allerdings deutlich eingeschränkt.[51] Das *Committee on Homeland Security and Governance Affaires* des US Senates stellte 2012 fest, dass der Schutz von Whistleblowern in Bundesbehörden durch Jahre herabgesetzt wurde wofür nach Ansicht des Ausschusses in hohem Maß die Judikatur des *United States Court of Appeals fort he Federal Circuit* verantwortlich war.[52] Der Kongress hat daher als Gegenmaßnahme den *Whistleblower Protectction Enhancement Act of 2012* beschlossen.[53] In Ergänzung dieses erfolgte die *Presidetial Policy Directive 19 (PPD 19),* die sich um den Schutz von Whistleblowern mit Zugang zu vertraulichen Informationen bemüht.[54]

Der Sarbanes Oxley Act (SOX), der für in den USA an Börsen notierte Unternehmen gilt, hat in Sec. 807 einen speziellen Schutz für Whistleblower. Geschützt ist das Aufdecken von Fehlverhalten, das im Gegensatz zu Bundesgesetzen und Regulierungen der *SEC (Security an Exchange Commission)*[55] steht, die zum Schutz von Aktionären erlassen wurden. Geschützt sind Arbeitnehmer der Unternehmen soweit sie die Information an eine Bundesbehörde, eine Regulierungsbehörde, einen Vorgesetzten oder sonst eine Person in der Organisation richten, die in der Lage scheint, dieses Fehlverhalten zu beenden. Der *Whistleblower* darf keinen persönlichen oder materiellen Schaden erleiden, weder durch den Dienstgeber noch durch Dritte, andernfalls ihm Schadenersatz zusteht. SOX verpflichtet die an der Börse notierten Unternehmen zur Einrichtung von Prozedere,

[47] Vgl. Gov.uk.Guide Whistleblowing,https://www.gov.uk/whistleblowing January 9 2013

[48] 95th United States Congress, An Act to reform the civil service laws and Related Developments Public law 94-454 ,92 Stat 111 October 13 1978

[49] Vgl Miceli/Near/Dworkin 2008 s. FN 12 S 155

[50] 101st United States Congress: An Act to amend title 5, United States Code, to strengthen the protections available to Federal employees against prohibited personell practices and othe purposes, (Whistleblower Protection Act of 1989), Public Law 101-12, 103 Stat. 16

[51] Supreme Court of the United States, Garcett v. Cellabos, 04-473 May 30 2006

[51] Vgl. Whistleblower Protection Enhancement Act of 2012 repoort of the committee on homeland security and government affairs, United States Senate to accompany S 743 http://www.gpo.gov

[53] 112th Congress of the United States, An Act to amend chapter 23 of title 5 , United States Code, to clarify the disclosures of information protected from prohibited personnel practices , require a statement in non – disclosure policy, forms and agreements that such policies, forms and agreements conform with certain disclosure protections, provide certain authority for the Special Counsel, and other purposes (Whistleblower Protection Enhancement Act of 2012) Nov 272012, Public Law 112 – 1999 126 Stat 1465

[54] Presidential Policy Directive 19 (PPD 19), Protecting Whistleblowers with Access to Clasified Information, https://obamawhitehouse.archieves.gov/sites/default/filesimage/ppd-19pdf

[55] Sec = US Börsenaufsichtsbehörde

in denen *Whistleblower* Botschaften auch anonym abgegeben werden können (*Whistleblower Hotlines).* Die Audit Committees[56] sind nach Sec. 301/4 für die Einrichtung und die Funktionsweise dieser Prozedere verantwortlich. Die Forderung zur Einrichtung solcher Hotlines besteht auch für ausländische Unternehmen, an denen an US Börsen notierte Unternehmen beherrschend beteiligt sind. Der *Whistleblower* Schutz gilt allerdings für diese Unternehmen nicht.[57] Die in Europa bestehenden Probleme, vor allem auf dem Datenschutzsektor, werden noch dargestellt. Der *Whistleblower* Schutz des SOX relativiert sich am Schicksal von *Mattew Lee*. Er war *Senior Vice President* von *Lehman Brothers* und informierte sowohl die Unternehmensleitung als auch den Abschlussprüfer (*Ernst &Young)* über die Unrechtmäßigkeit der sogenannten *Repo 105* Geschäfte. Im Rahmen dieser Geschäfte wurden am Ende eines Bilanzquartals iliquide Wertpapiere mit einem Bilanzwert 100 um 105 an eine andere Bank, oftmals *J.P Morgan,* gegen die Verpflichtung auf Rückkauf zu Beginn des neuen Bilanzquartals um 105 verkauft. Effekt: Im abgelaufenen Quartal wurde ein Gewinn von 5 erzielt, illiquide Vermögenswerte wurden gesenkt und liquide Mittel erhöht. Die andere Bank *kassierte ein Abwicklungshonorar und im nächsten Quartal standen höhere Vermögenswerte* zu Buche ohne dass eine wirkliche Wertsteigerung stattgefunden hat.[58] Trotz der Schutzbestimmungen des *SOX* für *Whistleblower* wurde *Matthew Lee* entlassen, wobei dafür als Begründung der Wegfall seines Aufgabenbereiches gewählt wurde.[59]

War SOX eine klassische Anlassgesetzgebung in der Folge der ENRON und WorldCom Skandale 2002, ist der „*Dodd Frank Wallstreet Reform and Consumer Protection Act"* die Wiederholung als Folge der Lehman-Pleite. Dieses Gesetz verstärkt den *Whistleblower* Schutz, bringt aber auch eine völlig neue Dimension in die Entwicklung der *Whistleblower* Gesetzgebung. SEC wird beauftragt eine Prämie an *Whistleblower* zu bezahlen, wenn diese einen Verstoß gegen die Wertpapiergesetzgebung anzeigen, die dieser bis dahin nicht bekannt war. Der *Whistleblower* muss zu der Information selbst gekommen sein und darf sie nicht aus einer behördlichen Untersuchung oder einer Publikation ableiten. Die Information muss dazu beitragen, dass die SEC gegen das Unternehmen eine Strafe verhängen kann. Die Prämie darf maximal 30 % der Strafe betragen.[60] Von einer Prämie ausgeschlossen sind Informanten, die vorsätzlich oder wissentlich falsche oder erfundene Angaben machen oder falsche oder erfundene Unterlagen unterbreiten. In der SEC ist ein eigenes *Whistleblower* Büro eingerichtet und dieses berichtet ein Mal pro Jahr an den *Congress.* Am 25.4.2017 hat SEC bekanntgegeben, dass US$ 153 Mio seit Bestehen des Programmes an 43 *Whistleblower* ausbezahlt wurden. Die Tipps dieser *Whistleblower* haben zu US$ 953Mio Strafen gegen diejenigen, die gegen Regeln verstoßen haben, geführt. Im Jahr 2014wurde eine Prämie von US$ 30 Mio. zugesprochen, im August 2019 eine solche von US$ 29 Mio.[61] Bereits vor dem *Whistelblower Awarding,* das im Dodd Frank Act eingeführt wurde, existierte das *IRS (Internal Revenue Service) Whistleblower Program,* das 2016 10 Jahre bestand.[62] Im Fiskal Jahr 2016 hat die US Steuerbehörde 418 Prämien im Wert von 61,4 Mio. US$ ausbezahlt. Durch die Hinweise der prämierten Whistleblower wurden US$ 368,9 Mio. Steuern eingefordert.[63]

[56] Das „Audit Committee" ist ein Ausschuss des vor allem im angloamerikanischen monistischen Governance System eingerichteten „Board of Directors" und besteht aus „non managing directors". Im zentraleuropäischen dualen Governance System ist der Prüfungsausschuss ein Ausschuss des Aufsichtsrates.

[57] Vgl. US Court of Appeals 1 st Circuit, Canero v Boston Scientific Corporation, January 5 2006, 04 – 1801, 04 - 2291

[58] Vgl United States Bankruptcy Court Southern District of New York in re Lehman Brothers Inc. et al, Report of Antonio Valaukas, Examiner Chapter 11 Case 08 135555nn(JPM) March 11 2010

[59] Vgl Clark Andrew, Lehman's Whistleblower feels "vindicated" and is pondering a new career, digital film, http://www.guardian.co.uk/business/andrew-clark-on-america/2010 download 15.06.2010

[60] Frank Dodd Act, Sec. 922 amending Securities Exchange Act 15 U.S.C. 78a, Sec. 21F

[61] Security ans Exchange Commission:, SEC Awards Nearly 4 Million to Whistleblower, Washington 2014, https://sec.gov./news/press-release/2017-84

[62] Internal Revenue Code 2623

[63] IRS (Internal Revenue Service) Whistleblower Program, Fiscal Year 2016, Annual Report to the Congress p 10

Eine durchaus interessante Kombination von Verfolgung eines *Whistleblowers* und Belohnung desselben durch verschiedene Behörden derselben Regierung stellt der Fall des *Bradley Birkenfeld* dar. Er war Banker bei der Schweizer UBS und arbeitete mit dem *US Department of Justice (DOJ)* zusammen um einen Teil des Schweizer Bankgeheimnisses zu brechen und der US Regierung reichlich Steuereinnahmen zu ermöglichen, die ihnen dank Nummernkonten bei der UBS vorenthalten wurden. Das *DOJ* erwies sich keineswegs dankbar, sondern verfolgte *Birkenfeld* solange bis er drei Jahre hinter Gittern landete. Das *US IRS (Internal Revenue Service)* sah die Rolle *Birkenfelds* allerdings völlig anders und sprach ihm US $ 104 Mio. Belohnung für das Aufdecken des UBS Skandals zu.[64] Die Lektüre seines Buches kann nur empfohlen werden.[65]

## 3.3. UN Konvention gegen Korruption

Im Vorwort zur „*United Nations Convention against Corruption*“[66] wird Korruption als heimtückische Plage mit zerstörenden Wirkungen auf die Gesellschaft bezeichnet, die die Demokratie und die Grundlagen des Rechts unterminiert, zur Verletzung der Menschenrechte und Verzerrung der Märkte führt, die Lebensqualität aushöhlt und es organisierter Kriminalität, Terrorismus und anderen Beeinträchtigungen der menschlichen Sicherheit erlaubt zu florieren, bezeichnet. Daher verlangt die Konvention unter anderen von den Mitgliedsstaaten Maßnahmen zu ergreifen und Systeme einzurichten, damit alle öffentlichen Funktionsträger Korruption an die angemessenen Autoritäten herantragen können. (Art. 8/4).

Die Mitgliedsstaaten sollen auch im privaten Sektor Standards für Rechnungswesen und Auditing schaffen um den privaten Sektor vor Korruption zu schützen. Dazu gehören interne Kontrollen und Interne Revision nach angemessenen Standards. (Art. 12/1). Weiterhin sollen die Mitgliedsstaaten angemessene Maßnahmen zum Schutz von Personen einrichten, die im guten Glauben und aus glaubhaften Gründen an kompetente Informationsinstanzen Informationen liefern, die Verstöße gegen Konvention gegen Antikorruption aufdecken (Art. 33). Die Mitgliedsstaaten sollen auch Maßnahmen setzen, um Personen zu ermuntern hilfreiche Informationen über Korruption an die Behörden zu liefern und mit diesen zusammen zu arbeiten.

## 3.4. Datenschutz in Europa

Seit 25.5.2018 wird die *EU-Datenschutzgrundverordnung (DSGVO)*[67] in allen Mitgliedsstaaten angewendet. Sie geht davon aus, dass der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ein Grundrecht ist (Erw 1). Die DSGVO legt fest, dass personenbezogene Daten in einer Weise verarbeitet werden müssen, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet einschließlich dem Schutz vor unbefugter und unrechtmäßiger Verarbeitung und von unbeabsichtigter Verbreitung (Art 5/1). Im Abschnitt 5.3 wird die DSGVO in Zusammenhang mit der Umsetzung kurz behandelt. Für die europäischen Überlegungen zum Thema *Whistleblowing* insbesondere zu *Whistleblower* Hotlines, soll ein Blick auf die „Artikel 29 Datenschutzgruppe“, die durch die Richtli-

[64] Baches Zoe, Millionen Belohnung für Bradley Birkenfeld, Neue Zürcher Zeitung,22.9.2012. www.nzz.millionen-belohnung-fuer-bradley-birkenfeld-1.17595188

[65] Birkenfeld Bradley, Des Teufels Banker. Wie ich das schweizer Bankgeheimnis zu Fall brachte,2. Auflage, Finanzbuch Verlag München 2017

[66] UN Convention against Corruption, General Assembly Resolution 58/4 of October 31 st 2003 entered in force December 14 th 2005, United Nations Office on Drugs and crime (UNDOC) www.undoc.org

[67] Verordnung des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46 EG (Datenschutzgrundverordnung) ABl L 119/1 vom 27. April 2016

nie durch die DSGVO aufgehobene RL 95/46 EG[68] geschaffen wurde und aus Vertretern aller EU Mitgliedsstaaten und der Europäischen Kommission besteht, geworfen werden. Sie übte ihre Aufgaben in völliger Unabhängigkeit aus.[69] Die Gruppe hat im Jahr 2006 Grundsätze aufgestellt, die auch heute noch das europäische Verständnis zu dieser Materie weitgehend darstellen.[70] Interne Verfahren zur Meldung von Missständen werden in der Regel aus dem Bedürfnis eingerichtet, zuverlässige Grundsätze der Unternehmensführung in den täglichen Betrieb des Unternehmens einzuführen. Sie sind als zusätzlicher Mechanismus gedacht, die die regulären Informations- und Meldekanäle ergänzen. Die Meldung von Missständen ist als Ergänzung zum internen Management zu sehen und nicht als Ersatz dafür. Vorhandene Regelungen und Leitlinien für die Meldung von Missständen gewähren den Hinweisgebern besonderen Schutz, erwähnen aber den Schutz der beschuldigten Person nicht oder unzureichend. Auch die beschuldigte Person hat Anspruch auf ihre Rechte bezüglich der Verarbeitung personenbezogener Daten. Verfahren zur Meldung von Missständen bergen eine ernste Gefahr der Stigmatisierung und Viktimisierung der beschuldigten Person, die damit Risiken ausgesetzt wird bevor ihr bewusst wird, dass sie überhaupt beschuldigt ist und bevor die angeblichen Fakten auf ihren Wahrheitsgehalt untersucht sind.[71]

Die Arbeitsgruppe lehnt Verfahren zur Meldung von Missständen nicht grundsätzlich ab, sondern hält sie für sinnvoll bei der Überwachung der Einhaltung von Regeln besonders in der Rechnungslegung und deren Kontrollen, der Wirtschaftsprüfung, der Korruptionsbekämpfung und der Bekämpfung von Banken- und Finanzkriminalität. Diese Verfahren müssen aber in Einklang mit der Richtlinie 95/46 stehen und das grundlegende Recht auf den Schutz personenbezogener Daten sowohl des Hinweisgebers als auch der beschuldigten Person, ist während des gesamten Verfahrens zu gewährleisten. Das Recht der beschuldigten Person auf Mitteilung von, Zugang zu, Berichtigung und Löschung von Daten ist grundsätzlich zu beachten und darf nur in bestimmten Fällen beschränkt werden, um das Gleichgewicht zwischen dem Recht auf Schutz der Privatsphäre und den Interessen des Gesellschaftssystems herzustellen.[72] Die Gruppe bringt zum Ausdruck, dass im Falle von *Whistleblowing* mehrere schutzwürdige Interessen zusammentreffen. Auf der einen Seite der Schutz der persönlichen Sphäre des Beschuldigten, dessen Recht auf faire Untersuchung und das Recht auf Hintanhaltung der „Vorverurteilung", auf der anderen Seite das Recht des Hinweisgebers auf Schutz vor Verfolgung und auch das Recht der Gesellschaft auf Schutz vor Missbrauch und Korruption.

## 3.5. Bemühungen des Europarates

Die Parlamentarische Versammlung des Europarates hat sich 2010 in einer Resolution mit *Whistleblowing* auseinandergesetzt.[73] Darin stellt sie die Bedeutung von *Whistleblower* als betroffene Personen die Alarm schlagen um Fehlverhalten zu beenden fest. Dies dient zur Stärkung der Verantwortlichkeit und Unterstützung des Kampfes gegen Missmanagement und Korruption sowohl im öffentlichen als auch im privaten Sektor (Art.1). Potentielle *Whistleblower* sind oft demotiviert aus Angst vor Repressalien und das Fehlen einer Reaktion auf ihre Warnungen (Art. 2). Die meisten Mitgliedsstaaten des Europarates haben keine umfassenden Gesetze zum Schutz von *Whistleblower* wie sie im UK und den USA bestehen (Art. 4). Whistleblowing verlangt Mut und Entschlossenheit und den Hinweisgebern

[68] Richtlinie 95/46 EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ABl. L 281 vom 23.11.1995

[69] RL 95/46 Begründung 65

[70] Artikel 29 Datenschutzgruppe, Stellungnahme 1 / 2006 zur Anwendung der EU – Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken – und Finanzkriminalität vom 1. Februar 2006 WP 117 009195/DE (WP 117)

[71] Vgl. WP 117 III

[72] Vgl. WP 117 V

[73] Council of Europe - Parliamentary Assembly – Resolution 1729 (2010): Protection of Whistleblowers, http://assembly.coe.int

sollte hinreichende Sicherheit geboten werden, dass ihre Warnungen gehört werden und sie nicht die Lebensumstände von sich und ihren Familien gefährden (Art. 5). *Whistleblower* Gesetze sollten folgende Eckpunkte enthalten: Die Definition der geschützten Hinweise (*protected disclosure)* sollte alle im guten Glauben ausgesprochene Warnungen vor gesetzwidrigen Verhalten enthalten, insbesondere die Verletzung von Menschenrechten wie Leben, Gesundheit und Freiheit, die Rechte der Personen als Gegenstand der öffentlichen Verwaltung, als Steuerzahler, sowie als Aktionäre, Arbeitnehmer und Kunden von privaten Gesellschaften (6.1.1.). Die Gesetzgebung soll sowohl auf den öffentlichen als auch den privaten Sektor anwendbar sein und soll auch Militärpersonen und Beschäftigte von Geheimdiensten (*special services)* einschließen (6.1.2). Die Gesetzgebung soll das Arbeitsrecht, das Strafrecht und das Medienrecht und das Antikorruptionsrecht einschließen (6.1.3). *Whistleblower* Prozedere sollen sicherstellen, dass Warnungen ernsthaft untersucht werden und wesentliche Inhalte das Top Management unverzüglich, nötigenfalls unter Umgehung der Hierarchie erreichen (6.2.1.1.). Die Identität der *Whistleblower* soll nur mit deren Zustimmung oder aus ernst zu nehmenden öffentlichen Interessen aufgedeckt werden (6.2.1.2). Die Gesetzgebung soll jene schützen, die in gutem Glauben bestehende interne *Whistleblower* Kanäle nutzen (6.2.2.). Nur in solchen Fällen, in denen keine internen Kanäle bestehen, oder diese nicht ausreichend funktioniert haben oder auf Grund des Charakters der Botschaft anzunehmen ist, dass sie nicht ausreichend funktionieren werden, kann externes *Whistleblowing* inklusive der Information der Medien geschützt werden (6.2.3). Es soll dem Whistleblower Handeln im guten Glauben anerkannt werden, wenn er gute Gründe hatte, dass die aufgedeckte Information wahr sei, auch dann, wenn sich hinterher ihre Unwahrheit herausstellen sollte. Dieser gute Glaube darf nicht unterstellt werden, wenn der Whistleblower ungesetzliche oder unethische Ziele verfolgte (6.2.4). *Whistleblower* Prozedere müssen auch einen angemessenen Schutz gegen Beschuldigungen, die in böser Absicht gemacht werden, gewährleisten (6.7.2.).

## 3.6. Der Europäische Gerichtshof für Menschenrechte

Am 21. Juli 2011 hat dieser internationale Gerichtshof in Straßburg, dessen Judikatur sich die Mitgliedsstaaten des Europarates unterworfen haben, in Sachen *Whistleblowing* eine bemerkenswerte Entscheidung getroffen.[74] Die Beschwerdeführerin war als Pflegerin in einem Altenpflegeheim beschäftigt, das von einer Gesellschaft betrieben wurde, die sich mehrheitlich im Eigentum des Landes Berlin befand. Der medizinische Dienst der Krankenkassen stellte bereits 2002 eine deutliche personelle Unterbesetzung des Heimes und daraus resultierende Pflegeengpässe fest. 2003 und 2004 meldeten die Beschwerdeführerin und ihre Kollegen regelmäßig an die Geschäftsführung, dass eine Überforderung des Personals wegen deutlicher Unterbesetzung bestand. Insbesondere wurden Pflegleistungen nicht ausreichend dokumentiert. Der Anwalt der Klägerin schrieb der Geschäftsführung 2004 erneut über hygienische Missstände und forderte diese zum Handeln auf. Diese Aufforderung war verbunden mit der Drohung einer Anzeige und einer öffentlichen Diskussion. In der Folge erstattet der Anwalt Anzeige, die bald von der Staatsanwaltschaft zurückgelegt wurde. Die Beschwerdeführerin wurde wegen anhaltender Krankheit gekündigt. Sie rief das Arbeitsgericht an und schaltete die Gewerkschaft ein. Die Gewerkschaft veröffentlichte ein Flugblatt, in dem die mangelhaften Zustände in dem Heim angeprangert wurden, ebenso der Umgang der Geschäftsleitung mit dem Personal. Der Betriebsrat des Heimes lehnte eine Zustimmung zur Kündigung der Beschwerdeführerin ab. Sie wurde daraufhin entlassen. Die Staatsanwaltschaft eröffnete die Untersuchung gegen die Leitung des Heimes neuerlich und stellte sie in der Folge wieder ein. Das Arbeitsgericht gab der Klägerin Recht und stellte die Unzulässigkeit der Kündigung als unzulässige Motivkündigung dar. Die Veröffentlichung der Gewerkschaft wurde zwar als

[74] European Court of Human Rights, Fifth Section, Case of Heinisch v Germany, Application no. 28274/08, Strassbourg, July 21 st 2011, http//: hudoc.echr.coe.int

polemisch erkannt, aber zulässig, da auf Fakten beruhend. Das Landesarbeitsgericht Berlin als zweite Instanz hob das erstinstanzliche Urteil auf. Die Anzeige gegen den Dienstgeber qualifizierte das Gericht als unangemessene Reaktion. Die Beschwerdeführerin hätte nach Ansicht dieses Gerichtes nicht im Rahmen ihrer verfassungsmäßigen Rechte gehandelt, sondern ihre Loyalitätsverpflichtung gegenüber dem Arbeitgeber gebrochen. Die Berufung an das Bundesarbeitsgericht wurde von diesem zurückgewiesen, eine Beschwerde beim Bundesverfassungsgericht blieb erfolglos. Der Europäische Gerichtshof für Menschenrecht fand die fristlose Entlassung als unangemessen und sprach der Beschwerdeführerin Schadenersatz zu. Der Gerichtshof warf den deutschen Gerichten vor, keine ausgewogene Abwägung des Rechtes auf freie Äußerung der Beschwerdeführerin und dem Recht des Dienstgebers auf Wahrung seiner Reputation vorgenommen zu haben, weshalb die Urteile eine Verletzung der Europäischen Konvention für Menschenrechte darstellen. Der Gerichtshof setzte das höhere Gut der freien Meinungsäußerung in einer demokratischen Gesellschaft über die Pflicht des Dienstnehmers zur Loyalität, Zurückhaltung und Diskretion. Der Gerichtshof setzt allerdings voraus, dass die Beschwerdeführerin nicht böswillig, sondern im guten Glauben gehandelt hat und dass ein öffentliches Interesse an der Offenlegung bestanden hat.

# 4. Europäische Union

Eine Studie von *Price Waterhouse Coopers (PWC)*[75] im Auftrag des Europäischen Parlamentes kam 2011 zu der Schlussfolgerung, dass die derzeitigen Regeln für *Whistleblowing* innerhalb der Institutionen der Europäischen Union keine effektiven Instrumente zur Bekämpfung von Korruption und Interessenkonflikten sind. Es ist nach Meinung der Autoren ein neues Whistleblower Rahmenwerk einzuführen, dem ein ausgeglichenes Verhältnis zwischen Missbrauch und Schutz der im guten Glauben Handelnden zu Grunde liegt. Dieser neue Rahmen soll Personen in einem Verhältnis zu Institutionen der Europäischen Union ermutigen Fehlverhalten aufzuzeigen, es soll eine effektive und unverzügliche Untersuchung der Vorwürfe sicherstellen, angemessene Reaktionen erreichen und einen starken Schutz für im guten Glauben Handelnde ebenso bringen wie böswillige *Whistleblower* entmutigen.

## 4.1. Bestehende europäische Rechtsakte

**RL 2013/36/EU**[76] (Kreditinstitute). Im Art. 71 wird von den Mitgliedstaaten verlangt, dass die zuständigen Behörden „wirksame und verlässliche Mechanismen schaffen, um zur Meldung von drohenden oder tatsächlichen Verstößen gegen nationale Vorschriften zur Umsetzung dieser Richtlinie und die Verordnung 575/2013[77] bei den zuständigen Behörden zu ermutigen (Art.71/1).“ Diese Mechanismen haben zumindest spezielle Verfahren für den Empfang der Meldungen über Verstöße und deren Weiterverfolgung zu enthalten (Art 71/2/a), weiterhin einen angemessenen Schutz vor Vergeltungsmaßnahmen, Diskriminierung und ungerechtfertigter Behandlung für die Mitarbeiter von Instituten, die Verstöße innerhalb ihres Instituts melden (Art. 71/2/b), ebenso den Schutz personenbezogener Daten sowohl für die Person, die Verstöße anzeigt, als auch für jene Person, die mutmaßlich für die Verstöße verantwort-

[75] European Parliament, Directorate General for Internal Policies, Policy Department, Budgetary Affairs: Corruption and conflict of interest in the European Institutions: the effectiveness of whistleblowers, study 2011, Authors Price Waterhouse Coopers PWC) Belgium, Responsible Administrator Helmut Werner, http://www.europarl.europa.eu/studiesConclusions and recommendation viii

[76] Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung […….] ABl L 176 vom 27.6.2013

[77] Verordnung des Europäischen Parlaments und des Rates 575/2013 vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen […….] ABL L 176/1 vom 27.6.2013

lich ist (Art.71/2/c) und auch klare Vorschriften zur Garantie der Vertraulichkeit der meldenden Person / art 71/2/d). Die Mitgliedstaaten haben die Institute zu verpflichten angemessene Verfahren einzurichten, über die Mitarbeitenden die Verstöße melden können. (Art. 71/3).

**RL 2014/56/EU** (Änderung der Abschlussprüferrichtlinie). In der Erw. 17 zur RL 2014/56[78] wird darauf verwiesen, dass „Informanten *(Whistleblower)*" den zuständigen Behörden neue Erkenntnisse liefern und damit bei der Aufdeckung und Sanktionierung von Unregelmäßigkeiten einschließlich Betrug helfen können. Die Angst vor Repressalien oder mangelnde Anreize können Personen von einer Anzeige abhalten. Die Mitgliedstaaten sollen daher angemessene Regelungen schaffen, die Informanten dazu ermutigen auf mögliche Verstöße der RL 2014/56 und der VO 537/2014[79] aufmerksam zu machen und Informanten vor Repressalien zu schützen. Anreize soll es nur dann geben, wenn neue Informationen geliefert werden und die Informanten zur Meldung nicht ohnehin rechtlich verpflichtet wären und die Information zu einer Sanktion führt. Die zu schaffenden Anreizregelungen müssen Vorkehrungen enthalten, die der angezeigten Person angemessenen Schutz bieten, insbesondere was den Schutz personenbezogener Daten betrifft und ihr Recht auf Anhörung und Verteidigung.

Art. 30e der RL 2104/56 hat die Überschrift „Meldung von Verstößen" und schreibt den Mitgliedstaaten v575/2013or wirksame Mechanismen zu schaffen, die Meldung von Verstößen gegen die RL 2014/56 und die VO 537/2014 zu fördern. Diese Mechanismen haben spezielle Verfahren zur Entgegennahme von Meldungen und entsprechende Folgemaßnahmen zu enthalten. Weiterhin haben sie den Schutz personenbezogener Daten sowohl des Meldenden als auch der verdächtigten Person zu umfassen, ebenso wie die Gewährleistung des Rechts der beschuldigten Person auf Verteidigung und Anhörung.

**VO EU 596/2014**[80] (Marktmissbrauchsverordnung). Erw.74 führt aus, dass Informanten den zuständigen Behörden neue Informationen zur Kenntnis bringen können, die diese bei der Aufdeckung von Insidergeschäften und Marktmanipulation unterstützen. Art. 32 verlangt von den Mitgliedstaaten die Schaffung wirksamer Mechanismen, um die Meldung tatsächlicher oder möglicher Verstöße gegen die VO 596/2014 zu ermöglichen (Art. 32/1). Diese Mechanismen müssen spezielle Verfahren zur Entgegennahme der Meldung und Nachverfolgung einschließlich der Einrichtung sicherer Kommunikationskanäle enthalten (Art.32/2/a). Weiterhin sind in ihnen ein angemessener Schutz jener Personen vor Vergeltungsmaßnahmen, Diskriminierung und ungerechter Behandlung vorzusehen, die im Rahmen ihrer Erwerbstätigkeit auf der Grundlage eines Arbeitsvertrages beschäftigt sind und die Verstöße melden oder denen Verstöße zur Last gelegt werden (Art 32/2/b). Der Schutz personenbezogener Daten sowohl der Meldenden als auch derjenigen, die mutmaßlich den Verstoß begangen haben einschließlich der Wahrung der Vertraulichkeit ihrer Identität ist zu gewährleisten (Art 32/2/c). Arbeitgeber, die der Finanzdienstleistungsregulierung unterliegen, sind von den Mitgliedstaaten zu verpflichten Verfahren einzurichten mit denen Mitarbeitende Verstöße melden können (Art 32/3). Mitgliedsstaaten können finanzielle Anreize für Personen bereitstellen, die relevante Informationen über mögliche Verstöße gegen die VO 596/2014 liefern, soweit diese nicht gesetzlich zur Meldung verpflichtet sind und sofern die Informationen neu sind und zur Verhängung von Sanktionen beitragen (Art 32/4).

**DRL EU 2015/2392**[81] (Durchführungsrichtlinie der Kommission zur Marktmissbrauchsverordnung). „Die RL enthält Vorschriften zur Festlegung der im Art 32/1 der VO 596/2014 genannten Verfahren,

[78] Richtlinie 2014/56/EU des Europäischen Parlaments und des Rates vom 16.April2014 zur Änderung der Richtlinie 2006/43/EG über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, ABl L 158/196 vom 27.5.2014

[79] Verordnung 537/2014 des Europäischen Parlaments und des Rates vom 17. April vom 16. April 2014 über spezielle Anforderungen an die Abschlussprüfung [……..] ABl L 158/74 vom 27.5.2014

[80] Verordnung des Europäischen Parlaments und des Rates 596/2014 vom 16. April 2014 über Marktmissbrauch (Marktmissbrauchsverordnung) und zur [……] ABl L 173 vom 12.6.2014

[81] Durchführungsrichtlinie EU 2015/2392 der Kommission vom 17. Dezember 2015 zur Verordnung EU 596/2014 des Europäischen Parlaments und des Rates hinsichtlich der Meldung tatsächlicher oder möglicher Verstöße gegen diese Verordnung ABl L 332/126 vom 18.12.2015

einschließlich zur Meldung und Nachverfolgung von Meldungen und der Maßnahmen zum Schutz von Personen, die auf der Grundlage eines Arbeitsvertrags tätig sind, sowie Maßnahmen zum Schutz personenbezogener Daten“ (DRL 2015/2392 Art.1). Die DRL wiederholt die Argumentation der VO wonach Personen , die den zuständigen Behörden tatsächliche oder mögliche Verstöße gegen die VO 596/2014 melden also Informanten sind, den Behörden neue Informationen zur Kenntnis bringen können, die diese bei der Aufdeckung von Marktmissbrauch und der Verhängung von Sanktionen unterstützen und dass Hinweise von Informanten bei Furcht vor Diskriminierung oder Offenlegung personenbezogener Daten unterbleiben können. Es sind daher angemessene Vorkehrungen vorzusehen, die den Schutz und die Einhaltung der Grundrechte sowohl der Informanten als auch der Personen gegen die sich die Vorwürfe richten sicherstellen. Personen, die bewusst falsche oder irreführende Angaben melden, sollten nicht als geschützte Informanten gelten. Es sollten auch anonyme Meldungen zugelassen werden (Erw. 1, 2 DRL 2015/2392). Personen, die im Rahmen eines Arbeitsvertrages tätig sind und Meldungen erstatten oder denen Verstöße zur Last gelegt werden sind vor Diskriminierung, Vergeltungsmaßnahmen oder ungerechter Behandlung zu schützen (Erw. 6 DRL 2015/2392). Ausdrücklich wird darauf verwiesen, dass der Schutz personenbezogener Daten des Informanten und des eventuell Beschuldigten ebenso wichtig ist, wie der Schutz der Rechte jener, denen Verstöße zur Last gelegt werden. (Erw. 10,11 DRL 2015/2392).

Die DRL regelt Informationen und Nachverfolgung einer Verstoßmeldung (DRL 2015/ 2392 Art 4), anwendbare Verfahren bei Verstoßmeldungen (DRL 2015/2392) sowie schreibt sie die Einrichtung spezieller unabhängiger und autonomer Kommunikationskanäle zur Entgegennahme und Nachverfolgung dieser Meldungen vor und legt fest wann solche Kanäle als autonom und unabhängig anzusehen sind (DRL 2015/2392 Art 6). Die Behörden sind zur Dokumentation der Meldungen verpflichtet (DRL 2015/2392 Art 7). Die Mitgliedstaaten haben Verfahren für einen Informationsaustausch und für die Zusammenarbeit zwischen allen relevanten Behörden zum Schutz von Personen, die im Rahmen eines Arbeitsvertrags tätig sind, die Verstöße melden oder denen Verstöße zur Last gelegt werdeneinzurichten (DRL 2015/2392 At 8). Ist die Identität der gemeldeten Person der Öffentlichkeit nicht bekannt, ist deren Identität ebenso zu schützen wie die Identität einer Person, gegen die die Behörde ermittelt (DRL 2015/2392 Art 11).

**Kronzeugenregelung für Kartellsachen.** Durch hohe Geldbußen können an Kartellen beteiligte Unternehmen bestraft werden und diese Geldbußen haben auch eine abschreckende Wirkung für die Kartellbildung in der Zukunft. „Die Kronzeugenstrategie ergänzt die Kartellbekämpfung wirksam: Durch ein Klima des Misstrauens werden bestehende Kartelle unterminiert. Die EU - Kommission hat am 8.12.2006 eine „Mitteilung[82] über den Erlass und die Ermäßigung von Geldbußen in Kartellsachen“ herausgegeben, die sie selbst als „Kronzeugenregelung“ bezeichnet. „Über diese Mitteilung werden Unternehmen, die Kartelle anzeigen, an denen sie selbst beteiligt sind oder waren, belohnt durch den vollständigen Erlass oder die Ermäßigung der Geldbußen, die sonst gegen sie verhängt worden wären. Die Regelung hat sich als besonders wirksam für die Aufdeckung, Unterminierung und Beendigung von Kartellen herausgestellt. Da Kartelle in der Regel geheim sind, ist ihre Aufdeckung und Untersuchung ohne Mitwirkung von Beteiligten sehr schwierig. Die verbesserte Kronzeugenregelung soll an Kartellen beteiligte Unternehmen noch häufiger veranlassen, die betreffenden Verhaltensweisen den Wettbewerbsbehörden zu melden. Geldbußen können nur erlassen oder ermäßigt werden, wenn das Unternehmen während des gesamten Verfahrens im vollen Umfang kontinuierlich und zügig mit der Kommission zusammenarbeitet und es muss seine Beteiligung am Kartell unmittelbar beendet haben.

[82] Mitteilung der Kommission über den Erlass und die Ermäßigung von Geldbußen in KartellsachenABl 298 vom 8.12.2006idF 17.5.2011 http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=URISERV:126119

## 4.2. Schutz der Geschäftsgeheimnisse versus Whistleblowing

Die bereits erwähnten „*Leitlinien zur Verarbeitung personenbezogener Informationen im Rahmen eines Verfahrens zur Meldung von Missständen (EDPS-LL2016)*[83] des Europäischen Datenschutzbeauftragten *(European Data Protection Supervisor EDPS) vom Juli 2016* zum besseren Umgang mit dem Thema *Whistleblowing* stehen zweifellos in einem Spannungsverhältnis zu der kurze Zeit davor veröffentlichten EU Richtlinie 2016/943 zum Schutz von Geschäftsgeheimnissen.[84] Auf der einen Seite steht ein allgemeines Interesse an der Aufdeckung von Missständen und Straftaten, auf der anderen Seite die Interessen des Unternehmens Betriebsgeheimnisse und internes know-how zu schützen.[85]

Die EDPSLL2016 geht davon aus, dass Vertraulichkeit die wirksamste Methode ist um Mitarbeiter dazu zu ermutigen Fehlverhalten am Arbeitsplatz zu melden und das Korruption der Wirtschaft schadet und das Vertrauen der Bürger in öffentliche Einrichtungen untergraben kann. Die EDPS Leitlinien „sollen die Organe und Einrichtungen der EU bei der Erarbeitung und Umsetzung von *Whistleblowing* Verfahren unterstützen, sodass diese den Pflichten entsprechen, die in der für die EU Verwaltung geltenden Datenschutzverordnung[86] festgelegt sind.[87] Der Zusammenfassung der EDPSLL2016 folgend, sind Hinweisgeber der Ansicht, dass sie im öffentlichen Interesse handeln, wenn sie eine beobachtete schwerwiegende Handlung melden, wobei sie häufig mit Vergeltungsmaßnahmen in Form von Schikanen, Entlassung oder Bedrohung sowie Aufnahme in sogenannte „schwarze Listen" konfrontiert sind und Offenlegungen häufig ignoriert werden. Die EDPS formuliert in den Leitlinien 9 Empfehlungen für den Umgang mit Meldungen. Es wird die Einrichtung festgelegter Kanäle für interne und externe Meldungen empfohlen (1), weiterhin die Sicherstellung der Vertraulichkeit der erhaltenen Informationen und der Identität der Hinweisgeber und aller anderen Personen (2). Es sollen nur jene personenbezogenen Informationen verarbeitet werden, die für den konkreten Fall angemessen, relevant und notwendig sind und es soll der Grundsatz der Datenminimierung beachtet werden (3). Es ist festzulegen was unter personenbezogenen Daten zu versehen ist und wer die betroffenen Personen sind, um ihr Recht auf Information, Auskunft und Berichtigung ihrer Daten gewährleisten zu können (4). Empfohlen wird ein zweistufiges Verfahren zur Information über die Art der Datenverarbeitung (5). Es ist sicher zu stellen, dass bei der Beantwortung von Anträgen über Auskunft nicht personenbezogener Informationen Dritter offen gelegt werden(6). Die Übermittlung von personenbezogenen Informationen ist auf jene Fälle zu beschränken, in denen dies für die rechtmäßige Durchführung der Aufgaben im Zuständigkeitsbereich des externen oder internen Empfängers notwendig ist (7). Es sind angemessene Aufbewahrungsfristen für personenbezogene Informationen, die im Verfahren zur Meldung von Missständen verarbeitet wurden, festzulegen (8). Es sind organisatorische und technische Sicherungsmaßnahmen zur Sicherstellung der rechtmäßigen und sicheren Verarbeitung personenbezogener Informationen einzurichten. (9).

Die Richtlinie 2016/943 definiert Geschäftsgeheimnisse als Informationen die deshalb als geheim gelten, weil sie weder in ihrer Gesamtheit noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen, die üblicherweise mit dieser Art von Informationen umgehen, bekannt oder ohne weiteres zugänglich sind. Sie sind auch geheim,

[83] European Data Protection Supervisor (EDPS), Leitlinien zur Verarbeitung personenbezogener Informationen im Rahmen eines Verfahrens zur Meldung von Missständen, Brüssel 18. Juli 2016, https:// edps.europa.eu/sites/edp/files/publication/16-07-18-whistleblowing-guidelines-de.pdf

[84] Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates zum Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung ABl L 157/1 vom 15.6.2016

[85] Vgl. Conrad Conrad, Schutz der Geschäftsgeheimnisse versus Whistleblowing, datenschutz-notizen, datenschutz nord gruppe, https://www.datenschutz-notizen.de/schutz-der-geschäftsgeheimnisse-versus-whistleblowing

[86] Verordnung (EG) 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr ABl L 8/1 vom 12.1.1001

[87] Vgl European Data Protection Supervisor, Pressemitteilung, Datenschutz und Whistleblowing in den EU Organen, EDPS 2016/12, Brüssel 18.7.2016

weil sie von kommerziellem Wert und Gegenstand von den Umständen entsprechenden Sicherungsmaßnahmen sind (Art 2/1). „Der rechtswidrige Erwerb, die rechtswidrige Nutzung oder Offenlegung von Geschäftsgeheimnissen durch einen Dritten könnte verheerende Folgen für den rechtmäßigen Inhaber des Geschäftsgeheimnisses haben (Erw. 26). Die Mitgliedsstaaten haben daher Maßnahmen, Verfahren und Rechtsbehelfe vorzusehen um einen zivilrechtlichen Schutz vor rechtswidrigem Erwerb oder Nutzung von Geschäftsgeheimnissen zu gewährleisten, wobei diese fair, gerecht und nicht unnötig kompliziert kostspielig sein müssen (Art 6/1, 6/2). Nach Ansicht der Richtliniengeber wahrt die RL das Recht auf Achtung des Privat- und Familienlebens und den Schutz der personenbezogenen Daten ebenso wie das Recht auf Freiheit der Meinungsäußerung und der Informationsfreiheit und die Berufsfreiheit, das Recht zu arbeiten, die unternehmerische Freiheit, das Eigentumsrecht und das Recht auf eine gute Verwaltung. Sie wahrt das Recht auf Zugang zu Dokumenten bei gleichzeitiger Wahrung des Geschäftsgeheimnisses, das Recht auf einen wirksamen Rechtsbehelf und auf ein faires Verfahren unter Wahrung der Verteidigungsrechte (Erw. 35). In der RL wird betont, dass die in ihr vorgesehenen Maßnahmen, Verfahren und Rechtsbehelfe nicht dazu dienen sollen, *Whistleblower* Aktivitäten einzuschränken. Der Schutz der Geschäftsgeheimnisse soll sich daher nicht auf Fälle erstrecken, in denen die Offenlegung eines Geschäftsgeheimnisses insoweit dem öffentlichen Interesse dient, als ein regelwidriges Verhalten, ein Fehlverhalten oder eine illegale Tätigkeit von unmittelbarer Relevanz aufgedeckt wird. Ebenso soll der Schutz des Geschäftsgeheimnisses zurücktreten, wenn die angebliche Nutzung oder Offenlegung zur Ausübung des Rechts der freien Meinungsäußerung und der Informationsfreiheit, der Freiheit du Pluralität der Medien oder zum Schutz des allgemeinen öffentlichen Interesses dient (Art. 5).

## 4.3. Entschließung des Europäischen Parlaments zur Rolle von Informanten

Im Jahr 2016 ist das Europäische Parlament (EP) der parlamentarischen Versammlung des Europarates gefolgt und hat sich mit seiner Entschließung (EP 2017/2055/INI)[88] mit *Whistleblowing* auseinandergesetzt, allerdings in Hinblick auf die Aufdeckung von Fehlverhalten bei der Verwaltung von EU Mitteln. Das EP verweist darauf, dass regelmäßig Privatpersonen und NGOs (*non govermental organizations)* auf Unregelmäßigkeiten bei aus EU Mitteln finanzierten Projekten hinweisen (Erw.E). Das EP ist der Meinung, dass Informanten eine zentrale Bedeutung für die Verhinderung, Aufdeckung und Meldung von Unregelmäßigkeiten und Aufdeckung von Korruption zukommt. In Europa muss eine Kultur des Vertrauens geschaffen und unterstützt werden, damit sich die Bediensteten der EU und die Bürger auf Grundeiner verantwortungsvollen Verwaltung geschützt fühlen, wozu auch die Unterstützung potentieller Hinweisgeber gehört (Erw F). *Whistleblowing* ist ebenfalls nach Meinung des EP eine wichtige Informationsquelle für den Kampf gegen organisierte Kriminalität und Korruption im öffentlichen Sektor (Erw I). Bei *Whistleblowing*, das auf den Grundsätzen der Transparenz und Integrität basiert, soll der Schutz der Hinweisgeber unter der Voraussetzung eines Handelns im guten Glauben und zum Zweck des Schutzes der öffentlichen Interessen gesetzlich gewährleistet werden (Erw K). Behörden sollen die Möglichkeiten von Hinweisgebern und Journalisten nicht beschränken und schmälern, wenn illegale, unrechtmäßige oder schädliche Praktiken überwiegend im öffentlichen Interesse aufgedeckt oder dokumentiert werden (Erw L). Das EP erachtet den Schutz von Hinweisgebern umso dringlicher als die von ihm selbst und dem Rat beschlossene RL 2017/2055 die Rechte der Hinweisgeber einschränkt und Personen von der Meldung von Misständen abhalten kann (Erw R). Es bedauert, „dass die Kommission es bislang versäumt hat, Legislativvorschläge zur Schaffung eines Mindestschutzes für europäische Hinweisgeber vorzulegen (1). Das EP „fordert die Kommission mit Nachdruck auf, unverzüglich einen

[88] EP (Europäisches Parlament) Entschließung des Europäischen Parlaments vom 14. Februar 2017 zur Rolle von Informanten beim Schutz der finanziellen Interessen der EU(EP 2016/2055/INI)

Legislativvorschlag vorzulegen, der ein wirksames und umfassendes europäisches Schutzprogramm für Hinweisgeber vorsieht, das auch Mechanismen für Unternehmen, öffentliche Einrichtungen und gemeinnützige Organisationen umfasst (2). Ebenso fordert das EP die Mitgliedsstaaten auf „wirksame Maßnahmen zur Bekämpfung der Korruption" durchzusetzen und internationale Normen und Leitlinien zum Schutz von Informanten in nationales Recht umzusetzen (7).

### 4.4. Europäische Kommission - Konsultationsverfahren und zweiseitiges Meldeprogramm

Die Europäische Kommission hat 2017 ein „zweiseitiges anonymes *Whistleblower* - Programm für Kartellverstöße" vorgestellt. Mit diesem können Einzelpersonen anonym das Vorgehen der Kommission gegen Kartelle und andere wettbewerbswidrige Praktiken unterstützen. Zu diesen Praktiken gehören Preisabsprachen ebenso wie der ungerechtfertigte Ausschluss von Wettbewerbsteilnehmern. Das neue Tool macht es möglich Informationen weiterzugeben, dabei selbst aber anonym zu bleiben. Diese Informationen können dazu beitragen, dass die Kommission mit ihren Ermittlungen rasch und effizient zum Ziel kommt – „zum Wohl der Verbraucher und zum Wohl der Wirtschaft in der EU insgesamt".[89] Das zweiseitige Programm, das die Kommission als Ergänzung des Kronzeugenprogramms in Kartellsachen sieht, ermöglicht auf der einen Seite den Hinweisgebern anonym zu bleiben, auf der anderen Seite der Kommission unklare und unvollständige Meldungen zu hinterfragen und eine Ergänzung zu veranlassen.[90] Parallel zur Einführung des neuen anonymen Meldeprogrammes für Kartellverstöße hat die Europäische Kommission ein „öffentliches Konsultationsverfahren zum Schutz für *Whistleblower*" eingerichtet. Bis 29. Mai 2017 wurden öffentlichen Behörden, Richtern, Staatanwälten. Bürgerbeauftragten, EU Institutionen, privaten Unternehmen, internationalen Organisationen, Berufs- und Wirtschaftsverbänden, Gewerkschaften, Journalisten, Medienvertretern, Vertretern der Zivilgesellschaft, Universitäten und der allgemeinen Öffentlichkeit Gelegenheit geboten zum *Whistleblower – Schutz* Stellungnahmen abzugeben, die es der Kommission erleichtern sollen der Aufforderung des Europäischen Parlaments nachzukommen und diesbezügliche Legislativvorschläge vorzulegen.[91]

## 5. Österreichischer Ist-Zustand und weitere Entwicklungen

Grundsätzlich nimmt in der österreichischen Rechtsordnung *Whistleblowing* noch keinen besonderen Raum ein. Während die meisten internationalen und europäischen Vorschläge und Lösungsansätze ein Gleichgewicht zwischen der Wahrung der Rechte der Aufdecker und der Beschuldigten als Zielvorstellung erkennen lassen, gehen Überlegungen zur Schaffung finanzieller Anreize, wie im US *Dodd Frank Act* nach Meinung des Verfassers in die falsche Richtung. Geschütztes *Whistleblowing* sollte es nur dann geben, wenn dafür lautere Motive erkennbar sind und das Streben nach ausgelobten Geldprämien scheint nicht als Qualifikation für lautere Motive geeignet zu sein. In diesem Zusammenhang scheint auch der Ankauf von unrechtmäßig erworbenen, also gestohlenen Daten zur Aufdeckung von Steuerhinterziehung durch Behörden nicht nur moralisch bedenklich, sondern allenfalls auch strafrechtlich fragwürdig.

[89] Vestager Margrethe, Kommission startet neues Instrument für anonymes Whistleblowing, Europäische Kommission – Pressemitteilung, 16. März 2017, http://europa.eu/rapid/press-release-IP-17-59l-de.html

[90] Vgl. Batge Fabian, EU Kommission: Neues zweiseitiges Whistleblower – Programm für Kartellverstöße, https://noerr.com.de/newsroom/News/eu-kommission-neues-zweiseitiges-whistleblower-programm

[91] Europäische Kommission – Vertretung in Deutschland, Schutz für Whistleblower – Ihre Meinung ist gefragt, https://ec.europa.eu/germany/news/schutz-für-whistleblower-ihre-meinung-ist-gefragt.de

Im österreichischen Strafgesetzbuch (StGB)[92] gibt es eine Strafbestimmung für Hehlerei, in der es heißt: „Wer den Täter einer mit Strafe bedrohten Handlung gegen fremdes Vermögen nach der Tat dabei unterstützt, eine Sache, die dieser durch sie erlangt hat, zu verheimlichen oder zu verwerten ist zu bestrafen. (§164 /1 StGB). Ebenso ist zu bestrafen, wer eine solche Sache kauft, sonst an sich bringt oder einem Dritten verschafft (§ 164/2 StGB).

## 5.1. Allgemeine Grenzen für Whistleblowing im derzeit geltenden Recht

Generell besteht in der Österreichischen Rechtsordnung keine Anzeigepflicht für jedermann, wohl aber ein ausdrückliches Anzeigerecht (§ 80 StPO). Eine Anzeigepflicht besteht allerdings dann, wenn durch die Anzeige eine Straftat verhindert werden kann (StGB § 286). Für Behörden und öffentliche Dienststellen, denen der Verdacht einer Straftat bekannt wird, die ihren gesetzmäßigen Wirkungsbereich betrifft, besteht sehr wohl eine Anzeigepflicht an Staatsanwaltschaft oder Polizei (§ 78/1 StPO). Diese Anzeigepflicht besteht allerdings nicht wenn die Anzeige eine amtliche Tätigkeit beeinträchtigen würde, deren Wirksamkeit eines persönlichen Vertrauensverhältnisses bedarf (§ 78/2 StPO). Für alle Personen, die Geschäfte beruflich mit Finanzinstrumenten tätigen, besteht über Transaktionen die ein Insidergeschäft oder eine Markttransaktion darstellen eine Anzeigepflicht an die FMA (Finanzmarktaufsichtsbehörde) (BörseG §48d/9).[93] Im § 48d/10 BörseG wird ein Schutz für Anzeigende „im guten Glauben" statuiert. Eine Verpflichtung zur Anzeige an Kriminalpolizei oder Staatsanwaltschaft besteht für Behörden und öffentliche Dienststellen, wenn ihnen der Verdacht einer Straftat bekannt wird, die ihren gesetzmäßigen Wirkungsbereich betrifft. Diese Anzeigepflicht besteht nicht, wenn eine amtliche Tätigkeit beeinträchtigt würde, deren Wirksamkeit eines persönlichen Vertrauensverhältnisses bedarf, wenn hinreichende Gründe zur Annahme vorliegen, dass die Strafbarkeit durch schadenbereinigende Tätigkeit binnen kurzem beseitigt wird. Die Behörde hat alles zu unternehmen was zum Schutz der Opfer oder anderer Personen notwendig ist (§ 78 StPO).

Sieht man *Whistleblowing* stärker in Richtung der Deutung als Verrat ist auf den Straftatbestand des Hochverrates zu verweisen, der es unter Strafe stellt die Verfassung der Republik oder eines der Bundesländer mit Gewaltandrohung oder Gewalt zu ändern oder ein zur Republik gehörendes Gebiet abzutrennen (§ 2442 StGB). Der Landesverrat mit dem Verrat von Staatsgeheimnissen ist nach § 252 StGB zu bestrafen. Grenzen für *Whistleblowing* finden sich im Schutz des Versicherungsgeheimnisses (§ 321 VAG),[94] des Bankgeheimnisses (§ 38/BWG)[95] und im Verbot des Missbrauchs von Insiderinformationen (§ 48b Börse G). Die Verletzung des Berufsgeheimnisses fällt generell unter § 122 StGB, die des Amtsgeheimnisses unter § 310 StGB. Zu beachten ist hier auch der Missbrauch der Amtsgewalt (§ 302 StGB) und das Verbot der Veröffentlichung bestimmter Inhalte von Gerichts- und Verwaltungsverfahren (§ 301 StGB). Eine besondere Verschwiegenheitspflicht besteht für Vorstandsmitglieder einer Aktiengesellschaft (§ 84/1 AktG).[96] Demnach haben sie über vertrauliche Angelegenheiten Stillschweigen zu bewahren. Diese generelle Vertraulichkeitsverpflichtung wird etwa durch die Berichtspflichten an den Aufsichtsrat § 81/1 AktG durchbrochen. Weiterhin sind Vortäuschen einer mit Strafe bedrohter Handlung (298 StGB), Verleumdung (§ 297 StGB), gefährliche Drohung (§ 74/5, § 107 StGB), Nötigung (§ 105, § 106 StGB), Erpressung (§§ 144, 145 StGB), üble Nachrede (§ 111 StGB), Vorwurf einer

[92] Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch – StGB) BGBl 60/1974 idF bis BGBl I 25/2013

[93] Bundesgesetz vom 8. November 1989 über die Wertpapier- und allgemeine Warenbörsen und über Änderungen des Börsensensale – Gesetz 1949 und der Börsegesetz Novelle 1903 (Börsegesetz 1989 – Börse G) BGBl 555/1989 idF bis BGBl i 70/2013

[94] Bundesgesetz über den Betrieb und die Beaufsichtigung der Vertragsversicherung (Versicherungsaufsichtsgesetz 2016 – VAG) BGBlI 34/2015 idF BGBl I 107/2017

[95] Bundesgesetz über das Bankwesen (Bankwesengesetz – BWG) BGBl 532/1993 idF bis BGBl I 70/2013

[96] Bundesgesetz über Aktien (Aktiengesetz – AktG) BGBl 98/1965 idF bis BGBl 135/2012

strafbaren Handlung (§ 113 StGB) und Beleidigung (§ 115 StGB) und Kreditschädigung (§ 152 StGB) zu beachten. Unter Strafe stehen die Verletzung des Briefgeheimnisses (§ 118 StGB), das Telekommunikationsgeheimnis (§ 119 StGB), der widerrechtliche Zugriff auf Computersysteme (§ 118a StGB), das missbräuchliche Abfangen von Daten (§ 119a StGB), der Missbrauch von Tonanlagen (§ 120 StGB) und das Auskundschaften von Betriebsgeheimnissen (§ 123 StGB). Betriebsratsmitglieder unterliegen einer generellen Verschwiegenheitspflicht gemäß § 115/4 ArbVG.[97] Sie haben „über alle in Ausübung ihres Amts bekanntgewordenen Geschäfts- und Betriebsgeheimnisse, insbesondere über die ihnen als geheim bezeichneten technischen Einrichtungen, Verfahren und Eigentümlichkeiten des Betriebes Verschwiegenheit zu bewahren". Es hat aber eine Interessenabwägung zwischen den Interessen des Arbeitgebers und den vom Betriebsrat vertretenen Interessen der Arbeitnehmer vorzugehen.[98] Informationen über andere Arbeitnehmer, die dem Betriebsrat im Rahmen seiner Tätigkeit bekannt geworden sind, insbesondere auch im Zuge seiner Mitwirkung in personellen Angelegenheiten und ihrem Inhalt nach einer vertraulichen Behandlung bedürfen, dürfen nicht Preis gegeben werden (§ 115/4 S 2 ArbVG). Das Allgemeine Bürgerliche Gesetzbuch (ABGB § 1339)[99] gewährt Schadenersatz bei Gewinnentgang durch Ehrenbeleidigung. Eine vertrauliche Anzeige an eine Behörde, die zur vertraulichen Behandlung und gewissenhaften Nachprüfung verpflichtet ist, die im Interesse der Allgemeinheit erfolgt, ist nicht schlechthin verpönt und rechtswidrig, auch wenn sich die Tatsachenmitteilung hinterher als falsch herausstellt, es sei denn der Anzeigende handelt wider besseres Wissen.[100]

## 5.2. Arbeitsrechtliche Grenzen

Der Arbeitgeber ist gemäß § 72 / 1 Angestelltengesetz[101] berechtigt eine fristlose Entlassung eines Arbeitnehmers auszusprechen, wenn er unter anderem „im Dienst untreu ist" oder „er sich einer Handlung schuldig macht, die ihm des Vertrauens des Dienstgebers unwürdig erscheinen lässt" (§ 27/1 AngG) oder er sich einer „erheblichen Ehrverletzung" des Dienstgebers, anderer Mitarbeiter oder Angehöriger des Dienstgebers schuldig macht (§ 27 / 6 AngG). Ein Angestellter, der die Verschwiegenheitspflicht verletzt, kann wegen Untreue im Dienst, aber auch wegen Vertrauensunwürdigkeit nach § 27 Z 1 AngG entlassen werden. Der hier festgelegte Entlassungsgrund geht über den einfachen Verrat von Geschäfts- und Betriebsgeheimnissen wie dem Entlassungsgrund[102] nach § 82 lit e 1 GewO hinaus. „Bei der Verletzung der arbeitsrechtlichen Verschwiegenheitspflicht muss nicht unbedingt eine Tatsache verraten werden, die nur dem Arbeitgeber und seine Angestellten bekannt ist. Es reichen kredit- und rufschädigende Äußerungen beziehungsweise Mitteilungen von Informationen, die dem Adressaten bereist bekannt waren, um eine Verletzung der aus der Treuepflicht erwachsenden Identifikation mit den Interessen des Arbeitsgebers darstellen".[104] Um der Verschwiegenheitspflicht nachkommen zu können, muss für den Arbeitnehmer erkennbar sein, welche Tatsachen dem Geheimnisschutz unterliegen, also unternehmensbezogene Tatsachen, die nicht allgemein bekannt sind, ein subjektiver Geheimhaltungswille und ein objektiv bestimmbares Geheimhaltungsinteresse.Die Rechtsprechung beurteilt allerdings die Treuepflicht des Arbeitnehmers gegenüber dem Arbeitgeber als weniger schwerwiegend wie die [moralische] Pflicht zur Anzeige gegen die Allgemeinheit, sofern die Anzeige nicht aus „ver-

[97] Bundesgesetz vom 14. Dezember 1973 betreffend die Arbeitsverfassung (Arbeitsverfassungsgesetz – ArbVG) BGBl 22/1974 idF I 71/2013

[98] Vgl Aschauer a.a.O. FN 21

[99] Allgemeines bürgerliches Gesetzbuch für die gesamten deutschen Erbländer der Österreichischen Monarchie (Allgemeines Bürgerliches Gesetzbuch – ABGB) JGS 946/1811 idF bis BGBl I 50/2013

[100] Vgl. Oberster Gerichtshof (OGH) 6 Ob 2133/96m vom 1.10.1996 und 1 Ob 658/83 vom 31.8.1983 zu § 1330 ABGB

[101] Bundesgesetz vom 11. Mai 1921 über den Dienstvertrag der Privatangestellten (Angestelltengesetz – AngG) BGBl 292/1921 idF bis BGBl I 58/2010

[102] Gewerbeordnung 1994 (GewO) BGBl 194/1994 idF bis BGBl I85/2012

[103] Aschauer a.a.O FN 21 57 f

[104] Vgl. Aschauer,s. FN 21 S 59

leumderischen Gründen“ erfolgt. Voraussetzungen für legitimes *Whistleblowing* ist vorerst das Vorliegen einer Handlung des Arbeitgebers gegen das Gesetz oder gegen geschützte Interessen des Arbeitnehmers. Weiterhin ist das Vorliegen eines ernsthaft begründeten Verdachtes erforderlich und die Anzeige darf nicht aus verleumderischen Gründen erfolgen. Die Interessen des Arbeitgebers an Geheimhaltung und des Arbeitnehmers an Aufklärung sind abzuwägen und die Vorgangsweise des Arbeitnehmers muss die schonendste sei. Das bedeutet, dass der Arbeitnehmer wohl vorerst interne Anlaufstellen prüfen muss, bevor er externe wählt. Dabei ist vorerst die zur Geheimhaltung und objektiven Prüfung verpflichtete Behörde zu wählen und erst in letzter Konsequenz die Öffentlichkeit. Das Aufzeigen von Missständen wird als Staatsbürgerpflicht gesehen und scheint grundsätzlich höherwertig als die arbeitsrechtliche Treupflicht.[105]

## 5.3. Datenschutz und Whistleblower Meldesysteme

Wie bereits dargestellt trat die EU - Datenschutzgrundverordnung (DSGVO) als unmittelbar in den Mitgliedsstaaten anzuwendendes Recht in Österreich am 25.5.2018 in Kraft. Das bisherige Datenschutzgesetz2000 (DSG 2000)[106] bleibt parallel dazu bestehen, allerdings in der Fassung des Datenschutz Anpassungsgesetzes 2018.[107] Der als Verfassungsbestimmung ausgeprägt § 1/1 DSG2000 ist weiterhin gültig und besagt, dass jedermann in Hinblick auf die Achtung seines Privat- und Familienlebens Anspruch auf die Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Die DSGVO spricht allerdings von den Grundrechten natürlicher Personen zum Schutz persönlicher Daten (DSGVO Art. 2). Eine Auseinandersetzung mit den Datenschutzbestimmungen würde auch nur ansatzweise den Rahmen dieses Beitrages deutlich sprengen. Es soll nur darauf verwiesen werden, dass der Begriff eines „Verantwortlichem“ eingeführt wird, unter dem eine natürliche oder juristische Person oder Behörde verstanden wird, die über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet (DSGVO Art 4/7). Die personenbezogenen Daten müssen in einer Weise verarbeitet werden, die ihre angemessene Sicherheit gewährleistet einschließlich der Sicherheit vor unbefugter und unrechtmäßiger Verarbeitung und Zerstörung, Integrität und Vertraulichkeit (DSGVO Art. 5/1/f). Der Verantwortliche ist für die Einhaltung der Bestimmungen verantwortlich und muss ihre Einhaltung nachweisen können (Art 5/2). Alle Personen, die wegen Verstößen gegen die DSGVO einen materiellen oder immateriellen Schaden erleiden, haben Anspruch gegenüber dem Verantwortlichen (DSGVO Art 82) und der Verantwortliche ist auch von empfindlichen Geldbußen bedroht (DSGVO Art. 83). Das Datenschutzanpassungsgesetz 2018 legt im § 9 DSG unter der Überschrift „Freiheit der Meinungsäußerung und Informationsfreiheit“ fest, dass die DSGVO in bestimmten Teilen nicht zur Anwendung kommt, insoweit es dafür nötig ist das Recht auf freie Meinungsäußerung und Informationsfreiheit in Einklang mit dem Recht auf den Schutz personenbezogener Daten zu bringen (§ 9 DSG idF 2018). Hinzuweisen ist auf die Strafdrohungen für das widerrechtliche Verschaffen des Zuganges zu persönlichen Daten und für Verletzung des Datengeheimnisses (§§ 62, 83 DSG idF 2018). In diesem Zusammenhang ist auf die bisweilen skurrile Umgangsweise von Politikern mit dem Datenschutz hinzuweisen, wobei die Problematik der parlamentarischen Immunität im nächsten Unterkapitel noch behandelt wird. Auf der einen Seite wird Transparenz in der und von der Verwaltung verlangt solange sich eine Partei in einer Gebietskörperschaft in Opposition befindet, auf der anderen Seite verbirgt man sich in einer anderen Gebietskörperschaft in der gleichen Angelegenheit hinter dem Datenschutz, wenn man die Regierungsbank drückt.[108]

---

[105] Im Wesentlich nach Aschauer,s. FN 21 S 70

[106] Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz – DSG) BGbl I 165/1999 idF bis BGBl I 57/2013

[107] Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird(Datenschutzanpassungsgesetz 2000 BGBl I 120/2017 vom 31. Juli 2017

[108] Vgl. See Manfred, Transparenzinitiative der Grünen mit Schönheitsfehlern in Wien, Die Presse 16.5.2013 9

Bei Einrichtung von *Whistleblower* Systemen sind sowohl ein arbeitsrechtlicher als auch ein datenschutzrechtlicher Aspekt zu beachten. Besteht ein Betriebsrat wird die Eirichtung der *Whistleblower* Hotline den Abschluss einer Betriebsvereinbarung erzwingen, wenn die Vorgaben derartige Eingriffe in das Persönlichkeitsrecht des Arbeitnehmers darstellen, dass dadurch die Menschenwürde berührt wird (§ 96/1/3 ArbVG). Besteht kein Betriebsrat kann die Zustimmung des einzelnen Arbeitnehmers erforderlich sein (§ 10 AVRAG).[109] „Das Recht auf Datenschutz der Arbeitnehmer kann durch Wahrung überwiegender berechtigter Interessen des Arbeitgebers durchbrochen werden. Wenn eine Offenbarungspflicht bestimmte Vorgänge oder Daten besteht, so soll eine damit zusammenhängende Datenermittlung zulässig sein. Dies gilt auch, wenn der Arbeitgeber die Information von einem anderen als dem betroffenen Arbeitnehmer erhält und personenbezogene Daten automationsunterstützt verarbeitet und übermittelt werden."[110] Die Systeme sind gemäß § 17 ff DSG bei der Datenschutzkommission (DSK) zu melden, die im Rahmen der Vorabkontrolle Auflagen erteilen kann für die Registrierung im DVR (Datenverarbeitungsregister). Wird ausschließlich eine natürliche Person, wie beispielsweise ein Ombudsmann, mit der Entgegennahme von Hinweisen betraut, ist eine Meldung beim DVR nicht erforderlich. Die DSK erteilt die Genehmigung zur Übermittlung von Arbeitnehmerdaten an ausländische Konzernmütter um ein SOX-fähiges *Whistleblowersystem* einzurichten nur unter der Voraussetzung eines zweistufigen Whistleblower Verfahrens, das bedeutet, dass nicht SOX notwendige Daten retourniert werden. Hier kann aber trotzdem ein Widerspruch zum österreichischen Arbeitsverfassungsrecht vorliegen.[111]

## 5.4. Meldeverfahre nach dem Börsegesetz

Arbeitgeber, die in Bereichen tätig sind, welche in § 2 Finanzmarktbehördengesetz[112] genannt sind, also im Wesentlichen Banken, Sparkassen, Bausparkassen, Versicherungen, Pensionskassen, Kapitalanlagegesellschaften und Wertpapierfirmen haben nach § 48h BörseG[113] über angemessene Verfahren zu verfügen, die es ihren Mitarbeitern unter Wahrung der Vertraulichkeit der Identität ermöglichen, betriebsinterne Verstöße gegen die Bestimmungen dieses Bundesgesetzes, gegen auf Grund dieser Bestimmungen erlassenen Verordnungen und Bescheide oder gegen die Verordnung EU 596/2014 und aufgrund dieser Verordnung erlassene Rechtsakte an eine geeignete Stelle zu melden. Arbeitnehmer, die Verstöße im Rahmen solcher betrieblicher Verfahren der FMA melden, dürfen deswegen nicht benachteiligt werden insbesondere beim Entgelt, beruflichem Aufstieg, Weiterbildung, Versetzung und der Beendigung des Dienstverhältnisses. Sie dürfen auch strafrechtlich nicht zur Verantwortung gezogen werden. Die Österreichische Nationalbank (ÖNB) hat in teilweiser Umsetzung des „*Ethical Framework*" des „Europäischen Systems der Zentralbanken - ESZB) ein anonymes Meldesystem eingerichtet, in dem Verstöße gegen Strafgesetze oder über rufschädigendes Verhalten von ÖNB Mitarbeitern gemeldet werden können.[114] Selbstverständlich besteht auch eine Hotline der FMA, bei der Verstöße anonym gemeldet werden können. Sie bedient sich ebenfalls des BKS Systems.[114]

[109] Arbeitsvertragsrechts – Anpassungsgesetz (AVRAG) BGBl 459/1993 idF bis BGBl I 71/2013

[110] Aschauer s. FN 21 S 67

[111] Vgl. Aschauer s. FN 21 S 268

[112] Bundesgesetz über die Errichtung und Organisation der Finanzmarktaufsichtsbehörde (Finanzmarktaufsichtsbehördengesetz – FMABG) BGBl I 97/2001 idF I 107/2oo1)

[113] Bundesgesetz vom 8. November 1989 über die Wertpapier- und allgemeinen Warenbörsen [……..] BGBl 555/1989 idF BGBl I 118/2016

[114] Vgl ÖNB Österreichische Nationalbank , Sie haben Kenntnis von Verstößen [….] https://www.bkms-system.net/bkwebanon/repor/clientInfo[.....]

[115] FMA Hotline

## 5.5. Deutscher Corporate Governance Kodex

Auf die Verpflichtungen des *Sarbanes Oxley Act (SOX)* zur Einrichtung eines eigenen organisationsinternen *Whistleblower* Prozederes braucht an dieser Stelle nicht näher eingegangen werden, da dies bereits im Kapitel 3.2 behandelt wurde. An dieser Stelle soll der deutsche Corporate Governance Kodex[116] erwähnt werden. Er richtet sich an deutsche Unternehmen, deren begebbare Wertpapiere an Börsen notiert sind deren etliche in Österreich tätig sind. Die Verbindlichkeit dieses Kodex leitet sich aus dem deutschen Aktiengesetz ab (DAktG 3 161 Abs 1 2. Satz).[117] Nach dem DCGK soll der Vorstand dafür sorgen, dass Beschäftigten auf geeignete Weise die Möglichkeit eingeräumt wird, geschützt Hinweise auf Rechtsverstöße im Unternehmen zu geben, wobei auch Dritten die Möglichkeit gegeben werden soll. Die österreichische Datenschutzbehörde sieht in diesem Zusammenhang unter einem Hinweisgebersystem eine spezielle Möglichkeit der Kommunikation innerhalb eines Konzerns, mit deren Hilfe Mitarbeiter, Kunden und Lieferanten unter Umgehung der normalen Hierarchie einen Missstand an die Konzernspitze melden können. Damit soll es möglich sein derartige Missstände an untätigen oder möglichweise korrupten Konzernorganen vorbei zu melden. In der Praxis werden die Mitarbeiter in einem „*Code of Conduct*“ oder „*Code of Ethics*“ aufgefordert Missstände zu melden. Die Ermittlung und Übermittlung von Daten stützt sich auf das überwiegend berechtigte Interesse. Die österreichische Datenschutzbehörde sieht das überwiegend berechtigte Interesse der Konzernmutter nur auf maßgebliche Verstöße leitender Mitarbeiter beschränkt. Ein überwiegend berechtigtes Interesse der Konzernspitze an der Kenntnis aller Verstöße ist aber nicht anzunehmen.[118]

## 5.6. Parlamentarische Immunität und Redaktionsgeheimnis

Externes Whistleblowing ist auch unter Berücksichtigung eines allfälligen politisch motivierten Missbrauches solcher Hinweise zu sehen. Grund ist die privilegierte Stellung der gewählten Vertreter des Volkes, die sich selbst gegenüber den von ihnen Vertretenen in eine bedeutend komfortablere Situation setzen, was den Umgang mit den von ihnen für alle anderen beschlossenen Gesetze betrifft. So dürfen Abgeordnete zum Nationalrat wegen der von ihnen in dieser Eigenschaft gemachten mündlichen oder schriftlichen Äußerungen nur vom Nationalrat verantwortlich gemacht werden (Art 57/1 BVG).[119] Hausdurchsuchungen bei Mitgliedern des Nationalrates bedürfen der Zustimmung des Nationalrates (Art. 57/2 B-VG). Mitglieder des Nationalrates dürfen ohne Zustimmung des Nationalrates wegen strafbarer Handlungen nur verfolgt werden, wenn diese offensichtlich nicht im Zusammenhang mit der politischen Tätigkeit als Abgeordneter stehen. Verlangt der Abgeordnete eine Entscheidung des Nationalrates über diese Frage hat eine Verfolgungshandlung bis zur Entscheidung zu unterbleiben. Mitglieder des Bundesrates unterliegen derselben Immunität wie die Mitglieder des Landtages, der sie entsandt hat (Art 57/3 B-VG). Die Immunität der Abgeordneten zum Landtag ist der der Angeordneten zum Nationalrat sinngemäß nachempfunden (Art. 96 B-VG) Die Berichterstattung aus den gesetzgebenden Körperschaften ist immunisiert soweit sie den Inhalt der Sitzung wiedergibt. Ob das, was dort geredet wurde, wahr ist hat auf die Immunisierung keinen Einfluss. (§ 30 Mediengesetz). Was nun den Umgang mit *Whistleblowern* betrifft hat diese Immunisierung fatale Folgen, insbesondere für den möglicherweise fälschlich Beschuldigten. Die Veröffentlichung von Vernehmungsprotokollen oder von sensiblen personenbezogenen Akteninhalten im gerichtlichen oder Verwaltungsverfahren ist verboten. Derjenige, der

[116] Regierungskommission Deutscher Corporate Governance Kodex , Deutscher Corporate Governance Kodex idF vom 7. Februar 2017, www. Dcgk/Usercontent/de/download/kodex/170424-kodex-mark-up-finale-version-D-pdf

[117] Bundesrepublik Deutschland, Gesetz vom 6.9.1965 (Aktiengesetz DAktG) dBGBl I S 1089 idF Gesetz vom 17.7.2017 dBGBl I S 2446

[118] Vgl Lechner Georg, Datenschutzbehörde, Hinweisgebersysteme, Österreichische Datenschutzbehörde, dsb@dsb.gv.at

[119] Bundesgesetz vom 8. November 1989 über die Wertpapier- und allgemeinen Warenbörsen [……..] BGBl 555/1989 idF BGBl I 118/2016

sie weiterleitet, macht sich strafbar und das zurecht (Amtsverschwiegenheit, Amtsmissbrauch §§ 301, 302 StGB). Geht die Information allerdings an einen Abgeordneten und dieser zitiert genüsslich während einer Sitzung daraus oder legt sie einer parlamentarischen Anfrage bei, so kann jedes Medium darüber berichten. Ob der so Beschuldigte, der im Gegensatz zum Abgeordneten in der gesetzgebenden Körperschaft nicht reden darf, im Nachhinein freigesprochen oder vielleicht nicht einmal angeklagt wird, ist unerheblich und ohne Konsequenz. Der Ruf, die Karriere ja selbst die persönlichen Lebensumstände können nachhaltig ge- oder sogar zerstört sein. Der *Whistleblower,* gleichgültig ob er im guten oder schlechten Glauben gehandelt hat, gleichgültig ob seine Botschaft wahr oder erfunden war, bleibt ungeschoren.

Medieninhaber, Herausgeber, Medienmitarbeiter und Arbeitnehmer eines Medienunternehmens haben das Recht in einem Strafverfahren oder einem sonstigen Verfahren vor Gericht oder in einem Verwaltungsverfahren das Recht als Zeuge die Beantwortung von Fragen zu verweigern, die die Person des Verfassers, Einsenders oder Gewährsmannes von Beiträgen und Unterlagen oder von Mitteilungen betreffen, die ihnen in Hinblick auf die Tätigkeit in einem Medienunternehmen gemacht wurden (§31/1 Medien G).[120] Dieses Recht darf auch nicht durch die Beschlagnahme oder den Auftrag zur Herausgabe von Schriftstücken, Druckwerken, Tonträgern oder Datenträgern umgangen werden (§ 31/2 MedienG). Dieses sogenannte „Redaktionsgeheimnis" bedeutet, dass etwa der durch Amtsmissbrauch hervorgerufene Bruch der Amtsverschwiegenheit, also ein eindeutiger ernsthafter strafbarer Tatbestand, nicht geahndet werden kann.

## 5.7. Kronzeugenregelung und Justiz Hotline

In der Novelle 2005 zum Wettbewerbsgesetz[121] wurde im § 11 Abs. 3 der Bundeswettbewerbsbehörde (BWB) die Möglichkeit eingeräumt, für die Mitwirkung eines Unternehmens an der Aufdeckung eines Kartells von der Beantragung einer Geldbuße Abstand zu nehmen oder, wenn der Sachverhalt der BWB bereits bekannt ist eine niedrigere Geldbuße zu beantragen.[122] Mit der sogenannten „großen Kronzeugenregelung" des § 209a der Strafprozessordnung (StPO)[123] wird die bisherige „kleine Kronzeugenregelung" des § 41a StGB, die kaum praktische Bedeutung erlangt hat, ergänzt und ausgeweitet. Mit der Regelung nach § 41a StGB kann das gesetzliche Mindestmaß für Strafen unterschritten werden wenn ein Täter nach § 277 StGB (Verbrecherisches Komplott zu Mord, Sklavenhandel; Raub etc.), § 278a (Kriminelle Organisation) und § 278b (Terroristische Vereinigung) mit der Staatsanwaltschaft zusammenarbeitet und dazu beiträgt die Gefahr durch diese Vereinigung zu beseitigen oder zu mildern und/oder die Aufklärung der Straftat fördert und/oder zur Ausforschung der Straftäter beiträgt. Gemäß der neuen Kronzeugenregelung kann die Staatsanwaltschaft von einer Strafverfolgung dann absehen, wenn ein Beschuldigter freiwillig sein Wissen über eine Straftat der Behörde bekanntgibt, die noch nicht Gegenstand eines gegen ihn gerichteten Ermittlungsverfahrens ist. Dieses bekanntgegebene Wissen muss die Aufklärung einer Straftat fördern, deren Aufklärung in die Kompetenz der WKStA[124] fällt oder deren Ahndung in die Zuständigkeit eines Schöffen- oder Geschworenengerichtes fällt oder dazu verhelfen, führende Mitglieder einer kriminellen oder terroristischen Organisation auszuforschen. Ein als Kronzeuge Anerkannter geht nicht völlig frei, er hat eine Geldstrafe bis zu 240 Tagsätzen oder gemeinnützige Arbeit zu leisten oder von der Strafverfolgung wird für eine Probezeit Abstand

[120] Bundesgesetz vom 12. Juni 1981 über die Presse und andere publizistische Medien (Medien Gesetz) BGBl 314/1981 idF bis BGBl I 50/2012

[121] Bundesgesetz über die Einrichtung einer Bundeswettbewerbsbehörde (Wettbewerbsgesetz – WettbG) BGBl I 62 /2002 idF bis BGBl I 13/2013

[122] BWB Bundeswettbewerbsbehörde, http://www.bwb.gv.at

[123] Strafprozessordnung 1975 (StPO) BGBl 631/1975 idF bis BGBl I 2/2013

[124] WKStA = Zentrale Staatsanwaltschaft zur Verfolgung von Wirtschaftsstrafsachen und Korruption bei der Oberstaatsanwaltschaft Wien (Wirtschafts- und Korruptionsstaatsanwaltschaft)

genommen.[125] Gerade im Hinblick auf die Verfolgung von Wirtschaftsstrafsachen und Korruption gilt es neue Strategien und Maßnahmen zu entwickeln. Wirtschaftskriminalität und Korruption sind oftmals dadurch geprägt, dass sich die Täter im hohen Maße abschotten und konspirativ handeln. Kriminelle Strukturen können vielfach nur dann aufgebrochen werden, wenn aussagewilligen Beteiligten ein hinreichender Anreiz zur Kooperation mit den Strafverfolgungsbehörden geboten wird." In Ergänzung zur Kronzeugenreglung wird von der WKStA vorerst befristet auf zwei Jahre ein Internet basiertes anonymes Anzeigesystem eingeführt, dass dem Staatsanwalt die Möglichkeit bietet mit einem anonym bleibenden Hinweisgeber zu kommunizieren. Damit besteht die Möglichkeit der Nachfrage beim Hinweisgeber zur Objektivierung des Wertes des Hinweises bei Wahrung der Anonymität, da die Rückverfolgung der IP Adresse ausgeschlossen ist. Über diese Hotline sind Hinweise zu Korruption, Wirtschaftsstrafsachen, Sozialbetrug, Finanzstrafsachen, Bilanz- und Kapitalmarktdelikten und zu Geldwäsche erwünscht.[126] Ein gewisser Whistleblower Schutz ist im Finanzstrafgesetz (FinStrG)[127] § 79/2 durch die Einschränkung der Akteneinsicht im Finanzstrafverfahren gegeben, wenn die Offenlegung eine Schädigung berechtigter Interessen dritter Personen herbeiführen würde.

Der erste „Kronzeuge nach der „neuen" Kronzeugenregelung war der ehemalige Telecom Vorstand Gernot Schieszler, der sich durch seine Zusammenarbeit mit der Staatsanwaltschaft und seine Aussagen im Prozess statt einer Strafe eine „Diversion" von 120 Stunden Sozialarbeit und einer Schadenszahlung von € 300.000 unterziehen durfte. In dem Verfahren ging es auf der einen Seite um unzulässige Parteienfinanzierungen – die Telecom Austria wurde scherzhaft als „Bankomat der Parteien" bezeichnet, auf der anderen Seite um Manipulationen des Aktienkurses, der dem Topmanagement unberechtigte Boni verschaffte.[128] Im Telecom Prozess wurde auch der Lobbyist Peter Hochegger verurteilt. Er zählt auch zu den Angeklagten des während des Abschlusses dieses Beitrags laufenden BUWOG Prozess. Er hat überraschend ein Teilgeständnis abgelegt und einen Teil seiner Mitangeklagten schwer belastet. Offensichtlich fällt er nicht unter die „Kronzeugenregelung" nach § 209, 209a StPO, möglicherweise nach § 41a StGB und kann jedenfalls auf einen „besonderen Milderungsgrund" nach § 34/1 StGB hoffen, der bei „einem reumütigen Geständnis" oder bei einer Aussage die „wesentlich zur Wahrheitsfindung beiträgt" anzuwenden ist.[129]

## 6. Die Rolle der Internen Revision im Whistleblowingprozess

De Interne Revision und ihre Mitarbeiter kommt oft in den Besitz von heiklen Informationen, die von grundlegender Bedeutung für die Organisation sind und bedeutende Konsequenzen nach sich ziehen können. Die Informationen können sich auf Drohungen, Sicherheitsmängel, Verschwendung, illegale Aktivitäten, Betrug, Machtmissbrauch etc. haben.[130] Diese Informationen können auch im Wege von Whistleblowing zur Kenntnis der Internen Revision gelangen. *Richard Chambers*[131] vergleicht die Rolle der Internen Revision im Whistleblowing Prozess mit einem Spiel des American Football. Ein Interner

[125] Vgl. Mirtl Alexander, Straffrei durch neue Kronzeugenregelung, Führende Wirtschaftsanwälte zu aktuellen Themen, www.wirtschaftsanwaelte.at, download 10.5.2013

[126] Justiz. Die Österreichische Justiz. Wirtschafts– und Korruptionsstaatsanwaltschaft. Anonymes Hinweisgebersystem zur Korruptionsbekämpfung, http://justiz.gv.at, download 20.5.2013

[127] Bundesgesetz vom 26. Juli 1985 betreffend das Finanzstrafrecht und das Finanzverfahrensrecht (Finanzstrafgesetz - FinStrG) BGBl 129/1958 idF bis BGBl I 70/2013

[128] Vgl. Sankholkar Ashwien, Der geplünderte Staat und seine Profiteure, Residenz Verlag, Salzburg-Wien 2017 S 35ff

[129] Vgl. Graber Renate, Meischberger zu Hochegger: Fang nicht an zu lügen, 11.1.2018 und BUWOG Prozess: Geheimagent Hochegger und Haiders Gewicht, 25.1.2018, derStandard.at/Wirtschaft

[130] Vgl IIA Institute of Internal Auditors, Practice Advisory 2440-2, Communicating Sensitive Information Within and Outside the Chain of Command 2010

[131] Richard Chambers ist President und CEO des International Institute of Internal Auditors , Salt Lake City

Revisor kann demgemäß am Rande des Spielfeldes sitzen und als Zuschauer das Spiel beobachten, er kann aber auch die Rolle des Schiedsrichters ausüben und neben der Beobachtung des Spieles Regelverstöße aufzeigen. Sie sollen „die Pfeife blasen bevor Schwierigkeiten auftreten".[132] Sieht man die Interne Revision als Schiedsrichter muss berücksichtigt werden, dass ihr selbstverständlich die Sanktionsmöglichkeiten fehlen. Aus der Verantwortung der Internen Revision gegenüber der Organisation und der Rolle des „trusted Advisors" hat sie jeden Verdacht auf Missmanagement, Betrug und Verschwendung in irgendeiner Form dem Topmanagement zur Kenntnis zu bringen. Aus den Ergebnissen der empirischen Untersuchung 2007 ergibt sich, dass offensichtlich der Internen Revision verschiedene Aufgaben mit verschiedener Intensität im Whistleblowing Prozess zugeordnet werden können, dass sie aber im Wesentlichen aus diesem nicht wegzudenken ist. In der nachstehenden Darstellung bedeutet der erste Wert, dass sie die Aufgabe immer durchzuführen hat, der zweite Wert nur unter Umständen und ausnahmsweise. Suche nach Verbesserungen 73,7% (26,2%), Suche nach Schwachstellen 72,2% (27,1%), Beurteilung der Botschaft des Whistleblowers 61,4% (36,3%), Beurteilung der Folgen 56,2% (41,1%) und Beurteilung des Umfeldes 38,7% (61,0%).[133]

## 6.1. IIA - Practice Advisory 2440 – 2[134]

Der „praktische Ratschlag" (Practice Advisory) 2440-2 des IIA beruht auf IIA Standard 2440[135] und hält einleitend fest, dass Interne Revisoren oft in den Besitz von kritischen und/oder sensiblen Informationen kommen, die möglicherweise bedeutsame Konsequenzen für die Organisation haben. Diese Informationen können Enthüllungen, Bedrohungen, Unzuverlässigkeit, Betrug, Verschwendung, Missmanagement, Gefährdung der öffentlichen Gesundheit oder Sicherheit oder sonstiges Fehlverhalten betreffen und die Reputation, das Image, die Wettbewerbsfähigkeit, den Erfolg, die Rentabilität, den Marktwert oder die materiellen oder immateriellen sonstigen Werte der Organisation beeinträchtigen (PA2440-2/1). In dem Augenblick in dem ein Revisionsleiter (Chief Audit Executive) die Information als glaubwürdig, seriös und substantiell erkennt, soll diese Information an die Leitung der Organisation weitergegeben werden, wobei dies vorerst im Wege der hierarchischen Berichtslinie (chain of command) erfolgt. Dieses übliche Vorgehen kann wegen regulatorischer oder gesetzlicher Vorschriften oder „common practice" zu beschleunigen sein (PA 2440-2/2). Ebenso ist auf Standard 2600 im Falle unangebrachter Risikoübernahme zu verweisen (PA 2440-2/3). Das typische Vorgehen innerhalb der chain of command kann aber abseits des Absatz 2 in manchen Situationen zu beschleunigen sein (PA 2440-2/4). Die Weitergabe der Information innerhalb der Organisation, aber außerhalb der chain of command, wird als internes Whistleblowing bezeichnet, außerhalb der Organisation als externes Whistleblowing. Es stürzt den internen Revisor jedenfalls in ein Dilemma einen dieser Wege zu gehen (PA 2440-2/5). Die meisten Whistleblower halten Informationen innerhalb der Organisation, allerdings außerhalb der chain of command, wenn sie Vertrauen in die Unternehmenspolitik und die Mechanismen zur Untersuchung von illegalem oder unangebrachtem Verhalten und zum Ergreifen adäquater Maßnahmen haben. Wenn Personen, die im Besitz von Informationen sind und Vergeltung befürchten oder Zweifel an ordnungsgemäßer Aufklärung oder Sorge haben, dass der Tatbestand vertuscht wird, können sich mit ihren Informationen nach außen wenden, sofern sie Beweise für illegale oder unangebrachte Aktivitäten haben, die die Gesundheit, Sicherheit oder das Wohlbefinden von Angehörigen der Organisation oder der Gesellschaft gefährden können (PA 2440-2/6).

[132] Chambers Richard, Trusted Advisors. Key Attributes of Outstanding Internal Auditors, Internal Audit Foundation Lake Mary 2017 S 13

[133] Vgl. Hauser 2008 s. FN 8 S 258 f

[134] The Institute of Internal Auditors, Practice Advisory 2440-2, Communicating Sensitive Information Within and Outside the Chain of Command, Lake Mary 2010

[135] Internationale Standards für die berufliche Praxis der Internen Revision (deutsche Übersetzung),DIIR-Deutsches Institut für Interne Revision, Institut für Interne Revision Österreich (IIA-Austria), Schweizerischer Verband für Interne Revision (IIA Switzerland), 1.Auflage 2017

## 6.2. Die Interne Revision als unbeteiligter Zuseher

In den meisten Fällen wenden sich internes und externes Whistleblowing nicht an die Interne Revision, sondern direkt an die Spitze der Organisation, die nun ihrerseits die Interne Revision einbinden kann. Ist im festgelegten Whistleblowing Prozess der Internen Revision keine spezielle Rolle zugedacht, sollte unbedingt sichergestellt werden, dass die Interne Revision Whistleblowing Botschaften zur Kenntnis erhält. Ebenso ist es notwendig, dass die Interne Revision das Ergebnis der Untersuchungen von *Whistleblower* Botschaften erhält, die von anderen Einheiten in der Organisation wie Compliance oder HR durchgeführt wurden, da dies für ihre Prüfungen von eminenter Bedeutung sein kann. Wie schon in den Vorbemerkungen zu diesem Abschnitt erwähnt ist einfaches „Wegschauen" für Interne Revisoren mit ihrem Berufsethos nicht vereinbar, gleichgültig was in allfälligen Ordnungen steht. Grundsätzlich ist daran zu erinnern, dass die Interne Revision und ihre Mitarbeiter besonderen Vertraulichkeitsgeboten unterliegen. Daher ist es auch notwendig, dass die Interne Revision nach Möglichkeit die Stellung des *Whistleblowers* erfährt, da aus der Tatsache, dass dieser tätig wurde auch Hinweise auf das Führungsverhalten und das Klima aber auch des IKS in dessen Tätigkeitsbereich bieten kann und der Internen Revision unverzichtbare Informationen für unmittelbare oder spätere Prüfungshandlungen bieten kann.

## 6.3. Interne Revision als definierte Anlaufstelle

Die Interne Revision als definierte Anlaufstelle für *Whistleblowing* etwa innerhalb eines unternehmensinternen *Whistleblowing*-Systems wurde in der österreichischen Versicherungswirtschaft nicht unterstützt. Nur 22 % der Befragungsteilnehmer in der Untersuchung 2007 wollten sie als ständige oder gar ausschließliche Anlaufstelle definiert sehen. Die Interne Revision war aber durchaus als zusätzliche Anlaufstelle von über 2/3 der Teilnehmer akzeptiert und sie gehört auch zu den Anlaufstellen im Unternehmen, die für das Kriterium des „internen *Whistleblowing*" akzeptiert sind. Sehr wohl wird der Internen Revision aber eine Rolle im *Whistleblowing* Prozess zugeordnet. Nur eine verschwindende Minderheit von Teilnehmern, nämlich unter 10%, waren der Meinung, dass *Whistleblowing* ignoriert werden soll und darf.[136] Es ist also davon auszugehen, dass der aus einer *Whistleblower* Botschaft resultierende Prüfauftrag an die Interne Revision entweder vom Vorstand zu erteilen ist oder sich aus einem internen *Whistleblower* Regulativ oder der Revisionsordnung automatisch ergibt. Dieser Prüfauftrag hat das Ziel der Prüfung zu enthalten, wobei sich hier auch durch das Erhebungsergebnis unterstützt vorerst die Auseinandersetzung mit der Mitteilung selbst ergibt. Es ist festzustellen, ob tatsächlich ein Fehlverhalten vorliegt oder ob die Botschaft an sich erfunden ist oder eine böswillige Verleumdung darstellt. Aus der umfassenden Prüfkompetenz der Internen Revision, die sich aus dem Gesetz ergibt, kann diese Verifizierung der Mitteilung auch derart erfolgen, dass nicht nur der eine gemeldete Tatbestand untersucht wird, sondern eine Prüfung der betroffenen Einheit oder besser des betroffenen Prozesses stattfindet. Im Zuge dieser Prüfung ist nach Feststellung des Wahrheitsgehaltes der Mitteilung eine Untersuchung notwendig, ob überhaupt ein Fehlverhalten vorliegt oder ob regelkonform gehandelt wurde. Regelkonformes Handeln muss allerdings nicht immer auch sinnvolles oder richtiges Verhalten sein, sodass die Internen Revision sich generell nicht nur auf den Soll-Ist-Vergleich beschränken kann, sondern auch die Zielvorgabe zu untersuchen hat. Das Ziel jeglicher Tätigkeit der Internen Revision ist es einen Mehrwert für das Unternehmen zu schaffen. Das Erkennen des Fehlers dient nicht als Zweck an sich. Nach dem Erkennen ist der Fehler zu beseitigen und die Folgen des Fehlers sind zu analysieren und es sind allfällige Schadenbegrenzungsmaßnahmen zu empfehlen. Die wesentlichste Aufgabe besteht darin Vorschläge zu unterbreiten, wie das erkannte Fehlverhalten in Zukunft zu vermeiden ist. Dabei ist zu klären ob

[136] Vgl Hauser 2008 s. FN 8 S 254 f

ein kriminelles Einzelverhalten vorliegt oder einfach Unwissenheit, ob der Prozess das Fehlverhalten ermöglicht oder gar begünstigt und wie das Kontrollsystem funktioniert und es derartige Vorkommen zulässt oder sogar begünstigt.

## 6.4. Interne Revision als undefinierte Anlaufstelle

Sieht man von der Einbindung der Internen Revision in das offizielle *Whistleblowing* Prozedere ab, kann die Interne Revision auch Adressat von *Whistleblowing* Botschaften sein. Zum ersten hat jeder Revisionsleiter schon mindestens einmal einen anonymen Brief erhalten, der auf irgendein tatsächliche oder vermeintliches oder erfundenes Fehlverhalten hinweist. Hier hat der Revisionsleiter zu entscheiden, wie er mit dieser Mitteilung umgeht. Zum ersten ist die Entscheidung zu treffen, die Mitteilung zu ignorieren oder weiter zu verfolgen. Besteht im Unternehmen ein formalisiertes *Whistleblower* Prozedere ist zu entscheiden, ob die vorliegende Mitteilung in den formalen Kanal eingebracht wird oder nicht. Im Regelfall sollte auch die Interne Revision diese Kanäle zu nutzen.

Ist kein spezielles Prozedere definiert, hat die Interne Revision eine Vorprüfung durchzuführen ob die Mitteilung einfach der Linienorganisation oder einem definierten Beschwerdemanagement übergeben wird oder von sich aus gehandelt werden soll. Die Interne Revision wird zu prüfen haben ob ein Tatbestand vorliegt, der der Compliance Organisation unverzüglich zu überantworten ist oder und ob es zielführend ist das Top Management zu informieren.

Besteht der Verdacht auf eine Straftat, wird die Interne Revision von sich aus handeln müssen und unverzüglich das Top Management einschalten. Es kann allerdings eine Situation geben, wo die Einschaltung des Top Management aus verschiedenen Gründen, auf die im Abschnitt „Interne Revision als *Whistleblower*“ noch eingegangen wird, kontraproduktiv ist. In manchen Revisionsordnungen findet sich eine Ermächtigung des Leiters der Internen Revision von sich aus eine Prüfung anzuordnen und erst nachträglich das Top Management zu informieren. Besteht eine solche Ermächtigung wird der Revisionsleiter doppelt abzuwägen haben, ob die Mitteilung des *Whistleblowers* ausreicht eine derartige Prüfung einzuleiten. Gibt die Interne Revision eine erhaltene Information ohne eigene Prüfung an eine andere Stelle wie etwa Compliance weiter, sollte sie den Vorfall allerdings in Evidenz nehmen und den betroffenen Prozess oder die betroffene Einheit jedenfalls anlässlich der nächsten Prüfung damit konfrontieren. Wesentlich ist, dass die Interne Revision verpflichtet ist, „umsichtig und interessenwahrend“ mit den im Verlauf der Tätigkeit erhaltenen Informationen umzugehen. Informationen dürfen nicht zum persönlichen Vorteil oder zu ungesetzlichen Zwecken verwendet werden, ebenso darf die Verwendung der Informationen den legitimen und ethischen Zielen der Organisation nicht schaden.[137] Sie haben ein Höchstmaß an Objektivität an den Tag zu legen und müssen ihre Aufgaben korrekt, sorgfältig und verantwortungsbewusst wahrnehmen.[138] Daraus resultiert auch, dass die Rechte der Beschuldigten ebenso zu wahren sind wie die der Hinweisgeber.

Eine spezielle Form des *Whistleblowings,* mit der die Interne Revision konfrontiert wird, ist das unbewusste oder beiläufige *Whistleblowing.* Im Zuge der Revisionsarbeit werden vielerlei Informationen gesammelt. Die Informationserzielung ist keineswegs auf Unterlagen beschränkt, sondern erfolgt oftmals im persönlichen Gespräch mit Mitarbeitern in den geprüften Einheiten oder Prozessen. Gelingt es dem Revisor eine Vertrauensbasis zu dem Interviewten aufzubauen, wird dieser bisweilen zum wissentlichen oder unbewussten *Whistleblower*, indem er auf seiner Meinung nach unbefriedigende Zustände hinweist. In diesen Fällen ist ein besonderes Fingerspitzengefühl des Prüfers gefragt, der tunlichst die erhaltene Botschaft auf ihren Wahrheitsgehalt untersuchen

[137] Vgl. Verhaltensregeln zum Ethikkodex in Internationale Standards 2017 S 13

[138] Vgl. Ethikkodex in Internationale Standards S 11

muss, ohne die Vertrauensbasis zum Informanten zu gefährden, und daher vorsichtig mit der Information umzugehen hat. Auf der einen Seite verpflichten die IIA Standards für die Interne Revision die Revisoren die für die Begründung der Schlussfolgerungen und Revisionsergebnisse relevanten Informationen aufzuzeichnen.[139] Dabei sind ausreichende Informationen „sachlich, angemessen und überzeugend, so dass eine umsichtige und sachverständige Person die gleichen Schlussfolgerungen wie der Prüfer ziehen würde".[140] In den FMA Mindeststandards für die Interne Revision für Versicherungsunternehmen verlangt die FMA, dass jede Prüfung durch Arbeitsunterlagen dokumentiert wird, „aus denen zumindest die durchgeführten Prüfungshandlungen sowie die Prüfungsfeststellungen hervorgehen, und für sachverständige Dritte jederzeit nachvollziehbar sind".[141] Will die Interne Revision die Anonymität des unbeabsichtigten Hinweisgebers wahren, muss sie wohl den Sachverhalt derart erheben und dokumentieren, dass die Mitteilung, zumindest im Nachhinein auch aus anderen Quellen nachvollziehbar ist.

## 6.5. Interne Revision als Opfer

Jede nachträgliche Kontrollinstanz, gleichgültig ob es sich um die Interne Revision oder eine öffentlich-rechtliche Institution wie etwa den Rechnungshof oder ein Kontrollamt handelt, kommt immer wieder in die Gefahr, dass Prüfberichte oder Prüfergebnisse in einem Stadium der Erstellung und vor endgültiger Freigabe veröffentlicht oder verwendet werden. Ist ein Prüfbericht einer Internen Revision einer österreichischen Versicherung fertiggestellt ergibt sich ein klarer gesetzlicher Auftrag zur Verteilung. Gemäß § 108 VAG ist er wie die Berichte der anderen *Governance* Funktionen den Vorstandsmitgliedern, Verwaltungsratsmitgliedern und anderen Mitgliedern des „*Senior Managements*" zu übermitteln. Der Vorsitzende des Aufsichtsrates und der Prüfungsausschuss des Aufsichtsrates sind über die Prüfgebiete und wesentliche Prüfungsfeststellungen zu informieren (VAG § 119). Das interne Regelwerk kann auch beinhalten, dass die Revisionsberichte zur Gänze dem Aufsichtsorgan/Aufsichtsrat zu unterbreiten sind (Die FMA Mindeststandards fordern, dass die Leiter der geprüften Einheiten über die Prüfungsfeststellungen informiert werden und Gelegenheit zur Stellungnahme erhalten[142]). Kommt ein Bericht an die Öffentlichkeit, ohne dass es die Verfügungsberechtigten gewünscht haben, kann sowohl für das Unternehmen als auch für die Interne Revision eine ungemütliche Zeit beginnen. In diesem Fall ist wohl die Frage im Vordergrund, wer aus einem vorerst relativ kleinen Empfängerkreis als „*Whistleblower*" in Frage kommt. Aus der Praxis gesprochen ist aber der Kreis derer die zum Revisionsbericht Zugriff haben deutlich größer als angenommen. Unterstellt man einen fünfköpfigen Vorstand und zwei geprüfte Organisationseinheiten, dann ergibt sich folgendes Bild: 5 Vorstandsmitglieder, 5 Sekretärinnen, 5 Assistenten, 2 Bereichsleiter, 2 Sekretärinnen, mindestens 2 Mitarbeiter in jedem Bereich, der Revisionsleiter, seine Sekretärin, der Prüfungsleiter, mindestens ein Prüfer, der Systemadministrator für den Vorstand, der Systemadministrator für die Revision und der Systemadministrator für beide Bereiche ergibt im Minimum von 30 Personen, die Zugriff auf den Revisionsbericht haben, wobei davon auszugehen ist, dass die Revisionsberichte in Papier der Vergangenheit angehören. Je brisanter der Bericht ist und je schwerwiegender die Feststellungen, umso mehr steigt die Vertraulichkeitsstufe auf der einen Seite und die Zahl derer die den Bericht kennen, wie Aufsichtsratsvorsitzender, Prüfungsausschussmitglieder, Sekretär des Aufsichtsrates, Compliance Officer, Rechtsabteilung sowie zumeist noch externe Berater, Anwälte und Wirtschaftsprüfer.

Die Konzernrevision der Ergo Versicherungsgruppe kam beispielsweise zu ungewollter Publizität. Nachdem das Handelsblatt bereits am 19. Mai 2011 erstmals über „Sexspiele" anlässlich von Incentivereisen

[139] IIA Ausführungsstandard 2330

[140] IIA Ausführungsstandard 2310 Erläuterung

[141] Finanzmarktaufsichtsbehörde - FMA, Mindeststandards für die Interne Revision von Versicherungsunternehmen vom 20. September 2005 7.6.

[142] FMA MSIR 7.7

berichtet hatte, stellte die Konzernrevision am 3.Juni 2011 den Bericht darüber fertig. Am 14.8.2012 berichtete das Handelsblatt dann über den Inhalt dieses Berichtes und merkte süffisant an:“ Lange blieb der Revisionsbericht der Öffentlichkeit verschlossen“.[143] Auch nicht wirklich glücklich wird die Interne Revision des US Internal Revenue Service (IRS) sein, dass in den Medien zu lesen war, dass eine hausinterne Untersuchung der US Steuerbehörde zu Tage brachte, dass von dieser Behörde konservative Gruppen benachteiligt und liberale sowie linke Gruppen bevorzugt wurden. Nun ermittelt das FBI und der Behördenchef musste gehen.[144] Besonders schwierig ist die Situation für die Interne Revision, wenn Teile von Rohberichten veröffentlicht werden. In einem ordnungsgemäßen und fairen Revisionsablauf werden die Geprüften mit den Erkenntnissen der Internen Revision konfrontiert, sofern dies nicht den Prüfungszweck vereiteln beziehungsweise gefährdet, wie dies etwa bei der Untersuchung von strafbaren Handlungen der Fall sein könnte. In diesem Fall würde der Täter gewarnt, allenfalls hätte er auch noch die Gelegenheit Beweismaterial zu vernichten oder zu verfälschen. In allen anderen Fällen legt die Revision ihre Erkenntnisse vor, der Geprüfte nimmt Stellung und wenn irgendwie möglich kommen Revision und Geprüfter zu einer einvernehmlichen Auffassung sowohl über den Tatbestand als auch über die zu ergreifenden Maßnahmen. In meiner langen Praxis ist es mehrmals vorgekommen, dass sich erst in der Konfrontation zwischen Prüfer und Geprüften der wahre Sachverhalt herausgestellt hat. Keinem Prüfer steht es schlecht an zuzugeben, dass auch er sich einmal geirrt hat. Gerade die Schlussbesprechung zwischen der Leitung der geprüften Einheit, der Leitung der Internen Revision und den Prüfern, gehört zu einer Maßnahme der Qualitätskontrolle der Internen Revision. Wird nun aber ein solcher Berichtsentwurf (Rohbericht) vor Einholung der Stellungnahme bekannt, kann dies die Verbreitung verzerrter Sichtweisen, aber auch falscher Beurteilungen sein. Dies gefährdet aber nicht nur das Image und oftmals auch die Existenz des Geprüften, sondern auch den Ruf der Internen Revision. Es wäre durchaus reizvoll diese Gedanken weiter zu spinnen, würde aber den Rahmen dieses Beitrages deutlich sprengen. Zusammenfassend ist darauf zu verweisen, dass innerhalb des Revisionsprozesses alle Beteiligten gut beraten sind, die Vertraulichkeit zu wahren bis ein eindeutiges und nachvollziehbares Prüfungsergebnis vorliegt. Für die Mitarbeiter der Internen Revision bewahrheitet sich hier wieder die Verpflichtung zur Verschwiegenheit, die nicht nur das Ausplaudern von Revisionsdetails, sondern auch den sorglosen Umgang mit Informationen bedeutet. Dies erfordert eine spezielle Sicherung der Revisionsdatenbank und ein striktes limitiertes Berechtigungssystem für seine Nutzung. Je größer eine Revisionseinheit ist, umso mehr kommt sie in das Spannungsverhältnis zwischen möglichst umfassenden Zugang zu allen Revisionsdaten als Wissensdatenbank auf der einen Seite und der gebotenen Vertraulichkeit insbesondere was noch nicht gesicherte Erkenntnisse betrifft, auf der anderen Seite.

## 6.6. Revision im Zwielicht

Besonders schwierig wird die Situation für die Interne Revision oder eine andere derartige Institution, wenn sie in den Geruch gerät nicht absolut korrekt zu handeln oder es an der unverzichtbaren Objektivität mangeln lässt. Als Beispiel darf an die Affäre rund um das *„European Anti Fraud Office“ (OLAF)* erinnert werden, die keineswegs noch ausgestanden ist. Der Kontrollausschuss *(Supervisory Committee)*[145] dieser Europäischen Behörde hat in seinem Jahresbericht 2012[146] festgestellt, die Behörde „scheint den rechtlichen Rahmen großzügig auszulegen“. Sie soll dabei bei der Suche nach Beweismitteln nicht immer nach der geltenden Dienstordnung *ISIP (Instruction to Staff on Investigative Procedures)* vor-

[143] Vgl. u.a. Iversen Sönke, Interner Bericht enthüllt Details der Ergo Affäre. 14.8.2012, www.handelsblatt.com, download 21.5.2013

[144] Vgl. u.a. Grimm Oliver, FBI ermittelt gegen US Finanzbehörde, Die Presse 16.Mai 2013 7

[145] Supervisory Committee eingerichtet mit Regulation No 1073/1999 of the European Parliament and of the Council of 25 th May 1999 concerning investigations conducted by the European Anti – Fraud Office (OLAF) Official Journal of the European Countries L 136/3 31.5.1999

[146] Activity Report of the OLAF Supervisory Committee, January 2012 – January 2013 Rat 8791 / 13 2.5.2013, www.parlament.gv.at, 113192 / EU XXIV GP

gegangen sein, der Generaldirektor von OLAF soll in Untersuchungen direkt eingegriffen haben. Mindestens in einem Fall wurde vom „*European Data Protection Supervisor*" festgestellt, dass *OLAf* die Rechte eines *Whistleblowers* auf Vertraulichkeit verletzt hat. Besonders kritisch wurde vom Kontrollausschuss die Rolle von *OLAF* in der Untersuchung jener Vorgänge gesehen, die zum erzwungenen Rücktritt eines EU Kommissars führten.[147]

Ein besonderer Beigeschmack entsteht in dieser Angelegenheit auch darin, dass der Generaldirektor von *OLAF* offensichtlich in der Zusammenarbeit mit dem unabhängigen Kontrollausschuss eine sehr restriktive Informations- und Offenlegungspolitik betrieben und dessen Ressourcen eingeschränkt hat.[148] Hier liegt eindeutig ein Interessenkonflikt vor. Vorerst ist festzuhalten, dass Regeln für die Überwachung einer Behörde oder Institution niemals von dieser selbst zu interpretieren sind, sondern dafür objektive Vorgaben zu geben sind und eine unabhängige Schiedsinstanz zu installieren ist. Weiterhin ist festzustellen, dass auch eine Prüfungsinstanz nicht frei von Fehlern ist und einer Kontrolle bedarf. Die Rolle von Arthur Anderson als Abschlussprüfer von ENRON und WorldCom hat eindeutig bewiesen, dass auch die Arbeit des unabhängigen Prüfers nicht frei von Fehlverhalten sein muss.[149] IIA Standard 1312 sieht eine externe Evaluierung der Internen Revision alle fünf Jahre vor.[150]

## 6.7. Interne Revision als Whistleblower

Ein besonderes Dilemma der Internen Revision tritt zu Tage, wenn sie selbst oder ihre Angehörigen zum *Whistleblower* werden. Vorerst gilt der Grundsatz der besonderen Verschwiegenheitspflicht für jeden Internen Revisor vor allem auch nach internationalen Standards. Punkt 3 des *IIA Code of Ethics* für Interne Revisionen legt fest, dass Interne Revisoren „den Wert und das Eigentum der erhaltenen Informationen" beachten und diese „ohne entsprechende Befugnis" nicht offenlegen, es sei denn dafür bestehen „rechtliche oder berufliche Verpflichtungen".[151] *Cynthia Cooper*, *Vicepresident of InternalAudit* von *WorldCom* ist nach wie vor das beste Beispiel für eine Internen Revisorin, die zum Whistleblower wurde. Als *Chief Audit Executive (CAE)* war sie direkt dem damaligen *CFO (Chief Financial Officer)* unterstellt. Nicht zuletzt aus den Erfahrungen mit *WorldCom* ist es nunmehr eher verpönt, die Interne Revision dem CFO alleine zu unterstellen. Sie wurde von einem internen *Whistleblower* informiert, dass im Rechnungswesen und im Reporting „*malpractice*" anzutreffen sei. Sie informierte ihren Vorgesetzten, der sie zurückpfiff, sie kontaktierte den Abschlussprüfer, der ihre Bedenken zu zerstreuen versuchte. Daraufhin untersuchte sie die Vorwürfe mit einer Mitarbeiterin weiter, allerdings im Geheimen und kam zu dem Schluss, dass tatsächlich ein gigantischer Bilanzbetrug vorlag und dass dieser von höchster Stelle, also vom Top Management, gebilligt, ja sogar angeordnet sei und vom Abschlussprüfer, eben jenen Arthur Anderson, der sich schon als Abschlussprüfer von Enron ausgezeichnet hatte, gedeckt würde. Nachdem alle Möglichkeiten der internen Information hin bis zum CEO ausgeschöpft waren, informierte sie das *Audit Committee*, das ebenfalls erst nach ihrem Insistieren aktiv wurde. Am Ende stand die bis damals größte Pleite der Wirtschaftsgeschichte, ein zu Gefängnistrafen verurteiltes Topmanagement, ein als Wirtschaftsprüfer verschwundener bisheriger Angehöriger der „*Top Five*" und eine Ex – Revisionsdirektorin, die zwar zahlreiche Ehrungen erhalten hat aber aus ihrem Job gemobbt wurde und heute als Vortragende zu Unternehmensethik buchbar ist.

Die IIA Standards versuchen den Revisionsleitern ein Hilfsmittel dadurch zu geben, dass sie fordern,

[147] Laczinski Michael, Europas Betrugsfahnder im Zwielicht, Die Presse.com 25.4.2013

[148] OLAF Supervisory Committee 10 12 17 32 43 53

[149] Vgl. Cooper Cynthia, Extraordinary Circumstances. The Journey of a Corporate Whistleblower, Hoboken NY, 2008 und Eichenwald Kurt, Verschwörung der Narren. Der Enron Skandal Eine wahre Geschichte, München 2007, Original Conspiary of Fools, New York 2005

[150] IIA Standard 1213

[151] IIA: Code of Ethics in Internationale Standards 2017 S 11

dass Revisionsleiter, die zum Schluss kommen, dass Führungskräfte nicht tragbare Risiken akzeptieren, sich an das Top Management wenden müssen und wenn dies erfolglos ist an das Überwachungsorgan (IIA Standard 2600). Im Versicherungsaufsichtsgesetz 2016 wird festgehalten, dass „wesentliche Verfügungen, welche jene Personen betreffen, die *Governance* – Funktionen [also auch die Interne Revisionsfunktion] wahrnehmen von mindestens zwei Mitgliedern des Vorstandes bzw. des Verwaltungsrates zu treffen sind (VAG § 108/2) und dass quartalsweise wesentliche Feststellungen der Internen Revision dem Vorsitzenden des Aufsichtsrates/Verwaltungsrates und dem Prüfungsausschuss mitzuteilen sind (VAG § 119/3). Ähnliches findet sich im § 42 BWG (Bankwesengesetz) und § 38 PKG (Pensionskassengesetz).[152] Das Dilemma des Leiters der Internen Revision bleibt aber grundsätzlich ungelöst. Bei allen Objektivierungsanordnungen und Beteuerungen der Unabhängigkeit der Internen Revision in ihrer Beurteilung der Sachlage und Berichterstattung bleibt der Leiter der Internen Revision ein Angestellter des Unternehmens, der einem Vorstandsmitglied - im Idealfall dem Vorstandsvorsitzenden oder dem Gesamtvorstand - untersteht. Dieser Vorgesetzte entscheidet über Entlohnung und Fortkommen des Revisionsleiters ebenso wie über die ihm zur Verfügung stehenden Ressourcen. Der Leiter der Internen Revision hat in einem besonderen Vertrauens- und Loyalitätsverhältnis zum *Chief Executive Officer (CEO)* zu stehen. Wenn dieser kein Vertrauen zur sachlichen Richtigkeit der Arbeit und zum Augenmaß des Revisionsleiters bei der Abwägung formeller, vor allem externer Vorschriften und den Bedürfnissen des Unternehmens hat, besteht die Gefahr, dass die Interne Revision nicht ernst genommen wird und so nicht in der Lage ist, den geforderten Mehrwert für das Unternehmen zu schaffen. Nichts ist gefährlicher für eine Interne Revision, wenn sie als verlängerter Arm der Aufsichtsbehörde empfunden wird.

## 7. Persönliche Conclusio des Verfassers

Der vorstehende Beitrag erhebt für sich nicht den Anspruch, eine wissenschaftliche Arbeit zu sein und der Verfasser erlaubt sich daher Ungenauigkeiten bei der Anwendung von Zitierregeln. Im Interesse der leichteren Lesbarkeit wird auf gendergerechte Schreibweise verzichtet und alle männlichen Bezeichnungen können auch für weibliche Personen angewendet werden ohne dass eine Diskriminierung beabsichtigt wäre. Für sprachliche und formale Schlampigkeiten wird um Nachsicht gebeten, Der Beitrag ist eine Weiterentwicklung des Abschnittes „*Whistleblowing*“ im Skriptum zum Schwerpunkt „Interne Revision“ des Masterstudienganges „Integriertes Risikomanagement“ an der University of Applied Sciences FH_ Campus Wien im WS 2017/2018.[153] Die Auswahl der verwendeten Literatur und der gewählten Beispiele für *Whistleblowing* erfolgte nach Empfinden und Erfahrung des Verfassers und erhebt keinen Anspruch auf Vollständigkeit. Die ausgewählten Teilergebnisse der Untersuchung des Verfassers in der österreichischen Versicherungswirtschaft sind zwar schon 10 Jahre alt, doch ist eine jüngere vergleichbare Studie zumindest dem Verfasser nicht bekannt. Die nachstehende Conclusio beruht ebenfalls auf der persönlichen Wertung des Verfassers.

Bei der anstehenden und notwendigen Ausweitung des Schutzes von Informanten sollte als Voraussetzung gelten, dass die Weitergabe der Information nur dann schutzwürdig ist, wenn sie in gutem Glauben an die Richtigkeit oder zumindest Wahrscheinlichkeit dieser Information erfolgte und keinesfalls aus verpönten persönlichen Motiven wie Eitelkeit, Streben nach Anerkennung, Streben nach beruflichen oder privaten Vorteilen oder Gewinnstreben, Vergeltung oder aus politischen Motiven. Eine Prämie für Informanten scheint dem Verfasser als ungeeignetes und unethisches Instrument. *Externes Whistleblowing* sollte erst dann ermöglicht und geschützt werden, wenn zumutbare organisationsinterne Kanäle

[152] Bundesgesetz vom 17. Mai 1990 über die Einrichtung, Verwaltung und Beaufsichtigung von Pensionskassen (Pensionskassengesetz – PKG) BGBl 281/1990 idF BGGBl I 68/2015

[153] Hauser Peter, Whistelblowing, Materialien zur Internen Revision, Version 2017-09-04-final, S 134 -168 FH Campus Wien, 2017

vollständig genutzt wurden, nicht zur Verfügung standen oder ihre Verwendung kontraproduktiv wäre. Externes *Whistleblowing* kann nur als ultimatives Mittel zur Erreichung objektiv bedeutsamer gesellschaftlicher Ziele akzeptiert werden. Botschaften von *Whistleblowern* sollten sowohl Strafverfolgungsbehörden als auch Finanzbehörden zugänglich sein, auch wenn sie vordergründig durch parlamentarische Rituale oder vermeintlich notwendige Mediengeheimnisse geschützt scheinen. Ebenso wichtig wie der Schutz des *Whistleblowers* ist dem Verfasser der Schutz der Interessen und der Rechte der Organisation, der beschuldigten oder in Verdacht gebrachten Personen und des unbeteiligten Umfeldes. Die Nutzung anonymer Informationen ist mit besonderer Sorgfalt und unter Wahrung des Rechtes von jedermann auf ein faires Verfahren vor dem gesetzmäßigen Richter vorzunehmen und auch Vorverurteilungen durch Medien, Öffentlichkeit oder Politiker sind an diesem Recht zu messen.

Interne Revisoren haben sich vor allem der Organisationen verantwortlich zu fühlen, sie können niemals absolut objektiv sein, da sie ein Teil der Organisation sind.[144] Sie haben Verantwortung, dass Informationen über Fehlverhalten in der Organisation weiterverfolgt und objektiv untersucht werden, ebenso, dass Gefahren für die Organisation aufgedeckt und an die Verantwortungsträger unverzüglich herangetragen werden. Bei dem Umgang mit *Whistleblowing* sind für die Interne Revision nicht nur die Aussagen selbst zu evaluieren, sondern sind die Person und das Umfeld des Informanten von Bedeutung. Revisionsleiter sollten unbedingt dafür sorgen die Rolle der Internen Revision im Zusammenhang mit *Whistleblowing* in der Revisionsordnung geklärt zu haben. Bei der Entscheidung selbst zum *Whistleblower* zu werden, sollte sich jeder Interne Revisor bewusst sein, dass er der Organisation angehört, ihr Loyalität schuldet und zur Hebung ihres Wertes beizutragen hat und dies nach Ansicht des Verfassers durchaus das Recht der freien Meinungsäußerung einschränken kann und soll.

[154] Vgl. Vortrag von Richard Chambers anlässlich der Präsentation seines Buches „Trusted Advisors“ am 13.11.2017 im Institut für Interne Revision Österreich, Wien

# SAP und die Datenschutzgrundverordnung – Teil II

**Mag. Walter Pichl**
CIA, CFSA, CIPP/E, CISA, CISM, CGEIT, CRISC & SAP TERP10
wurde 1999 zum ABAP Entwickler ausgebildet und betreut seit 2002 in der Konzern-IT eines Finanzdienstleisters eine der größten SAP-Installationen Mittel- und Osteuropas. Walters Schwerpunkte sind SAP Security Management & Security Operations, Risk Assessment & Management, ISAE3402, Self-Audit, Compliance & Datenschutz – immer als interner Mitarbeiter im SAP Competence Center.

## Disclaimer

Die Interne Revision (IR) unterstützt die Geschäftsführung sowie gegebenenfalls die Aufsichtsorgane beratend bei der Ausgestaltung bzw. Verbesserung des unternehmensweiten Risikomanagements (Enterprise Risk Management: ERM) und prüft zumeist die im Unternehmen implementierten ERM-Systeme. In der am Institut für Managementwissenschaften (TU Wien) durchgeführten ERMMA-Studie 2017 [1] wird die Qualität der ERM-Systeme von österreichischen Unternehmen anhand von fünf Reifegraden gemessen. Dabei zeigt sich, dass der ERM-System-Reifegrad signifikant von der Dauer der IR-Tätigkeit abhängig ist. In diesem Beitrag wird die Analyse vertieft, um zu eruieren, in welchen Bereichen der ERM-System-Ausgestaltung die IR-Tätigkeitsdauer die größten Wirkungen zeigt. Für Unternehmen, welche an der Verbesserung ihres ERM-Systems arbeiten, liefert der dabei festgestellte Befund interessante Hinweise für konkrete Verbesserungsmöglichkeiten.

## Inhalt

# Vorbemerkung

Dieser Beitrag führt „*SAP und die Datenschutzgrundverordnung*“ (Jahrbuch 2016: „*Die Kunst der Revision*“) als Teil II fort und kann auch ohne die Kenntnis von Teil I gelesen werden. Die Begriffe *privacy, Datenschutz* und *data protection* werden austauschbar nebeneinander verwendet. Ziel ist die Darstellung der Ableitung von Prüfprogrammen aus Standards und Referenzmaterialien.

# 1. Prüfauftrag für Maria Nicoleta: Vorbereitungsstand des SAP-Systems auf die DSGVO

Als Kommunikations- und Darstellungsform wird in verkürzter Form die *Persona* angewandt - ein methodologisches „Bordmittel“ der SAP, die „*User Story*“ aus dem Entwicklungs- & Designprozess. Wir begleiten die Persona *Maria Nicoleta Sapia* bei ihrer Prüfertätigkeit und ihren Erfahrungen mit SAP und der DSGVO.

**Persona Maria Nicoleta Sapia, CIA bei der Future Bank in der EU**

Maria ist 44 Jahre alt, hat einen Abschluss in BWL und mehr als 17 Jahre Erfahrung in Wirtschaftsprüfung und Interner Revision. Im Verlauf der Jahre hat sie sich in der Kollegenschaft wegen ihrer ungewöhnlichen und erfolgreichen Arbeitsmethodik hohe fachliche Anerkennung erworben. Maria ist nun das dritte Jahr Leiterin der Revision.

Ihre erste erfolgreiche SAP Prüfung war 2016 eine Sonderprüfung über den Vorbereitungsgrad der SAP-Systeme auf die Datenschutzgrundverordnung (DSGVO). Damals hatte sie sich breites Wissen über SAP und Datenschutz angeeignet und wurde auch Mitglied der IAPP (www.iapp.org), der *International Associaton of Privacy Professionals*. Sie hatte erkannt: In den komplexen SAP-Landschaften kann nur gegen Standards, Referenzmodelle und Referenzwerke geprüft werden. Dies gilt auch für den Datenschutz.

Nun ist ein Jahr vergangen und in wenigen Wochen gilt die DSGVO. Wie überall, wird nun auch in der Future Bank verstärkt gefragt: „*Sind wir so weit, sind wir bereit?*“ Und Maria Nicoleta bekommt erneut den Auftrag zu prüfen, wie es nun um die Fitness der SAP-Systeme für die DSGVO steht.

# 2. Methodologie: Wie kann die DSGVO im SAP geprüft werden?

Es werden einige Jahre vergehen, bis praxiserprobte Prüfleitfäden und allgemein anerkannte Vorgehensmodelle zur Verfügung stehen. Maria Nicoleta weiß, dass in solchen Situationen nur gegen Standards und Referenzwerke geprüft werden kann.

## 2.1. „Comply or Explain“

Schon bei der ersten SAP-Prüfung hatte Maria das Prüfen mit „*Comply or Explain*“ und die Tautologie „*SAP wird im SAP-Standard mit SAP-Standard gegen den SAP-Standard geprüft*“ zu schätzen gelernt. Sie ist sich sicher: „*Comply or Explain*“ wird sie auch diesmal erfolgreich anwenden können.

**Theorie:** „*Comply or Explain*“ ist ein vom Verfasser aus der Welt der Compliance abgeleiteter Prüfansatz. Seit Artikel 20 der EU-Richtlinie 2013/34/EU[1] und § 243c Unternehmensgesetzbuch (UGB)[2] informieren Unternehmen im Lagebericht über die Corporate Governance und die Einhaltung der Vorschriften eines Governance-Kodex. Abweichungen müssen erklärt werden.

Bei „*Comply or Explain*“ unterstellt der Verfasser, dass „*Comply*“ zur Einhaltung der *Grundsätze ordnungsmäßiger Buchführung (GoB)* gem. § 190 UGB und des „*Stands der Technik*“ gem. Artikel 32 EU-DSGVO führt.

## 2.2. GoB und Stand der Technik

**Theorie:** Der *Stand der Technik* ist gem. Artikel 32 DSGVO beim technischen Schutz der Daten einzuhalten, jedoch sehr schwierig zu interpretieren.[3] So werden – je nach Literatur – u.a. die Erwägungsgründe 74, 75, 76, 77, 78, 79, und 83 als damit in Beziehung stehend genannt. Die Auslegung des *Standes der Technik* ist für die Abschätzung des Risikos aus Datenschutz und allfälliger Strafen entscheidend.

Für das Prüfen der SAP Systeme gibt es im Prinzip nur zwei relevante Fragen:

- **Dürfen die personenbezogenen Daten überhaupt verarbeitet werden?**
- **Werden die Daten entsprechend dem Stand der Technik geschützt?**

Anzumerken ist, dass im österreichischen Recht der unbestimmte Gesetzesbegriff des *Stands der Technik* schon früher vorhanden und auszulegen war, so § 2 Abs. 8 ArbeitnehmerInnenschutzgesetz[4] oder § 71a der Gewerbeordnung.[5]

---

[1] Richtlinie 2013/34/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Jahresabschluss, den konsolidierten Abschluss und damit verbundene Berichte von Unternehmen bestimmter Rechtsformen und zur Änderung der Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinien 78/660/EWG und 83/349/EWG des Rates
http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1518373873550&uri=CELEX:32013L0034

[2] **Corporate Governance-Bericht**
§ 243c. (1) Eine Aktiengesellschaft, deren Aktien zum Handel auf einem geregelten Markt im Sinn des § 1 Z 2 BörseG 2018 zugelassen sind oder die ausschließlich andere Wertpapiere als Aktien auf einem solchen Markt emittiert und deren Aktien mit Wissen der Gesellschaft über ein multilaterales Handelssystem im Sinn des § 1 Z 24 WAG 2018 gehandelt werden, hat einen Corporate Governance-Bericht aufzustellen, der zumindest die folgenden Angaben enthält:
(Anm.: infolge eines Redaktionsversehens wurde durch Art. 43 Z 3, BGBl. I Nr. 107/2017, der ganze § 243c Abs. 1 UGB neu gefasst und nicht bloß dessen Einleitung. Z 1 bis 4 sind daher weggefallen und lauteten bisher:
1. die Nennung eines in Österreich oder am jeweiligen Börseplatz allgemein anerkannten Corporate Governance Kodex;
2. die Angabe, wo dieser öffentlich zugänglich ist;
3. soweit sie von diesem abweicht, eine Erklärung, in welchen Punkten und aus welchen Gründen diese Abweichung erfolgt;
4. wenn sie beschließt, keinem Kodex im Sinn der Z 1 zu entsprechen, eine Begründung hiefür.)
(2) In diesem Bericht sind anzugeben: ... [ausgelassen]. [3] Art. 32 DSGVO - Sicherheit der Verarbeitung [Ausschnitt]
(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: .....

[4] BGBl. 450/1994 idF. BGBl. I. Nr. 126/2017, § 2 Abs. 8: Stand der Technik im Sinne dieses Bundesgesetzes ist der auf einschlägigen wissenschaftlichen Erkenntnissen beruhende Entwicklungsstand fortschrittlicher technologischer Verfahren, Einrichtungen und Betriebsweisen, deren Funktionstüchtigkeit erprobt und erwiesen ist. Bei der Bestimmung des Standes der Technik sind insbesondere vergleichbare Verfahren, Einrichtungen und Betriebsweisen heranzuziehen.

Spätestens zu diesem Zeitpunkt wird Maria klar, dass auch eine gut ausgebildete und erfahrene Prüferin wie sie scheitern wird, sobald sie sich im Alleingang in das gefahrenvolle Land der juristischen Auslegung unbestimmter Gesetzesbegriffe wagt. Deshalb nutzt Maria die Analogie zum Prüfen der SAP-Systeme im Zuge der kaufmännischen Jahresabschlussprüfung.

**Theorie:** Die Referenz zum *SAP Standard* und die *Speicherbuchführung*. Allen kaufmännischen Abschlussprüfern ist bekannt, dass SAP-Systeme als Systeme der *Speicherbuchführung* den *GoB* entsprechen müssen. *Speicherbuchführung* liegt vor, wenn der Buchhaltungsstoff im System erzeugt, verarbeitet und gespeichert wird. So wird der *„Buchhaltungsautomat"* SAP selbst zum Prüfobjekt und die Anfordungen der *GoB* müssen erfüllt werden. Dies reicht vom Gebot der Nachvollziehbarkeit und das Radierverbot über die Tabellenprotokollierung, das Change Management, die Benutzer- und Rechteverwaltung, den Betrieb bis hin zur Sicherheit von Servern, Netzwerk und Datenbank - nicht zu vergessen das Audit.[6]

Nur wenigen Anwendern und SAP-Experten ist bekannt: Wird das SAP-System *„sachgerecht"* betrieben (und der SAP Standard ist sachgerecht), dann werden die *GoB* und der *Stand der Technik* erfüllt. Dazu sogleich die Herleitung.

## 2.3. SAP Softwarebescheinigungen & vermutete Ordnungsmäßigkeit

**Theorie: Werden SAP-Systeme im Standard betrieben, dann haben sie die Vermutung der Ordnungsmäßigkeit für sich.** Jetzt werden sich die geschätzten Leser fragen, worauf diese Aussage beruht und welche Implikationen dies hat.

Softwarebescheinigung: SAP lässt die Software von Wirtschaftsprüfern untersuchen, ob die Anforderungen der Ordnungsmäßigkeit eingehalten werden. Weiters lässt sich die SAP auch laufend nach verschiedenen Security-Standards zertifizieren.

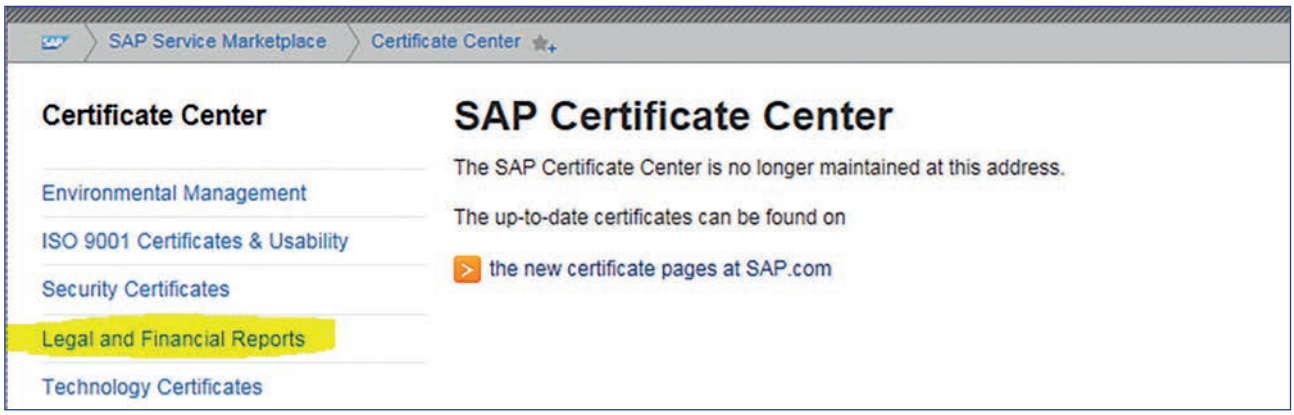



**ABB. 1: SAP Zertifikate / https://service.sap.com/certificates / a**

[5] BGBl. 194/1994 (WV) idF BGBl. I Nr. 107/2017, § 71a Abs. 1: Der Stand der Technik (beste verfügbare Techniken – BVT) im Sinne dieses Bundesgesetzes ist der auf den einschlägigen wissenschaftlichen Erkenntnissen beruhende Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen, Bau- oder Betriebsweisen, deren Funktionstüchtigkeit erprobt und erwiesen ist. Bei der Bestimmung des Standes der Technik sind insbesondere jene vergleichbaren Verfahren, Einrichtungen Bau- oder Betriebsweisen heranzuziehen, welche am wirksamsten zur Erreichung eines allgemein hohen Schutzniveaus für die Umwelt insgesamt sind; weiters sind unter Beachtung der sich aus einer bestimmten Maßnahme ergebenden Kosten und ihres Nutzens und des Grundsatzes der Vorsorge und der Vorbeugung im Allgemeinen wie auch im Einzelfall die Kriterien der Anlage 6 zu diesem Bundesgesetz zu berücksichtigen.

[6] Pichl, Walter. Grundsätze ordnungsmäßiger Buchführung beim Einsatz von SAP - rechtliche, organisatorische und technische Grundlagen. Diplomarbeit Wirtschaftsuniversität Wien, Wien 2009.


**ABB. 2: SAP Zertifikate / https://service.sap.com/certificates / b**

*„Nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse ermöglicht das von uns geprüfte Softwareprodukt SAP S/4HANA Finance Edition 1503 SPS 1508 in der Haupt-, Debitoren-, Kreditoren- und Anlagenbuchhaltung bei sachgerechter Anwendung eine den Grundsätzen ordnungsgemäßer Buchführung entsprechende Rechnungslegung und entspricht den vorstehend aufgeführten Kriterien.“*

Softwarebescheinigung der KPMG für S/4 HANA Finance Ed. 1503 SPS 1508 (Prüfungsstandard IDW Prüfungsstandards: Die Prüfung von Softwareprodukten (IDW PS 880) mit Stand vom 11. März 2010), S. 8.

SAP SE, Bescheinigung IDW PS880, SAP S/4HANA Finance Edition, 27. Januar 2016

Die Nachweise sind auf folgenden Seiten zu finden:
Mit SAP Kundenuser: https://service.sap.com/certificates (Seite wird abgelöst),
im freien Internet: https://www.sap.com/corporate/en/company/quality.html --> certificates
oder https://www.sap.com/corporate/en/company/quality.html#certificates

Hier findet sich auch ein Datenschutz-Zertifikat des BSI (British Standards Institute).

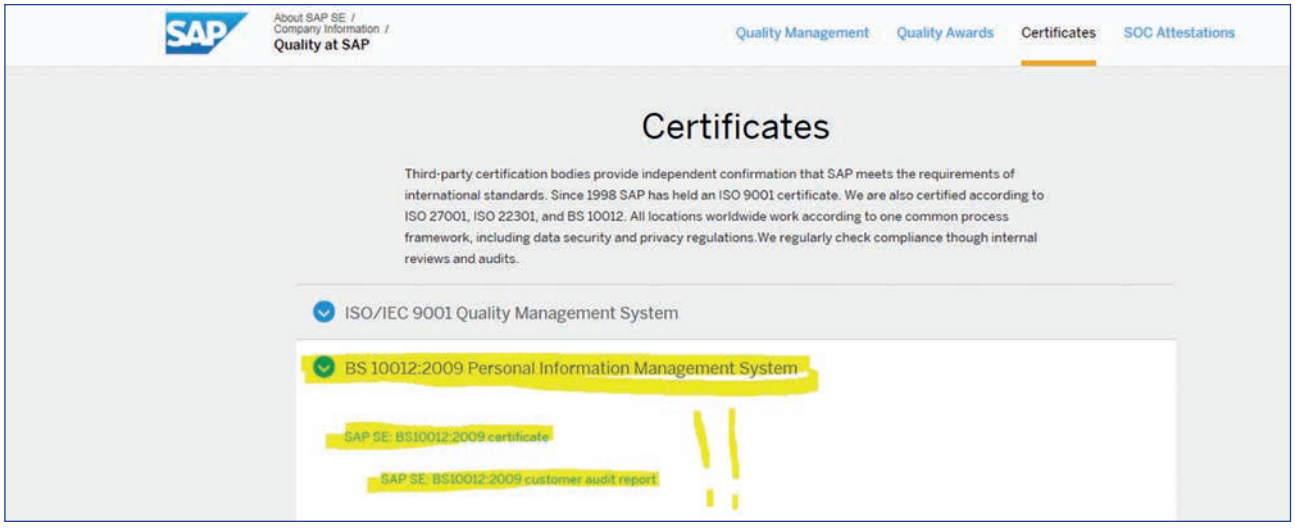



**ABB. 3: https://www.sap.com/corporate/en/company/quality.html#certificates**

# 3. Jetzt wird es konkret: Maria entwickelt ihr Prüfprogramm

Nach einiger Zeit des Nachdenkens und der Analyse entschließt sich Maria, folgende sieben Teilprüfungen durchzuführen.

1. **Governance**
2. **Framework**
3. **Metriken**
4. **Technische Sicherheit & Stand der Technik im SAP**
5. **Rechtmäßigkeit der Verarbeitung**
6. **Data Breach**
7. **Datenbank SAP HANA**

Für alle sieben Prüfgebiete leitet Maria Nicoleta die einzelnen Prüfhandlungen aus Referenzmaterialien ab – in Kombination mit der Risikosituation des Unternehmens. Im Folgenden werden nicht die einzelnen Checklisten dargestellt, sondern das Ableiten derselben aus Referenzmaterialien, welche unbestritten zum „*Stand der Technik*" zählen. Ist die Ableitung stringent, qualitativ und nachvollziehbar, dann gilt - nach Auffassung des Verfassers - auch für das entwickelte Prüfprogramm die Vermutung der Erfüllung des *Stands der Technik* im Einklang mit Artikel 32 DSGVO.

## 3.1. Checklisten-Ableitung aus dem Body-of-Knowledge des CIPM

Als erste Referenz verwendet Maria das bei der Zertifizierung zum CIPM abgeprüfte und bei Densmore[7] beschriebene Privacy Management Model der IAPP, den BoK des CIPM. Es beschreibt die Implementierung eines Datenschutzprogramms.[8]

*"The privacy management model presented in this book leverages many past and current best practices, including books, manuals, and education and training data, to build a privacy program. …* [Referenz auf Swire, Ahmad und Herath, ausgelassen durch den Verfasser] *… This privacy management book expands on those ideas and topics to prepare the privacy professional to establish a privacy governance model or refine current privacy management and then to use the privacy operational lifecycle to maintain privacy management through best practices to assess, protect, sustain and respond to privacy-related events."*[9]

**Begriff: CIPM – Certified Information Privacy Manager**

Im europäischen Datenschutz kennen wir bislang als Berufsbilder lediglich die Datenschutz-Juristen und die Datenschutzbeauftragten. In den USA haben sich durch das Wirken der IAPP folgende drei (zertifizierbare) Berufsbilder etabliert:

Jurist → CIPP – Certified Information Privacy Professional[10]

Techniker → CIPT – Certified Information Privacy Technologist[11]

Manager → CIPM – Certified Information Privacy Manager[12]

Marias Audit wird sich v.a. auf den Body-of-Knowledge (BOK) des CIPM stützen. Daraus wird Maria große Teile ihres Prüfprogramms ableiten.

---

[7] Vgl. Densmore, Russell R. (2013). Privacy Program Management. Tools for Managing Privacy Within Your Organization. IAPP, Portsmouth.

[8] Authoritative Resource List = CIPM Bibliography. Empfehlenswert: Densmore, Russell R. (2013). Privacy Program Management: Tools for Managing Privacy Within Your Organization. IAPP, Portsmouth; Determann, Lothar (2017). Determann's Guide to Data Privacy Law: International Corporate Compliance, 3ed. Edward Elgar, Cheltenham. Im Handel nicht mehr verfügbar: Herath, Kirk M. (2011). Building a Privacy Program: A Practitioner's Guide. IAPP, Portsmouth. Ein sehr gutes Grundlagenbuch ist Swire, Peter P.; Ahmad, Kenesa; McQuay, Terry (Hrsg.) (2012). Foundations of Information Privacy and Data Protection. IAPP, Portsmouth. Wer sich intensiv mit der DSGVO auseinandersetzen möchte, greift zum Lehrbuch für den CIPP/E: Ustaran, Eduardo (Hrsg.) (2017). European Data Protection. Law and Practice. IAPP, Portsmouth.

[9] Densmore, Russell R. (2013) Privacy Program Management: Tools for Managing Privacy Within Your Organization. IAPP, Portsmouth, S. IX-X.

[10] Der CIPP kann in folgenden Ausprägungen erworben werden: CIPP/E für Europa (DSGVO) (https://iapp.org/certify/cippe/), CIPP/US für die US-Privatwirtschaft (https://iapp.org/certify/cippus/), CIPP/G für die US-Regierung (https://iapp.org/certify/cippg/), CIPP/C für Kanada (https://iapp.org/certify/cippc/) und CIPP/A für Asien (https://iapp.org/certify/cippa/).


**ABB. 4: Die drei Berufsbilder im Datenschutz: Jurist, Privacy Manager, Techniker**

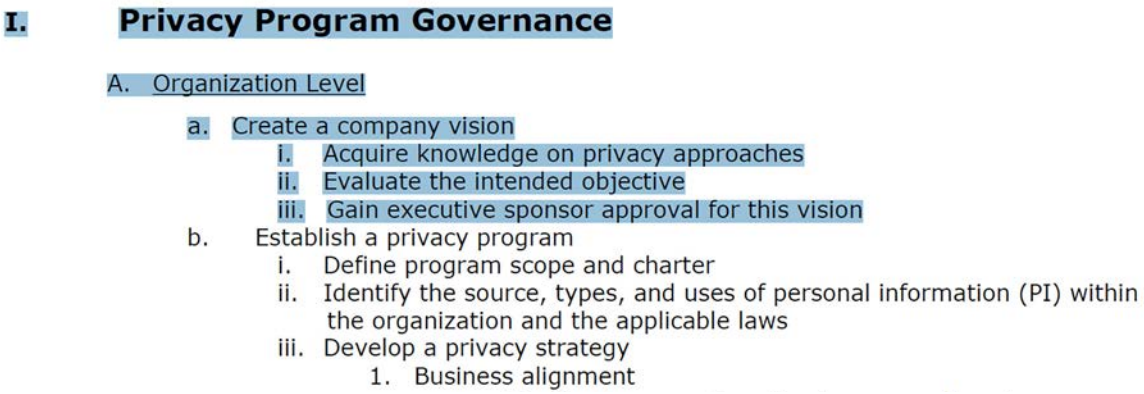



**ABB. 5: Ableitungsbeispiel CIPM / BoK – Strategie (BoK gesamt: 7 A4-Seiten!)**

Nun erkennt Maria, dass die ihr bislang bekannte Literatur über Datenschutz-Audit zwar extrem detailliert und genau Audit-Ziele aus dem Gesetz ableitet, aber – wie in Europa üblich - die betriebswirtschaftlichen Aspekte nicht oder nur am Rande behandelt werden. Datenschutz wird vordringlich als Compliance-Thema gesehen.[13]

Der BoK lässt Maria erkennen, dass jedwedes Datenschutz-Projekt verfehlt ist, wenn die strategischen Aspekte und die Wertschöpfungskette nicht behandelt werden. Wenn Datenschutz nur als wertvernichtende Compliance-Übung ohne Beitrag zur Wertschöpfung des Unternehmens gesehen wird, dann wird Datenschutz nie in die Prozesse eingebunden werden und voll wirken können.

[11] https://iapp.org/certify/cipt/, https://iapp.org/certify/get-certified/cipt/,
BOK: https://iapp.org/media/pdf/certification/CIPT_BOK_2.1.0_after%208.1.17.pdf,
Empfohlene Literatur: https://iapp.org/media/pdf/certification/CIPT-Bibliography-3.0.0.pdf

[12] https://iapp.org/certify/get-certified/cipm/, https://iapp.org/certify/get-certified/cipm/
BOK: https://iapp.org/media/pdf/certification/CIPM_BoK.pdf
Empfohlene Literatur: https://iapp.org/media/pdf/certification/CIPM-Bibliography-3.0.pdf

[13] Z.B. das österreichische Standardwerk Pachinger, Michael; Beham, Georg (2017). Datenschutz-Audit. Recht – Organisation – Prozess – IT. Der Praxisleitfaden zur Datenschutz-Grundverordnung. LexisNexis, Wien widmet der Verzahnung zwischen Unternehmensstrategie und Datenschutzzielen weniger als eine halbe Seite und einen einzigen Prüfpunkt (ORG. 19), S. 134.


**ABB. 6: Datenschutz-Governance: Ein CIA blickt über den Tellerrand des Gesetzes und den Tag hinaus**

Und dann wird auch nicht überlegt werden, ob aus Datenschutz nicht etwa Value für die Kunden und damit ein Wettbewerbsvorteil oder gar ein Alleinstellungsmerkmal generiert werden kann. Als CIA ist Maria den gegenwärtigen und zukünftigen Erfolgs- und Ertragsquellen verpflichtet. Keinesfalls darf die zukünftige Wertschöpfung des Unternehmens behindert werden. Datenschutz muss – so wie Security und Audit – als Enabler zum Unternehmenserfolg beitragend implementiert werden.

## 3.2. Checkliste Governance (nach BoK CIPM) (Teilmenge)

**Checkliste Datenschutz-Governance**
Angeregt durch: *CIPM-BOK I. A. a – Create a company vision*
- Ist Datenschutz / Privacy in der Unternehmensstrategie abgebildet?
- Wie wird Datenschutz strategisch gesehen? Nur als reiner Kostenfaktor oder als Mittel zur Differenzierung am Markt, als Teil der Produkt- und Service-Qualität oder gar als entscheidender Wettbewerbsfaktor?
- Ist bestimmt, welchen Reifegrad die Datenschutz-Organisation im Unternehmen erreichen soll?
- Ist Datenschutz in Überstimmung mit der Unternehmensstrategie und den Unternehmenszielen?

Nochmals, weil das wichtig ist: Ist die Frage der Datenschutz-Governance nicht beantwortet, dann wird - in betriebswirtschaftlichen Kategorien – jedes Datenschutz-Projekt scheitern. Juristisch „erfolgreich“ wird das Gesetz um des Gesetzes willen erfüllt. Ob das angestrebte Niveau in Bezug auf die Unternehmensstrategie angemessen ist, wird nicht gefragt und die Höhe der zu dotierenden Budgets strittig.

**Nun ist dargestellt, wie der gesamte BoK als Rahmenbedingung des SAP-Einsatzes abzufragen ist.** Mit diesem Ansatz ist sichergestellt, dass beim Auditieren des Datenschutzprogrammes keine Bausteine vergessen werden. Die Bausteine des BoK CIPM sind:

I. Privacy Program **Governance**
   A. **Organisation**
   B. **Entwicklung** des Privacy **Rahmenwerk**s
   C. **Implementierung** des Privacy **Rahmenwerk**s
   D. **Metriken**
II. Privacy **Operational Lifecycle**
   A. **Assess** – Evaluierung der Organisation
   B. **Protect** – Schutzkonzepte & Controls entwickeln
   C. **Sustain** – Controls im Einsatz (Measure, Align, Audit, Communicate, Monitor)
   D. **Respond** – Reaktionen und Maßnahmen

## 3.3. Datenschutz-Audit entlang der DSGVO (Pachinger, Beham)

Hier ist auf **das** österreichische Standardwerk zu verweisen. In großer Detailfülle wird ein Prüfprogramm auf 200 eng bedruckten Seiten vorgestellt. *Pachinger / Beham* ermöglicht eine detallierte Komplettprüfung des Datenschutzes hin auf alle Aspekte.

Pachinger, Michael; Beham, Georg (2017).
**Datenschutz-Audit.**
Recht – Organisation – Prozess – IT. Der Praxisleitfaden zur Datenschutz-Grundverordnung. LexisNexis, Wien.

Für Marias Sonderprüfung mit Schwerpunkt SAP muss hier das Prüfprogramm durchgesehen werden. Maria wählt die für ihr Vorhaben geeigneten Kontrollen aus. Jetzt sind bereits die ersten Teile des Prüfprogramms erarbeitet.

✓ **Governance** (BoK CIPM & Pachinger / Beham)
❖ **Framework** (BoK CIPM & COBIT 5)
❖ **Metriken** (BoK CIPM & COBIT 5)
➢ **Technische Sicherheit & Stand der Technik im SAP** (Lehnert & SAP)
❖ **Rechtmäßigkeit der Verarbeitung** (abgeleitet aus Pachinger / Beham & Lehnert)
➢ **Data Breach** (Pollirer, allfällig erweitert mit Pachinger / Beham)
➢ **Datenbank SAP HANA** (SAP)

## 3.4. COBIT 5 für das Prüfen der Einbettung des Datenschutzes in die IT-Governance

Im Rechenzentrum der Future Bank wird für die Governanz der IT-Anwendungen und des SAP-Einsatzes **COBIT 5** angewandt. **COBIT 5** besteht aus 37 Governance und Management Prozessen. Für jede Managementpraktik gibt es eine RACI-Chart: **R**esponsible, **A**ccountable, **C**onsulted, **I**nformed. Aufgelistet werden 26 Unternehmensfunktionen, darunter auch Audit und der Privacy Officer (idealerweise mit CIPM-Ausbildung). In der deutschsprachigen Übersetzung wird hier der Datenschutzbeauftragte genannt, was der Verfasser als kritisch erachtet. Hier sollten beide Funktionen, nämlich der in der Berichtslinie verankerte Privacy Officer und der „unabhängige" Datenschutzbeauftragte gemeinsam eingebunden werden.

**APO13 RACI Chart**

| Management Practice | Board | Chief Executive Officer | Chief Financial Officer | Chief Operating Officer | Business Executives | Business Process Owners | Strategy Executive Committee | Steering (Programmes/Projects) Committee | Project Management Office | Value Management Office | Chief Risk Officer | Chief Information Security Officer | Architecture Board | Enterprise Risk Committee | Head Human Resources | Compliance | Audit | Chief Information Officer | Head Architect | Head Development | Head IT Operations | Head IT Administration | Service Manager | Information Security Manager | Business Continuity Manager | Privacy Officer |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| APO13.01 Establish and maintain an ISMS. | | C | | C | C | I | C | I | I | | C | A | C | C | | C | C | R | I | I | I | R | I | R | C | C |
| APO13.02 Define and manage an information security risk treatment plan. | | C | | C | C | C | C | I | I | | C | A | C | C | | C | C | R | C | C | C | R | C | R | C | C |
| APO13.03 Monitor and review the ISMS. | | | | | C | R | C | | R | | | A | | | | C | C | R | R | R | R | R | R | R | R | R |

**ABB. 7: COBIT 5 / APO13 / Manage Security - die Einbindung des Privacy Officers**[14]

Maria prüft die gesamte Struktur von COBIT 5 über alle 37 COBIT-Prozesse und die dazugehörigen Managementpraktiken mit einem einfachen Ansatz:

- Welche COBIT 5-Prozesse und Managementpraktiken haben wir im Einsatz und welche nicht?
- Für alle Prozesse und Managementpraktiken, welche wir nicht verwenden:
  - ➢ Hat die Privacy Managerin / der Datenschutz beauftrage in diesen nicht verwendeten Prozessen / Praktiken eine Funktion? Welche RACI-Funktion?
  - ➢ Brauchen wir diesen Prozess, diese Praktik für den Datenschutz?
- Für alle Prozesse und Managementpraktiken, welche wir bereits verwenden:
  - ➢ Ist die Privacy Managerin / der Datenschutzbeauftragte richtig einbezogen?
  - ➢ Gibt es Berichtslinien und sind diese angemessen?
  - ➢ Sind die Metriken sinnvoll? (Referenz auf den BoK des CIPM)

Danach wird Maria wissen, ob die Datenschutzfunktion in der IT-Governance sinnvoll verankert ist oder ob Lücken bestehen. Weitere Teile des Prüfprogramms sind nun abgeleitet und einsatzbereit:

- ✓ **Governance** (BoK CIPM & Pachinger / Beham)
- ✓ **Framework** (BoK CIPM & COBIT 5)
- ✓ **Metriken** (BoK CIPM & COBIT 5)
- ➢ **Technische Sicherheit & Stand der Technik im SAP** (Lehnert & SAP)
- ❖ **Rechtmäßigkeit der Verarbeitung** (abgeleitet aus Pachinger / Beham & Lehnert)
- ➢ **Data Breach** (Pollirer, allfällig erweitert mit Pachinger / Beham)
- ➢ **Datenbank SAP HANA** (SAP)

[14] COBIT 5: Enabling Processes. ISACA 2012, S. 114. http://www.isaca.org/COBIT/Pages/Product-Family.aspx

## 3.5. Pollirers Checklisten aus der DaKo (Datenschutz Konkret)

Hans-Jürgen Pollirer veröffentlicht in der Zeitschrift *Datenschutz Konkret (DaKo)* Checklisten zu Sonderthemen, welche bei Bedarf sehr effektiv und effizient eingesetzt werden können. Diese Checklisten sind auch nach gesetzlichen Veränderungen immer noch relevant und einsetzbar.

- Bring Your Own Device (BYOD)[15]
- E-Recruiting[16]
- Internationaler Datenverkehr (IDVK)[17]
- Videoüberwachung[18]
- Cloud-Computing[19]
- (Allfällig von Interesse nach Schrems 2.0) (Knyrim, Trieb) Datentransfer nach Safe Harbor[20]
- E-Mail-Marketing[21]
- Datensicherheitsmaßnahmen gem § 14 DSG 2000 (Teil I)[22]
- Datensicherheitsmaßnahmen gem § 14 DSG 2000 (Teil II)[23]
- Gesetzeskonformer Webauftritt[24]
- Erfolgreiche Zertifizierung für das Datenschutzgütesiegel EuroPriSe[25]
- Social-Media-Richtlinie (Social-Media-Guideline)[26]
- Löschkonzept[27]
- Auskunftsrecht nach Art 15 DSGVO[28]
- Einwilligungserklärungen der Art 7 und 8 DSGVO[29]
- **Meldepflicht von Datenschutzverletzungen**[30]
- (Knyrim): Auftragsverarbeiter[31]

Maria hat oft gehört, dass die Meldepflichten bei Datenschutzverletzungen als sehr herausfordernd gelten. Nach ihrer Meinung sollte die Meldepflicht genauso geübt und auditiert werden wie bei Business Continuity & Disaster Recovery – mit *Paper Tests*, *Erreichbarkeitstests* etc. Hier wird sie Pollirers Checkliste **„Meldepflichten von Datenschutzverletzungen"** einsetzen. Sollte sich im Zuge der Prüfung zeigen, dass vertieftes Audit geboten ist, dann wird Maria mit **„5.7. Kontrollgruppe: Datenvorfall"** (Pachinger / Beham) fortsetzen.[32] Ein weiterer Teil des Prüfprogramms ist abgeleitet.

[15] Pollirer, Hans-Jürgen (2014). Checkliste - Bring Your Own Device (BYOD). In: Datenschutz Konkret (DaKo), 2014/6, Heft 1, S. 12-17.
[16] Pollirer, Hans-Jürgen (2014). Checkliste E-Recruiting. In: DaKo 2014/17, Heft 2, S. 37-40.
[17] Pollirer, Hans-Jürgen (2015). Checkliste - internationaler Datenverkehr (IDVK). In: DaKo 2015/23, Heft 2, S. 37-39.
[18] Pollirer, Hans-Jürgen (2015). Checkliste Videoüberwachung. In: Dako 2015/39, Heft 3, S. 68-71.
[19] Pollirer, Hans-Jürgen (2015). Checkliste Cloud-Computing. In: DaKo 2015/49, Heft 4, S. 91-96.
[20] Knyrim, Rainer; Trieb, Gerald (2015). Checkliste Datentransfer nach Safe Harbour. In: DaKo 2015/61, Heft 5, S. 117-118.
[21] Pollirer, Hans-Jürgen (2016). Checkliste E-Mail-Marketing. In: DaKo 2016/7, Heft 1, S. 13-16.
[22] Pollirer, Hans-Jürgen (2016). Datensicherheitsmaßnahmen gem § 14 DSG 2000 (Teil I). In: DaKo 2016/25, Heft 2, S. 40-43.
[23] Pollirer, Hans-Jürgen (2016). Datensicherheitsmaßnahmen gem § 14 DSG 2000 (Teil II). In: DaKo 2016/39, Heft 3, S. 64-66.
[24] Pollirer, Hans-Jürgen (2016). Checkliste für einen gesetzeskonformen Webauftritt. In: DaKo 2016/53, Heft 4, S. 86-88.
[25] Pollirer, Hans-Jürgen (2016). Checkliste für eine erfolgreiche Zertifizierung für das Datenschutzgütesiegel EuroPriSe. In: DaKo 2016/74, Heft 5, S. 112-114.
[26] Pollirer, Hans-Jürgen (2017). Checkliste für eine Social-Media-Richtlinie (Social-Media-Guideline). In: DaKo 2017/8, Heft 1, S. 15-16.
[27] Pollirer, Hans-Jürgen (2017). Checkliste Löschkonzept. In: DaKo 2017/23, Heft 2, S. 41-43.
[28] Pollirer, Hans-Jürgen (2017): Checkliste Auskunftsrecht nach Art 15 DSGVO. In: DaKo 2017/38, Heft 3, S. 66-67.
[29] Pollirer, Hans-Jürgen (2017). Checkliste für die Einwilligungserklärungen der Art 7 und 8 DSGVO. In: DaKo 2017/56, Heft 4, S. 90-92.
[30] Pollirer, Hans-Jürgen (2017). Checkliste Meldepflicht von Datenschutzverletzungen. In: DaKo 2017/68, Heft 5, S. 114-116.
[31] Knyrim, Rainer (2018). Checkliste für Auftragsverarbeiter. In: DaKo 2018/9, Heft 1, S. 14-16.
[32] Pachinger, Michael; Beham, Georg (2017). Datenschutz-Audit. Recht – Organisation – Prozess – IT. Der Praxisleitfaden zur Datenschutz-Grundverordnung. LexisNexis, Wien, S. 99-108.

- ✓ **Governance** (BoK CIPM & Pachinger / Beham)
- ✓ **Framework** (BoK CIPM & COBIT 5)
- ✓ **Metriken** (BoK CIPM & COBIT 5)
- ➢ **Technische Sicherheit & Stand der Technik im SAP** (Lehnert & SAP)
- ❖ **Rechtmäßigkeit der Verarbeitung** (abgeleitet aus Pachinger / Beham & Lehnert)
- ✓ **Data Breach** (Pollirer, allfällig erweitert mit Pachinger / Beham)
- ➢ **Datenbank SAP HANA** (SAP)

**Anmerkung des Verfassers:** Es ist zu vermuten, dass sich die Prüfpunkte zum Data Breach als hochkritisch erweisen werden und sehr viele Audits mit dem detaillierten Ansatz nach Pachinger / Beham gefahren werden müssen.

Ist für das Datenschutz-Audit nur ein sehr knappes Zeitbudget vorhanden, dann sollte vorrangig der Prüfpunkt *Data Breach* bearbeitet werden. Für die IT sind die Meldepflichten eine echte Herausforderung, weil hier noch stärker als bei Disaster Recovery unter großem Zeitdruck mit anderen Abteilungen außerhalb der IT zusammengearbeitet werden muss. Ohne detaillierte Pläne, Training und Übungen wird es wohl nicht gehen.

# 4. Prüfen im SAP

## 4.1. Noch einmal „Comply or Explain" und der Stand der Technik im SAP

Beim Prüfen mit dem BoK des CIPM, mit COBIT 5 oder der Fachliteratur war die Referenz auf den Stand der Technik implizit verständlich. Die IAPP ist die weltweit führende Berufsvereinigung von mit Privacy und Datenschutz befassten Personen und hat in über 100 Ländern mehr als 30.000 Mitglieder. Auch in Österreich dokumentieren immer mehr auf Datenschutz spezialisierte Anwälte, Wirtschaftsprüfer und Datenschutzbeauftrage ihr Fachwissen durch Zertifikate und Mitgliedschaften der IAPP.[33] Dass die von der IAPP vertretenen Ansichten, gelehrten Modelle und Vorgehensweise Stand der Technik sind, ist nach Meinung des Verfassers unbestritten gegeben.[34] Dasselbe gilt für die ISACA, welche in 188 Ländern mehr als 135.000 Mitglieder hat und über das IT Governance Institut COBIT entwickelt und hütet.[35] Bei IAPP und ISACA basiert der Referenzcharakter der entwickelten Produkte auf der Kompetenz der vielen Mitglieder, des regen Austausches in der Community und der breiten Verwendung der Produkte, Leitlinien und Standards.

Doch nun geht es in die Welt der SAP hinein. SAP-Installationen sind vielfältig, werden an den Kunden angepasst und sind individualisiert. Weiter oben wurden die Softwarebescheinigungen bereits erwähnt. Wie kann hier gegen eine Referenz geprüft werden?

Als Referenz zu *Ordnungsmäßigkeit* und *Stand der Technik* ist anzumerken: SAP liefert nicht Software alleine aus, sondern dazu eine Fülle von Betriebsmodellen, Vorgehensmodellen, best practices etc. Dies wurde in Teil I bereits dargestellt. Der Verfasser meint, dass die Nicht-Einhaltung der Empfehlungen der SAP mit der Nicht-Einhaltung einer technischen Gebrauchsanleitung gleichzusetzen ist. Es wird die Mindestforderung des Stands der Technik sein, dass

[33] (Rechtsanwälte:) Marija Križanac, Wien, CIPP/E, CIPM; Rainer Knyrim, Wien, CIPM; Thomas Schweiger, Linz, CIPP/E; Lukas Feiler, Wien, CIPP/E; Markus Kastelitz, Wien, CIPP/E; Michael M. Pachinger ist Mitglied der IAPP.

[34] https://iapp.org/about/; https://iapp.org/about/mission-and-background/

[35] http://www.isaca.org/About-ISACA/Press-room/Documents/ISACA_Fact-Sheet_0118.pdf

wenigstens die Anleitungen und Empfehlungen des Lieferanten eingehalten werden. Wer dies verabsäumt, der geht der Vermutung der *Ordnungsmäßigkeit* und des *Stands der Technik* verloren.

Auch eine gutausgebildete und erfahrene Prüferin kann nicht päpstlicher sein als der Papst und keinesfalls bessere und tiefere Produktkenntnisse aufweisen als die SAP selbst. Aber Maria kann prüfen, ob die Empfehlungen der SAP in der Future Bank eingehalten werden. Werden die SAP Systeme im Standard gefahren, dann sind sie in derselben Risikosituation wie tausende andere Installationen, welche laufend auditiert, geprüft und auf Schwachstellen untersucht werden. Werden Lücken gefunden, dann stellt der Lieferant Updates oder Konfigurationsempfehlungen bereit. Somit bilden sich aus dieser intensiver Prüftätigkeit in Kombination mit den Anleitungen der SAP der *„Stand der Technik"* und die *GoB* von selbst heraus – als weitverbreitete Übung und Ansicht einer Vielzahl weitweit tätiger Experten.

**PRAXIS 01:** SAP-Systeme sind ein unteilbares Software-Produkt. Fragen der allgemeinen IT-Sicherheit sind aus Sicht der Ordnungsmäßigkeit des Rechnungswesens genauso zu sehen wie Fragen des technischen Datenschutzes. Somit gilt

- Alle technischen Security-Checks und Überprüfungen im Zuge des Jahresabschlusses sind gleichzeitig auch Überprüfungen des Standes des technischen Datenschutzes.
- Sämtliche SAP-Security-Leitfäden, sämtliche bislang bekannten Dokumente, Checklisten, Prüfleitfäden & technischen Vorgehensweisen gelten auch für den technischen Datenschutz im SAP.

## 4.2. Maria Nicoleta auditiert die technische Sicherheit der SAP HANA

**Maria Nicoleta prüft die Datenbank SAP HANA**

Die Future Bank hat im Verlauf des letzten Jahres die SAP-Systeme auf die neue Datenbank HANA migriert. Eine riesige Anzahl personenbezogener Datensätze wird nun dort gehalten. Es wurde noch niemals gegen die HANA auditiert, auch nicht vom IT-Audit. Technologie und Produkt sind neu und es gibt noch keine Erfahrungen – ein klassischer Anwendungsfall für *„Comply or Explain"*!

Schon nach wenigen Minuten Recherche wird Maria auf http://help.sap.com fündig und orientiert sich in den 278 Seiten des **SAP HANA Security Guide**.[36] Wie bei den Security Guides üblich, ist das Dokument übersichtlich gegliedert, gut strukturiert und eine perfekte Ausgangsbasis für das bereits bekannte Ableiten der Checklisten. Doch diesmal kann sich Maria das Ableiten sparen! Gleich im ersten Absatz des ersten Kapitels verweist die SAP auf eine Checkliste zum Prüfen der kritischen Teile der Konfiguration, auf die **SAP HANA Security Checklists and Recommendations (For SAP HANA Database)**.[37]

Wenige Mouse-Clicks später ist Maria bereits im Besitz des Dokuments. Hinweis: Achten Sie auf den richtigen Release-Stand der Dokumentation! Das 34-seitige Dokument ist perfekt, kann ohne jedwede Adaptierung für die erste Prüfung der Datenbank herangezogen werden und ist auch für Nicht-Techniker verständlich. Somit ist nun auch das Prüfprogramm für die Datenbank einsatzbereit. Das Audit selbst ist einfach: Abfragen der Checkliste und Verifikation der Antworten. Maria sieht da absolut kein Problem und ist mehr als überrascht, wie einfach das wird.

[36] SAP HANA Security Guide, SAP HANA Platform SPS 12, Document Version: 1.2 – 2018-01-24. https://help.sap.com/doc/eec734dbb0fd1014a61590fcb5411390/1.0.12/en-US/SAP_HANA_Security_Guide_en.pdf

[37] SAP HANA Security Checklists and Recommendations, SAP HANA Platform 2.0 SPS 01, Document Version: 1.0 – 2017-04-12. https://help.sap.com/doc/3cffa43c8e3843cdae23f9abfe47355e/2.0.01/en-US/SAP_HANA_Security_Checklists_and_Recommendations_en.pdf

**SYSTEM User**

Table 1:

| | |
|---|---|
| Default | The database user `SYSTEM` is the most powerful database user with irrevocable system privileges. The `SYSTEM` user is active after database creation. |
| Recommendation | Use `SYSTEM` to create database users with the minimum privilege set required for their duties (for example, user administration, system administration). Then deactivate `SYSTEM`. |
| How to Verify | In the system view `USERS`, check the values in columns `USER_DEACTIVATED`, `DEACTIVATION_TIME`, and `LAST_SUCCESSFUL_CONNECT` for the user `SYSTEM`. |
| Related Alert | No |
| More Information | See the sections on predefined users and deactivating the SYSTEM user in the *SAP HANA Security Guide*. |

**ABB. 8: Prüferfreundliche Checkliste zur Security der HANA (Beispiel User SYSTEM)**[38]

- ✓ **Governance** (BoK CIPM & Pachinger / Beham)
- ✓ **Framework** (BoK CIPM & COBIT 5)
- ✓ **Metriken** (BoK CIPM & COBIT 5)
- ➢ **Technische Sicherheit & Stand der Technik im SAP** (Lehnert & SAP)
- ❖ **Rechtmäßigkeit der Verarbeitung** (abgeleitet aus Pachinger / Beham & Lehnert)
- ✓ **Data Breach** (Pollirer, allfällig erweitert mit Pachinger / Beham)
- ✓ **Datenbank SAP HANA** (SAP)

## 4.3. Datenschutz-Audit im SAP „mit dem Lehnert in der Hand"

Als Letztes verbleibt der Stand des Datenschutzes in der Applikation, im SAP selbst. Bislang hatte Maria sich v.a. um die Einbettung der SAP-Systeme in die Compliance-Landschaft und die Prozesse gekümmert. Jetzt geht es um die komplexe Anwendung selbst. Und auch hier wird Maria „*Comply or Explain*" einsetzen.

Beim applikatorischen Datenschutz stützt sich Maria wiederum auf ein Referenzwerk, auf das im November 2017 bei Rheinwerk erschienene Buch „*Datenschutz mit SAP*". Angeführt von Volkert Lehnert treten mit Iwona Luther, Björn Christoph, Carsten Pluder & Co ausgewiesene Experten der SAP als Autoren auf. Alle sind sie in der SAP in für das Thema Datenschutz zentralen Positionen tätig, haben die Produkte entwickelt und konzipiert und eine große Anzahl an Projekten abgewickelt. Lehnert war ab 2012 bei SAP SE *Product Owner Datenschutz SAP Business Suite & S/4HANA* und ist seit 2018 *Chief Product Expert / Senior Director Data Protection S/4HANA*. Er ist Co-Autor des aus Teil I bereits bekannten Datenschutzleitfadens der DSAG und Mitverfasser der Standardwerke zum Berechtigungswesen. Iwona Luther ist *Product Standard Owner für ILM*, das *Information Lifecycle Management*, das im Buch ausführlich dargestellt wird. Und auch all die anderen Autoren und Co-Autoren sind mit den im Buch vorgestellten Produkten bestens vertraut.[39]

SAP Vorstand Bernd Leukert schreibt im Vorwort auf S. 17: *„Das Autorenteam des vorliegenden Werks hat in den letzten Jahren alle Funktionalitäten in der SAP Business Suite und SAP S/4HANA geschaffen, um einen datenschutzkonformen Betrieb zu ermöglichen. Nun war es diesem Team ein Anliegen, eine*

[38] SAP HANA Security Checklists and Recommendations, SAP HANA Platform 2.0 SPS 01, Document Version: 1.0 – 2017-04-12, S. 6.

[39] Lehnert, Volker. Luther, Iwona. Christoph, Björn. Pluder, Carten et. a. (2018). Datenschutz mit SAP. SAP Business Suite und SAP S/4HANA. Aktuell zur DSGVO. Rheinwerk Verlag, Bonn, S. 425-427.

*Anleitung bereitzustellen, die wesentlich detaillierter als in einer Dokumentation beschreibt, was Sie tun können, um diese hochgradig vernetzten und komplexen Funktionalitäten datenschutzrechtlich ‚zum Fliegen' zu bringen.*"[40] Nach diesen Zeilen ist klar: Dieses Buch ist kein Werk verschrobener Denker mit irrelevanten Einzelmeinungen, sondern ein Vorstand der SAP bestätigt im Vorwort explizit die fachliche Kompetenz der Autoren und die besondere Qualität des Buches. Somit beschreibt dieses Buch den „*Stand der Technik*" und ist Gebrauchsanleitung und Referenz. An diesem Buch wird niemand vorbeigehen können, der sich mit SAP und Datenschutz befasst.

Wer mehr über dieses exzellente Buch wissen will, der möge die vom Verfasser geschriebene Rezension auf Amazon nachlesen.[41] Eine weitere Besprechung des Buches ist im Newsletter 01/2018 des Instituts für Interne Revision erschienen.


**ABB. 9: Der Lehnert, das Referenzwerk: https://www.rheinwerk-verlag.de/datenschutz-mit-sap_4524/**

Volker Lehnerts Photo wurde der Amazon-Autorenseite entnommen[42] und der Anzeige des Rheinwerk-Verlags hinzugefügt.

[40] Lehnert, Volker; Luther, Iwona; Christoph, Björn; Pluder, Carsten et. al. (2018). Datenschutz mit SAP. SAP Business Suite und SAP S/4HANA. Aktuell zur DSGVO. Rheinwerk Verlag, Bonn, S. 17.

[41] Pichl, Walter. DAS Referenzwerk zum „Stand der Technik!" Buchrezension zu Lehnert et. al, Datenschutz im SAP, Rheinwerk 2017. Gepostet am 10. Dezember 2017, https://www.amazon.de/Datenschutz-mit-SAP-Praxisleitfaden-EU-Datenschutz-Grundverordnung/dp/3836259893/ref=asap_bc?ie=UTF8

[42] https://www.amazon.de/Volker-Lehnert/e/B004JE7Y1G/ref=ntt_dp_epwbk_0

**Maria Nicoleta auditiert Datenschutz im SAP „mit dem Lehnert in der Hand“**

Maria ist begeistert. Im *Lehnert* findet sich eine vollständige Darstellung des Themas Datenschutz im SAP. Von der Einführung in die rechtlichen Grundlagen über die Darstellung der hochkomplexen Lösung *ILM (Information Lifecycle Management)* bis zu einzelnen wichtigen, den Datenschutz unterstützenden Produkten wie *RAL (Read Access Logging)* oder *TDMS (Test Data Migration Server)*. Besonders angetan ist Maria Nicoleta von Kapitel 12. Hier ist nichts abzuleiten, die Prüfhandlungen und Checks sind klar beschrieben und können ohne weitere Nacharbeiten übernommen werden! Die Prüfung geht tief in den technischen Systemkern hinein. SAP-kundige Prüfer und Systemadministratoren bestätigen ihr: Genau so sollte geprüft werden!
Wie in allen überragenden Fachbüchern üblich, finden sich viele weiterführende Hinweise in die Fachliteratur und ein professionelles Literaturverzeichnis.
Maria Nicoleta stimmt der Amazon-Rezension des Verfassers zu:
*„Den Auditoren und Prüfern ist ein eigenes Kapitel 12 (S. 353 bis 413) gewidmet. Hier findet sich eine Vielzahl einzelner Prüfhandlungen, welche auch einzeln durchgeführt werden können. Wer mit diesen 61 Seiten ein SAP System auditiert hat, hat ein hochwertiges und v.a. referenzierbares Prüfprogramm durchgeführt. Mich hat dieses Prüfprogramm mehr als überzeugt. Ich werde meine eigenen Prüfpfade kritisch reviewen und auf das Buch referenzieren.“*[43]

Mit Kapitel 12 aus dem Lehnert hat Maria das Prüfprogramm vervollständigt. Zum Abschluss macht sie noch zwei Qualitäts- und Vollständigkeitschecks.

**PRAXIS 02**: Maria lädt das 76-seitige Dokument SAP SE: BS10012:2009[44], studiert es sorgfältig und gleicht ihren bereits entwickelten Fragenkatalog mit dem Katalog im Dokument ab. Solche Prüfprogramme sind sehr selten öffentlich zugänglich.

**PRAXIS 03**: Noch vor dem Start des Audit bemüht sich Maria um einen Termin beim Vorstand. Sie möchte erfahren, welchen Reifegrad der Datenschutz-Organisation der Vorstand als angemessen und notwendig erachtet. Maria vermutet, dass sie vorerst auf Ratlosigkeit treffen wird. Aber: **Datenschutz ist nicht alleine gegen das Gesetz zu prüfen, sondern gegen die Strategie und die Ziele des Unternehmens.**

- ✓ **Governance** (BoK CIPM & Pachinger / Beham)
- ✓ **Framework** (BoK CIPM & COBIT 5)
- ✓ **Metriken** (BoK CIPM & COBIT 5)
- ✓ **Technische Sicherheit & Stand der Technik im SAP** (Lehnert & SAP)
- ✓ **Rechtmäßigkeit der Verarbeitung** (abgeleitet aus Pachinger / Beham & Lehnert)
- ✓ **Data Breach** (Pollirer, allfällig erweitert mit Pachinger / Beham)
- ✓ **Datenbank SAP HANA** (SAP)

- finis -

[43] Pichl, Walter. DAS Referenzwerk zum „Stand der Technik!“ Buchrezension zu Lehnert et. al, Datenschutz im SAP, Rheinwerk 2018. Gepostet am 10. Dezember 2017, https://www.amazon.de/Datenschutz-mit-SAP-Praxisleitfaden-EU-Datenschutz-Grundverordnung/dp/3836259893/ref=asap_bc?ie=UTF8

[44] bsi. BS 10012. Customer Audit Report 2016. Data protection Certification of SAP British Standards Institution (BSI), BSI Group Deutschland GmbH, Frankfurt am Main, 2016 December 31. https://assets.cdn.sap.com/sapcom/docs/2016/05/f082a383-707c-0010-82c7-eda71af511fa.pdf

# Abbildungsverzeichnis



# Abkürzungsverzeichnis

| | |
|---|---|
| Abs | Absatz |
| Art | Artikel |
| BGBl | Bundesgesetzblatt |
| BOK | Body-of-Knowledge, Summe des Wissens eines Fachgebietes |
| BYOD | Bring Your Own Device |
| CIA | Certified Internal Auditor |
| CIPP | Certified Information Privacy Professional |
| CIPM | Certified Information Privacy Manager |
| CIPT | Certified Information Privacy Technologist |
| DaKo | Datenschutz Konkret (Zeitschrift) |
| DSGVO | Datenschutzgrundverordnung |
| gem | gemäß |
| GoB | Grundsätze ordnungsmäßiger Buchführung |
| IAPP | International Association of Privacy Professionals |
| idF | in der Fassung |
| ILM | Information Lifecycle Management |
| IDVK | Internationaler Datenverkehr |
| RAL | Read Access Logging |
| SAP | Systeme, Anwendungen und Produkte in der Datenverarbeitung |
| TDMS | Test Data Migration Server |
| UGB | Unternehmensgesetzbuch |
| WV | Wiederverlautbarung |

# Wie Unternehmenskommunikation und Good Governance zusammenspielen

**Ines Schubiger**
absolvierte das Studium der Betriebswirtschaftslehre an der Universität Linz. Bereits während ihres Studiums beschäftigte sie sich mit Themen der Organisationsentwicklung und Besonderheiten der Steuerung öffentlicher Verwaltungen bzw. Unternehmen. Seit 2009 verantwortet sie die Bereiche Revision und Organisationsentwicklung bei viadonau – Österreichische Wasserstraßen-Gesellschaft mbH. Ines Schubiger ist Mitglied des IIRÖ-Vorstandes.

**Eva Michlits**
ist seit September 2017 Senior Beraterin bei wikopreventk in Wien. Davor leitete sie viele Jahre die Unternehmenskommunikation bei viadonau und war zudem Pressesprecherin. In ihrer Funktion verantwortete sie die interne und externe Kommunikation sowie die Public Affairs-Agenden. Michlits studierte Geographie und Deutsche Philologie an der Universität Wien und hat ein MBA-Studium für Communications and Leadership an der Donau-Universität Krems absolviert.

Die beiden Autorinnen haben zum Thema passend das Seminar Kommunikation.Wirkung.Revision gestaltet, in dem sie einmal mehr zeigen, wie gut sich Kommunikation und Interne Revision verstehen.

## Inhalt

# 1. Eine Lanze für das Kommunikationscontrolling

*In der Kommunikationsbranche ist man sich einig: Kommunikation ist ein zentraler Bestandteil des Unternehmenserfolgs. In der Betriebswirtschaftslehre wird die Kommunikation aber weder als Führungs- noch als Kernprozess, sondern lediglich als Unterstützerprozess gesehen. Kommunikationscontrolling gilt als ein wirksames Instrument, um den Wertschöpfungsbeitrag für die Unternehmensführung sichtbar zu machen. Die Interne Revision erhält damit nicht nur ein neues Prüfgebiet, sondern auch wertvolle Inputs für die Good Governance. Setzen die Kommunikatoren mit Kommunikationscontrolling auf das richtige Pferd und welche Antworten bekommen die Internen RevisorInnen? Dieser Frage gehen Ines Schubiger und Eva Michlits in ihrem Beitrag nach.*

Good Governance und die damit einhergehenden Führungs- und Steuerungssysteme sind in aller Munde – nicht zuletzt durch die zahlreich geführten Governance-, Risk and Compliance-Diskussionen und das Three-Lines-of-Defense-Modell (TLoD). Dieses veranschaulicht das Zusammenspiel der Verteidigungslinien sehr gut und fördert das Verständnis für Führung und Überwachung im Unternehmen.

In der zweiten Verteidigungslinie des TLoD denkt man vorrangig an das Enterprise Risk Management, das Compliance-System, die IT-Governance oder QM-Systeme. Das Controlling – als umfassendes Planungs- und Steuerungssystem eines Unternehmens – ist ebenso ein wichtiger und zentraler Bestandteil der zweiten Verteidigungslinie. Kosten-, Personal-, Produktions- sowie Vertriebs- und Einkaufscontrolling sind dabei die bekanntesten Disziplinen.

> Für mich als Interne Revisorin ist Kommunikationscontrolling ein Prüffeld mit Potenzial.
> *Ines Schubiger, IIRÖ-Vorstandsmitglied*

Kommunikationscontrolling gilt bislang als eine vernachlässigte Disziplin. Das Gießkannenprinzip und für jede Stakeholdergruppe das „passende Budget" erscheinen in Zeiten von Budgetreduktionen, Erfolgsmessung und Wirkungsorientierung nicht mehr angebracht.

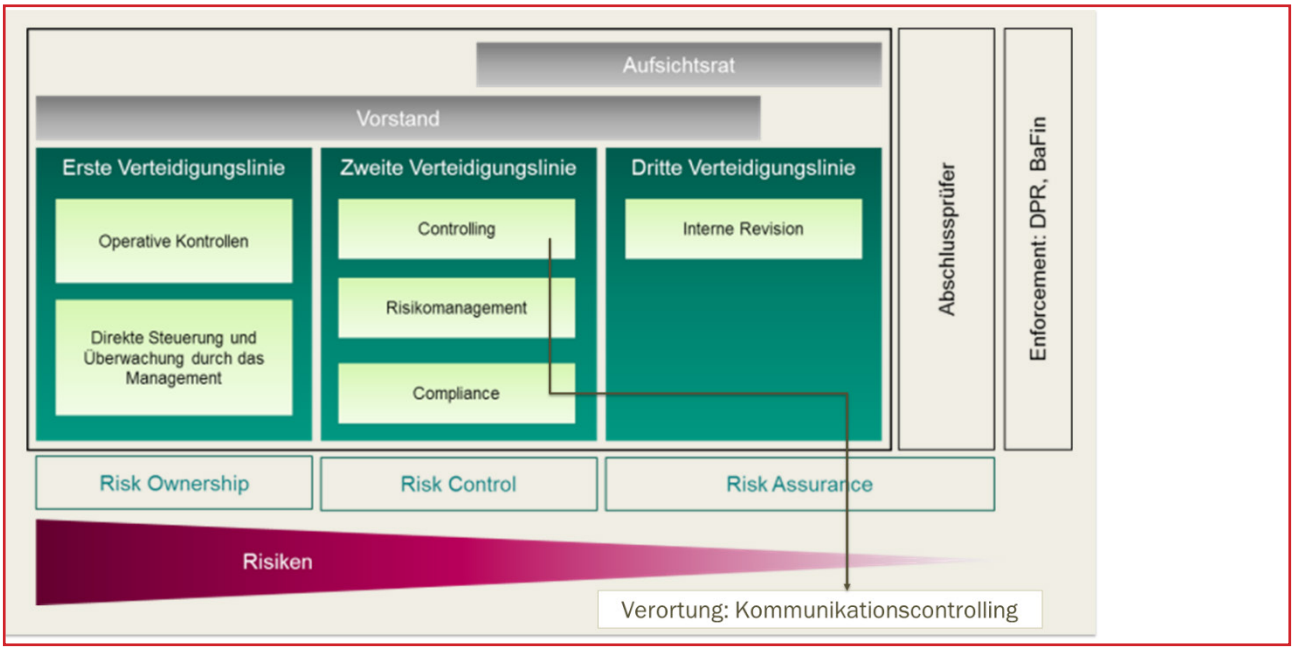



**ABB. 1: angelehnt an FERMA/ECIIA: Guidance on the 8th EU Company Law Directive, article 41**

In Übertragung und Anwendung des allgemeinen Controllingbegriffs meint Kommunikations-controlling die *Planung, Steuerung und Kontrolle* der Aktivitäten der Unternehmens-kommunikation.

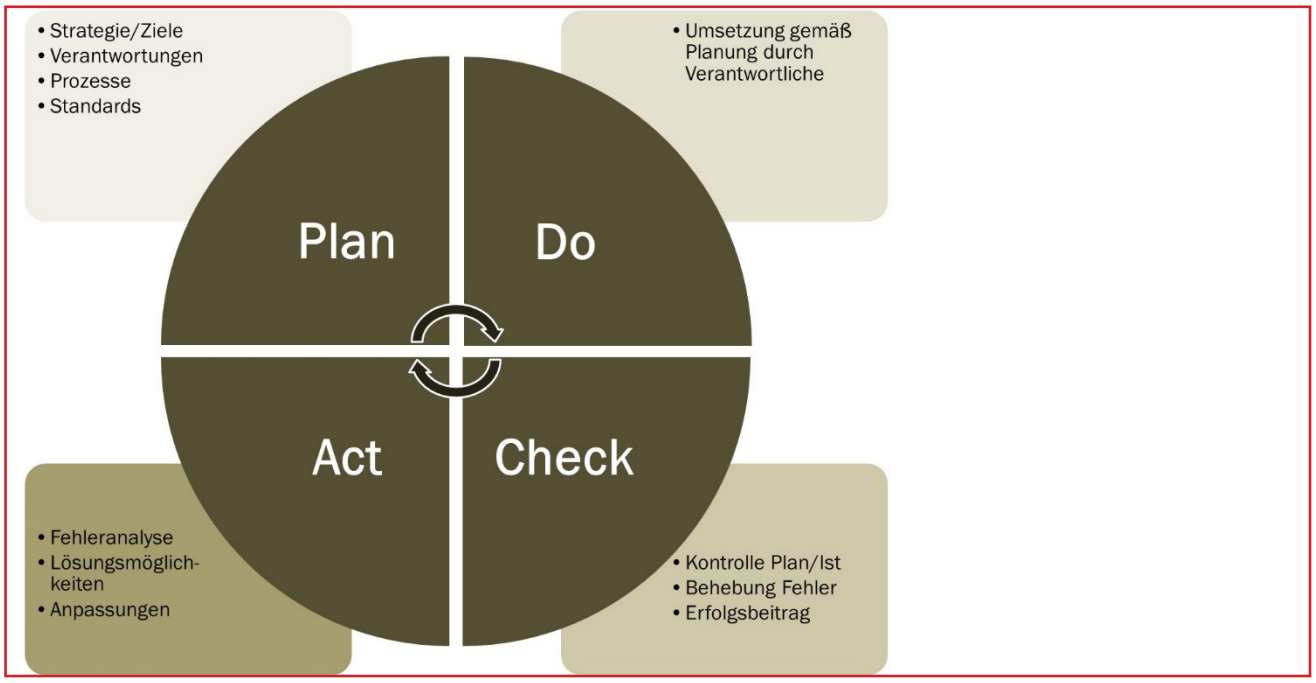



**ABB. 2: PDCA-Zyklus - Eigene Darstellung Schubiger/Michlits**

## 2. Verknüpfte Strategien

Entscheidend für den Erfolg von Kommunikations-controlling ist die Verknüpfung der Kommunikationsziele mit der strategischen Ausrichtung und den Zielen eines Unternehmens. Denn nur eine an der Unternehmensstrategie ausgerichtete Unternehmens-kommunikation kann einen Beitrag zur Wertschöpfung und Reputation eines Unternehmens liefern.

Die Definition einer Kommunikationsstrategie abgeleitet von der Unternehmensstrategie, die Festlegung von Kommunikationszielen sowie das Umsetzen und Steuern der Projekte bzw. Kommunikations-maßnahmen zählen somit zu den zentralen Aufgaben des Kommunikationscontrollings.

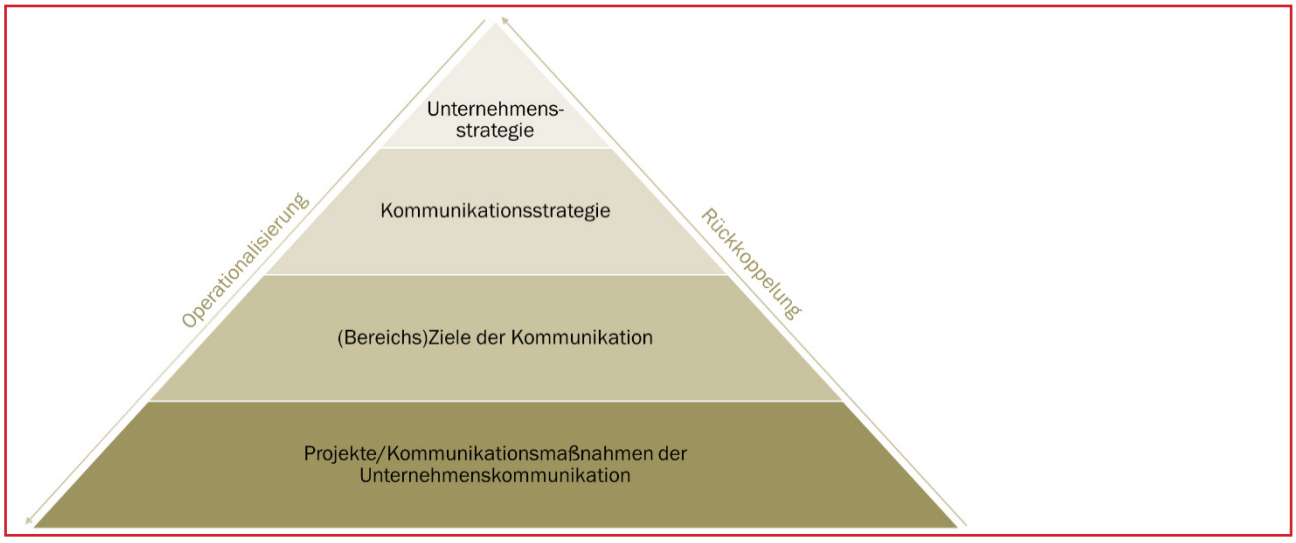



**ABB. 3: Kaskadierendes Zielsystem - Eigene Darstellung Schubiger/Michlits**

Als wirksam kann die Arbeit der Unternehmenskommunikation dann bezeichnet werden, wenn sich die gesetzten Kommunikationsmaßnahmen auf den monetären sowie den nicht monetären Erfolg des Unternehmens beziehen.

Aus der Perspektive der Good Governance braucht es eine wirksame Kommunikation, um

- die Stakeholder-Interessen ausgewogen zu wahren,
- die Anteilseigner/Eigentümer stets über wesentliche Unternehmensaktivitäten informiert zu halten,
- das Handeln des Managements transparent zu machen und
- den Erfolg des Unternehmens nachhaltig zu sichern.

Aus Sicht der Internen Revision, der dritten Verteidigungslinie des TLoD, braucht es eine wirksame Kommunikation, um

- die Strategie und strategischen Ziele des Unternehmens bestmöglich zu unterstützen,
- Schaden vom Unternehmen, insbesondere in Krisenfällen, abzuwehren,
- das Vertrauen relevanter Stakeholder in das Unternehmen zu fördern und damit die Nachhaltigkeit des Unternehmens zu sichern,
- einen Wertschöpfungsbeitrag zum Unternehmen zu leisten sowie
- die interne Kommunikation durch entsprechende Informations- und Kommunikationswege sicherzustellen.

Eine regelmäßige Prüfung der Aktivitäten der Unternehmenskommunikation muss und soll deshalb Bestandteil der Prüflandkarte der Internen Revision sein.

## 3. Wie Kommunikation messen?

In der Realität sind Kommunikationsabteilungen nicht selten „Blackboxes". Der Input in Form von Personal- und Sachkosten und der Output bzw. das Endprodukt – wie Internet- und Intranetauftritte, Social Media, KundInnenmagazine, Veranstaltungen etc.– sind in der Regel bekannt. Welche konkreten Ziele die einzelnen Projekte und Kommunikationsmaßnahmen verfolgen bzw. welchen substanziellen Beitrag diese zu den Unternehmenszielen leisten, sind oftmals weniger bekannt. In vielen Fällen bleibt es bei reinen Ordnungsprüfungen. Eine Blitzumfrage unter Revisionsleiterinnen und Revisionsleitern hat gezeigt, dass die Unternehmenskommunikation in der Prüflandkarte sehr wohl ihren Platz hat, aber unisono herrscht die Meinung, dass man *„daraus mehr machen könnte"*. Aber wie lässt sich der Beitrag der Unternehmenskommunikation zum Unternehmenserfolg messen? Welche Voraussetzungen müssen gegeben sein?

In einem ersten Schritt braucht es ein Bekenntnis zu einem Kennzahlensystem und somit zur damit einhergehenden Transparenz. Um den Erfolg der gesamten Unternehmenskommunikation bewerten und steuern zu können, muss ein brauchbares und gelebtes Kennzahlensystem alle Kommunikationsziele und -maßnahmen berücksichtigen. Dabei sind die strategischen Ziele des Unternehmens ebenso einzubeziehen wie die Kernziele und Prozesse der Unternehmenskommunikation. Das System muss einfach handhabbar und ökonomisch sinnvoll sein, denn nur so kann der direkte Wert der Kommunikation für das Unternehmen gemessen und sichtbar gemacht werden.

Für das Kennzahlensystem ist in einem ersten Schritt die Kommunikationsrealität des Unternehmens in einer Matrix abzubilden und in einen Zusammenhang zwischen Unternehmenszielen, Kommunikationszielen, Zielgruppen, Prozessen und Maßnahmen zu bringen. Gleichzeitig werden Kennzahlen definiert, die einen sinnvollen Erkenntnisgewinn im Hinblick auf die Erfüllung der Kommunikationsziele bieten. Anschließend sind relevante Kennzahlen den jeweiligen Messinstrumentarien zuzuordnen. Aus der Kommunikationsrealität lassen sich in Folge Reports für das Kommunikationscontrolling generieren.

Kommunikationscontrolling dient letztendlich der Professionalisierung der Branche als auch der Kommunikatoren.
Eva Michlits, wikopreventk

## 4. Die Krux mit den Kennzahlen

Klassische Kennzahlen wie Fehlerquoten oder Zeittreue sind zwar einfach zu erheben, die Signifikanz in der Kommunikation ist allerdings zu hinterfragen. Auf die Servicequalität zahlen hingegen Kennzahlen wie die Reaktionszeit für Medienanfragen ein – also jene Stunden, die aufgewendet werden, um die Anfrage einer Journalistin bzw. eines Journalisten zu beantworten. Der Unternehmenskultur hilft wiederum ein laufend aktualisiertes und optisch ansprechendes Intranet mit interaktiven Elementen. Es ist nicht immer leicht, den ausgetretenen, allerdings bequemen Pfaden auszuweichen. Viele Maßnahmen haben durch den Lauf der Jahre oder aufgrund von Veränderungen in den Unternehmen an Aussagekraft und Wirkung verloren. Die Etablierung eines Kennzahlensystems geht einher mit einem kritischen Hinterfragen der Maßnahmen und kann durchaus auch zu einer Reduktion der bislang umgesetzten Aktivitäten führen.

Die Visualisierung der Kennzahlen ist dabei essentiell – als Werkzeug, aber auch für das Reporting intern. Ein Kommunikationshaus kann ein Beispiel für die Darstellung eines Kennzahlensystems sein. Die Grafik zeigt ein Kommunikationshaus mit drei Kernbereichen der Unternehmenskommunikation und jeweils zwei aussagekräftigen Kennzahlen.

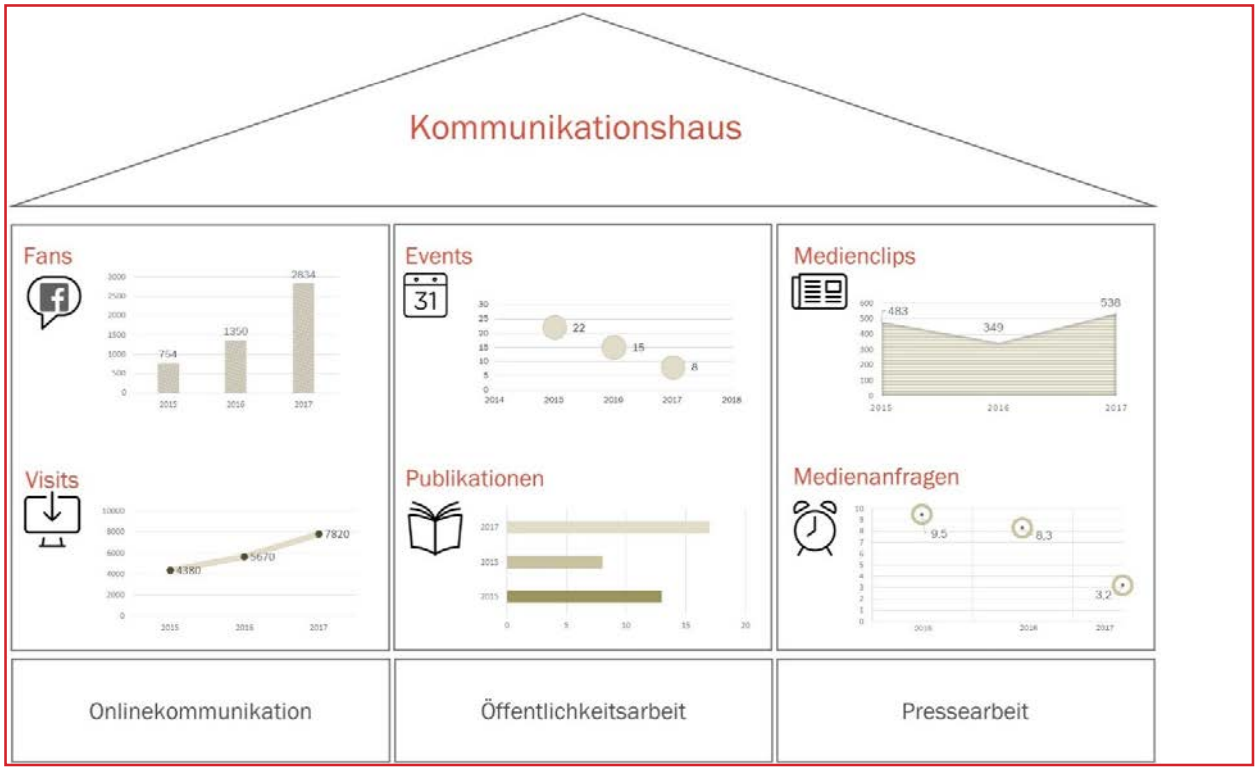



**ABB. 4: Kommunikationshaus als Reporting (fiktives Beispiel) - Eigene Darstellung Michlits**

Die jährlich erhobenen Kennzahlen zahlen im Idealfall auf die Kommunikationsziele ein. So bedient die Kennzahl „Visits" die Websitenutzung und damit das Kommunikationsziel „*Die Stakeholder mit Informationen zum Unternehmensgegenstand versorgen*". Die Tendenz dieser Kennzahl ist eindeutig positiv. Die Maßnahme wirkt somit und die Mittel sind richtig eingesetzt. Am Beispiel „Publikationen" hingegen lässt sich gut darstellen, wie Kennzahlen optimiert werden können. Als erster Schritt kann eine rein quantitative Erhebung der produzierten Publikationen erfolgen – eine richtige, aber einflusslose Aussage. Die Definition als Kennzahl für Publikationen, die den Kriterien des Österreichischen Umweltzeichens entsprechen, steigert den Wert der Aussage deutlich. Zudem gelingt damit die Verknüpfung zur CSR-Strategie oder zu den EMAS-Zielen eines Unternehmens. Ein Kennzahlensystem ist somit kein starres Element, sondern ein lebendes Instrument für die strategische Arbeit der Kommunikationsverantwortlichen.

## 5. Das System prüfen

Erst durch ein etabliertes Kommunikationscontrolling ist eine umfassende Prüfung der Unternehmenskommunikation durch die Interne Revision möglich. Diese kann mit Hilfe vorhandener Instrumentarien – über reine Ordnungs- und Wirtschaftlichkeitsprüfungen hinaus – die Treffsicherheit und Wirksamkeit von Kommunikationsmaßnahmen und -aktivitäten systematisch überprüfen. Sich mit diesem Prüfthema näher auseinanderzusetzen bietet die Chance, die Unternehmenskommunikation ganzheitlich zu prüfen und die Wirkungen in den Prüfungsfocus zu setzen.

Die Reputation eines Unternehmens hat nicht nur Einfluss auf seine MitarbeiterInnen und KundInnen. Auch für Investoren ist das Image entscheidend für den Unternehmenswert. Die Unternehmenskommunikation ist es also wert, durch die Interne Revision genauer unter die Lupe genommen zu werden.

# Zu klein für eine eigene Interne Revision

## Externe Interne Revisionen bei kleineren Unternehmen des öffentlichen Sektors

**Hannes Schuh**
Dr. Hannes Schuh ist Leiter der Internen Revision des Bundesministeriums für Finanzen, Sprecher des Kontrollkollegiums der Europäischen Patentorganisation und war langjähriges Vorstandsmitglied des Österreichischen Institutes für Interne Revisionen

## Inhalt

# 1. Vorbemerkungen

## 1.1. Allgemein

Öffentliche Unternehmen besitzen hohe gesellschaftspolitische und ökonomische Relevanz bei der Wahrnehmung von öffentlichen Aufgaben.[1] In Österreich entfällt auf staatseigene und staatsnahe Unternehmen ein großer Teil des BIP, der Beschäftigung und der Marktkapitalisierung. Es kommt daher auf die Corporate Governance dieser Unternehmen an, um sicher zu stellen, dass sie einen positiven, fairen, transparenten Beitrag zur gesamtwirtschaftlichen Effizienz und Wettbewerbskraft Österreichs in einer Weise leisten, die allgemein anerkannt, geschätzt und akzeptiert ist.[2]

Unter Corporate Governance versteht man in der Regel das System, nach dem Unternehmen geführt und kontrolliert werden, sowie eine Reihe definierter Beziehungen zwischen der Führung und dem Leitungsorgan eines Unternehmens sowie zu seinen Aktionären und sonstigen Akteuren.[3] Staatseigene Unternehmen sollten eine interne Audit-Stelle einrichten.[4] Die Interne Revision ist dabei, dem Three Lines of Defence-Modell folgend, als Überwachungsinstanz derart in der Organisation positioniert, dass sie für die Unternehmensführung und den Aufsichtsrat grundsätzlich die Leistungsfähigkeit der unternehmensweiten Kontrollen der internen Kontroll- und Überwachungssysteme prüft.[5]

Die für Interne Revisionen maßgeblichen Standards sind jene des Institute of Internal Auditors, im weiteren Sinne umfassen sie die Mission, Grundprinzipien, Definition, Ethikkodex, Standards, Implementierungsleitlinien.[6] Die Internationale Vereinigung der Rechnungshöfe (INTOSAI) legt ihrem Verständnis von Interner Revision diese Standards zugrunde und sieht in der IR ein wichtiges Element der Good Governance.[7]

Die Sinnhaftigkeit der Nutzung einer Internen Revisionsfunktion steht außer Zweifel. Die Frage der verpflichtenden Nutzung kann jedenfalls für jene öffentlichen Unternehmen beantwortet werden, für die der Bundes Public Corporate Governance Kodex (B-PCGK) oder der Österreichische Corporate Governance Kodex gilt.[8] Explizite Ableitungen aus gesetzlichen Bestimmungen sind nicht möglich, sie ergeben sich zumeist aus Verpflichtungen in Zusammenhang mit der Führung eines Internen Kontrollsystems.[9]

[1] Papenfuß / Eulerich, ZIR 1/13 Seite 36

[2] Vgl. B-PCGK, Seite 6

[3] Vgl. EK-Grünbuch, Seite 2 f.

[4] OECD-Leitsätze, Seite 46

[5] Eulerich, ZIR 2/12 Seite 56

[6] Internationale Grundlagen für die berufliche Praxis der Internen Revision 2017–im Folgenden IPPF (International Professional Practices Framework) genannt.

[7] INTOSAI GOV 9140, Punkt 1.6

[8] Wegen der Fokussierung dieses Artikels auf Kleinunternehmen und im Hinblick auf den Adressatenkreis des ÖPCGK (d.s. österreichische börsennotierte Aktiengesellschaften) wird darauf nicht weiter Bezug genommen.

[9] Vgl. etwa Aigner / Aigner / Aigner, SWK 20/21, Seite 944 f

## 1.2. Eigene oder externe Interne Revision?

Die Grundsatzentscheidung, ob eine eigene Organisationseinheit eingerichtet wird, eine entsprechende Dienstleistung zugekauft wird oder die Aufgabe unmittelbar durch das Leitungs- und/oder Kontrollorgan wahrgenommen wird, ist durch das jeweilige Unternehmen zu treffen und kann nicht allgemein beantwortet werden.

Zu berücksichtigen sind wohl

- Art und Umfang der Geschäfte des Unternehmens
- Anzahl der beschäftigten Personen des Unternehmens
- Reifegrad der strategischen Ausrichtung der Internen Revision
- Art, Umfang und Häufigkeit der erforderlichen Revisionen
- Inkompatibilität der Prüfungstätigkeit mit anderen Funktionen
- Mindestzahl an Revisoren um die Aufgaben objektiv, unabhängig und qualitätsvoll wahrnehmen zu können.

Der B-PCGK verpflichtet in Abschn. 13.1 Unternehmen mit mehr als 30 Bediensteten oder einem Jahresumsatz von mehr als 1 Mio. € und Konzerne interne Revisionsstellen einzurichten, die auf Basis allgemein anerkannter internationaler Revisionsstandards innerbetriebliche Revisionen durchführen und führt in der Anmerkung aus, dass dies nicht bedeutet, hierfür eine eigene Organisationseinheit zu schaffen.

Selbst wenn man die „Enquêtes“[10] der deutschsprachigen Revisionsinstitute zu Rate zieht, ergibt sich für kleine Unternehmen kein stabiles Bild. Aufgrund des Erhebungsergebnisses von 1,97 Revisoren pro 1.000 Mitarbeiter bei Unternehmen mit 1.000 bis 2.000 Mitarbeitern[11] kann mit einiger Vorsicht behauptet werden, dass bei Unternehmen mit mindestens 1.000 Mitarbeitern eine eigene Revisionsstelle jedenfalls Sinn macht.

# 2. Ausgangslage

Der Artikel geht von folgender Ausgangslage aus:

- Das Unternehmen ist aufgrund eines Ausgliederungsgesetzes ausgegliedert.
- Es steht im Eigentum des Bundes.
- Der B-PCGK ist anzuwenden.
- Die Eigentümerfunktion des Bundes wird letztlich über ein Ministerium wahrgenommen, das Unternehmen verfügt über ein Aufsichtsorgan (Aufsichtsrat[12]) und ein Leitungsorgan (Vorstand oder Geschäftsführung).
- Die Funktion einer Internen Revision wird über qualifizierte externe Experten ausgeübt.

Er versucht, zunächst die in den Corporate Governance Kodices erwähnten allgemeinen Kontrollpflichten darzustellen und in der Folge die in den Internationalen Grundlagen für die berufliche Praxis der Internen Revision 2017 (IPPF - The International Professional Practices Framework) enthaltenen verbindlichen Elemente funktional zuzuordnen.

[10] Als Enquêtes werden hier Mitgliederbefragungen des deutschen, österreichischen und schweizerischen Revisionsinstitutes verstanden, Publikationen: Eulerich, Enquête 2011, Eulerich, Enquête 2014, Eulerich, Enquete 2017

[11] Enquête 2014, Seite 55

[12] Vgl. auch Abschn. 7.6.1 B-PCGK: C-Regel für Überwachungsorgan bei Unternehmen mit mehr als 30 Bediensteten oder einem Jahresumsatz von mehr als 1 Mio. €, sofern es keine rechtliche Verpflichtung gibt.

# 3. Allgemeine Kontrollpflichten auf Basis des Corporate Governance Kodex

Die sich für die Gesellschaftsorgane ergebenden Kontrollpflichten werden aus der Perspektive der OECD-Leitsätze zu Corporate Governance in staatseigenen Unternehmen (2006), ergänzt um die OECD-Grundsätze für Corporate Governance (2015), sowie aus der Perspektive des Bundes Public Corporate Governance Kodex (2017) betrachtet.

Begriffe, welche die Organe der Gesellschaft betreffen sind innerhalb ihres jeweiligen Funktionskreis (Eigentum, Aufsicht, Leitung) synonym zu lesen. Die unterschiedliche Bezeichnung ist im Allgemeinen der jeweiligen Quelle geschuldet.

## Eigentümer

Die organschaftliche Stellung der Eigentümer basiert auf allgemeinen gesellschaftsrechtlichen Grundsätzen bzw. den gesellschaftsrechtlichen Bestimmungen des Einzelfalls. Vorgelagerte Willensentscheidungen des Anteilseigners (z.B. Bund) sind strikt von Willensbildungen des Eigentümers (Organ der Gesellschaft) zu trennen.

Die OECD hält fest:

- Die Eigentümerfunktion des Staats sollte klar von den anderen Funktionen des Staats getrennt sein.[13]
- In seiner Eigenschaft als Unternehmer sollte der Staat die Unabhängigkeit der Gesellschaftsorgane (Boards) respektieren.[14]
- Der Staat sollte als aktiver Unternehmenseigner seine Eigentumsrechte entsprechend der jeweiligen Rechtsform ausüben,[15] dazu zählt grundsätzlich auch die Aufrechterhaltung eines kontinuierlichen Dialogs mit den externen Abschlussprüfern und den spezifischen Kontrollinstanzen des Staats.[16]

Der B-PCGK fokussiert auf die vom Bund gehaltenen Anteile innerhalb des Eigentümerorgans.

- Die Anteilseignerrechte ergeben sich aus den auf das Unternehmen anzuwendenden gesetzlichen und satzungsmäßigen Rechtsvorschriften.[17]
- Maßstab für die Wahrnehmung der Rechte sind dabei die Gesetze, die Grundsätze der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit, der Transparenz sowie das öffentliche Interesse an der optimalen Wahrnehmung der Aufgaben des Unternehmens.[18]
- Zur Sicherstellung eines angemessenen Einflusses des Bundes bzw. der Unternehmen des Bundes ist in der Geschäftsordnung für die Geschäftsleitung ein entsprechender Katalog zustimmungspflichtiger Geschäfte durch das Überwachungsorgan vorzusehen.[19]
- Eine sachfremde Einflussnahme auf die Unternehmensführung und -kontrolle ist unzulässig.[20]

Anders als die Abschlussprüfer wird die Interne Revision weder von der OECD noch im B-PCGK erwähnt. Es kann daher geschlossen werden, dass eine institutionalisierte unmittelbare Informationslinie der IR zu den Eigentümern nicht vorgesehen ist.

[13] OECD-Leitsätze, Anmerkungen zu Kapitel 1, Seite 20
[14] OECD-Leitsätze, II.C
[15] OECD-Leitsätze, II.F
[16] OECD-Leitsätze, II.F.4
[17] B-PCGK, Abschnitt 7.1
[18] B-PCGK, Abschnitt 7.3
[19] B-PCGK, Abschnitt 7.6.2
[20] B-PCGK, Abschnitt 7.6.4

## Aufsichtsorgan / Überwachungsorgan

Die Position des Aufsichtsorganes lässt sich bei der OECD wie folgt skizzieren:

- Die Aufsichtsorgane (Boards) sollten über die Autorität, die Befugnisse und die Objektivität verfügen, die notwendig sind, damit sie ihre Funktion der Festlegung der strategischen Ausrichtung und der Überwachung der Geschäftsführung erfüllen können.[21]
- Sie sollten dem Eigentümer Rechenschaft schuldig sein und (u.a.) im besten Interesse des Unternehmens zu handeln.[22]

Der B-PCGK hält fest:

- Bei Unternehmen mit mehr als 30 Bediensteten oder einem Jahresumsatz von mehr als 1 Mio. € ist jedenfalls ein Überwachungsorgan einzurichten.[23]
- Geschäftsleitung und Überwachungsorgan arbeiten zum Wohle des Unternehmens eng zusammen.[24]
- Die Geschäftsleitung stimmt auf der Grundlage des Unternehmensgegenstandes und allfälliger Zielvorgaben des Anteilseigners die Unternehmensstrategie mit dem Überwachungsorgan ab und erörtert mit ihm in regelmäßigen Abständen den Stand der Umsetzung.[25]
- Das Überwachungsorgan hat die Geschäftsleitung bei der Führung des Unternehmens regelmäßig zu überwachen und in grundsätzlichen Angelegenheiten des Unternehmens zu beraten.[26]

Die Kontrolle des Führungsorganes ist zweifelsfrei eine der Kernaufgaben des Aufsichtsorganes.

## Führungsorgan / Leitungsorgan / Geschäftsführung

Die Kontrollaufgaben und -verantwortlichkeiten der Leitungsorgane sind eher spärlich beschrieben.

Die OECD hält fest:

- Vollzugsorgane sollten über die notwendige Autorität und Integrität sowie über die erforderlichen Ressourcen verfügen, um ihren Pflichten professionell und objektiv nachkommen zu können.[27]

Ein wenig ausführlicher ist der B-PCGK:

- Die Geschäftsleitung hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und auf deren Beachtung hinzuwirken.[28]
- Die Geschäftsleitung informiert von sich aus das Überwachungsorgan regelmäßig, zeitnah und umfassend (u.a.) über alle für das Unternehmen relevanten Fragen der Planung, der Geschäftsentwicklung, der Risikolage, des Risikomanagements und die Überwachung der Einhaltung der für das Unternehmen geltenden Regelungen.[29]
- In der Geschäftsordnung für die Geschäftsleitung sind die Informations- und Berichtspflichten an das Überwachungsorgan durch das für deren Erlassung zuständige Organ (zB Anteilseigner, Überwachungsorgan) näher festzulegen.[30]

Einmal mehr wird die Kontrollkompetenz des Aufsichtsorganes über das Leitungsorgan bestätigt. Das Leitungsorgan hat die Einhaltung der sie betreffenden Regelungen zu überwachen und seiner Informations- und Berichtspflicht gegenüber dem Aufsichtsorgan nachzukommen.

[21] OECD-Leitsätze, VI
[22] OECD-Leitsätze, VI.B
[23] Vgl. B-PCGK, Abschnitt 7.6.1
[24] B-PCGK, Abschnitt 8.1.1
[25] B-PCGK, Abschnitt 8.1.2
[26] B-PCGK, Abschnitt 11.1.1.1
[27] OECD-Grundsätze, I.E
[28] B-PCGK, Abschnitt 9.1.3
[29] B-PCGK, Abschnitt 8.1.4
[30] B-PCGK, Abschnitt 8.1.6

## Interne Revision

OECD und B-PCGK betonen die Bedeutung der Internen Revision.

Die OECD führt aus:

- Interne Prüfer sind wichtig zur Gewährleistung eines effizienten und konsequenten Offenlegungsprozesses sowie ordnungsgemäßer interner Kontrollen im weiteren Sinne.[31]
- Staatseigene Unternehmen sollten eine interne Audit-Stelle einrichten, die direkt dem Aufsichtsorgan berichtet und seiner Aufsicht unterstellt ist.[32]
- Im Interesse ihrer Unabhängigkeit und Autorität sollten die internen Prüfer im Auftrag des Aufsichtsrats[33] tätig werden und direkt an ihn berichten.
- Interne Prüfer sollten die uneingeschränkte Möglichkeit haben, mit dem Vorsitzenden und den Mitgliedern des Aufsichtsrates in Kontakt zu treten.

Der B-PCGK hält fest:

- Die Interne Revision ist auf Basis allgemein anerkannter internationaler Revisionsstandards durchzuführen.[34]
- Mehrere kleinere Unternehmen können eine gemeinsame Revisionsstelle einrichten oder durch eine externe Beauftragung ihrer Verpflichtung nachkommen.[35]
- Die interne Revision soll unmittelbar der Geschäftsleitung unterstellt werden.
- Die Bestellung des Leiters der internen Revision soll durch das Überwachungsorgan genehmigt werden.[36]
- Die Prüfungsaufträge sind schriftlich zu erteilen.[37]
- Über die Prüfaufträge ist das Überwachungsorgan des Unternehmens zu informieren.
- Die Prüfberichte der internen Revision sind auch dem Überwachungsorgan auf Verlangen zu übermitteln.[38]

Beide Quellen erwähnen Kontrollpflichten des Aufsichtsorganes in Zusammenhang mit Internen Revisionen. Die OECD sieht vor, dass die IR im Auftrag des Aufsichtsrates tätig ist, seiner Aufsicht unterstellt ist und an ihn berichtet. Demgegenüber unterstellt der B-PCGK die IR dem Leitungsorgan, sieht allerdings eine Informationspflicht über die Erteilung eines Prüfauftrages vor. Das Aufsichtsorgan hat das Recht die Vorlage von Prüfberichten zu verlangen und die Bestellung des Leiters der IR zu genehmigen.

Im Gegensatz zur OECD enthält der B-PKCG zwar einen kurzen Verweis zu Unternehmen, die keine eigene Revisionsstelle führen, dieser geht aber über die Verpflichtung zur Inanspruchnahme externer Unterstützung nicht hinaus. Eine vertiefende Betrachtung der IR-Funktion anhand der Berufsstandards der IR ist wegen der geringen Aussagedichte der Kodices jedenfalls erforderlich. Beim Fehlen der Organisationseinheit „Revisionsstelle“ ergibt sich das Erfordernis, die Standards den organisatorischen Einheiten Aufsichtsorgan, Leitungsorgan und Externe Prüfer zuzuordnen.

[31] OECD-Leitsätze, Anmerkungen zu Kapitel V.B
[32] OECD-Leitsätze, V.B
[33] Vgl. OECD-Leitsätze, Anmerkungen zu Kapitel V.B, die Quelle erwähnt Board , Audit Board, Prüfungsausschuss, und Aufsichtsrat.
[34] Vgl. B-PCGK, Abschnitt 13.1
[35] Vgl. B-PCGK, Abschnitt 13.2
[36] Vgl. B-PCGK, Abschnitt 13.3
[37] Vgl. B-PCGK, Abschnitt 13.4
[38] Vgl. B-PCGK, Abschnitt 13.5

# 4. Internationale Revisionsgrundlagen

Die Internationalen Grundlagen für die berufliche Praxis der Internen Revision 2017 (IPPF - The International Professional Practices Framework)[39] haben weltweite Geltung. Der Weltverband der Rechnungshöfe (INTOSAI)[40] bezieht sich darauf, wenn es um Interne Revision geht.

Die verbindlichen Elemente des IPPF[41] sind:

- Grundprinzipien für die berufliche Praxis der Internen Revision
- Definition der Internen Revision
- Ethikkodex
- Internationale Standards für die berufliche Praxis der Internen Revision (Standards)

## 4.1. Mission, Definition, Prinzipien, Ethikkodex

Die Mission der IR, nämlich

*Den Wert einer Organisation durch risikoorientierte und objektive Prüfung, Beratung und Einblicke zu erhöhen und zu schützen.*[42]

und die Definition der IR, nämlich

*Die Interne Revision erbringt unabhängige und objektive Prüfungs- und Beratungsdienstleistungen, welche darauf ausgerichtet sind, Mehrwerte zu schaffen und die Geschäftsprozesse zu verbessern.*

*Sie unterstützt die Organisation bei der Erreichung ihrer Ziele, indem sie mit einem systematischen und zielgerichteten Ansatz die Effektivität des Risikomanagements, der Kontrollen und der Führungs- und Überwachungsprozesse bewertet und diese verbessern hilft.*[43]

beziehen sich auf die Revisionsfunktion und gelten auch dann, wenn sie über Externe ausgeübt wird.

Die nachstehenden Prinzipien müssen vorhanden und wirksam sein. Die Nichteinhaltung eines der Prinzipien würde bedeuten, dass eine Interne Revision im Erreichen ihrer Mission nicht so wirksam wäre, wie sie es sein könnte.

- Zeigt Integrität.
- Zeigt Sachkunde und berufsübliche Sorgfalt.
- Ist objektiv und frei von ungebührlichem Einfluss (unabhängig).
- Richtet sich an Strategien, Zielen und Risiken der Organisation aus.
- Ist geeignet positioniert und mit angemessenen Mitteln ausgestattet.
- Zeigt Qualität und kontinuierliche Verbesserung.
- Kommuniziert wirksam.
- Erbringt risikoorientierte Prüfungsleistungen.
- Ist aufschlussreich, proaktiv und zukunftsorientiert.
- Fördert organisatorische Verbesserungen.[44]

Die Zuordnung der Verantwortlichkeiten für diese Prinzipien ist differenziert zu sehen, liegt aber stets

[39] DIIR - Deutsches Institut für Interne Revision e. V., Frankfurt am Main / Institut für Interne Revision Österreich (IIA Austria), Wien /Schweizerischer Verband für Interne Revision (IIA Switzerland), Zürich, Internationale Grundlagen für die berufliche Praxis der Internen Revision 2017, (deutsche Auflage),
The Institute of Internal Auditors, The International Professional Practices Framework (Original)

[40] Vgl. etwa INTOSAI GOV 9100, Seite 50 : „Zur fachlichen Orientierung sollten interne Revisoren das Professional Practices Framework (PPF) des Institute of Internal Auditors (IIA) einschließlich der Definition, der berufsethischen Grundsätze, der Standards und der Praktischen Ratschläge zu Rate ziehen."

[41] IPPF, Seite 7

[42] IPPF, Seite 11

[43] IPPF, Seite 13

[44] IPPF, Seite 12

im Bereich des Unternehmens und der externen Prüfer. Z.B. ist Sachkunde eine Verpflichtung der externen Prüfer, aber auch eine Verantwortung der Organisation bei der Auswahl und beim Erkennen erheblicher Fehlleistungen. Eine vertiefende Befassung erfolgt bei den Standards.

Der Ethikkodex gilt sowohl für Einzelpersonen als auch für Organisationen, die Dienstleistungen im Bereich Interne Revision erbringen. Primäre Adressaten sind hier daher die externen Prüfer. Von ihnen wird Integrität, Objektivität, Vertraulichkeit und Fachkompetenz erwartet.[45]

Auch hier steht der Einhaltung des Ethikkodex durch die externen Prüfer die sorgfältige Auswahl, vertragliche Gestaltung und zeitnahe, angemessene Reaktion bei „Worst Case" seitens des Unternehmens gegenüber.

## 4.2. Revisionsstandards

Die Standards sind eine Sammlung prinzipienbasierter, verbindlicher Anforderungen. Sie umfassen zusammen mit dem Ethikkodex alle verbindlichen Elemente der Internationalen Grundlagen für die berufliche Praxis der Internen Revision. [46] Die Standards umfassen zwei Hauptkategorien: Attribut- und Ausführungsstandards. Attributstandards beschreiben die Merkmale von Organisationen und Personen, die Aufgaben der Internen Revision wahrnehmen. Ausführungsstandards beschreiben die Tätigkeitsfelder der Internen Revision und stellen Qualitätskriterien auf, mit denen die Ausführung dieser Leistungen bewertet werden kann. Attribut- und Ausführungsstandards gelten für alle Dienstleistungen der Internen Revision.[47]

### 4.2.1. Attributstandards

#### Geschäftsordnung / Grundlagenpapier

Gemäß Standard 1000 müssen Aufgabenstellung, Befugnisse und Verantwortung der Internen Revision formell in einer Geschäftsordnung der Internen Revision bestimmt sein.

Der Standard trifft keine Aussage für den Fall, dass es keine IR gibt.

*Anmerkung: Das (interne) Handbuch Beteiligungsmanagement sieht beispielsweise für diesen Fall anstelle der Revisionsordnung und des Jahresprüfungsplanes ein Grundlagenpapier bezüglich Mandatierung und Ergebniskommunikation vor.*[48]

*In Analogie zum Standard 1000 (Genehmigung durch Geschäftsleitung bzw. Überwachungsorgan) und unter Berücksichtigung unserer Ausgangslage (Leitungsorgan und Aufsichtsorgan sind vorhanden) wird das Grundlagenpapier durch das Leitungsorgan erstellt und im Hinblick auf die berührten Kontrollpflichten des Aufsichtsorganes von diesem beschlossen.*

#### Unabhängigkeit und Objektivität

Die Standards 1100 (Unabhängigkeit und Objektivität), 1110 (Organisatorische Unabhängigkeit) sowie 1111 (Direkte Zusammenarbeit mit Geschäftsleitung bzw. Überwachungsorgan) weisen primär auf Verpflichtungen des Prüfkörpers (hier der externen Prüfer) hin, dennoch sind auch Aspekte enthalten, welche das öffentliche Unternehmen selbst betreffen.

Zunächst muss vertraglich sichergestellt sein, dass die externen Prüfer ihre Aufgaben im Rahmen des Prüfmandates unbeeinflusst wahrnehmen können. Der endgültige Prüfbericht (Schlussbericht) ist je-

[45] IPPF, Seite 15 ff
[46] Vgl. IPPF, Seite 18
[47] IPPF, Seite 19
[48] BMF, Handbuch Beteiligungsmanagement, Anhang, Abschnitt 6.2

denfalls der Geschäftsleitung und dem Überwachungsorgan zugänglich zu machen.

Objektivität wird als eine unbeeinflusste Geisteshaltung gesehen, die es erlaubt, den Auftrag so auszuführen, dass die Arbeitsergebnisse und deren Qualität vorbehaltlos vertreten werden kann. Ihre Verletzung berührt das Unternehmen insofern, als über eine vorzeitige Beendigung des Mandatsvertrages zu befinden ist. Kleinere Verletzungen wären über den Prüfprozess bzw. das Berichtswesen abzuhandeln.

Die organisatorische Unabhängigkeit[49] des Prüfkörpers ist durch die Bestellung externer Prüfer per se gegeben. Die Vertragsunterzeichnung durch das Leitungsorgan ist empfehlenswert, jedenfalls aber ist ein direkter und unbeschränkter Zugang zu diesem sicherzustellen[50], welcher auch die Berichtsvorlage umfasst. Die, auch von INTOSAI GOV 9140[51] geforderte Bestätigung über die organisatorische Unabhängigkeit, ist hier als verpflichtendes Element des Prüfberichtes zu sehen. Die externen Prüfer dürfen – unter Beachtung des Rahmens des Prüfmandates - bei der Festlegung des Umfangs der Prüfung, bei der Auftragsdurchführung und bei der Berichterstattung der Ergebnisse nicht behindert werden. Sie müssen der Geschäftsleitung bzw. dem Überwachungsorgan solche Beeinflussungen offenlegen und die Auswirkungen besprechen.[52]

In Analogie zum Standard 1112 kann festgehalten werden, dass bei einer „Doppelrolle“ - zugleich Leitungsorgan und geprüfte Stelle - Vorkehrungen zur Begrenzung von Beeinträchtigungen der Unabhängigkeit und der Objektivität getroffen werden müssen. Dies kann ganz gut durch einen prüfungsfallbezogenen Ausbau der Rolle des Aufsichtsorganes bzw. seines Vorsitzenden umgesetzt werden. (er wäre dann z.B. Auftraggeber, Ansprechperson und direkter Berichtsadressat).

Analog zu Standard 1120 müssen die externen Prüfer unparteiisch und unvoreingenommen sein und jeden Interessenkonflikt vermeiden. Die IPPF-Erläuterungen definieren Interessenkonflikte als Situationen, in denen der Prüfer in einer Vertrauensstellung ein konkurrierendes berufliches oder privates Interesse hat. Gemäß Standard 1130 liegt eine Beeinträchtigung bereits dann vor, wenn sie dem Anschein nach besteht.

Die realen Probleme liegen wohl nicht bei jenen Fällen, wo der Prüfer eine Geschäftsbezieheng zum geprüften Unternehmen unterhält bzw. unterhielt, die Brisanz liegt dort, wo Bedienstete des Eigentümervertreters als externe Prüfer des Unternehmens auftreten. Das Prüfmandat darf nicht als direktes Einfallstor für Eigentümerwünsche angesehen werden. Prüfthemen sind unternehmensintern, allenfalls unter Einbindung des Eigentümervertreters, abzuklären und vom Leitungsorgan in einem Prüfmandat festzulegen. Im Verhältnis zwischen Eigentümervertreter und „seinen“ externen Prüfern ist klarzustellen, dass keine Interventions- und Informationsrechte bestehen, d.h. der Eigentümervertreter stellt bloß gegen Kostenersatz Ressourcen zur Verfügung. Der Prüfbericht geht über das Leitungs- oder Aufsichtsorgan an den Eigentümervertreter. Alles andere bedarf der Zustimmung des Unternehmens und ist vertraglich (im Prüfmandat) festzulegen.

## Fachkompetenz und berufliche Sorgfaltspflicht

Gem. Standard 1210 müssen das Prüfteam insgesamt und die Prüfer bezogen auf ihren Arbeitsbereich das Wissen, die Fähigkeiten und sonstige Qualifikationen verfügen, die erforderlich sind, um ihre Verantwortlichkeiten zu erfüllen. Reicht dies nicht aus, muss kompetenter Rat und Unterstützung eingeholt werden.[53] Kann die fachliche Anforderung nicht erfüllt werden, ist der Auftrag von den externen Prüfern abzulehnen[54], analog gilt wohl auch: darf er vom Unternehmen nicht erteilt werden.

[49] Vgl. IPPF 1110
[50] Vgl. IPPF 1111
[51] INTOSAI GOV 9140, Abschn. 7.5
[52] Vgl. IPPF 1110.A1
[53] Vgl. IPPF, Standard 1210.A1
[54] Vgl. IPPF, Standard 1210.C1

Die Beiziehung dritter Personen (zB IT-Experten, Bau-Experten, o.ä.) ist allein schon aufgrund des besonderen Vertrauensverhältnisses nicht automatisch Bestandteil des Mandatsvertrages und muss eigens vereinbart werden.

Bezieht sich das Mandat nicht ausdrücklich auf die Prüfung doloser Handlungen, beschränkt sich die allgemeine Erwartungshaltung des Unternehmens darauf, dass die externen Prüfer über ausreichendes Wissen verfügen, um Risiken für dolose Handlungen und die Art, wie diese Risiken in der Organisation gehandhabt werden, beurteilen zu können. Vertieftes Expertenwissen kann aber nicht erwartet werden.[55] Gleiches gilt für IT-Kenntnisse.[56]

Die externen Prüfer müssen jenes Maß an Sorgfalt und Sachkunde anwenden, das üblicherweise von einem sorgfältigen und sachkundigen Internen Revisor erwartet werden kann.[57] Sie müssen sich der wesentlichen Risiken bewusst sein, die Auswirkungen auf Geschäftsziele, Geschäftsprozesse oder Ressourcen haben können.[58] Bedingt durch die Verpflichtung der regelmäßigen fachlichen Weiterbildung[59] kann seitens des Unternehmens erwartet werden, dass die Prüfung nach den aktuellen Erkenntnissen des Berufsstandes Interner Revisoren durchgeführt wird.

### 4.2.2. Ausführungsstandards

Die Ausführungsstandards beinhalten einerseits Managementaufgaben der Revisionsleitung und andererseits Ablaufprozesse der Prüfung.

Bedingt durch das Fehlen einer Internen Revisionsstelle fällt die grundsätzliche Verantwortung für die Revisionsaufgaben an das Leitungsorgan zurück[61], wobei das Aufsichtsorgan jedenfalls so stark einzubinden ist, dass nicht der Eindruck entsteht, das Leitungsorgan kontrolliere sich selbst.

#### Qualitätssicherung

Die Qualitätssicherung für Interne Revisionen ist in den Standards 1300 bis 1322 geregelt. Hervorzuheben ist bloß, dass es sich um ein verpflichtendes System laufender Qualitätsverbesserungen handelt. Von besonderem Interesse ist Standard 1312, nach ihm müssen externe Beurteilungen mindestens alle fünf Jahre von einem qualifizierten, unabhängigen Beurteiler durchgeführt werden.

Alle Anforderungen an externe Prüfer, welche unter Bezugnahme auf die Standards in diesem Artikel angesprochen werden, können durch das Unternehmen leicht überprüft werden: sie braucht nur die Vorlage der letzten externen Beurteilung iSd Standards 1312 verlangen, diese darf nicht älter als 5 Jahre sein. Ist die Vorlage nicht möglich (zB Wirtschaftsprüfungsgesellschaften fallen nicht darunter), sollte zumindest einer der externen Prüfer ein *CIA – Certified Internal Auditor*[60] sein. Liegt auch dies nicht vor, müssten die Voraussetzungen in Einzelfall geprüft werden.

#### Grundsätzliche Verantwortung (Leitung)

Aus der analogen Anwendung des Standard 2000 ergibt sich, dass das Leitungsorgan über die Prüfungsmaßnahmen einen Wertbeitrag für das Unternehmen sicherzustellen hat. Dieser ist dann gegeben, wenn Strategien, Ziele und Risiken berücksichtigt werden, Wege zur Verbesserung der Führungs- und Überwachungs-, Risikomanagement- und Kontrollprozesse aufgezeigt werden und objektiv relevante Prüfungsleistungen erbracht wer-

[55] Vgl. IPPF, Standard 1210.A2
[56] Vgl. IPPF, Standard 1210.A3
[57] Vgl. IPPF, Standard 1220
[58] Vgl. IPPF, Standard 1220.C1
[59] Vgl. IPPF, Standard 1230
[60] Weltweit gültige Zertifizierung auf Basis eines Berufsexamens , verliehen vom Institute of Internal Auditors
[61] Vgl. etwa Bünis / Gossens, Das 1x1 der Internen Revision, Seite 15 oder Amling / Bantleon, Handbuch der Internen Revision, Seite 32; aber auch Standard 2070: „Sofern ein externer Dienstleister die Aufgaben der Internen Revision übernommen hat, muss dieser die Organisation auf ihre Verantwortung zum Aufrechterhalten einer funktionsfähigen Internen Revision hinweisen."

den. Dazu muss das Leitungsorgan einen risikoorientierten Prüfungsplan im Einklang mit den Organisationszielen erstellen und regelmäßig warten[62]. Plan und wesentliche Planänderungen wären in analoger Anwendung dem Aufsichtsorgan zur Zustimmung vorzulegen.[63] Prüfungen anderer Einheiten sind zu beurteilen, auch um Doppelprüfungen zu vermeiden.[64]

Das Leitungsorgan ist für das Ressourcen-Management (hier das Budget der extern vergebenen Prüfaufträge) verantwortlich[65], wobei der Mittelbedarf durch das Aufsichtsorgan genehmigt wird.[66] Die separate Darstellung und Genehmigung im Rahmen des Unternehmensbudgets ist dafür wohl ausreichend.

Das Leitungsorgan hat dem Überwachungsorgan über die Planerfüllung und wesentliche Risiko- und Kontrollthemen zu berichten. Häufigkeit und Inhalt der Berichterstattung werden gemeinschaftlich festgelegt. (vgl. Standard 2060). Im Hinblick auf die geringe Größe der Unternehmen wird ein jährlicher Bericht ausreichend sein.

## Art der Arbeiten

Analog zu Standard 2100 geht es darum, durch die Anwendung eines systematischen, zielgerichteten und risikoorientierten Vorgehens Führungs- und Überwachungsprozesse einschließlich der Ethik und der IT[67], Risikomanagementprozesse einschließlich der Möglichkeit des Auftretens doloser Handlungen[68] und Kontrollprozesse[69] der Organisation zu bewerten und zu deren Verbesserung beitragen. Die ausgewählten Prüfthemen sollten neue Einblicke ermöglichen und zukünftige Auswirkungen berücksichtigen.

Letztlich ist diese Gruppe an Standards (2100 bis 2130) eine gute Orientierungshilfe für den vom Leitungsorgan zu erstellenden jährlichen oder mehrjährigen Prüfplan.

## Planung und Durchführung einzelner Aufträge

Die Planung einer konkreten Prüfung muss die Ziele, Umfang, Zeitplan und zugeordnete Ressourcen umfassen.[70] Das Leitungsorgan muss mit den externen Prüfern eine schriftliche Vereinbarung betreffend Ziel, Umfang, Verantwortlichkeiten sowie anderer Erwartungen einschließlich Beschränkung der Ergebnisverbreitung und Zugang zu den Auftragsakten treffen.[71] Vor der Auftragsdurchführung müssen die externen Prüfer eine Einschätzung der Risiken des zu prüfenden Tätigkeitsbereiches vornehmen. Die Auftragsziele müssen diese Einschätzung widerspiegeln.[72] Aus diesem Standard lässt sich wohl ableiten, dass das Leitungsorgan nicht nur einen Auftrag zur Prüfung eines Themas erteilt, sondern auch die Auftragsziele (Schwerpunkte) abnimmt. Der festgelegte Umfang muss ausreichend sein, um das Erreichen der Auftragsziele zu ermöglichen.[73]

Der Verpflichtung der externen Prüfer ausreichende, zuverlässige, relevante und konstruktive Informationen zu identifizieren[74] steht die Verpflichtung des Leitungsorgans gegenüber, für den Zugang zu derartigen Informationen zu sorgen.

[62] Vgl. IPPF, Standard 2010
[63] Vgl. IPPF, Standard 2020
[64] Vgl. IPPF, Standard 2050
[65] Vgl. IPPF, Standard 2030
[66] Vgl. IPPF, Standard 2020
[67] Vgl. IPPF, Standard 2110
[68] Vgl. IPPF, Standard 2120
[69] Vgl. IPPF, Standard 2130
[70] Vgl. IPPF, Standard 2200
[71] Vgl. IPPF, Standard 2201.A1
[72] Vgl. IPPF, Standard 2210.A1
[73] IPPF, Standard 2200
[74] Vgl. IPPF, Standard 2310

Die Aufzeichnung und Aufbewahrung von Informationen (Arbeitsunterlagen, nicht Bericht) liegt im Verantwortungsbereich der externen Prüfer. Die Weitergabe an das Unternehmen bzw. an andere bedarf einer expliziten Vereinbarung oder rechtlichen Regelung.[75]

Wenn im Verlauf eines Prüfungsauftrags ein wesentlicher Beratungsbedarf auftritt, sollte – sofern er über die externen Prüfer wahrgenommen wird - darüber eine gezielte schriftliche Vereinbarung getroffen werden.[76]

## Berichterstattung

Die Berichterstattung muss Ziele, Umfang und Ergebnisse des Auftrags enthalten.[77] Sie müssen richtig, objektiv, klar, prägnant, konstruktiv und vollständig sein und zeitnah erstellt werden.[78] Enthält ein Schlussbericht wesentliche Fehler oder Auslassungen, müssen die externen Prüfer allen Parteien, die den ursprünglichen Bericht erhalten haben, die berichtigten Informationen übermitteln.[79]

Die Angabe, dass der Auftrag „in Übereinstimmung mit den *Internationalen Standards für die berufliche Praxis der Internen Revision durchgeführt*“ wurden, ist nur sachgerecht, wenn die Beurteilung des Programms zur Qualitätssicherung und –verbesserung diese Aussage zulässt.[80] Falls sich ein Abweichen von dem Ethikkodex oder von den Standards auf den Auftrag auswirkt, müssen bei der Berichterstattung die verletzten Prinzipen bzw. Regelungen, die Gründe und die Auswirkungen offengelegt werden.[81]

Bei der Verbreitung der Ergebnisse, die im Sinne der Standards beim Leiter der Internen Revision liegt, ist im gegenständlichen Fall zwischen Leitungsorgan und externen Prüfern zu differenzieren. Die Verantwortung für die Durchsicht und Genehmigung des Schlussberichtes liegt bei den externen Prüfern, sie übergeben den Bericht an das Leitungsorgan. Das Leitungsorgan wiederum muss alle zweckmäßigen Parteien über die Ergebnisse informieren.

## Überwachung des weiteren Vorgehens

Das Leitungsorgan muss zur Überwachung der Erledigung der Feststellungen aus den Revisionsberichten ein entsprechendes System entwickeln und pflegen.[82]

Es muss dazu ein Follow-up-Verfahren einrichten, mit dem überwacht und sichergestellt wird, dass vereinbarte Maßnahmen wirksam umgesetzt werden sofern nicht das Unternehmen das Risiko auf sich nimmt, keine Maßnahmen durchzuführen.[83] Obwohl in den Standards nicht explizit angeführt, gibt es – z.B. aus dem Gebot einer direkten Zusammenarbeit mit dem Aufsichtsorgan[84] – eine entsprechende Informationsverpflichtung.

## Kommunikation der Risikoakzeptanz

Ergibt sich aus der Prüfung, dass die Führungskräfte ein für das Unternehmen nicht tragbares Risiko akzeptieren, so müssen die externen Prüfer diese Sachlage mit dem Leitungsorgan besprechen. Falls die externen Prüfer der Auffassung sind, dass die Angelegenheit nicht zufriedenstellend gelöst wurde, müssen sie die Angelegenheit dem Überwachungsorgan vortragen.[85]

Dieser besonderen „Redepflicht“ wird primär durch Darstellung im Prüfbericht entsprochen.

[75] Vgl. IPPF, Standard 2330.A2 aber auch 2330.C1
[76] Vgl. IPPF, Standard 2220.A2
[77] Vgl. IPPF, Standard 2410
[78] Vgl. IPPF, Standard 2420
[79] Vgl. IPPF, Standard 2421
[80] IPPF, Standard 2430
[81] Vgl. IPPF, Standard 2431
[82] Vgl. IPPF, Standard 2500
[83] Vgl. IPPF, Standard 2500.A1
[84] Vgl. IPPF, Standard 1111
[85] Vgl. IPPF, Standard 2600

## 5. Zusammenfassung

Mit der Internen Revision wird eine der wesentlichen Kontrollfunktionen innerhalb eines Unternehmens des öffentlichen Sektors angesprochen. Wird im Unternehmen keine eigene Revisionsstelle geführt, ist – jedenfalls nach dem B-PCGK – eine externe Prüfungsdienstleistung in Anspruch zu nehmen, zumindest sofern ein Aufsichtsorgan eingerichtet ist.

Die sich aus der Revisionsfunktion ergebenden Rechte und Pflichten sind in den Corporate Governace Kodices angedeutet und können über die Revisionsstandards, abgebildet im IPPF, besser dargestellt werden. Diese Revisionsstandards sind verpflichtend anzuwenden.

Die Eigentümer sind von der Revisionsfunktion zu weit entfernt und haben keinen direkten Bezug zu externen Revisoren. Anders verhält es sich etwa bei Abschlussprüfern.

Das Aufsichtsorgan kontrolliert (und steuert) das Leitungsorgan und hat einen unmittelbaren Bezug zur Revisionsfunktion. Rechte – und zugleich auch Verpflichtungen - bestehen zumindest bezüglich

- der Information über geplante und beauftragte Prüfungen, Prüfungsergebnisse und Umsetzungsmaßnahmen
- der Möglichkeit der direkten Kontaktaufnahme mit den externen Prüfern

Die Genehmigung des Prüfmandates durch das Aufsichtsorgan ist jedenfalls dann geboten, wenn Tätigkeiten des Leitungsorganes geprüft werden.

Aus den in den Revisionsstandards verankerten Aufgaben eines Revisionsleiters lässt sich in Verbindung mit der in den Corporate Governace Kodices festgelegten Informationspflicht ableiten, dass das Leitungsorgan einen risikoorientierten, mehrjährigen Prüfplan erstellt und zumindest die geplanten Prüfungen der nächsten Periode (zumeist des Jahres) dem Aufsichtsorgan bekannt zu geben hat.

Der Abschluss eines Vertrages mit externen Revisoren ist in der Verantwortung des Leitungsorganes. Bei Auswahl der Vertragspartner ist auch darauf zu achten, dass keine Befangenheit bzw. Anscheinsbefangenheit vorliegt und die in den Revisionsstandards genannten Attributstandards (Objektivität, Unabhängigkeit, Fachkompetenz, berufliche Sorgfaltspflicht, Qualitätssicherung) eingehalten werden können. Der Nachweis einer anerkannten externen Qualitätsprüfung, allenfalls der Zertifizierung einer Person als Certified Internal Auditor dürfte hier im Allgemeinen ausreichend sein.

Das Leitungsorgan ist über die gemeinsame Festlegung der Prüfschwerpunkte und Stellungnahmen in der Berichtsphase eingebunden und hat dafür Sorge zu tragen, dass die Prüfer alle im Rahmen ihres Mandates erforderlichen Informationen und IT-Zugänge erhalten. Es ist Adressat des Prüfberichtes und hat für seine Weiterverteilung (Aufsichtsorgan, Eigentümer) zu sorgen. Art und Umfang der Kommunikation zu den Mitarbeiterinnen und Mitarbeitern liegt ausschließlich im Verantwortungsbereich des Leitungsorgans.

Die Aufgabe der externen Prüfer ist am besten beschreibbar. Sie haben die Prüfung im Rahmen des Prüfmandates und auf Basis der Revisionsstandards durchzuführen. Durch den allgemeinen Bezug zu den Standards sind z.B. auch die Attributstandards mit eingeschlossen. Wesentliche Beeinträchtigungen bei der Arbeit sind in den Prüfbericht aufzunehmen, ebenso das Akzeptieren eines nichttragbaren Risikos durch das Leitungsorgan.

Um die allgemeinen Anforderung an die besondere Situation „externe Interne Revision“ bestmöglich zu beschreiben und verbindlich festzulegen, empfiehlt sich die Erstellung eines „Grundlagenpapiers Interne Revision“ durch das Leitungsorgan und seine Genehmigung durch das Aufsichtsorgan. Ein Muster ist dem Artikel beigefügt.

# 6. Mustertext Grundlagenpapier Interne Revision

## Präambel

(1) *(Das Unternehmen)* hat sich in ihrer Satzung zur Einhaltung der Bestimmungen des B-PCGK bekannt.
(2) Die Interne Revision ist eine wesentliche Säule der Corporate Governance eines Unternehmens. Der Art. 13 des B-PCGK sieht die verpflichtende Einrichtung der Funktion einer Internen Revision vor, die auf Basis allgemein anerkannter internationaler Revisionsstandards tätig ist. Im Hinblick auf die geringe Mitarbeiterzahl wird diese Funktion – in Übereinstimmung mit dem B-PCGK und dem Handbuch Beteiligungsmanagement - nicht über eine eigene Organisationseinheit, sondern über einen qualifizierten externen Dienstleister wahrgenommen.

## Definition

(1) Die Interne Revision erbringt objektive und unabhängige Prüfungs- und Beratungsleistungen, die darauf ausgerichtet sind, Mehrwerte zu schaffen und Geschäftsprozesse zu verbessern. Sie unterstützt die Organisation bei der Erreichung ihrer Ziele, indem sie mit einem systematischen und zielgerichteten Ansatz die Effektivität des Risikomanagements, der internen Kontrollsysteme und der Führungs- und Überwachungssysteme analysiert und bewertet, sowie Maßnahmen zur Verbesserung identifiziert und deren Umsetzung überwacht

## Geltungsbereich

(1) Das Grundlagenpapier spezifiziert die für den Aufsichtsrat, *den Vorstand/ die Geschäftsführung*, die Mitarbeiterinnen und Mitarbeiter des Unternehmens und die beauftragten externen Revisoren maßgeblichen Rechte und Pflichten in Zusammenhang mit der Internen Revision.
(2) Über geltende Normen, bzw. bei den externen Prüfern über das konkrete Mandat, hinausgehende Rechte und Pflichten werden nicht begründet.

## Mittelfristige Planung

(1) *Der Vorstand / die Geschäftsführung* ist für den effizienten und wirksamen Einsatz externer Revisoren verantwortlich. *Er / sie* hat auf Basis eines mittelfristigen Konzeptes die Prüfthemen unter Berücksichtigung der Strategien, Ziele und Risiken des Unternehmens zu planen und dem Aufsichtsrat zumindest die Planung des nächsten Jahres offen zu legen.
(2) Bei Prüfthemen ist die gesamthafte Betrachtung von Systemen oder Teilsystemen der Vorzug gegenüber Detailthemen bzw. Einzelfällen zugeben.

## Prüfungen

### Prüfmandat

(1) Das Prüfmandat ist ein zwischen *dem Unternehmen*, vertreten durch *den Vorstand / die Geschäftsführung*, und einem Wirtschaftsprüfer, einer Prüfungsgesellschaft bzw. einer Internen Revisionsstelle abgeschlossener, schriftlicher Vertrag zur Durchführung einer konkreten Prüfung.
(2) Ein Vertragsabschluss mit einer Internen Revisionsstelle bzw. der Organisation, der sie zugehört, ist nur dann zulässig, wenn diese Interne Revisionsstelle eine gültige, positive externe Qualitätsbeurteilung im Sinne des IIA-Standards 1312 vorweisen kann.
(3) Der Aufsichtsrat ist über die Erteilung eines Prüfmandates zu informieren.
(4) Ist beabsichtigt, einen Rahmenvertrag für mehrere Prüfungen abzuschließen, ist wie bei der Bestellung eines Abschlussprüfers vorzugehen.
(5) Neben den allgemeinen Erfordernissen eines Vertrages sollte das Prüfmandat enthalten:

- Prüfziele, ggf. Nichtziele
- Ressourceneinschätzung
- Tätigwerden der externen Prüfer auf Basis der IIA-Standards
- Allgemeiner Arbeitsablauf
- Stellung der externen Prüfer gegenüber *dem Unternehmen*
- Pflichten nach Abgabe der Prüfberichtes

## Prüfungsablauf, Rechte und Pflichten während der Prüfung

(1) Die externen Revisoren erstellen nach einem Erstgespräch mit *dem Vorstand / der Geschäftsführung* und den erforderlichen Vorbereitungsarbeiten ein Prüfkonzept, in dem Schwerpunkte und Meilensteine vorgeschlagen werden. Das Prüfkonzept wird, allenfalls nach Abänderung, *vom Vorstand / von der Geschäftsführung* durch Unterschrift abgenommen und vom Leiter der externen Revisoren gegengezeichnet.
(2) Die Prüfung liegt in der Eigenverantwortung der externen Revisoren. *Der Vorstand / die Geschäftsführung* trägt Sorge, dass die externen Revisoren die erforderlichen Unterlagen einsehen können, Befragungen der Führungskräfte und Mitarbeiter durchführen können und die erforderlichen IT-Zugangsberechtigungen erhalten. Allfällige Beeinträchtigungen werden von den externen Revisoren im Prüfbericht aufgezeigt.
(3) Vor Durchführung einer Schlussbesprechung wird der festgestellte Sachverhalt von den externen Revisoren mit *dem Vorstand / der Geschäftsführung* abgeklärt, allenfalls werden ergänzenden Erhebungen durchgeführt und danach eine Besprechungsunterlage erstellt.
(4) Die Einladung zur Schlussbesprechung sowie die Besprechungsunterlage werden durch die externen Revisoren versendet. Die Leitung der Schlussbesprechung erfolgt durch die externen Revisoren.
(5) Nach der Schlussbesprechung wird von den externen Revisoren, sofern *der Vorstand / die Geschäftsführung* nicht darauf verzichtet, ein Berichtsentwurf übermittelt. Anmerkungen zu diesem Berichtsentwurf sind binnen vereinbarter Zeit über *den Vorstand / die Geschäftsführung* an die externen Revisoren weiter zu leiten.
(6) Der Schlussbericht wird *dem Vorstand / der Geschäftsführung* übermittelt. Die Verteilung des Schlussberichtes oder einzelner Kapitel an die Mitarbeiter, wie auch deren weitere Information liegt im Ermessen des Vorstandes.

## Informationen nach Ende der Prüfung

(1) Die Information des Aufsichtsrates und *des Eigentümervertreters* über das Prüfungsergebnis und allfällige Anordnungen zu Umsetzungsmaßnahmen erfolgen durch *den Vorstand / die Geschäftsführung*. Die externen Revisoren berichten dem Aufsichtsrat nur über ausdrückliches Ersuchen *des Vorstandsvorsitzenden / des Sprechers der Geschäftsführung* oder des Aufsichtsratsvorsitzenden.
(2) Weitere Informations- und Auskunftspflichten, wie zB gegenüber dem Rechnungshof, dem Wirtschaftsprüfer u.a., sind *vom Vorstand / von der Geschäftsführung* wahrzunehmen.

## Umsetzung und Follow Up

(1) Die Verantwortung für die Umsetzung bzw. Nicht-Umsetzung der Empfehlungen der externen Revisoren liegt *beim Vorstand / der Geschäftsführung*. Über den Stand der Umsetzung der Empfehlungen ist dem Aufsichtsrat zumindest jährlich zu berichten.
(2) Zur Klärung der Weiterentwicklung aufgezeigter Sachverhalte bzw. des Standes der Umsetzungsmaßnahmen können vom *Vorstand / der Geschäftsführung* Follow-Up-Prüfungen beauftragt werden bzw. vom Aufsichtsrat angeregt werden.

(Datum, Unterschrift Vorstandsvorsitzenden / des Sprechers der Geschäftsführung)
(Datum, Unterschrift Aufsichtsratsvorsitzender)

# 7. Literaturverzeichnis

Aigner / Aigner / Aigner, SWK 20/21
Aigner / Aigner / Aigner, Corporate Governance, SWK 20/21 15.7.2017
BMF, Handbuch Beteiligungsmanagement
Bundesministerium für Finanzen, Beteiligungsmanagement Handbuch, 2017, nicht veröffentlicht
B-PCGK:
Bundeskanzleramt, Bundes Public Corporate Governance Kodex 2017
Bünis / Gossens, Das 1x1 der Internen Revision
Bünis / Gossens, Das 1x1 der Internen Revision
EK-Grünbuch:
Europäische Kommission, Grünbuch Europäischer Corporate Governance-Rahmen, KOM(2011) 164 endgültig
Eulerich, Enquête 2011
Eulerich (Verfasser), Enquête-Kommission des DIIR, des IIRÖ und des SVIR, Die Interne Revision in Deutschland, Österreich und der Schweiz 2011
Eulerich, Enquête 2014
Eulerich (Verfasser), Enquête-Kommission des DIIR, des IIRÖ und des SVIR, Die Interne Revision in Deutschland, Österreich und der Schweiz, 2014
Eulerich, Enquête 2017
Eulerich (Verfasser), Projektgruppe Enquete des DIIR, des IIRÖ und des SVIR, Die Interne Revision in Deutschland, Österreich und der Schweiz, Enquete 2017
Eulerich, ZIR 2/12
Eulerich, Das Three Lines of Defence-Modell, ZIR 2/12
INTOSAI GOV 9100
INTOSAI, INTOSAI Richtlinien für die internen Kontrollnormen im öffentlichen Sektor
INTOSAI GOV 9140
INTOSAI, INTOSAI GOV 9140 Unabhängigkeit der Internen Revision im öffentlichen Sektor
IPPF:
DIIR - Deutsches Institut für Interne Revision e. V., Frankfurt am Main / Institut für Interne Revision Österreich (IIA Austria), Wien /Schweizerischer Verband für Interne Revision (IIA Switzerland), Zürich, Internationale Grundlagen für die berufliche Praxis der Internen Revision 2017, (deutsche Auflage), The Institute of Internal Auditors, The International Professional Practices Framework (Original)
OECD-Grundsätze
OECD, OECD-Grundsätze der Corporate Governance, 2015
OECD-Leitsätze:
OECD, OECD-Leitsätze zu Corporate Governance in staatseigenen Unternehmen, 2016
ÖCGK
Österreichischer Arbeitskreis für Corporate Governance, Österreichischer Corporate Governance Kodex 2015.
Papenfuß / Eulerich, ZIR 1/13
Papenfuß / Eulerich, Substanzielle Anforderungsunterschiede zur Internen Revision in Public Corporate Governance Kodizes, ZIR 1/13

# Damit Kontrolle nicht zum Selbstzweck wird

## Über die Bedeutung der transparenten Anwendung von Prüfungsgrundsätzen und Prüfungsmaßstäben bei Wirtschaftlichkeitsprüfungen der öffentlichen Finanzkontrolle

**Mag.ª Stefanie Schlögl, MBA**
Die Autorin ist Prüferin in der Abteilung Banken und Finanzmanagement im Rechnungshof Österreich. Der vorliegende Artikel ist ein gekürzter und adaptierter Auszug aus der im Rahmen des MBA-Programms Public Auditing der WU Executive Academy entstandenen Masterthesis „Die Anwendung von Prüfungsgrundsätzen und Prüfungsmaßstäben bei Wirtschaftlichkeitsprüfungen der öffentlichen Finanzkontrolle im Hinblick auf die Erfüllung von Transparenz und Rechenschaftspflicht der öffentlichen Finanzkontrolle“ aus dem Jahr 2017.

## Inhalt

# 1. Einleitung

Während für Rechnungsprüfungen und für Recht- und Ordnungsmäßigkeitsprüfungen der öffentlichen Finanzkontrolle standardisierte und klar abgegrenzte Prüfungsgrundsätze und Prüfungsmaßstäbe zur Anwendung kommen, ist dies für Wirtschaftlichkeitsprüfungen der öffentlichen Finanzkontrolle nicht der Fall. Dadurch ergeben sich gerade für Wirtschaftlichkeitsprüfungen hohe Anforderungen an die Transparenz der angewendeten Prüfungsmethodik, um die Erfüllung der Rechenschaftspflicht der öffentlichen Finanzkontrolle sicherzustellen. Denn bei Wirtschaftlichkeitsprüfungen handelt es sich üblicherweise um sehr komplexe, nicht standardisierte Prüfungsvorhaben, an die besonders hohe Transparenzanforderungen hinsichtlich der angewendeten Methode gestellt werden müssen. Es kann dabei mit großen Herausforderungen verbunden sein bei Wirtschaftlichkeitsprüfungen methodische Ansätze zu entwickeln, welche allgemein anwendbar und auch nachvollziehbar sind. Der Artikel soll dieses Spannungsfeld anhand relevanter internationaler Standards, bestehender gesetzlicher Grundlagen, der einschlägigen Literatur und Good Practice - Beispielen herausarbeiten und ein praxisorientiertes Modell für die transparente Anwendung von Prüfungsgrundsätzen und Prüfungsmaßstäben bei Wirtschaftlichkeitsprüfungen der öffentlichen Finanzkontrolle entwickeln.

Das Erkenntnissinteresse des vorliegenden Artikels liegt darin herauszuarbeiten wie die Anwendung von Prüfungsgrundsätzen und Prüfungsmaßstäben bei Wirtschaftlichkeits-prüfungen der öffentlichen Finanzkontrolle idealtypisch aussehen sollte. Dabei werden im Wesentlichen folgende zwei Fragen beantwortet:

- Welche internationalen Standards gibt es zur Anwendung von Prüfungsgrundsätzen und Prüfungsmaßstäben bei Wirtschaftlich-keitsprüfungen der öffentlichen Finanzkontrolle im Hinblick auf die Erfüllung von Transparenz und Rechenschafts-pflicht der öffentlichen Finanzkontrolle?

- Welche Good Practice - Beispiele gibt es im Hinblick auf die Erfüllung von Transparenz und Rechenschaftspflicht hinsichtlich des Einsatzes von Prüfungs-grundsätzen und Prüfungsmaßstäben in nationalen und internationalen Einrichtungen der öffentlichen Finanzkontrolle?

# 2. Transparenzmängel der öffentlichen Verwaltung

Transparenzmängel der öffentlichen Verwaltung sind regelmäßig Thema der politischen Debatte in Österreich. In einem unter 100 Staaten durchgeführten Vergleich der Rechte von Bürgerinnen und Bürger auf Verwaltungsinformationen („right to information“) liegt Österreich seit vielen Jahren an letzter Stelle.[1] Die negativen Folgen, die sich daraus für die Effizienz des Verwaltungshandelns ergeben, sind unumstritten. So hält beispielsweise Bartel (1993) fest, dass “das Auftreten und die Persistenz des Effizienzproblems im öffentlichen Sektor“ auf „ein Informationsdefizit der Konsumenten und

[1] Siehe Jahresbericht 2015 des Forum für Informationsfreiheit auf https://www.informationsfreiheit.at/jahresbericht/ (Seite 1) und http://www.rti-rating.org/?s=austria - beide abgefragt am 3.8.2017.

Finanziers öffentlicher Leistungen“ zurückzuführen sei.[2] Auch die OECD stellte 2011 in einem Working Paper fest, dass die mangelnde Transparenz der im internationalen Vergleich qualitativ hochwertigen öffentlichen Leistungserbringung in Österreich ein wesentlicher Grund für die Ineffizienzen im öffentlichen Sektor ist.[3]

Anforderungen an die Erfüllung von Transparenz und Rechenschaftspflicht der öffentlichen Finanzkontrolle ergeben sich

- aus den UN-Nachhaltigkeitszielen, die die Einrichtung von rechenschaftspflichtigen Institutionen als ein globales Entwicklungsziel sehen,
- aus den relevanten internationalen Standards, welche im ISSAI-Regelwerk[4] zusammengefasst sind und (3) aus dem Eigeninteresse der öffentlichen Finanzkontrolle selbst. Letzteres spielt insbesondere bei der Durchführung von Wirtschaftlichkeitsprüfungen eine große Rolle, da es sich hierbei – im Vergleich zu Rechnungsprüfungen und Recht- und Ordnungsmäßigkeitsprüfungen – um komplexe, nicht-standardisierte Verfahren handelt.

## 3. Der idealtypische Modellzyklus einer Wirtschaftlichkeitsprüfung

Die Anforderungen der ISSAIs an die Elemente einer Wirtschaftlichkeitsprüfung zeichnen sich durch methodische Konsistenz und Transparenz aus. Der idealtypische Modellzyklus einer Wirtschaftlichkeitsprüfung ist demnach folgendermaßen gestaltet: Die Ergebnisse einer Wirtschaftlichkeitsprüfung, das sind Prüfungsfeststellungen und Prüfungsempfehlungen, müssen sich aus geeigneten Prüfungsnachweisen ableiten lassen. Diese wiederum müssen ausgerichtet sein an den Prüfungsmaßstäben, welche sich aus den zu beantwortenden Prüfungsfragen ergeben. Die Prüfungsfragen richten sich nach dem Prüfungsgegenstand und den Prüfungszielen, welche schließlich ausgerichtet sind an den „Geboten“ der Wirtschaftlichkeitsprüfung, nämlich den Prüfungsgrundsätzen.

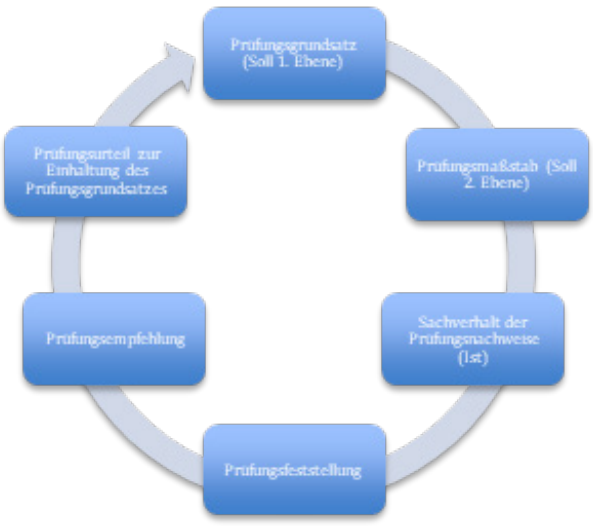



**ABB. 1: Modellzyklus des Soll-Ist-Vergleichs einer Wirtschaftlichkeitsprüfung, Quelle: ISSAIs; eigene Darstellung**

[2] Bartel, Rainer: Zur Ökonomie der öffentlichen Finanzkontrolle, Arbeitspapier des Instituts für Volkswirtschaftslehre, 1993, Johannes Kepler Universität Linz, Seite 4.

[3] Fischer, Karin/Gönenç, Rauf/Price, Robert W.R.: Austria: Public Sector Inefficiencies Have Become Less Affordable, OECD Economics Department Working Papers Number 897, 2011, Paris: OECD Publishing

[4] Die Internationalen Normen für Oberste Rechnungskontrollbehörden, auch International Standards of Supreme Audit Institutions (ISSAI) sind die professionellen Normen und Richtlinien für die staatliche Finanzkontrolle. Sie werden von der Internationalen Organisation der Obersten Rechnungskontrollbehörden (INTOSAI) beschlossen und veröffentlicht.

Konsistenz und Transparenz von Wirtschaftlichkeitsprüfungen der öffentlichen Finanzkontrolle sind grundlegende Qualitätsmerkmale, die sich aus den internationalen Standards für die öffentliche Finanzkontrolle ableiten lassen. Die einschlägige wissenschaftliche Literatur geht dabei einen Schritt weiter und fordert von den Wirtschaftlichkeitsprüfungen der öffentlichen Finanzkontrolle sogar vollständige Replizierbarkeit, die sie auch gleichzeitig als Schwäche identifiziert.[5] Dies erweist sich insofern als gerechtfertigt, als die Nachvollziehbarkeit bei Wirtschaftlichkeitsprüfungen von Einrichtungen der öffentlichen Finanzkontrolle schon alleine durch die uneinheitliche Verwendung der Begriffe Prüfungsgrundsätze und Prüfungsmaßstäbe – zwei wesentliche prüfungsmethodische Elemente einer Wirtschaftlichkeitsprüfung – stark beeinträchtigt ist. Dennoch ist einschränkend festzuhalten, dass die internationalen Standards der öffentlichen Finanzkontrolle derzeit keine vollständige Replizierbarkeit von Wirtschaftlichkeitsprüfungen fordern.

## 4. Prüfungsgrundsätze als Sollvorgaben erster Ebene

Prüfungsgrundsätze und Prüfungsmaßstäbe sind als die Sollvorgaben erster bzw. zweiter Ebene der Ausgangspunkt für die Durchführung einer jeden Wirtschaftlichkeitsprüfung. Ihre systematische und transparente Anwendung ist ausschlaggebend für die Zuverlässigkeit der Prüfungsergebnisse. Sie können – bei ISSAI-konformer Anwendung – einen wesentlichen Beitrag zur Erhöhung der Rechenschaftspflicht der öffentlichen Finanzkontrolle leisten. Gemäß ISSAIs sind die anzuwendenden Prüfungsgrundsätze bei Wirtschaftlichkeitsprüfungen die Grundsätze der Sparsamkeit, Wirksamkeit und Zweckmäßigkeit. Diese dienen jedoch nur als Grundlage für die Annahme oder Erarbeitung eigener Prüfungsgrundsätze durch die Einrichtungen der öffentlichen Finanzkontrolle selbst. So kommen neben den rechtlichen Vorgaben auch eigene Überlegungen der Organisation oder Handlungsmaßstäbe für die öffentliche Verwaltung aus der Verwaltungslehre als Quellen für mögliche Prüfungsgrundsätze in Frage. Die Bandbreite der unterschiedlichen Zugänge zur Identifikation von Prüfungsgrundsätzen wird in der folgenden Tabelle zusammenfassend dargestellt:

| ISSAIs* | Österreichischer Rechnungshof | Stadtrechnungshof Graz | Europäischer Rechnungshof* | Verwaltungslehre |
|---|---|---|---|---|
| Sparsamkeit | Sparsamkeit | Sparsamkeit | Sparsamkeit | Erfolgsmaßstäbe (Effektivität und Effizienz) |
| Wirtschaftlichkeit | Wirtschaftlichkeit | Wirtschaftlichkeit | Wirtschaftlichkeit | Rechtmäßigkeit |
| Wirksamkeit | Zweckmäßigkeit | Zweckmäßigkeit | Wirksamkeit | Sachgerechtigkeit |
| Ordnungsmäßigkeit | Ordnungsmäßigkeit | Wirksamkeit | Ordnungsmäßigkeit | Objektivität |
| Rechtmäßigkeit | Rechtmäßigkeit | Kostenwirksamkeit | Rechtmäßigkeit | Rationalität |
| | Wirkungsorientierung | Ordnungsmäßigkeit | | Anpassungs- und Innovationsfähigkeit |
| | Rffizienz | Nachhaltigkeit | | |
| | Transparenz | Gleich-stellungsorientierung | | |
| | „true and fair view“ | | | |

**Tabelle 1: Prüfungsgrundsätze der öffentlichen Finanzkontrolle**

* Die Prüfungsgrundsätze der ISSAIs und des Europäischen Rechnungshofes richten in den vorliegenden Darstellungen explizit an Wirtschaftlich keitsprüfungen. Zur besseren Vergleichbarkeit wurden die Grundsätze der Ordnungsmäßigkeit und Rechtmäßigkeit in dieser Tabelle ergänzt, da sie auch zu den allgemeinen Prüfungsgrundsätzen der ISSAIs bzw. des Europäischen Rechnungshofes zählen.

Quellen: ISSAIs; Rechnungshof Österreich; Stadtrechnungshof Graz; Europäischer Rechnungshof; Schauer, Reinbert (2015): Öffentliche Betriebswirtschaftslehre - Public Management. Wien: Linde Verlag; eigene Ausarbeitungen.

[5] Vgl. IPPF, Standard 1210.A2

Die ISSAIs sehen hinsichtlich der Transparenz der Prüfungsgrundsätze vor, dass diese allgemein zugänglich veröffentlicht werden sollten und schlagen dafür die Websites der Einrichtungen der öffentlichen Finanzkontrolle vor. Hier ist als Good Practice - Beispiel die Veröffentlichung des Handbuchs der Wirtschaftlichkeitsprüfung des Europäischen Rechnungshofes auf dessen Website zu beurteilen, da dieses neben den Definitionen der Prüfungsgrundsätze auch Beispiele für mögliche Risiken und mögliche Prüfungsfragen zu den einzelnen Prüfungsgrundsätzen umfasst.[6] Dies erscheint im Hinblick auf die Transparenz seiner Prüfungstätigkeit zweckmäßig, da die Begriffe der Sparsamkeit, Wirtschaftlichkeit und Wirksamkeit ohne weitere Erläuterungen inhaltlich schwer abzugrenzen sind. Mögliche Prüfungsfragen dienen der Förderung des Verständnisses der hinter den Prüfungsgrundsätzen liegenden Konzepte.

In der Phase der Prüfungsplanung sollten der geprüften Stelle gemäß ISSAIs die angewendeten Prüfungsgrundsätze im Rahmen der Bekanntgabe der Prüfungsziele einer Wirtschaftlichkeitsprüfung transparent übermittelt werden. Und auch für die Phase der Berichterstattung sehen die ISSAIs hohe Transparenzanforderungen vor. So fordern sie im Sinne einer Nutzenerhöhung für die Berichtsempfängerinnen und -empfänger auch für Wirtschaftlichkeitsprüfungen die Abgabe eines Prüfungsurteils über die Einhaltung der angewendeten Prüfungsgrundsätze. Dieses Prüfungsurteil kann gesamthaft getroffen werden oder, wenn dies nicht möglich ist, auf Ebene einzelner Elemente der Wirtschaftlichkeitsprüfung (z.B. auf Ebene der Prüfungsfragen oder auf Ebene einzelner Prüfungsfeststellungen) getroffen werden.

Abschließend ist festzuhalten, dass sich das öffentliche Verwaltungshandeln durch seine Vieldimensionalität auszeichnet. Rechtliche, sachliche, ethische, politische, soziale, qualitative und nicht zuletzt ökonomische Maßstäbe bilden den Rahmen für den Umgang mit den Steuermitteln, welche von den Bürgerinnen und Bürgern aufgebracht und der Verwaltung „zur Verfügung" gestellt werden. Für die öffentliche Finanzkontrolle bedeutet dies, dass auch die Grundsätze ihrer Prüfungstätigkeit diese Vieldimensionalität abbilden sollten, damit die Ergebnisse ihrer Wirtschaftlichkeitsprüfungen möglichst wirksam und relevant für die öffentliche Verwaltung sind.

# 5. Prüfungsmaßstäbe als Sollvorgaben zweiter Ebene

## 5.1. Prüfungsmaßstäbe gemäß ISSAIs

Detailliertere Definitionen und Anforderungen an Prüfungsmaßstäbe bei Wirtschaftlichkeitsprüfungen der öffentlichen Finanzkontrolle finden sich im ISSAI 300 „Allgemeine Grundsätze der Wirtschaftlichkeitsprüfung", sowie im ISSAI 100 „Allgemeine Grundsätze der staatlichen Finanzkontrolle". Letzterer enthält eine Definition für Wirtschaftlichkeitsprüfungen, die ein guter Ausgangspunkt für die Auseinandersetzung mit dem Begriff der Prüfungsmaßstäbe ist: „Bei der Wirtschaftlichkeitsprüfung wird untersucht, ob staatliche Maßnahmen, Vorhaben und Einrichtungen den Grundsätzen der Sparsamkeit, Wirtschaftlichkeit und Wirksamkeit genügen und ob Verbesserungspotenzial besteht. Dies erfolgt durch Würdigung der festgestellten Sachverhalte anhand geeigneter Prüfungsmaßstäbe und einer Analyse der Ursachen für etwaige Abweichungen von den Maßstäben oder sonstigen Unzulänglichkeiten. Ziel ist die Klärung von Prüfungsfragen und das Unterbreiten von Verbesserungsvorschlägen."[7]

[6] Handbuch der Wirtschaftlichkeitsprüfung, Europäischer Rechnungshof, 2015, http://www.eca.europa.eu/de/Pages/AuditMethodology.aspx - abgefragt am 24.8.2017.

[7] ISSAI 100.22.

Die Definition von Wirtschaftlichkeitsprüfungen des ISSAI 100 macht die Abgrenzung zwischen Prüfungsgrundsätzen und Prüfungsmaßstäben deutlich: Prüfungsmaßstäbe sind das methodische Werkzeug dafür, festzustellen inwieweit ein bestimmter Sachverhalt einen Prüfungsgrundsatz erfüllt. Die Prüfungsmaßstäbe dienen demnach dazu die übergeordneten Prüfungsgrundsätze zu operationalisieren, in dem sie die Basis für die Beurteilung des Sachverhalts und für die Erarbeitung einer Prüfungsfeststellung bilden.

Ein Beispiel, das das Zusammenwirken von Prüfungsgrundsätzen und Prüfungsmaßstäben deutlich macht, ist eine Prüfungsfeststellung aus einem Bericht des Rechnungshofes Österreich. So heißt es im Bericht des Rechnungshofes Reihe Bund RH 2011/07 „Verträge der geschäftsführenden Leitungsorgane in öffentlichen Unternehmen („Managerverträge“)“ auf Seite 537: „Der Managervertrag der Wiener Zeitung wich in Teilbereichen von den Bestimmungen der Vertragsschablonenverordnung des Bundes ab.“ Mittels Heranziehung der Vertragsschablonenverordnung des Bundes als Prüfungsmaßstab (Soll-Vorgabe der zweiten Ebene) wurde eine Feststellung über die Einhaltung des Grundsatzes der Recht- und Ordnungsmäßigkeit (Soll-Vorgabe der ersten Ebene) des Verwaltungshandelns des geprüften Unternehmens in Bezug auf die Gestaltung des überprüften Managervertrags getroffen. Idealerweise wird aus dieser Prüfungsfeststellung eine Prüfungsempfehlung abgeleitet, welche schließlich ein Prüfungsurteil über die Einhaltung des angewendeten Prüfungsgrundsatzes erlaubt (= Modellzyklus der Wirtschaftlichkeitsprüfung).

Um schon in einem frühen Stadium einer Wirtschaftlichkeitsprüfung sicherzustellen, dass der Modellzyklus einer Wirtschaftlichkeitsprüfung eingehalten werden kann, schlägt ISSAI 3200.51-55 die Erstellung einer Prüfungskonzeptmatrix vor. Sie sollte dazu dienen das Prüfungskonzept zu gliedern und dabei alle Aspekte eines Prüfungsziels abzudecken.

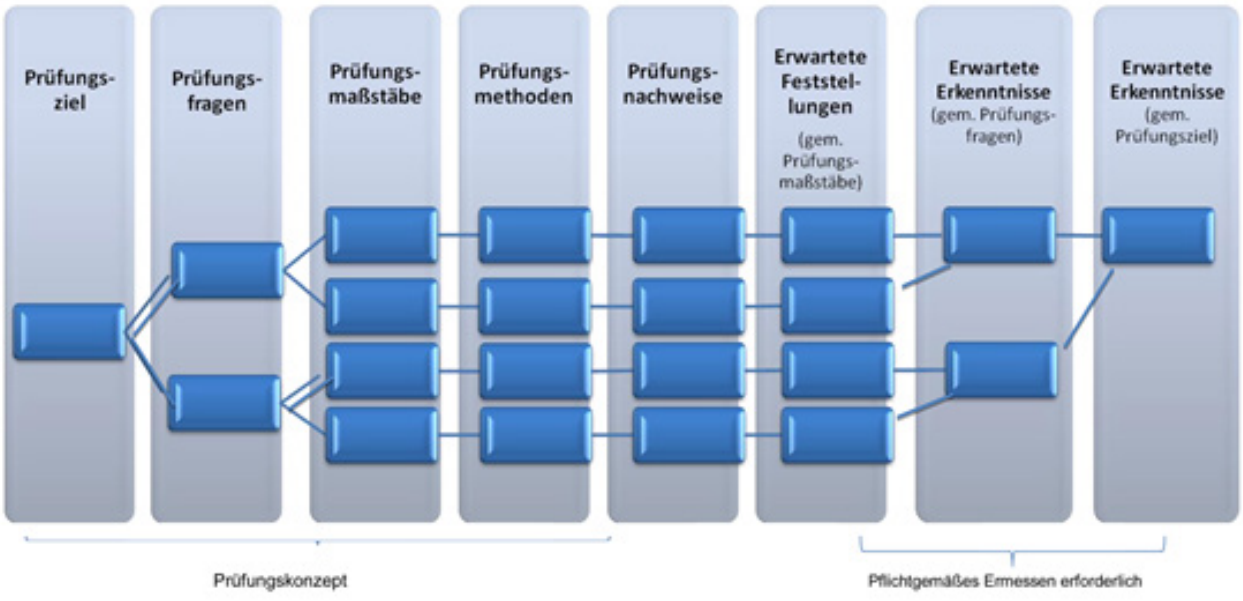



**ABB. 2: Prüfungskonzeptmatrix gemäß ISSAIs, Quelle: ISSAIs.**

Die Auswahl von geeigneten Prüfungsmaßstäben richtet sich im Wesentlichen an der Prüfungsart und am Prüfungsziel aus. Während bei Jahresabschlussprüfungen mit den anwendbaren Rechnungslegungsvorschriften und bei Recht- und Ordnungsmäßigkeitsprüfungen die gesetzlichen Grundlagen als Prüfungsmaßstäbe vorgegeben sind, können bei Wirtschaftlichkeitsprüfungen die Prüfungsmaßstäbe aus sehr unterschiedlichen Quellen stammen.

Für Wirtschaftlichkeitsprüfungen, die Elemente von Recht- und Ordnungsmäßigkeitsprüfungen umfassen, kommen folgende Quellen für die Auswahl von Prüfungsmaßstäben in Frage:

| Quellen für Prüfungsmaßstäbe | Verweise |
|---|---|
| Gesetze, Vorschriften, Normen | ISSAI 100.27<br>ISSAI 300.27<br>ISSAI 3000.47 |
| Politische Ziele oder Erklärungen der Legislative | ISSAI 3200.40 |
| Entscheidungen der Legislative oder Exekutive | ISSAI 3200.40 |
| Allgemein anerkannte Leitsätze („Guidelines“) | ISSAI 100.27<br>ISSAI 300.27<br>ISSAI 3000.47 |
| Wissenschaftliche Erkenntnisse, Standards aus Forschung, Fachliteratur, Fachbereich bzw. internationalen Organisationen | ISSAI 300.27<br>ISSAI 3000.47 |
| Good Practices/Best Practices | ISSAI 100.27<br>ISSAI 300.27<br>ISSAI 300.34 |
| Relevante Zielvorgaben | ISSAI 300.27 |
| Benchmarks: unterschiedliche Jahre der geprüften Stelle oder gleiche Maßnahme bei verschiedenen Stellen | ISSAI 3200.40 |
| Internationale Benchmarks zu Leistungsstandards | ISSAI 3200.40 |
| „Idealzustand“ unter optimalen Bedingungen | ISSAI 300.27<br>ISSAI 3000.47<br>ISSAI 3200.40 |

**Tabelle 2: Quellen für Prüfungsmaßstäbe, Quelle: ISSAIs.**

Die Auswahl der geeigneten Prüfungsmaßstäbe ist Aufgabe und liegt im Ermessen des Prüfungspersonals.[8] Da es für Wirtschaftlichkeitsprüfungen üblicherweise keine eindeutigen Prüfungsmaßstäbe gibt, kommt der Auswahl von geeigneten und zuverlässigen Prüfungsmaßstäben aus prüfungsmethodischen Gründen, aber auch aus Gründen von Transparenz und Rechenschaftspflicht eine besondere Bedeutung zu. Deshalb werden an Prüfungsmaßstäbe von Wirtschaftlichkeitsprüfungen der öffentlichen Finanzkontrolle in den ISSAIs hohe Anforderungen gestellt: „Von den gewählten Prüfungsmaßstäben hängt zudem maßgeblich das Vertrauen der Berichtsempfänger in die Stichhaltigkeit der Prüfungsfeststellungen und Schlussfolgerungen ab. Daher sind an die Zuverlässigkeit und Objektivität der Prüfungsmaßstäbe hohe Maßstäbe anzulegen.“[9] Ergänzend dazu hält ISSAI 100.27 fest: „Prüfungsmaßstäbe (...) gelten dann als geeignet, wenn sie für Berichtsempfänger zweckdienlich und verständlich sowie vollständig, zuverlässig und objektiv sind (d.h. unvoreingenommen, allgemein anerkannt und vergleichbar mit Maßstäben ähnlicher Prüfungen).“

[8] Siehe ISSAI 300.16 und ISSAI 300.20

[9] ISSAI 300.27.

Zusammenfassend ergeben sich aus den ISSAIs die in der folgenden Tabelle dargestellten Anforderungskriterien für die Auswahl von Prüfungsmaßstäben für Wirtschaftlichkeitsprüfungen der öffentlichen Finanzkontrolle:

| Anforderungskriterium | Erklärung | Verweise |
|---|---|---|
| Quantifizierbarkeit bzw. Qualifizierbarkeit | geeignet zur Durchführung eines quantitativen oder qualitativen Soll-Ist-Vergleichs | ISSAI 300.27<br>ISSAI 3000.47 |
| Zuverlässigkeit | führen zu einer schlüssigen Würdigung, zu der auch andere Prüferinnen und Prüfer gelangen würden | ISSAI 300.27<br>ISSAI 3000.47<br>ISSAI 3100.56 |
| Objektivität | unvoreingenommen und allgemein anerkannt | ISSAI 100.27<br>ISSAI 300.27<br>ISSAI 3000.47<br>ISSAI 3100.56 |
| Zweckdienlichkeit | relevant im Hinblick auf die Prüfungsfragen | ISSAI 100.27<br>ISSAI 3000.47<br>ISSAI 3100.56 |
| Nachvollziehbarkeit | eindeutig formuliert, verständlich | ISSAI 100.27<br>ISSAI 3000.47<br>ISSAI 3100.56 |
| Vollständigkeit | ausreichend, um das Prüfungsziel abzudecken | ISSAI 300.27<br>ISSAI 3000.47<br>ISSAI 3100.56 |
| Vergleichbarkeit | vergleichbar mit Prüfungsmaßstäben ähnlicher Prüfungen | ISSAI 100.27 |

**Tabelle 3: Anforderungskriterien an Prüfungsmaßstäbe gemäß ISSAIs, Quelle: ISSAIs.**

Angemessene Prüfungsmaßstäbe sind für die Qualitätssicherung einer Wirtschaftlichkeitsprüfung von Bedeutung, da „Klärung und Erarbeitung dieser Maßstäbe den Zusatznutzen der Prüfung selbst ausmachen."[10] Dieser Zusatznutzen kann aber nur dann eintreten, wenn die angewendeten Prüfungsmaßstäbe alle Anforderungskriterien erfüllen. Nur dann ist sichergestellt, dass eine durchgeführte Wirtschaftlichkeitsprüfung nicht nur dem Selbstzweck der öffentlichen Finanzkontrolle dient.

Hinsichtlich der Auswahl der Prüfungsmaßstäbe im Rahmen der Durchführung einer Wirtschaftlichkeitsprüfung legen die ISSAIs an mehreren Stellen eindeutig fest, dass die Prüferinnen und Prüfer „erhebliches Ermessen"[11] bei der Erarbeitung und Festlegung des Prüfungsgegenstandes bzw. der Prüfungsmaßstäbe haben. Dass dies aber nicht bedeuten darf, dass sie nur den Prüferinnen und Prüfern selbst bekannt sein sollen, legt ISSAI 300.27 nahe, der besagt, dass die „Prüfungsmaßstäbe (...) zwar mit den geprüften Stellen erörtert, letztlich aber allein vom Prüfungspersonal festgelegt werden (sollten)." Eine Kommunikation über die Prüfungsmaßstäbe ist grundsätzlich sowohl in der Phase der Prüfungsplanung als auch in der Phase der Prüfungsdurchführung vorzunehmen.[12]

Eine Festlegung und Kommunikation von Prüfungsmaßstäben bereits in der Phase der Prüfungsplanung kann den Vorteil haben, dass die Zuverlässigkeit der Prüfungsmaßstäbe und deren Akzeptanz bei der geprüften Stelle erhöht wird.[13] Aufgrund der üblicherweise hohen Komplexität der Sachverhalte von Wirtschaftlichkeitsprüfungen kann

[10] ISSAI 3000.46.

[11] ISSAI 300.16 und 300.20.

[12] Siehe ISSAI 3000.49, wobei ISSAI 3100.60 besagt, dass die Kommunikation spätestens in der Phase der Prüfungsdurchführung erfolgen sollte.

[13] Siehe ISSAI 300.27.

eine frühe Festlegung (aller) Prüfungsmaßstäbe oftmals ohnehin gar nicht möglich bzw. auch gar nicht zweckmäßig sein. Dieser Umstand spielt auch eine Rolle, wenn ein problemorientierter Prüfungsansatz gewählt wird. Hauptzweck dieses Prüfungsansatzes ist die Ermittlung der Ursachen für eine Abweichung vom Sollzustand bzw. einem Idealzustand. Der Soll-Ist-Vergleich anhand einzelner Prüfungsmaßstäbe tritt dabei häufig in den Hintergrund.

Für die Phase der Berichterstattung sieht ISSAI 300.23 schließlich folgendes vor: „Zur hinreichenden und umfänglichen Unterrichtung der Berichtsempfänger sind häufig die dem Prüfungsbericht, den Schlussfolgerungen und Empfehlungen zugrunde liegenden Entscheidungen näher zu erläutern." Zur Sicherstellung von Glaubwürdigkeit und Nachvollziehbarkeit soll jede Würdigung in einem Prüfungsbericht inhaltlich an den gewählten Prüfungszielen und Prüfungsmaßstäben ausgerichtet sein.[14] ISSAI 3100.30 nennt dafür folgendes modellhafte Beispiel: „Angesichts der Feststellungen A, B, C und D und nach Maßgabe des Prüfungsmaßstabes X ergibt sich folgende Würdigung: (...)." Es ist gemäß ISSAIs demnach konkret darzulegen, in welchem Zusammenhang die Prüfungsfeststellungen zu einzelnen Schlussfolgerungen stehen und gegebenenfalls zu einer übergreifenden Würdigung führen.[15] „Dies bedeutet, dass die erarbeiteten und angewandten Prüfungsmaßstäbe näher zu erläutern sind und festzustellen ist, dass alle relevanten Standpunkte berücksichtigt wurden und auf dieser Grundlage ein ausgewogener Bericht erstellt wurde."[16] ISSAI 3000.122 hält dazu ergänzend eindeutig fest, dass im Prüfungsbericht die Prüfungsmaßstäbe und deren Quelle zu nennen sind, „weil von ihnen das Vertrauen des Berichtsempfängers in die Prüfungsfeststellungen und Würdigung weitgehend abhängt."

## 5.2. Fallbeispiel Europäischer Rechnungshof

Der Europäische Rechnungshof definiert als Prüfungsmaßstäbe bei Wirtschaftlichkeitsprüfungen „Vergleichs- oder Evaluierungsmaßstäbe für die tatsächliche Ergebniserbringung (Angemessenheit von Systemen und Vorgehensweisen sowie Sparsamkeit, Wirtschaftlichkeit und Wirksamkeit von Tätigkeiten)".[17] Prüfungsmaßstäbe helfen demnach dabei, die Einhaltung der Prüfungsgrundsätze der Sparsamkeit, Wirtschaftlichkeit und Wirksamkeit im Hinblick auf einen Prüfungsgegenstand zu überprüfen. Die ausgewählten Prüfungsmaßstäbe sollen „objektiv, relevant, angemessen und erreichbar" sein. Der Aufwand zur Feststellung der Angemessenheit eines Prüfungsmaßstabes hängt von seiner Quelle ab, wobei der Europäische Rechnungshof im Wesentlichen drei Arten von Quellen für Maßstäbe von Wirtschaftlichkeitsprüfungen unterscheidet:[18]

1. Allgemein anerkannte Quellen wie Gesetze, Verordnungen oder anerkannte berufsständische Grundsätze, Berufsverbände, anerkannte Expertengremien und Fachliteratur

2. Sonstige Hauptquellen wie vom Management der geprüften Stelle angenommene Normen, Maßstäbe und Ergebnisvorgaben

3. Wenn aus 1. und 2. keine Prüfungsmaßstäbe ableitbar sind: Ergebniserbringung in vergleichbaren Organisationen, durch Benchmarking oder Beratung ermittelte Verfahren oder durch Analyse von den Prüferinnen und Prüfern selbst entwickelte Prüfungsmaßstäbe

Der Europäische Rechnungshof sieht hinsichtlich der Transparenz der angewendeten Prüfungsmaßstäbe in

[14] Siehe ISSAI 300.23 sowie ISSAI 3100.29: *„Daher wird die Würdigung inhaltlich auf die gewählten Prüfungsziele und Prüfungsmaßstäbe ausgerichtet und so abgefasst, dass die Bewertung des geprüften Sachverhalts für die Berichtsempfänger glaubwürdig und nachvollziehbar ist."*

[15] Siehe ISSAI 300.23.

[16] ISSAI 300.23.

[17] Handbuch der Wirtschaftlichkeitsprüfung, Europäischer Rechnungshof, 2015, Seite 49.

[18] Handbuch der Wirtschaftlichkeitsprüfung, Europäischer Rechnungshof, 2015, Seite 49f.

seinen Wirtschaftlichkeitsprüfungen eine sehr enge Abstimmung mit der geprüften Stelle schon in der Phase der Prüfungsplanung vor. Die geprüfte Stelle ist „bei frühestmöglicher Gelegenheit“[19] über Zweck der Prüfung, Prüfungsfragen, Prüfungshandlungen, Prüfungsmaßstäbe und Prüfungsmethodik zu informieren. Während das Handbuch der Wirtschaftlichkeitsprüfung an einer Stelle festhält, dass für Wirtschaftlichkeitsprüfungen üblicherweise keine vorgegebenen Prüfungsmaßstäbe vorhanden sind und die Auswahl von den Prüferinnen und Prüfern vorzunehmen ist, ist an anderer Stelle für die Festlegung der Prüfungsmaßstäbe ein „vollständiger Meinungsaustausch“[20] mit der geprüften Stelle vorgesehen. Die vorab festgelegten Prüfungsmaßstäbe sollten schriftlich festgehalten werden und im Idealfall noch vor Weiterleitung des Prüfungsplans innerhalb des Europäischen Rechnungshofes ein Einvernehmen mit der geprüften Stelle (bzw. mit der jeweils betroffenen Generaldirektorin oder dem Generaldirektor der Kommission) hergestellt sein. Dieser sehr strikte Ansatz in der Kommunikation von Prüfungsmaßstäben folgt einen Grundprinzip des Europäischen Rechnungshofes: „Diese Vorgehensweise entspricht der bewährten Prüfungspraxis und dem Ansatz des Hofes, der keine Überraschungen vorsieht.“[21]

Für die Abfassung der Prüfungsfeststellungen, die der geprüften Stelle zur Stellungnahme übermittelt werden, fordert das Handbuch der Wirtschaftlichkeitsprüfung des Europäischen Rechnungshofes, dass Prüfungsfeststellungen eine „klare und logische Struktur“[22] aufweisen sollten, die die angewendeten Prüfungsmaßstäbe, den erhobenen Sachverhalt und die ermittelte Abweichung transparent und nachvollziehbar darstellen. Dabei muss auch die Orientierung der Prüfungsfeststellungen an den Prüfungsgrundsätzen der Sparsamkeit, Wirtschaftlichkeit und Wirksamkeit erkennbar sein. Der Europäische Rechnungshof weist hier indirekt auf die Wichtigkeit eines transparenten und nachvollziehbaren „Prüfungspfades“ hin.

Der veröffentlichte Prüfungsbericht über eine Wirtschaftlichkeitsprüfung des Europäischen Rechnungshofes sollte schließlich „Prüfungsgegenstand, Gründe für die Prüfung, zugrunde gelegte Prüfungsfragen, Prüfungsumfang, Prüfungsmaßstäbe, Prüfungsmethodik und Prüfungsansatz, Datenquellen und alle etwaigen Beschränkungen der verwendeten Daten enthalten, wobei ausführlichere Informationen als Anhänge dem Prüfungsbericht beigefügt werden sollten.[23]

## 5.3. Fallbeispiel US General Accountability Office

Das US-amerikanische General Accountability Office, das im Jahr 1921 als General Accounting Office per Bundesgesetz gegründet wurde, ist die Oberste Rechnungskontrollbehörde der Vereinigten Staaten von Amerika. Grundlage für die Tätigkeit des US General Accountability Offices bilden die Generally Accepted Government Auditing Standards (GAGAS)[24], die vom US General Accountability Office herausgegeben werden und als Rahmenwerk für Prüfungen der öffentlichen Finanzkontrolle in den USA gelten.

Die Festlegung von Prüfungsmaßstäben („audit criteria“) bei Wirtschaftlichkeitsprüfungen ist im Kapitel 6.37 der GAGAS geregelt, wobei ein Prüfungsmaßstab allgemein als erforderlicher oder gewünschter Soll-Zustand („required or desired state“) definiert ist. Wie in den ISSAIs werden

[19] Handbuch der Wirtschaftlichkeitsprüfung, Europäischer Rechnungshof, 2015, Seite 31.

[20] Handbuch der Wirtschaftlichkeitsprüfung, Europäischer Rechnungshof, 2015, Seiten 27 und 31.

[21] Handbuch der Wirtschaftlichkeitsprüfung, Europäischer Rechnungshof, 2015, Seite 31. Interessant erscheint hierbei, dass diese Vorgehensweise ähnlich der Vorgehensweise der Internen Revision ist, bei der eine Abstimmung der anzuwenden Prüfungsmaßstäbe mit dem Management vorgesehen ist.

[22] Handbuch der Wirtschaftlichkeitsprüfung, Europäischer Rechnungshof, 2015, Seite 74.

[23] Handbuch der Wirtschaftlichkeitsprüfung, Europäischer Rechnungshof, 2015, Seite 29.

[24] Auch bezeichnet als „Yellow Book“.

mögliche Quellen für Prüfungsmaßstäbe aufgezeigt, welche von Gesetzen bis „expert opinions" und anderen Benchmatks reichen.[25] Die ausgewählten Prüfungsmaßstäbe einer Wirtschaftlichkeitsprüfung sollen relevant im Hinblick auf die Prüfungsziele sein und eine konsistente Beurteilung des Prüfungsgegenstandes erlauben.[26]

Hinsichtlich der Kommunikation der Prüfungsmaßstäbe während des Prüfungsprozesses finden sich in den GAGAS keine konkreten Angaben. Wie in den ISSAIs ist aber auch in den US-amerikanischen Standards eine offene Kommunikation der Prüfungsmethodik in der Phase der Prüfungsplanung, in der auch potentielle Prüfungsmaßstäbe festgelegt werden sollten, vorgesehen: „Auditors should communicate an overview of the objectives, scope, and methodology and the timing of the performance audit and planned reporting (...)"[27] Klar formuliert sind die GAGAS auch, was die Kommunikation der Prüfungsmaßstäbe im veröffentlichten Prüfungsbericht betrifft: „In reporting audit methodology, auditors should explain how the completed audit work supports the audit objectives, including the evidence gathering and analysis techniques, in sufficient detail to allow knowledgeable users of their reports to understand how the auditors addressed the audit objectives. Auditors should identify significant assumptions made in conducting the audit; describe comparative techniques applied; describe the criteria used; (...)"[28]

Der Prozess der Auswahl und Anwendung von Prüfungsmaßstäben ist beim US General Accountability Office durch eigene interne Richtlinien sehr detailliert festgelegt.[29] Die Anforderungen an ausgewählte Prüfungsmaßstäbe gehen dabei über jene in den GAGAS gestellten Anforderungen hinaus, in dem jeder Prüfungsmaßstab bei seiner Auswahl darauf getestet wird, ob er zweckdienlich im Hinblick auf die geprüfte Maßnahme («relevant»), angemessen im Hinblick auf die geprüfte Stelle und den geprüften Zeitraum („appropriate"), ausreichend anwendbar auf die gesamte Maßnahme oder nur Teile davon („sufficient"), qualitativ oder quantitativ operationalisierbar („operationalized") und ausreichend getestet und überprüft („valid") ist.

Eine Dokumentation über die Ergebnisse der Beurteilung eines Prüfungsmaßstabes ist tabellarisch zu dokumentieren. Folgendes Beispiel zeigt die Beurteilung eines Prüfungsmaßstabes für eine durchgeführte Wirtschaftlichkeitsprüfung des US General Accountability Office über Zweckmäßigkeit und Transparenz der von der US central bank durchgeführten Bankenstresstests der Jahre 2014 und 2015 (in Auszügen):

| **Criteria/ Criteria assessment elements** | **Relevant** | **Appropriate (1)** | **Appropriate (2)** | **Sufficient** | **Operationalized** | **Valid** |
|---|---|---|---|---|---|---|
| | Applicable to activity | Applicable to institution | Applicable to time period | Apply to whole activity or some part | Qualitative or quantitative application | Sufficient testing or review |
| National Research Council (NRC) principles and best practices in complex modeling and risk management. | Yes.<br>Describes best practices for scenario testing. | Yes.<br>The NRC is charged with advising the federal government on science and technology. | Yes.<br>Issued publicly in 2012. | Part of the activity. Applies to design of stress testing. | Qualitative comparison of the stress testing mdeldesign with principles and best practices for moel design. | Yes.<br>Developed by academics and research experts, reviewed and verified by technical experts committee. |

**Tabelle 4: Beurteilungsmatrix für Prüfungsmaßstäbe (Beispiel US General Accountability Office), Quelle: US General Accountability Office.**

[25] Siehe im Wesentlichen GAGAS Kapitel 6.37 und A6.02.

[26] Siehe GAGAS Kapitel 6.37.

[27] GAGAS Kapitel 6.12a und 6.47. Ergänzend halten die GAGAS im Kapitel 6.07 fest, dass bei Wirtschaftlichkeitsprüfungen die Planung ein kontinuierlicher Prozess ist, der bis zur Fertigstellung der Prüfungstätigkeit Änderungen in der Methodologie erfordern kann.

[28] GAGAS Kapitel 7.13.

[29] Die folgenden Ausführungen basieren auf den vom US Government Accountability Office zusammengestellten Unterlagen für den „Workshop on Criteria in Financial Sector Audits", der am 10.5.2017 im Rahmen eines Arbeitsgruppentreffens der INTOSAI-Arbeitsgruppe „Finanzielle Modernisierung und Regulierungsreform" beim US Government Accountability Office in Washington abgehalten wurde.

Der im US General Accountability Office definierte Prozess zur Auswahl und Anwendung von Prüfungsmaßstäben bei Wirtschaftlichkeitsprüfungen sieht nicht nur eine Beurteilung der Prüfungsmaßstäbe in der Phase der Prüfungsplanung vor, sondern auch eine abermalige Beurteilung der Prüfungsmaßstäbe während des Prüfungsprozesses. Sollten sich Prüfungsmaßstäbe als nicht mehr oder doch nicht geeignet erweisen, wären neue Prüfungsmaßstäbe zu finden bzw. gegebenenfalls zu adaptieren, sodass sie schließlich wieder sämtliche Anforderungskriterien erfüllen.

Auch wenn diese Maßnahmen des US General Accountability Office mit einem erhöhten Dokumentationsaufwand verbunden sind, stellt sie sicher, dass Transparenz und Rechenschaftspflicht im Hinblick auf die Anwendung von Prüfungsmaßstäben bei Wirtschaftlichkeitsprüfungen erreicht werden und die Durchführung der Wirtschaftlichkeitsprüfungen nicht zum Selbstzweck wird. Sowohl eine eingehende interne Auseinandersetzung mit der angewendeten Prüfungsmethodik, als auch eine transparente Berichterstattung nach Außen sind notwendig, um eine zufriedenstellende Erfüllung der Transparenz und Rechenschaftspflicht bei Wirtschaftlichkeitsprüfungen der öffentlichen Finanzkontrolle zu gewährleisten.

## 6. Vergleich mit verwandten Disziplinen: Beispiel Interne Revision

Die Interne Revision hat hinsichtlich des Prüfungsansatzes starke Ähnlichkeiten mit der Wirtschaftlichkeitsprüfung der öffentlichen Finanzkontrolle. Aus relevanten Standards ableitbare Prüfungsgrundsätze sind Effektivität (bzw. Zweckmäßigkeit), Gesetzmäßigkeit und Ordnungsmäßigkeit. Und auch Prüfungsmaßstäbe (in den Internationalen Grundlagen für die Interne Revision als „Kriterien“ bezeichnet) spielen eine Rolle in der Prüfungstätigkeit der Internen Revision. Obwohl in den Internationalen Grundlagen für die Interne Revision genauere Ausführungen zu Prüfungsgrundsätzen fehlen, ist der Begriff des „Kriteriums“ näher erläutert. So ist im Regelwerk folgendes festgehalten: „Zur Bewertung von Steuerung, Risikomanagement und Kontrollen sind angemessene Kriterien erforderlich. Interne Revisoren müssen ermitteln, inwieweit das Management und/oder Geschäftsleitung bzw. Überwachungsorgan angemessene Kriterien zur Beurteilung der Zielerreichung festgelegt hat. Soweit die Kriterien angemessen sind, müssen sie von Internen Revisoren bei der Beurteilung verwendet werden. Soweit die Kriterien nicht angemessen sind, müssen Interne Revisoren durch Diskussion mit Management und/oder Geschäftsleitung bzw. Überwachungsorgan angemessene Beurteilungskriterien identifizieren.“[30] Der Begriff des „Kriteriums“ entspricht demgemäß jenem des Prüfungsmaßstabes gemäß ISSAIs. Quellen für „Kriterien“ werden interne (z.B. Richtlinien der Organisation), externe (z.B. Gesetze) und praxiserprobte „Kriterien“ (z.B. Branchenstandards) genannt.[31] Hier wird deutlich, dass die Interne Revision innerhalb einer Organisation angesiedelt ist. Denn bei der Festlegung von Prüfungsmaßstäben muss die Interne Revision auf von der Organisationsleitung oder dem Kontrollorgan definierte Prüfungsmaßstäbe zurückgreifen, wenn diese angemessen sind. Wenn keine angemessenen Prüfungsmaßstäbe vorliegen, so sind in Abstimmung mit der Organisationsleitung oder dem Kontrollorgan welche festzulegen. Hierbei wird der im Vergleich zur öffentlichen Finanzkontrolle stark eingeschränkte Ermessensspielraum der Internen Revision deutlich.

[30] Internationale Grundlagen für die berufliche Praxis der Internen Revision 2017, Seite 48.

[31] Internationale Grundlagen für die berufliche Praxis der Internen Revision 2017, Seite 48.

## 7. Fazit

6.Der vorliegende Artikel legte seinen Schwerpunkt auf die Erarbeitung von prüfungsmethodischen Anforderungen an Wirtschaftlichkeitsprüfungen der öffentlichen Finanzkontrolle. Bei Wirtschaftlichkeitsprüfungen handelt es sich üblicherweise um sehr komplexe, nicht standardisierte Prüfungsvorhaben, weshalb sie bei mangelnder Transparenz hinsichtlich der angewendeten Prüfungsmethodik ein hohes Risiko mangelnder Nachvollziehbarkeit in sich bergen.

Prüfungsgrundsätze bilden die fundamentalen Anforderungen an das Verwaltungshandeln ab. Als Quellen für die Identifikation von Prüfungsgrundsätzen stehen gesetzliche Vorgaben, internationale Standards, Fachliteratur und Good Practice - Beispiele sowie nicht zuletzt auch eigene organisationsinterne Überlegungen zur Verfügung. Zur Erfüllung der Rechenschaftspflicht der öffentlichen Finanzkontrolle ist es dabei wichtig, dass die angewendeten Prüfungsgrundsätze transparent kommuniziert werden. Eine allgemeine Information über alle Prüfungsgrundsätze, die der Tätigkeit einer Einrichtung der öffentlichen Finanzkontrolle zugrunde liegen, kann gemäß Vorschlag der ISSAIs auf der Website der Einrichtung erfolgen. Denkbar wären hier ergänzend auch Social Media - Kanäle oder allgemeine Publikationen wie Tätigkeits- oder Rechenschaftsberichte. Zur Sicherstellung der Nachvollziehbarkeit von Prüfungsergebnissen wären auch in jedem Bericht über eine Wirtschaftlichkeitsprüfung die angewendeten Prüfungsgrundsätze zu erläutern, sowie eine Aussage über die Einhaltung der Prüfungsgrundsätze zu treffen.

Aufgrund des Fehlens eindeutig festgelegter Prüfungsmaßstäbe bei Wirtschaftlichkeitsprüfungen der öffentlichen Finanzkontrolle stellen die relevanten internationalen Standards hohe Anforderungen an die Auswahl geeigneter und zuverlässiger Prüfungsmaßstäbe. Gemäß ISSAIs müssen sie folgende sieben Anforderungskriterien erfüllen: Quantifizierbarkeit bzw. Qualifizierbarkeit, Zuverlässigkeit, Objektivität, Zweckdienlichkeit, Nachvollziehbarkeit, Vollständigkeit und Vergleichbarkeit.

Auch die Transparenzanforderungen an die Prüfungsmaßstäbe sind während des gesamten Prüfungsprozesses und insbesondere bei der Berichterstattung hoch. Die ISSAIs fordern eine umfassende Darstellung der Prüfungsmaßstäbe in den Prüfungsberichten, um die Ergebnisse der Wirtschaftlichkeitsprüfung nachvollziehbar zu machen. Zur Sicherstellung von Glaubwürdigkeit und Nachvollziehbarkeit soll jede Würdigung in einem Prüfungsbericht inhaltlich an den gewählten Prüfungszielen und Prüfungsmaßstäben ausgerichtet sein. Ziel dieser Anforderungen ist es, zu verhindern, dass die Durchführung von Wirtschaftlichkeitsprüfungen den Anschein erweckt, ein Selbstzweck der öffentlichen Finanzkontrolle zu sein.

Um Kontrolle nicht zum Selbstzweck werden zu lassen, darf die öffentliche Finanzkontrolle nicht aufhören, in einem ständigen Prozess Rechenschaft über sich selbst abzulegen und soll dabei nicht nur die Ergebnisse ihrer Prüfungstätigkeit transparent machen, sondern auch ihre angewendeten Prüfungsmaßstäbe, Prüfungsprozesse und Prüfungsmethoden. So kann die öffentliche Finanzkontrolle nicht nur zu mehr Transparenz und Rechenschaftspflicht bei den geprüften Stellen beitragen, sondern auch durch ihre eigene Vorbildwirkung das Verhalten anderer Stellen der öffentlichen Verwaltung positiv beeinflussen.

# Resilienz als Kernkompetenz für prüfende und beratende Berufe

## Die Erfolgsformel starker Menschen[1]

**StB. MMag. Harald Mairhofer, PMBA,**
leitete mehr als 10 Jahren den Geschäftsbereich Interne Revision in einem der größten Unternehmen Österreichs. Davor war er an einer der Big Four Wirtschaftstreuhandkanzleien sowie im Beteiligungsmanagement einer Großbank tätig. Er ist Autor des Buchs „Resilienz – Widerstandskraft für prüfende Berufe“[2].

## Inhalt



[1] Die Ausführungen in diesem Beitrag sowie darauf aufbauende Handlungsempfehlungen stellen die persönliche Sichtweise des Autors dar.
[2] Siehe Mairhofer (2014).

Der vorliegende Beitrag gibt einen Einblick in eine wichtige, dennoch noch oftmals unberücksichtigte Thematik: Resilienz als Kernkompetenz im Berufsstand der prüfenden und beratenden Berufe. Die zentralen Fragestellungen im Rahmen dieses Artikels rund um Resilienz werden in den einzelnen Kapiteln Schritt für Schritt beantwortet.

- Was macht den Menschen stark?
- Was gibt der Seele Halt?
- Kann man innere Stärke trainieren?
- Wie gewinnt man seine eigene Kraft wieder zurück?
- Wie kann man negativen Erlebnissen auch etwas Positives abgewinnen?
- Wie schafft man es in einem schwierigen Umfeld, die eigene Position nicht aufzugeben?

Die Themenfelder und Ziele dieses Beitrags lassen sich wie folgt zusammenfassen:

- die Bedeutung der Resilienz für den Berufsstand der Internen Revision
- der Weg zu innerer und mentaler Stärke; Erweiterung unserer Wahrnehmung – „Blick über den Tellerrand"
- Gesetzmäßigkeiten der „mentalen" Ebene; Energie-Management und weiterführende Tipps
- als Prüfer und Berater noch besser sein/werden

# 1. Problemstellung

Im Berufsstand der prüfenden und beratenden Berufe ist das Thema Resilienz (= persönliche Widerstandskraft) noch weitgehend unbekannt bzw. wird diesem so wichtigen Aspekt noch wenig Bedeutung beigemessen. Konkrete Äußerungen in der Kollegenschaft: „Ist etwas für Lebensund Sozialberater", „Klingt esoterisch angehaucht …",

„Ich bin doch zuständig für die Prüfung des Fachgebietes XY", „Habe so viel Fachspezifisches zu erledigen, dass ich dafür keine Zeit mehr habe". Faktum ist, dass man als Prüfer/Berater oft mit Widerstand und mit „Machtspielen" konfrontiert ist. Negative Prüfungsergebnisse und Berichte werden mitunter unfair attackiert. Aussagen der Geprüften wie „…bin im Stress", „… warum ich?", „… ich glaube, dass das anders abzuwickeln ist"; „… da steht, was Sie wissen wollen", gehören zum Prüfungsalltag. Darüber hinaus kann es vorkommen, dass Prüforgane im Unternehmen auch gemieden werden, was einen hohen emotionalen Druck und Frustration bei den Prüfern auslösen kann.

Folgende konkrete Beispiele aus der Prüfungsund Beratungspraxis verdeutlichen, dass es empfehlenswert ist, sich mit Resilienz in unserem Berufsstand zu beschäftigen:

- **Beispiel 1**: Viele Manager haben Angst (z. B. vor Verlust des aufgebauten Status, Verlust von Vermögen) bzw. tun Dinge nur deshalb, um die Erwartungen anderer zu erfüllen und vergessen dabei die eigenen Bedürfnisse und im Extremfall sich selbst. Sie sind somit die „Hamster im Berufs-Rad".

- **Beispiel 2**: In einem Unternehmen war das Unternehmensklima nicht „revisionsfreundlich", sodass sich eine neue Mitarbeiterin der Internen Revision entschieden hat, die Interne Revision noch im Probemonat zu verlassen.

- **Beispiel 3**: Im Zuge von Prüfungsgesprächen gibt es Personen, welche sich Details „aus der Nase ziehen lassen", jedoch später den Prüfern vorwerfen, nicht nach bestimmten Unterlagen gefragt zu haben.

- **Beispiel 4**: In einer internationalen Konzernrevision konnte der Revisor nicht mit einer uns fremden Kultur umgehen (arabischer, asiatischer Raum), nahm dieses Manko persönlich, konnte in weiterer Folge Berufliches nicht mehr von Privatem trennen und schied mit der Diagnose Burn out aus dem Team der Internen Revision aus.

Um mit solchen herausfordernden und durchaus schwierigen Situationen umzugehen, brauchen interne Revisoren bestimmte Eigenschaften, um an diesen Konfrontationen nicht zu zerbrechen. In diesem Zusammenhang rücken das in unserem Berufsstand noch immer relativ unbekannte Thema „Resilienz" und die damit verbundenen „Soft Skills" zunehmend in den Mittelpunkt. Wie bereits Prof. Dr. Eulerich und MSc. van Uum im Fachartikel „Die Interne Revision als Management Training Ground" in der ZIR 3/14 dargestellt haben, ist die Ausbildung von Revisoren auf der Ebene der „Soft Skills" ein zentraler Bestandteil im Kompetenzprofil eines Revisors.[3]

Resilienz darf keinesfalls missverstanden werden als „Widerstand leisten". Darüber hinaus ist Resilienz keine sofort wirkende „Wunderpille" auf Knopfdruck. Vielmehr soll der Artikel dazu beitragen, die eigene Kraft zu stärken und somit besser bzw. professioneller mit schwierigen Gesprächspartnern umgehen zu lernen. Revisoren müssen auch negative Informationen ansprechen und diskutieren ohne jedoch die eigene Position zu verlieren. Resiliente Menschen unterscheiden sich von anderen durch ihre Widerstandskraft und schaffen es durch ihre Flexibilität, auch in stressigen Zeiten entschlossen zu handeln und mit Zuversicht in die Zukunft zu schauen.

## 2. Resilienz für die Interne Revision

Unabhängig agierende Prüfer können als Bedrohung erlebt werden, da durch deren Tätigkeit Transparenz entsteht und diese nicht immer gewünscht ist. Weil die fachlichen Anforderungen an Prüfer stetig ansteigen, widmet sich dieser Beitrag den persönlichen Eigenschaften von Revisoren und insbesondere der Frage, wie eine hohe psychische Widerstandskraft (Resilienz) erreicht werden kann. Aufgrund der hohen Belastung im Beruf ist es erforderlich und unumgänglich, dass ein Prüfer im Sinne des Resilienzkonzeptes mit seiner persönlichen Energie bzw. „Energiebilanz" professionell umgehen muss, d.h. Prüfer benötigen einen höheren „Energiespeicher" und müssen diesen auch wieder auffüllen. In der Praxis haben Revisionsmitarbeiter auch Prüfungsabteilungen wieder verlassen, gerade weil man nicht überall wertgeschätzt, teilweise gemieden und im Extremfall sogar ausgegrenzt wird. Als Prüfer muss man mit solchen Themen bzw. Problemstellungen professionell umgehen. Umso wichtiger ist das Kriterium Resilienz als persönliches Charakteristikum sowie ein guter Umgang mit seinen persönlichen Energiereserven bzw. -speichern. Bei der geprüften Einheit kann im Verlauf der Prüfung ein Gefühl des „Bedrohtwerdens" entstehen, umgekehrt beim Prüfer ein Gefühl des „Getäuschtwerdens". Für Interne Revisoren sind daher nicht nur Resilienz-Faktoren sondern auch psychologisches Wissen für den konkreten Prüfungsalltag von Bedeutung. Es empfiehlt sich daher, hinter die Kulissen zu schauen und ein Verständnis für den geprüften „Menschen" sowie die dahinter stehende Persönlichkeit zu entwickeln, in weiterer Folge sich darauf einzustellen und diesen menschlichen bzw. „psychologischen

[3] Die Ausführungen in diesem Beitrag sowie darauf aufbauende Handlungsempfehlungen stellen die persönliche Sichtweise des Autors dar.

Aspekt“ für die Revisionstätigkeit zu nutzen. Resiliente Führungskräfte, Teams und Unternehmen unterscheiden sich wesentlich von anderen durch ihre Flexibilität, da es ihnen gelingt, selbst in turbulenten Zeiten und Krisen entschlossen und zuversichtlich zu handeln.

## 2.1. Übergeordnete Bedeutung des Themas

Stress stellt die größte Gefahr für unsere geistige Gesundheit dar.[4] Krankheiten im Zusammenhang mit Stress verursachen in den USA Kosten von mehr als 200 Mrd. USD p.a.[5] Wissenschaftliche Untersuchungen haben ergeben, dass bei Stress eine Kaskade physiologischer Vorgänge abläuft.[6]

In Deutschland wurden im Jahr 2011 bereits 59,2 Millionen Arbeitsunfähigkeitstage aufgrund von psychischen Erkrankungen vermerkt. Dies bedeutet einen Anstieg um mehr als 80 Prozent in den letzten 15 Jahren. Laut Schätzungen von Gesundheitsexperten und Krankenkassen sind in Deutschland bis zu 13 Millionen Arbeitnehmer von Burnout betroffen. Im Jahr 2010 waren in Deutschland fast zehn Millionen Krankenstandstage auf Erwerbstätige mit Burnout-Symptomen zurückzuführen. Ein Burnout verursacht – Untersuchungen der Weltgesundheitsorganisation zufolge – im Durchschnitt 30,4 Krankheitstage pro Jahr. In Deutschland waren 41 Prozent aller Neuzugänge zur Rente auf psychische Störungen zurückzuführen. Damit gehören psychische Belastungen inzwischen zur Ursache Nummer eins für Frühverrentungen, wobei das Durchschnittsalter in diesem Zusammenhang bei 48,3 Jahren liegt.[7] Auch in Österreich liegen ähnliche Daten zu dieser Thematik vor.[8] Das Thema Resilienz im Sinne von persönlicher psychischer Widerstandskraft wird somit nicht nur für Prüfer von höchstem Interesse sein, sondern auch für verwandte und ähnliche Berufsbranchen.

Im beruflichen Kontext versteht man unter „Resilienz“ die Fähigkeit, sich von einer schwierigen Situation nicht niederringen zu lassen bzw. nicht daran zu zerbrechen.

# 3. Was versteht man unter Resilienz?

Resilienz lässt sich vom lateinischen Verb „*resiliere*“ ableiten, was so viel wie „abprallen“ bedeutet. Im Englischen bedeutet das Wort „resilience“ Spannkraft, Widerstandsfähigkeit und bezeichnet im sozialpsychologischen Zusammenhang allgemein die Fähigkeit eines Menschen, erfolgreich mit unerwarteten, belastenden Situationen umzugehen.[9] Resilienz wird somit als „seelische Widerstandsfähigkeit in sehr belastenden, risikobehafteten […] Situationen verstanden“.[10]

Ein anschauliches Beispiel beschreibt die Fähigkeit eines „Stehaufmännchens“, welches sich aus jeder beliebigen Lage wieder aufzurichten vermag. Resilienz ist eine Eigenschaft, mit Belastungen in der Arbeitswelt professionell umzugehen und dient dazu, die psychische Gesundheit zu erhalten. Im beruflichen Kontext versteht man unter „Resilienz“ die Fähigkeit, sich von einer schwierigen Situation nicht niederringen zu lassen bzw. nicht daran zu zerbrechen.

[4] Vgl. Lambert (2013), S. 97.
[5] Vgl. Lambert (2013), S. 98 f.
[6] Vgl. Lambert (2013), S. 100 f.
[7] Vgl. TK Gesundheitsreport & KKH-Allianz & WHO & Stressreport Deutschland 2012.
[8] Vgl. Österreichischer Bundesverband für Psychotherapie (2010), S. 2 f.
[9] Vgl. Wustmann (2004).
[10] Vgl. Zander (2009), S. 12.

Resiliente Menschen verfügen über eine entsprechende (psychische) Widerstandskraft und geben auch nach Rückschlägen nicht auf. Resilienz ist somit die „seelische Kraft, die Menschen befähigt, Niederlagen, Unglück und Schicksalsschlägen besser und schneller standzuhalten."[11] Resiliente Menschen machen das Beste aus einer unglücklichen Situation, lernen daraus und wachsen über eine Leiderfahrung über sich selbst hinaus.[12]

Die richtige Haltung und Einstellung ist entscheidend. Probleme sollen als Herausforderung gesehen werden, Schwierigkeiten sollen nicht zur Handlungsunfähigkeit führen, sondern zu weiteren Leistungen anspornen.[13] Es geht somit darum, sich trotz widriger Umstände gut zu entwickeln und glücklich zu sein, und nicht darum, „unverwundbar" zu werden. Deshalb ist es wichtig, aus Situationen zu lernen und das Leben positiv zu gestalten.[14] Es wird empfohlen, Dinge, die man nicht ändern kann, zu akzeptieren. Daraus entsteht eine Kraft, Lösungen zu entwickeln. Ein entscheidender Fehler wäre, schwierige Situationen schönzureden. Wichtiger ist vielmehr, diese gelassen betrachten zu können, um sich entsprechende Lösungen zu überlegen.[15]

*Klein* verweist in diesem Zusammenhang auf die Fähigkeit, Negatives herausnehmen zu können, sowie eine aufmerksame Haltung gegenüber sich selbst, der Situation und den handelnden Personen einzunehmen.[16]

Resilienz ist nicht nur auf Personen, sondern auch auf Organisationen anwendbar: *Buchholz/ Knorre* verweisen darauf, dass das Handeln darauf ausgerichtet werden soll, eine erhöhte Widerstandsfähigkeit zu erreichen.[17] Resiliente Organisationen gelten als agil, anpassungsund adaptionsfähig, zeichnen sich somit durch hohe Wachsamkeit für etwaige Bedrohungen und Flexibilität aus, ohne ihre Identität und Einheit zu verlieren, sind realistisch in ihrer Einschätzung der individuellen Vulnerabilität.[18] Des Weiteren geht es um das erfolgreiche Registrieren von Veränderungen und Verarbeitung von Beobachtungen, um in Folge diese Lerneffekte für das individuelle Geschäftsmodell zu nutzen.[19] Resiliente Mitarbeiter wissen, dass es einen unvorhergesehenen Wandel geben wird und der Alltag somit widersprüchlich sein kann.[20]

## 3.1. Lösungsansätze aus der Resilienzforschung

Die Resilienzforschung geht auf Forschungen in den USA in den 1950er Jahren zurück, konkret auf den Universitätsprofessor für Psychologie Jack Block,[21] und beschäftigt sich mit der Frage, warum es manchen Menschen besser als anderen gelingt, mit Schwierigkeiten, Krisen und Schicksalsschlägen fertig zu werden. Resiliente Menschen haben gelernt, sich auf ihre Ziele zu fokussieren und Energieressourcen aufzubauen. Sie verfügen über eine hohe Selbstwirksamkeit und Problemlösungskompetenz. Ihre wesentlichen Grundhaltungen sind Optimismus, Akzeptanz und Lösungsorientierung. Daraus lassen sich folgende Resilienzfaktoren, die sogenannten sieben Säulen der Resilienz, ableiten:

[11] Maehrlein (2013), S. 19.
[12] Vgl. Maehrlein (2013), S. 19.
[13] Vgl. Klein (2011), S. 358.
[14] Vgl. Klein (2011), S. 359.
[15] Vgl. Klein (2011), S. 360.
[16] Vgl. Klein (2011), S. 363.
[17] Vgl. Buchholz/Knorre (2012), S. 3.
[18] Vgl. Buchholz/Knorre (2012), S. 8.
[19] Vgl. Buchholz/Knorre (2012), S. 14.
[20] Vgl. Buchholz/Knorre (2012), S. 5.
[21] Vgl. Borgert (2013), S. 12 f.

- **Akzeptanz**: Es ist wie es ist – Zurechtfinden mit Unabänderlichem
- **Optimismus**: Vertrauen, dass es besser wird, zuversichtlich sein für die eigene Zukunft
- **Selbstwirksamkeit**: Achtung der eigenen Bedürfnisse – Probleme als Herausforderung sehen
- **Verantwortung**: Verlassen der Opferrolle, Respektierung der persönlichen Leistungsgrenzen – Akzeptanz der Konsequenzen von persönlichen Handlungen
- **Netzwerkorientierung**: Hilfe annehmen und selbst Hilfe geben
- **Lösungsorientierung**: Entdeckung und Umsetzung der persönlichen Lebenswünsche – richtige Prioritätensetzung
- **Zukunftsorientierung**: Realisation der persönlichen Pläne – Wissen was man will[22]

## 3.2. Resilienz als immergrüner Bambus

Eine Weiterentwicklung der oben angeführten Resilienzfaktoren ist das Modell des immergrünen Bambus von Maehrlein.[23]

Abb. 1 zeigt eine Bambuspflanze, die eine sehr gute Versinnbildlichung für Resilienz darstellt. Ob Trockenzeit, Schnee, Wind oder andere Hindernisse:

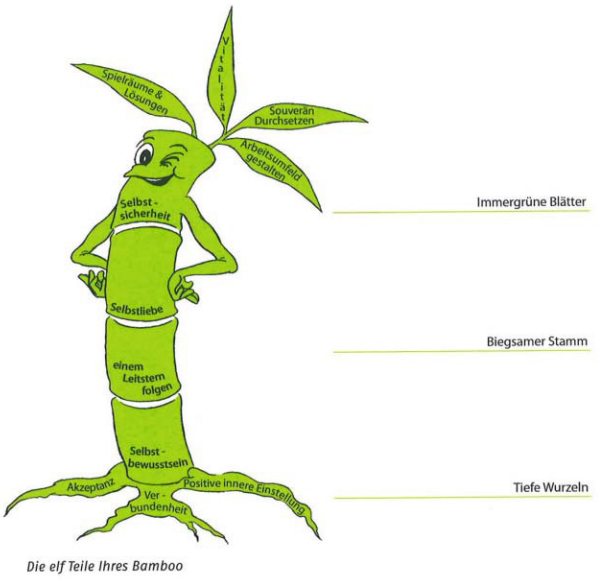



**ABB. 1: Die elf Teile des Bambus**[24]

Der Bambus wächst das ganze Jahr über weiter und entwickelt grüne Blätter, weil er all seine inneren Kräfte immer wieder gezielt mobilisiert und aktiviert.[25] Das, was der Bambus schafft, kann auch jeder Mensch realisieren. Denn jeder von uns trägt einen Bambus in sich, also eine Kraft bzw. innere Stärke, jeden Tag seine vielfältigen Aufgaben zu meistern, mit Druck, Konflikten, Misserfolgen und Niederlagen fertig zu werden und gleichzeitig gestärkt aus Krisen hervorzugehen – also die Fähigkeit zur Resilienz. Insgesamt sind es elf Teile, die die innere Stärke eines Menschen ausmachen:[26]

Die drei tiefen Wurzeln Akzeptanz, Verbundenheit und positive innere Einstellung unterstützen den Menschen, sich fest und dauerhaft im Leben zu verankern, um nicht aus dem Gleichgewicht zu geraten.[27] Außerdem hilft der biegsame Stamm des Bambus mit seinen vier Bestandteilen, den ICH-Stärken

- Selbstbewusstsein,
- einem Leitstern folgen,
- Selbstliebe und
- Selbstsicherheit

[22] Vgl. Heller (2013), S. 3, 15 ff.
[23] Vgl. Maehrlein (2013), S. 17.
[24] Vgl. Maehrlein (2013), S. 19.
[25] Vgl. Maehrlein (2013), S. 16.
[26] Vgl. Maehrlein (2013), S. 17.
[27] Vgl. Maehrlein (2013), S. 17.

selbst wie ein Bambus im Sturm zu sein, sich nicht unterkriegen zu lassen und nach Rückschlägen wieder aufzustehen und neue Triebe auszubilden.[28] Die Spitze des Bambus bilden die vier immergrünen Blätter. Diese bestehen aus den Energiespendern Spielräume und Lösungen, Vitalität, souveräne Durchsetzungskraft und dem Gestalten des eigenen Arbeitsumfeldes. Die Blätter ermöglichen einem, ähnlich wie beim Bambus, sich immer der Sonne zuzuwenden, um auch im härtesten Winter grün zu bleiben und nicht durch einen heftigen Sturm abzufallen.[29]

Eigenschaften, die einen resilienten Menschen ausmachen, sind vor allem Akzeptanz von Situationen, Lösungsorientierung, Verlassen der Opferrolle und Übernahme von Verantwortung für das eigene Handeln.

## 4. Auszüge der Ergebnisse der empirischen Untersuchung zum Thema Resilienz in der Internen Revision

Wie bereits erwähnt tragen Interne Revisoren zur Transparenz in einem Unternehmen bei und stoßen im Zuge ihrer Tätigkeit auch oftmals auf Widerstand. Umso wichtiger ist das Kriterium Resilienz als persönliches Charakteristikum sowie ein guter Umgang mit den ganz persönlichen Energiereserven bzw. -speichern. Aus diesem Grund stand im Zentrum des Forschungsinteresses der erstmaligen empirischen Untersuchung aus dem Jahr 2013 die persönliche psychische Widerstandskraft (Resilienz) von Personen, welche in der Internen Revision tätig sind.

Im Rahmen dieser Untersuchung wurde der Frage nachgegangen, wie die Befragten persönlich mit der Rolle als Revisor umgehen, wo man Energie benötigt und wie die persönlichen Energiespeicher aufgefüllt werden. Die Umfrage wurde in Österreich mit Unterstützung des IIA Austria durchgeführt. Die Rücklaufquote betrug 32 %, welche als äußerst positiv zu bewerten ist, da hierüber auch die Bedeutung und die Relevanz des Themas für den Berufsstand der Internen Revision bestätigt wurde.

Das Kriterium Resilienz ist für die befragten Teilnehmer eine Eigenschaft bzw. Fähigkeit, die für die Ausführung der Tätigkeiten der Internen Revision sehr wichtig bzw. wichtig ist. Resilienz ist demnach nicht nur für den einzelnen Revisor wichtig, sondern wird von den Befragten als eine große Unterstützung für das gesamte Revisionsteam gesehen. Um sich nach Krisen wieder aufrichten und gute Arbeit leisten zu können, bedarf es einer hohen eigenen Widerstandskraft. So schätzen sich 65 % der Befragten als sehr resilient bzw. resilient ein. Lediglich 2 % der Befragten schätzen ihre eigene Widerstandskraft als sehr gering ein. Eigenschaften, die laut den Befragten einen resilienten Menschen ausmachen, sind vor allem Akzeptanz von Situationen, Lösungsorientierung, Verlassen der Opferrolle und Übernahme von Verantwortung für das eigene Tun und Handeln. Der Großteil der Befragten ist der Meinung, dass man sich Resilienz aneignen kann.

Im Hinblick auf das Kriterium „Energie-Balance“ wurde festgestellt, dass für die Mehrheit der Befragten das Kriterium „Energie auftanken, abschalten, bewusst Zeit für sich nehmen“, eine sehr wichtige bzw. wichtige Rolle spielt, um sich von energieraubenden Tätigkeiten in der Internen Revision, wie insbesondere Schlussbesprechungen oder Gespräche mit Geprüften, zu „erholen“ und so die eigene persönliche Widerstandskraft zu erhöhen bzw. aufrecht zu erhalten. Kraft tanken die Teilnehmer der empirischen Untersuchung vor allem durch sportliche Aktivitäten in der Natur, wobei in diesem Zusammenhang auch die Spiritualität eine

[28] Vgl. Maehrlein (2013), S. 16.
[29] Vgl. Maehrlein (2013), S. 16.

wichtige Rolle spielt. So werden die Kraftreserven von 55 % der Befragten auch durch Lesen oder Musikhören aufgefüllt.

Die Befragten gaben neben den vorgegebenen Kriterien auch ein funktionierendes familiäres Umfeld und soziale Kontakte als persönliche Kraftquelle an. Dieses Ergebnis wurde auch in anderen Studien bestätigt. So haben zahlreiche resilienz-wissenschaftliche Untersuchungen belegt, dass funktionierende soziale Kontakte das Wohlbefinden fördern, eine starke und anhaltende Zufriedenheit erzeugen und die Lebenserwartung um bis zu 22 % steigern können.[30]

Aufbauend auf diesen Erkenntnissen wurde vom Autor dieses Fachartikels ein „**Quickcheck**“ zum Themenkomplex „Resilienz in der Internen Revision“ entwickelt. Durch Beantwortung von Fragen, wie:[31]

- Sind Sie gerne der Fels in der Brandung?
- Folgen Sie sich selbst und nicht der Meinung und Erwartung anderer?
- Geben Sie gerne Orientierung?
- Sind Sie ein Leuchtturm, der sein Licht sendet, während andere Lichter bereits ausgegangen sind?
- Haben Sie kein Problem mit dem Faktum, dass Sie als internes Prüforgan nicht „everybody`s darling“ sein können?
- Sind Sie jemand, der gerne „hinter den Vorhang“ schaut und kein Problem damit hat, die Realität so wie sie ist zu sehen, aufzuzeigen und zu präsentieren?
- Können Sie mit Widerstand umgehen (insbesondere in Schlussbesprechungen, Veränderungsprozessen)?
- Führen Sie die Prüfungsund Beratungstätigkeit mit Begeisterung aus?
- Haben Sie Durchhaltevermögen?

lässt sich mittels einer Bewertungsmatrix die eigene Resilienz beurteilen. Würde in diesem Fall ein Großteil der Fragen mit „Ja“ beantwortet werden, würde dies auf einen starken und resilienten Charakter des Befragten hinweisen, der die Herausforderungen im Berufsfeld der Internen Revision gut meistern kann. Wenn der Großteil der Fragen mit „Nein“ beantwortet wurde, gibt es trotzdem eine gute Nachricht: **Resilienz ist erlernbar**.

## 5. Tipps und Möglichkeiten zur Erhaltung und Steigerung der eigenen Widerstandskraft

Nachdem gezeigt werden konnte, dass Resilienz für den Berufsstand der Internen Revision ein wesentliches Charakteristikum darstellt, ist das folgende Kapitel insbesondere auf den Berufsstand der Internen Revision abgestimmt, gilt aber natürlich auch für andere Berufsgruppen, welche sich mit persönlicher innerer Widerstandskraft beschäftigen wollen.

Die folgenden Ausführungen stellen Möglichkeiten, Sichtweisen und Ansatzpunkte dar, um Belastungen souverän standzuhalten. Aufgrund der Komplexität des Themas können allerdings hier nur Teilaspekte dargelegt werden. Im Rahmen des folgenden Kapitels werden unter anderem folgende zentrale Fragen beantwortet:

- Was macht den Menschen stark?
- Was gibt der Seele Halt?
- Kann man innere Stärke trainieren?
- Wie gewinnt man seine eigene Kraft und Ruhe wieder zurück?
- Wie kann man negativen Erlebnissen auch etwas Positives abgewinnen?
- Wie schafft man es, in einem schwierigen Umfeld die eigene Position nicht aufzugeben?

[30] Vgl. Maehrlein (2013), S. 54 f.

[31] Auszug; ausführliche Umfrageergebnisse sind dem Fachbuch „Resilienz – Widerstandskraft für prüfende Berufe“ zu entnehmen.

## 5.1. Die Energie-Balance

Zu Beginn gilt es sich nach Auffassung des Autors bewusst zu machen, dass Energie nicht unbegrenzt zur Verfügung steht. Es ist daher wichtig, zu wissen, wohin man seine persönliche Energie „verteilt" und welche Ergebnisse damit verbunden sind. Hilfreich ist das Bild von zehn Behältnissen voller Energie, die täglich zur Verfügung stehen. Wie und wohin verteilen Sie diese? Des Weiteren sollte man daran denken, dass man die persönlichen Energiespeicher auch wieder befüllen muss (z. B. ausreichend Schlaf, Sport, Bewegung, Partnerschaft etc.), um Energie wieder zur Verfügung zu haben. Ein hilfreiches Bild stellt das (Energie)-Konto im wirtschaftlichen bzw. buchhalterischen Sinn dar. „Was zahlen Sie auf dieses Konto ein, welche Abhebungen tätigen Sie?" Ergänzend dazu gilt es, sich bewusst zu machen, welche Prioritäten man persönlich setzt, für welche Themen man Energie aufwendet, was man daher als wichtig erachtet und was nicht.

> Psychische Widerstandskraft beginnt mit der Bewusstmachung der individuellen Realität und persönlicher Glaubenssätze, die zum Teil antrainiert sind, um uns klein zu machen.

Der Autor hat folgende Fragen zum Einstieg in dieses Thema entwickelt:

- Hält sich Ihr Energieaufwand die Waage mit den von Ihnen gewünschten Ergebnissen?
- Wo erntet man mehr als man an Energie aufwendet?
- Wo weniger?

Reduzieren Sie daher Tätigkeiten, die Ihnen nichts einbringen. Wenn man permanent mehr Energie aufwendet, die individuelle Energiebalance somit im Ungleichgewicht ist, sollte man nach Meinung des Autors seine persönlichen Prozesse analysieren und eine Änderung herbeiführen. Falls dieses (Miss)-Verhältnis nämlich auf Dauer unausgewogen ist, läuft man Gefahr auszubrennen – „verlorene, vertrödelte Zeit ist versäumtes Leben."[32]

Egli (2009) erklärt in seinem Buch „Das LoLa Prinzip",[33] dass Kampf nur zur Verkrampfung führt, man verliert dabei Energie. Daher ist es auch ratsam, Hass, Ärger und Feindschaft loszulassen.[34] Jaffe et al (2013) vertiefen diese Thematik und erklären in ihrem Buch „Deine Energie in Aktion, Energy Balancing fürs tägliche Leben", detaillierte Aspekte der Energie, welche im Fachbuch kurz beschrieben werden.[35]

### Bewusstmachen der Energie-Blockaden

Nach Auffassung des Autors ist es wichtig, jene Dinge zu enttarnen, welche uns Lebensenergie rauben und unser Leben blockieren. Greisinger (2001) spricht in diesem Zusammenhang von der **Rückeroberung unseres seelischen Lebensraumes**.[36] Psychische Widerstandskraft beginnt mit der Bewusstmachung der persönlichen individuellen Realität und persönlicher individueller Glaubenssätze, die zum Teil antrainiert sind, um uns klein zu machen, damit andere Energie und Macht über uns haben.[37]

*„Es geht nicht darum, was die anderen sagen, welche Nachrede wir ernten; es geht einzig und allein darum, wie es Dir selber ergeht, wie Du Dich fühlst mit dem, was Du tust, bzw. dem, was Du Dir nicht zu tun erlaubst."*[38]

Psychische Widerstandskraft beginnt daher mit einer Reise zu uns selbst. In einem ersten Schritt geht es darum, sich bewusst zu machen, was wir nicht alles tun, d. h. also Energie investieren, um einer Erwartung oder einem Idealbild zu entsprechen. Greisinger (2001) beschreibt ausführlich in seinem

[32] Greisinger (2001), S. 171.
[33] LO steht für Loslassen, L für Liebe und A für Aktion=Reaktion, Vgl. Egli (2009), S. 101 ff.
[34] Vgl. Egli (2009), S. 101 ff.
[35] Vgl. Jaffe et al (2013), S. 8 f.
[36] Vgl. Greisinger (2001), S. 3.
[37] Vgl. Greisinger (2001), S. 28 f.
[38] Greisinger (2001), S. 13.

Buch „Entfesseltes ICH“ wie es möglich ist, der „Scheinwelt“ zu entfliehen und wieder in die „SEIN-Welt“ zurückzukehren. [39]

Auf diesem Weg sind etwaige Persönlichkeitseinschränkungen zu überwinden: „*Ängste […], Selbstentfremdung, Anpassung an die Vorstellung anderer […] selbstgeschaffene Grenzen, Stress, Reizüberflutung und Leistungsdruck, Bequemlichkeit, Kompromissstreben […] Statusdenken und vieles mehr*“. [40]

„*Aus diesen […] Elementen ist jenes Korsett gefertigt, das unseren Atem und unsere Bewegungsfreiheit einschränkt.*“[41] „*Wir rennen dem Glück und dem Erfolg nach, hecheln nach Frieden und Freude und sind blind für das wundervolle Leben im Hier und Jetzt.*“[42]

**Stellen Sie sich daher folgende Frage: Welche Energieräuber wohnen in Ihnen, nähren Sie (bewusst oder unbewusst) bzw. haben Sie selbst geschaffen?**

Nach Egli (2009) verliert man Energie in folgenden Fällen:[43]

- Nicht-Akzeptanz des IST-Zustandes
- Verurteilung
- Angst vor Misserfolg
- Vergleichen
- Hegen von negativen Gefühlen
- Kampf
- Hegen von Schuldgefühlen

Wenn Sie die oben angeführten Punkte vermeiden bzw. gar nicht erst aufkommen lassen, wird ihre Energiebalance nicht negativ beeinträchtigt. Ein Weg, um die Energien auch zu behalten, ist,

„Nein“ sagen zu können, um Energien, welche uns schaden, nicht aufzunehmen.[44] Nach Auffassung des Autors kann die Zufuhr und die Erhaltung von Energie und somit eine Erhöhung der Resilienz durch fernöstliche Techniken, wie z. B. Qi Gong, Yoga oder Kung Fu, unterstützt und gefördert werden. Interessant sind in diesem Zusammenhang der chinesische Schriftzug und die Übersetzung von Kung Fu:

„*Der allmähliche Aufbau der eigenen Energie durch tägliches Bemühen, welcher zu der reifen Kraft und der spirituellen Entwicklung eines Meisters führt.*“[45]

## 5.2. Mentale Stärke

Wie meistert man Extremsituationen? Antwort: Indem man lernt, seinen Geist zu beherrschen. Grundsätzlich gibt es nach Auffassung des Autors zwei Möglichkeiten: Entweder man lässt im Vorhinein die Situation so im Geist ablaufen, wie sie sein soll (das ist die bessere Alternative) oder man „um-erlebt“ die Situation im Nachhinein, wie man sie gerne erlebt hätte, wenn sie anders gelaufen ist als geplant. Fasching (1997) nennt das Arbeiten im mentalen Bereich „Feuer im Kopf“. In seinem gleichlautenden Buch beschreibt Fasching (1997) auf faszinierende Art, wie er zum Sieger des Race across America, eines der härtesten Radrennen und sportliche Wettbewerbe überhaupt, wurde.[46]

[39] Vgl. Greisinger (2001), S. 28.
[40] Greisinger (2001), S. 28. 41 Greisinger (2001), S. 28.
[42] Greisinger (2001),S. 34.
[43] Vgl. Egli (2009), S. 142 ff.
[44] Vgl. Egli (2009), S. 135.
[45] Danaos (2006), S. 24.
[46] Vgl. Fasching (1997), S. 75 f.

Als Grundvoraussetzung für psychische Stärke werden folgende Fähigkeiten genannt:[47]

- die Kenntnis über den eigenen Geist
- das Erkennen von Zusammenhängen
- die Bedeutung bzw. das Spiegelbild im Unterbewusstsein
- realistische Selbsteinschätzung
- Durchhaltevermögen
- kein Selbst-Belügen (bzw. kein Schönreden)

Ein Weg, um die Energien auch zu behalten, ist, „Nein" sagen zu können, um Energien, welche uns schaden, nicht aufzunehmen.

Des Weiteren muss man energieraubende „Programme" sofort verlassen sowie positiv denken und die Lehren bei einem Misserfolg ziehen. Eine eiserne Disziplin ist unumgänglich, d. h. die konsequente Verfolgung eines Zieles.[48] Greisinger (2001) beschreibt, dass man seine Freiheit und Verbundenheit mit unserem inneren Gespür wiedererlangen soll.[49] Die Kraft für persönlichen Erfolg kommt von innen.[50] Man soll sich zu seinem wahren SELBST, zu seiner persönlichen Marke bekennen und darauf vertrauen, dass sich auf Dauer Echtes und Wahrhaftes durchsetzt.[51]

*„Das Zauberwort […] ist die Authentizität: stimmig und echt sich selbst, seinen Talenten, Gefühlen, Überzeugungen treu zu bleiben."*[52] *„Die Menschen müssen[...] wieder lernen, freudig in das einzutauchen, was sie gerade tun."*[53]

Murphy (1996) geht in diesem Zusammenhang auf die Macht des Unterbewusstseins ein. Falls man sich selbst bzw. unbewusst falsch „programmiert", wird man nicht voranschreiten können und auf der Stelle treten.[54]

*„Geist und Körper müssen eins werden, der innere Schweinehund darf gar nicht aufkommen. Wer ihn pflegt und dann versucht, gegen ihn anzukämpfen, der hat schon verloren."*[55]

## 6. Resümee/Fazit

Im Artikel wurde versucht darzustellen, dass Resilienz eine notwendige Kernkompetenz für alle in der Internen Revision tätigen Personen ist. Demnach ist es sehr wichtig, dass Revisoren eine hohe seelische Widerstandskraft aufweisen, um den Berufsalltag meistern zu können und nicht an den Konflikten und Widerständen zu zerbrechen. Resilienz in der Internen Revision ist nicht nur für das Individuum in der Internen Revision von großem Vorteil, sondern vielmehr für das gesamte Revisionsteam. Eine hohe Resilienz der Mitarbeiter führt dazu, dass sowohl Menschen als auch Teams und Unternehmen herausfordernde Situationen und Krisen auf eine bessere Weise bewältigen und aus solchen Situationen auch Nutzen bzw. Lerneffekte ziehen können.

Aus diesem Grund ist es für Leiter der Internen Revision von großem Vorteil, resiliente Mitarbeiter für das Revisionsteam aufzubauen, um auch langfristig erfolgreich zu sein. Kriterien, die laut den Befragten aus der Umfrage mit resilienten Personen assoziiert werden können, sind vor allem:

[47] Vgl. Fasching (1997), S. 75 f.
[48] Vgl. Fasching (1997), S. 75 f.
[49] Vgl. Greisinger (2001), S. 54.
[50] Vgl. Kahn (2008), S. 24.
[51] Vgl. Greisinger (2001), S. 93.
[52] Greisinger (2001), S. 97.
[53] Greisinger (2001), S. 170.
[54] Vgl. Murphy (1996), S. 19.
[55] Fasching (1997), S. 26.

- Akzeptanz von Situationen
- Lösungsorientierung
- Verlassen der Opferrolle
- Übernahme von Verantwortung für das eigene Tun und Handeln

Da Resilienz jedoch als erlernbar gilt und diese Kriterien somit nicht zwingend angeboren sein müssen, wird es in Zukunft wichtig sein, dass bei Fortbildungen bzw. Coachings auf diese Faktoren hingewiesen wird und somit die Resilienz der Teilnehmer aufgebaut bzw. gestärkt wird. Aufgrund der mangelnden Seminarangebote zu diesem Thema ist es zukünftig sinnvoll, Seminare zum Themenbereich „Resilienz" für die Interne Revision in das Weiterbildungsprogramm aufzunehmen.

Die Ergebnisse der empirischen Untersuchung zeigten auf, dass für einen Großteil der Befragten das Kriterium „Energie-Balance" sehr wichtig ist. Einen hohen Stellenwert nehmen dabei „Energie auftanken", „abschalten", „sich bewusst Zeit für sich nehmen" ein. Daher ist es für Interne Revisoren sehr wichtig, sich nach energieraubenden Tätigkeiten wie zum Beispiel nach Schlussbesprechungen zu erholen und Kraft zu tanken. Für den Alltag bedeutet dies, dass man die Schlüsselfaktoren der Resilienz kennen und diese nutzbringend einsetzen soll.

## 7. Literaturverzeichnis

Borgert, S. (2013): Resilienz im Projektmanagement, Wiesbaden, 2013.

Buchholz, U./Knorre, S. (2012): Interne Unternehmenskommunikation in resilienten Organisationen, Berlin, Heidelberg, 2012.

Danaos, K. (2006): NEI Kung: Die innere Kraft entwickeln, Burgrain, 2006.

Egli, R. (2009): Das Lola Prinzip, 38. Aufl., Oetwil a. d. L., 2009.

Eulerich, M./van Uum, C. (2014): Die Interne Revision als Management Training Ground. Chancen und Herausforderungen bei der Weiterentwicklung von Führungskräfte., In: ZIR 3/2014, S. 132–138.

Fasching, W. (1997): Feuer im Kopf: Race across America, Salzburg, 1997.

Greisinger, M. (2001): Entfesseltes ICH, Loslassen-leben-sein, 4. Aufl., Allentsteig, 2001.

Heller, J. (2013): ‚Resilienz – 7 Schlüssel für mehr innere Stärke , München, 2013.

Jaffe, Ketal. (2013): Deine Energie in Aktion, Energy Balancing fürs tägliche Leben, Hanau, 2013.

Kahn, O. (2008): ICH. Erfolg kommt von innen, 4. Aufl., München, 2008.

Klein, S. (2011): Resilienz im Führungscoaching, in: Birgmeier (Hrsg): Coachingwissen, Wiesbaden 2011, S. 358–363.

Lambert, K.G. (2013): Lehrmeister Ratte, Berlin, Heidelberg, 2013.

Maehrlein, K. (2013): Die Bambus Strategie. Den täglichen Druck mit Resilienz meistern, 2. Aufl., Offenbach, 2013.

Mairhofer, H. (2014): Resilienz – Widerstandskraft für prüfende Berufe, Eigenverlag, Linz, 2014. Das Buch ist unter http://resilienz.united-branding.com/ erhältlich.

Murphy, J. (1996): Die Macht Ihres Unterbewusstseins, 58. Aufl., Krezlingen, 1996.

Salcher, A. (2013): Der zerbrechliche Manager, in: Trend 02/2013, S. 78 f.

Wustmann, C. (2004): Resilienz: Widerstandsfähigkeit von Kindern in Tageseinrichtungen fördern, Weinheim und Basel, 2004.

Zander, M. (2009): Resilienz: Resilienzförderung, Seelische Widerstandsfähigkeit. In: Sozial Extra 11/12/2009. S. 12.

**Online Quellen:**

Österreichischer Bundesverband für Psychotherapie: Information zur Burnout-Symptomatik, URL: http://www.psychotherapie.at/sites/default/files/files/ patientinnen/Psychische-Erkrankungen-InfoblattBurnout.pdf
Wien, 2010

INSTITUT FÜR
INTERNE REVISION
ÖSTERREICH

AUSTRIA

2017

# Jahrbuch

**Impressum**
Institut für Interne Revision Österreich - IIA Austria
Schönbrunner Strasse 218 - 220
U4 Center, Stiege B, 3. OG
A - 1120 Wien

**www.internerevision.at**