Heft 36 | Dezember 2022 | 16. Jahrgang | ISSN 1864-6557

IT-GOVERNANCE

Fachzeitschrift des ISACA Germany Chapter e.V.

AUSZUG
AUS HEFT 36

Aufsichtliche Anforderungen an die IT kleiner und mittlerer Institute

ISACA
Germany Chapter

dpunkt.verlag | it-governance.dpunkt.de | isaca.de

Liebe Leserinnen und Leser,

auch wenn in diesen Tagen vor allem verschiedene gleichzeitig stattfindende Krisen das gesellschaftliche und wirtschaftliche Leben prägen, ist uns – zumindest punktuell – eine Rückkehr zur Normalität gelungen: So war es dem ISACA Germany Chapter möglich, im September den IT-GRC-Kongress nach zwei Jahren wieder in Präsenz durchzuführen. Ganz grundsätzlich hat es uns gefreut, dass sich die Community treffen konnte, und auch wir Herausgeber haben Gespräche mit Autoren und ISACA-Mitgliedern geführt, über neue Themen diskutiert und es sind Ideen für zukünftige Beiträge entstanden. Es wäre schön, wenn das in Zukunft wieder die Regel und nicht die Ausnahme darstellen würde! In der Rubrik »Veranstaltungen« in diesem Heft finden Sie einen Beitrag zum diesjährigen Kongress und zur Mitgliederversammlung.

Martin Fröhlich

Matthias Goeken

Michael Klotz

Ingo Struckmeyer

Marc Weber

Den Anfang machen jedoch zwei Fachthemen: Alexander Koderman und Mirko Prehn stellen Graphdatenbanken als Werkzeuge zur Repräsentation von Standards und Normen vor und zeigen – neben technischen Aspekten – mögliche Vorteile deren Anwendung. Martin Fröhlich erläutert Relevanz und Inhalte der BAIT (Bankaufsichtliche Anforderungen an die IT) und MaRisk (Mindestanforderungen an das Risikomanagement) mit Blick auf kleinere und mittlere Institute und stellt darüber hinaus dar, wie diese umgesetzt und nachhaltig erfüllt werden können. Hierfür skizziert er ein projektmäßiges Vorgehen.

In der Rubrik »Standards« präsentiert Markus Gaulke den ISACA-Leitfaden »COBIT® Focus Area: DevOps« und beschreibt, wie COBIT im Zusammenhang mit diesem relativ neuen Ansatz der Softwareentwicklung und -bereitstellung zum Einsatz kommen kann bzw. wie sich COBIT hierfür adaptieren lässt.

Kilian Trautmann, Christian Ewel und Marc Weber thematisieren in der Rubrik »Aus den ISACA-Fachgruppen« die Prüfung von Smart Contracts als eine Maßnahme zur Förderung von Digital Trust und stellen damit ein erstes Ergebnis der gerade neu gegründeten Fachgruppe »Digital Trust« vor.

Das Heft schließt mit der Besprechung von zwei aktuellen Büchern – eines davon aus der ISACA-Buchreihe.

Wir wünschen Ihnen eine interessante Lektüre und hoffen, dass das Heft – wie auch die erfolgreiche Konferenz im September – zum Wissensaustausch in der ISACA-Community beiträgt. In diesem Sinne freuen wir uns auch immer über Beiträge und Anregungen von Ihnen!

Wenn das Heft erscheint, ist das Ende von 2022 schon mehr oder weniger in Sicht! Wir wünschen Ihnen daher eine schöne Adventszeit und einen guten Ausklang des Jahres.

Ihre Herausgeber

Heft 36 | 2022

IT-GOVERNANCE

Fachzeitschrift des ISACA Germany Chapter e.V.

Inhalt

Fachthemen

3 **Der Einsatz von Graphdatenbanken in der Compliance-Automatisierung**
Alexander Koderman, Mirko Prehn

10 **Aufsichtliche Anforderungen an die IT kleiner und mittlerer Institute**
Martin Fröhlich

Rubriken

17 **Standards**
COBIT® Focus Area: DevOps
Markus Gaulke

25 **Veranstaltungen**
IT-GRC-Kongress 2022 des ISACA Germany Chapter

27 **Aus den ISACA-Fachgruppen**
Prüfung von Smart Contracts als Maßnahme zur Förderung von Digital Trust

32 **Buchbesprechung**

35 **Inserenten**

35 **Vorschau**

36 **Impressum**

Dieser Ausgabe der IT-Governance liegt eine Beilage »Grundlagen der IT-Revision für den Einstieg in die Praxis« (2., akt. u. überarb. Aufl. Sept. 2022) des ISACA Germany Chapter e. V. bei.

Aufsichtliche Anforderungen an die IT kleiner und mittlerer Institute

Martin Fröhlich

Die BaFin hat mit den MaRisk und den BAIT umfangreiche Anforderungen an die Geschäftsorganisation einer Bank und deren IT formuliert, die kleine und mittlere Finanzinstitute vor besondere Herausforderungen bei der Umsetzung stellt. Dieser Beitrag erläutert die aufsichtsrechtlichen Anforderungen an die IT und stellt einen Projektansatz zur Umsetzung aufsichtlicher Anforderungen in kleinen und mittleren Instituten zur Diskussion. Zudem wird untersucht, ob der für KMU und Behörden entwickelte Standard CISIS12 die aufsichtlichen Anforderungen an einen »gängigen Standard« für Informationssicherheit erfüllen kann.

1 Aufsichtsrechtliche Anforderungen an die IT

§ 25a Abs. 1 Kreditwesengesetz (KWG) verlangt von allen Instituten[1] eine ordnungsgemäße Geschäftsorganisation, die die Beachtung gesetzlicher Bestimmungen und betriebswirtschaftlicher Notwendigkeiten gewährleistet. Ausdruck dieser Geschäftsorganisation ist ein angemessenes und funktionsfähiges Risikomanagementsystem, das u.a. die Einrichtung eines internen Kontrollsystems, eine angemessenen personelle und technisch-organisatorische Ausstattung und die Festlegung eines Notfallmanagements erforderlich macht.

Die Regelungen des § 25a Abs. 1 KWG beziehen sich auf alle Institute, wobei das Institut die konkrete Ausgestaltung des Risikomanagements abhängig von Art, Umfang und Risikogehalt der Geschäftstätigkeit selbst bestimmen muss. Somit betrifft § 25a Abs. 1 KWG nicht nur große Institute oder Institute in Finanzverbünden, sondern auch Leasinggesellschaften, Spezialfinanzierer, kleinere Vermögensverwalter oder auch Wohnungsbaugenossenschaften mit Sparverkehr.

Zur Interpretation der unbestimmten Rechtsbegriffe in § 25a Abs. 1 KWG (z.B. ordnungsgemäße Geschäftsorganisation, angemessene technisch-organisatorische Ausstattung) hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) die Mindestanforderungen an das Risikomanagement (MaRisk) [BaFin 2021c] und die Bankaufsichtlichen Anforderungen an die IT (BAIT) [BaFin 2021b] veröffentlicht. Beide Rundschreiben sind sogenannte norminterpretierende Verwaltungsvorschriften, die die Auslegung und Anwendung von Rechtsnormen insbesondere bei Vorliegen unbestimmter Rechtsbegriffe beinhalten. Mit den MaRisk hat die Aufsicht festgelegt, wie § 25a KWG in der aufsichtlichen Praxis angewendet wird [BaFin 2012]. Gleiches gilt auch für die BAIT.

Verwaltungsvorschriften betreffen zunächst nur die relevanten Behörden und haben keine rechtliche Bindung außerhalb des Adressatenkreises. Die faktische Bindungswirkung für Institute ergibt sich allerdings aus dem Umstand, dass MaRisk und BAIT bei aufsichtlichen Prüfungen nach § 44 KWG Beurteilungsmaßstab für die ordnungsgemäße Geschäftsorganisation gemäß § 25a Abs. 1 KWG sind. Wie aus der nachfolgenden Tabelle 1 ersichtlich, haben Prüfungen zu § 25a Abs. 1 KWG weiterhin den größten Anteil an den aufsichtlichen Sonderprüfungen:

Art der Prüfung	2020	2019	2018	2017
§ 25a Abs. 1 KWG	63	133	130	166
Andere Sonderprüfungen	16	28	23	33
Gesamtzahl	79	161	153	199

Tab. 1: Zahl der Sonderprüfungen [BaFin 2021d]

Die erste Novelle der MaRisk wurde im Jahre 2005 veröffentlicht. Ziel war die Interpretation des § 25a Abs. 1 KWG in Form eines prinzipienorientierten Ansatzes. Dies bedeutet, dass auf eine konkrete Festlegung von Maßnahmen zugunsten eines Rahmenwerkes verzichtet wurde, was den Instituten hinreichende Gestaltungsspielräume abhängig von der Größe des Instituts, Art, Umfang und Komplexität sowie dem Risikogehalt der Geschäftstätigkeit ermöglicht [BaFin 2012]. Mittlerweile liegen die MaRisk in der 6. Novelle mit Stand August 2021 vor. Zeitgleich mit der Veröffentlichung dieser 6. Novelle hat die BaFin die neue Fassung der BAIT veröffentlicht. Die BAIT wurden erstmals 2017 als Reaktion auf die zunehmende Bedeutung von Informationssicherheit und Risikomanagement in der IT der Finanzinstitute veröffentlicht und seitdem weiterentwickelt, um u.a. den Leitlinien der Europäischen Bankenaufsicht (EBA) Rechnung zu tragen.

Bei der Interpretation aufsichtsrechtlicher Anforderungen an die IT müssen § 25a Abs. 1 KWG, die MaRisk und die BAIT in einem gemeinsamen Kontext gesehen und interpretiert werden. Dies sei anhand des Beispiels IT-Strategie in der nachfolgenden Abbildung 1 erläutert.

1 Die unter das KWG fallenden Institute bestimmen sich nach § 1 KWG Abs. 1b als Kreditinstitute und Finanzdienstleistungsinstitute.

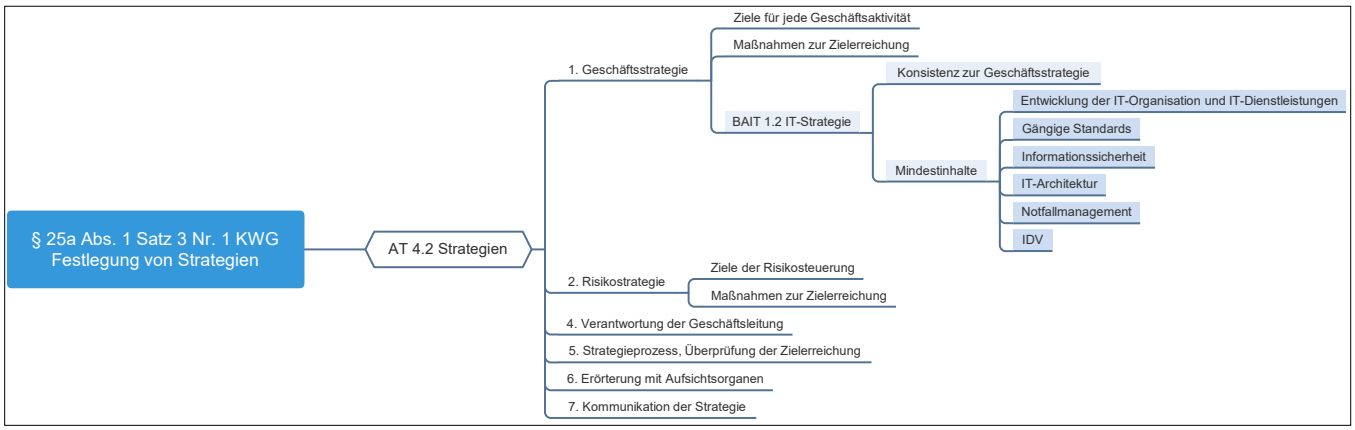


Abb. 1: Aufsichtsrechtliche Anforderungen an Strategien

§ 25a Abs. 1 Satz 3 Nr. 1 KWG verpflichtet Institute zur Festlegung von Geschäftsstrategien einschließlich einer Risikostrategie sowie zur Einrichtung von Prozessen zur Planung, Umsetzung, Beurteilung und Anpassung von Strategien. Diese Gesetzesvorgabe wird durch MaRisk AT 4.2 konkretisiert, z.B. durch inhaltliche Vorgaben für die Geschäfts- und Risikostrategie, den Strategieprozess und die Kommunikation der Strategien sowohl innerhalb des Unternehmens als auch in die Gremien. Die BAIT ergänzen diese allgemeinen Anforderungen an Strategien um spezielle Mindestinhalte einer IT-Strategie und die Forderung nach konsistenter Ableitung der IT-Strategie aus der Geschäftsstrategie. Eine alleinige Betrachtung der BAIT würde daher den aufsichtlichen Anforderungen an die IT-Strategie nicht gerecht; auch die IT-Strategie muss im Rahmen eines definierten Prozesses erstellt, geändert, deren Zielerreichung gesteuert und überwacht werden und ebenfalls an Mitarbeiter und die Gremien kommuniziert werden.

Noch deutlicher wird die führende Bedeutung der MaRisk und die nachgeordnete Rolle der BAIT beim Thema der Auslagerung. Die allgemeinen Regelungen in § 25b KWG zur Auslagerung von Aktivitäten und Prozessen werden durch AT 9 der MaRisk in insgesamt 15 Textziffern konkretisiert (vgl. Abb. 2).

Die BAIT konkretisieren lediglich einzelne Textziffern der MaRisk um spezielle Ausprägungen bei dem sogenannten sonstigen Fremdbezug von IT-Dienstleistungen. Hier gab es in der Vergangenheit immer wieder Diskussionen in der Praxis, ob und unter welchen Bedingungen etwa Programmiertätigkeiten als Auslagerung oder sonstiger Fremdbezug zu bewerten seien.

Die Beispiele machen deutlich, dass die Abdeckung aufsichtsrechtlicher Anforderungen stets nur unter gemeinsamer Betrachtung der Regelungsinhalte aus den MaRisk und der BAIT beurteilt werden kann. Gleichwohl sind auch die MaRisk und die BAIT nicht hinreichend konkret, um in der Praxis IT-Prozesse auszuprägen oder konkrete Vorgaben für die Umsetzung von Informationssicherheit in einem Institut zu machen. Hierzu verweisen die MaRisk in AT 7.2 auf die Verwendung gängiger Standards bei der Ausgestaltung von IT-Systemen und IT-Prozessen.

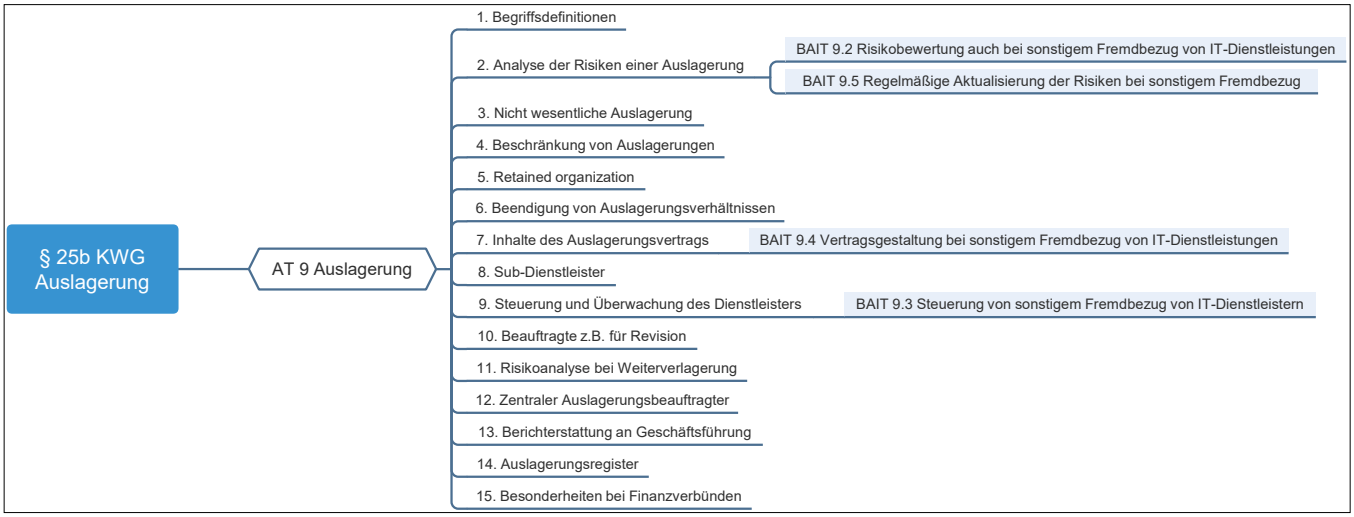


Abb. 2: Aufsichtliche Anforderungen an Auslagerung

2 Gängige Standards zur Gestaltung von IT-Systemen und Prozessen

In der Literatur wird als Standard die Beschreibung der Art und Weise bezeichnet, wie eine Aufgabe ausgeführt, ein Problem gelöst bzw. eine Technik oder ein Instrument gehandhabt wird. Ein Standard muss von einer anerkannten Organisation erstellt worden sein und die Regelungen von seinem Adressatenkreis akzeptiert und angewendet werden [Klotz 2020, S. 872]. In ähnlicher Form bezeichnet die DIN EN 45020 eine Norm als ein »Dokument, das mit Konsens erstellt und von einer anerkannten Institution angenommen wurde und das für die allgemeine und wiederkehrende Anwendung Regeln, Leitlinien oder Merkmale für Tätigkeiten oder deren Ergebnisse festlegt, wobei ein optimaler Ordnungsgrad in einem gegebenen Zusammenhang angestrebt wird« [DIN EN 45020, S. 15].

Das Wort »gängig« wird in den MaRisk bzw. den BAIT nicht weiter definiert; im Sprachgebrauch wird gängig als allgemein üblich, gebräuchlich oder in Mode interpretiert. In den MaRisk werden die Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder die ISO-Normen als Ausprägungen »gängiger Standards« genannt; Bretz nennt darüber hinaus noch ITIL, COBIT und die Rechnungslegungsstandards des Instituts der Wirtschaftsprüfer [Bretz 2012, S. 11 f.].

Mit dem Wort »Standard« will die Aufsicht weder Standardsoftware [BaFin 2021a, AT 7.2, Tz. 2] noch einen oder mehrere Standards präjudizieren. Gleichfalls darf die Forderung nach Verwendung gängiger Standards nicht als Zwang verstanden werden, einen oder mehrere Standards umfassend oder sogar vollständig einzuführen. Sofern nicht begleitend etwa eine Zertifizierung nach einem bestimmten Standard (z. B. ISO/IEC 27001) geplant ist, können die in einem Standard zur Lösung einer bestimmten Aufgabe beschriebenen Maßnahmen helfen, Regelungslücken in den MaRisk bzw. den BAIT zu schließen. Maßgabe für die Ausprägung von Maßnahmen oder Prozessen ist stets die institutsindividuelle Risikosituation; jede Maßnahme muss in einem angemessenen Verhältnis zum dadurch vermiedenen Risiko (z. B. Ausfall einer Anwendung) stehen [Bretz 2012, S. 13].

3 Umsetzung aufsichtsrechtlicher Anforderungen

Zur Umsetzung aufsichtsrechtlicher Anforderungen hat sich nach den Erfahrungen des Autors folgendes Projektvorgehen bewährt (vgl. Abb. 3).

Am Beginn eines Projektes zur Umsetzung aufsichtsrechtlicher Anforderungen in kleineren und mittleren Instituten sollte zunächst eine Erhebung des Istzustands an Regelungen und Prozessen in der IT stehen. Dabei können standardisierte Fragebögen eingesetzt werden, um anhand von Befragungen der für die IT verantwortlichen Führungskräfte und der Durchsicht von Dokumenten einen ersten Status zum Grad der Erfüllung aufsichtsrechtlicher Anforderungen zu erhalten. Dabei geht es weniger um eine Würdigung von Dokumenten und Prozessen im Detail, sondern um die Identifizierung der aufsichtsrechtlich relevanten Themen mit dem größten Handlungsbedarf.

In den Ergebnissen dieser Statusaufnahme sollte der Handlungsbedarf mit einer Priorisierung festgelegt werden. Aufsichtliche Themen mit hoher Relevanz und ggf. geringem Umsetzungsstand (typische Beispiele sind etwa unzureichende oder fehlende Berechtigungskonzepte) werden dabei mit höherer Priorität versehen (Quick Wins).

Bevor einzelne Themengebiete der MaRisk bzw. der BAIT näher beleuchtet werden, ist zunächst der Stand der in Abschnitt 3 (Informationsrisikomanagement) der BAIT erläuterten Bausteine zu erheben, die die Grundlage für die Gestaltung einer aufsichtsrechtlich angemessenen Geschäfts- bzw. IT-Organisation bilden:

1. Dokumentation des Informationsverbunds (BAIT Tz. 3.3)
2. Festlegung der zu steuernden und zu überwachenden Risiken (BAIT Tz. 3.2)
3. Durchführung einer Schutzbedarfsanalyse (BAIT Tz. 3.4 und 3.5)
4. Festlegung von (risikoinduzierten) Sollmaßnahmen (BAIT Tz. 3.6)
5. Vergleich zwischen Soll- und Istmaßnahmen (Gap-Analyse) (BAIT Tz. 3.7)

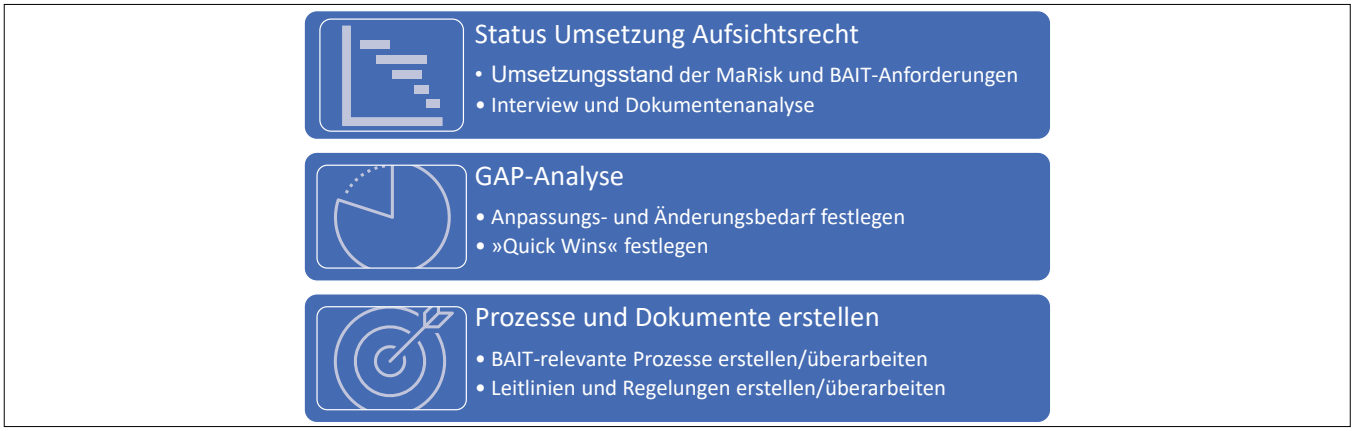


Abb. 3: Projektvorgehen zur Umsetzung aufsichtlicher Anforderungen

Ad 1.) Dokumentation des Informationsverbunds
Ausgangspunkt aller Risikoüberlegungen ist eine vollständige Dokumentation aller Elemente der IT-Systeme eines Instituts einschließlich u.a. Gebäude, Hardware, Software, Geschäftsprozesse, interne Schnittstellen und Schnittstellen zu Dienstleistern. Hilfestellung bei der Festlegung des Informationsverbunds und dessen grafischer Aufbereitung gibt etwa das BSI in seinem »Onlinekurs IT-Grundschutz«[2].

Ad 2.) Risikoermittlung und -bewertung
Sowohl die MaRisk als auch die BAIT betonen die Erhebung, Bewertung und die Reaktion auf Risiken als den zentralen Bestandteil einer ordnungsgemäßen Geschäftsorganisation. Relevante Risiken sind systematisch zu erfassen und in einem Risikoinventar abzubilden. Hierbei kann auf eine Vielzahl von Methoden und Werkzeugen zurückgegriffen werden (einen Überblick gibt [Knoll 2019, S. 184 ff.]).

Unterstützung bei der Zusammenstellung eines Risikoinventars geben Standards wie COBIT 2019 oder der daraus abgeleitete umfangreiche Risikokatalog einer Arbeitsgruppe der ISACA [ISACA 2013]. Das BSI unterscheidet in dem Grundschutz-Katalog 47 elementare Gefährdungen, die für die Risikoanalyse herangezogen werden können. Generell empfiehlt es sich, bei der Risikoerhebung auch auf Risikoindikatoren und Was-wäre-wenn-Szenarien zu setzen, um den Eintritt und die Auswirkungen von Risiken plastischer darstellen zu können.

Risikoindikatoren sind Messgrößen, die in einem inhaltlich-kausalen Zusammenhang zu den vorhandenen Risiken bzw. Risikoszenarien stehen. Beispielsweise korreliert das Risiko »Know-how-Verlust in der IT« mit den Risikoindikatoren »Kündigungsrate« oder »durchgeführte Schulungen der IT-Mitarbeiter«. Das Risiko einer Beeinträchtigung der Verfügbarkeit kann in Zusammenhang stehen mit einer erhöhten Anzahl an Störungen oder einer häufigen Beeinträchtigung der Netzverfügbarkeit.

In eine ähnliche Richtung gehen Was-wäre-wenn-Szenarien, bei denen der Eintritt von Risiken mit ihren potenziellen Auswirkungen verbunden werden. Beispiel hierfür wären: Welche Auswirkungen für die Geschäftsprozesse entstehen, wenn ein Störfall im Rechnerraum auftritt und die Server nicht mehr zur Verfügung stehen? Welche Auswirkungen hätte ein Remote-Zugriff eines Dienstleisters, dessen Aktivitäten nicht nachvollzogen werden können?

Zur Bewertung von Risiken stehen quantitative und qualitative Methoden zur Verfügung. Die bekannteste quantitative Methode ist die Bemessung der Auswirkungen eines Risikos aus der Multiplikation von Schadenspotenzial und Schadenshäufigkeit. Beides sind vielfach Schätzgrößen, die oft nur vermeintlich zu einem objektiven Wert führen, an dem sich die Kosten einer risikoreduzierenden Maßnahme messen lassen können. Daher werden in der Praxis qualitative Risikomatrizen verwendet, bei denen die Ausprägungen der Eintrittswahrscheinlichkeit (z.B. unwahrscheinlich, möglich, wahrscheinlich, sehr wahrscheinlich) in Matrixform mit den Ausprägungen des Schadenspotenzials (z.B. kein, Standard, erweitert, hoch) kombiniert werden (vgl. [Kühn 2012, S. 75 f.]) Aus dieser Matrix lassen sich die Risken ableiten, die einen erhöhten Handlungsbedarf erfordern bzw. aktiv gesteuert werden müssen.

Ad 3.) Schutzbedarfsanalyse
Über die Schutzbedarfsanalyse wird eine Beziehung zwischen einem Schutzbedarfsobjekt (z.B. Informationen, Infrastrukturen, Anwendungen), den potenziellen Risiken und dem daraus erwachsenden Schadenspotenzial, denen dieses Objekt ausgesetzt sein kann, und dem Grad der daraus abgeleiteten Schutzmaßnahmen hergestellt. Nach Tz. 3.4 der BAIT soll sich der Schutzbedarf an den Schutzzielen Integrität, Verfügbarkeit, Vertraulichkeit und Authentizität orientieren. In der Praxis werden häufig weitere qualitative und quantitative Auswirkungen eines potenziellen Schadens wie finanzielle Auswirkungen oder Reputationsschäden berücksichtigt.

Die Auswirkungen der potenziellen Schäden werden dann zu Schutzbedarfskategorien verdichtet. Der Hinweis auf früher gängige Schutzbedarfskategorien (niedrig, mittel, hoch, sehr hoch) wurde in den Erläuterungen der aktuellen BAIT gestrichen. Somit ist das Unternehmen bei der Abstufung der Schutzbedarfskategorien nicht an aufsichtsrechtliche Vorgaben gebunden.

In der Praxis beginnt die Schutzbedarfsanalyse zumeist mit einer Analyse der vom Unternehmen verarbeiteten Informationen/Daten im Hinblick auf die Schutzziele. Bei der weiteren Verdichtung wird das Prinzip der Vererbung angewandt, d.h., dass sich der Schutzbedarf einer Information immer nach dem höchsten Wert eines Schutzziels richtet. Wäre die Einstufung des potenziellen Schadens bei der Weitergabe von Mitarbeiterinformationen (Verlust der Integrität bzw. Authentizität) »hoch«, im Hinblick auf die Verfügbarkeit der Daten aber »normal«, würden Mitarbeiterdaten insgesamt mit der Schutzbedarfseinstufung »hoch« klassifiziert werden, was in Konsequenz entsprechend höhere Schutzmaßnahmen nach sich ziehen würde.

Dieses Prinzip der Vererbung setzt sich dann über die Daten verarbeitenden IT-Anwendungen, die Infrastruktur und die Gebäude fort. IT-Anwendungen erhalten den Schutzbedarf der Daten mit dem höchsten Schutzbedarf, Gleiches gilt auch für Server, auf denen u. U. unterschiedliche Anwendungen mit unterschiedlichem Schutzbedarf betrieben werden.

Ad 4.) Festlegung von Sollmaßnahmen
Für alle Elemente des Informationsverbunds sind Soll-Maßnahmen abhängig vom jeweiligen Schutzbedarf festzulegen. Hier bieten etwa der BSI IT-Grundschutz-Katalog oder die

2 Vgl. Lektion 3: Strukturanalyse, aufrufbar unter *https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_3_Strukturanalyse/Lektion_3_node.html (zuletzt aufgerufen am 29.09.2022).*

Norm »ISO/IEC 27002« umfangreiche Kataloge von technischen und organisatorischen Maßnahmen, die bei »hohem« oder »sehr hohem« Schutzbedarf beliebig erweitert werden können.

Für die Auswahl von Maßnahmen eher verwirrend ist die Einteilung des BSI nach Basisabsicherung, Standardabsicherung für den »normalen« Schutzbedarf und Anforderungen bei erhöhtem Schutzbedarf. Für kleine und mittlere Institute stellt sich bei Anwendung des BSI IT-Grundschutz-Katalogs die Frage, ob die Basisabsicherung für die Erfüllung der aufsichtlichen Anforderungen reicht (nach Ansicht des Autors eher nicht) oder ob die Standardanforderungen des BSI als Mindestmaß herangezogen werden müssen. Letzteres wird viele kleine und mittlere Institute technisch und organisatorisch überfordern und wird eventuell auch der spezifischen Risikolage nicht gerecht.

Ad 5.) Vergleich zwischen Soll- und Istmaßnahmen (Gap-Analyse)

Im letzten Schritt werden dem Sollmaßnahmenkatalog die bereits ergriffenen Istmaßnahmen gegenübergestellt und mittels einer GAP-Analyse der aktuelle Handlungsbedarf ermittelt. Die Feststellungen zu ausstehenden Maßnahmen bilden in Kombination mit den Ergebnissen der Statuserhebung in Bezug auf die aufsichtsrechtlichen Anforderungen das Arbeitsprogramm für ein anschließendes Projekt zur vollständigen Umsetzung aufsichtsrechtlicher Anforderungen.

4 Eignung von CISIS12 als gängiger Standard

Das IT-Grundschutz-Kompendium des BSI, COBIT 2019 oder die ISO 27002 sind für kleine und mittlere Institute mit großen Herausforderungen allein aufgrund der Komplexität und des Umfangs der in diesen Standards dargestellten Schutzmaßnahmen verbunden. In diesem Zusammenhang stellt sich die Frage, ob nicht auch andere als die genannten Standards geeignet sind, den Anforderungen der BAIT an die Verwendung »gängiger Standards« bei der Gestaltung von IT-Systemen und Prozessen zu genügen. Wie bereits oben ausgeführt, bezieht sich die Formulierung der BaFin nach Berücksichtigung gängiger Standards nicht auf die vollständige Implementierung eines Standards, sondern auf die flankierende Berücksichtigung beim Design und der Implementierung von IT-Systemen, Dokumenten und IT-Prozessen.

Diese Fragestellung wird im Folgenden am Beispiel des Standards CISIS12 untersucht. CISIS12 ist ein Synonym für »Compliance Informations-Sicherheitsmanagement in 12 Schritten« und wurde von dem privatwirtschaftlichen Verein IT-Sicherheitscluster e.V. mit Sitz in Regensburg entwickelt. CISIS12 besteht aus drei Dokumenten:

- Vorgehensmodell [IT-Sicherheitscluster 2021c]
- Handbuch [IT-Sicherheitscluster 2021b]
- Baustein- und Maßnahmenkatalog mit nahezu 1000 Seiten [IT-Sicherheitscluster 2021a]

Die Dokumente können gegen eine Schutzgebühr per Download bezogen werden, zudem werden Schulungen und Akkreditierungen für Berater und Auditoren angeboten. Zertifizierungen nach diesem Standard werden u.a. durch die Deutsche Gesellschaft zur Zertifizierung von Managementsystemen (DQS) und die datenschutz cert GmbH durchgeführt, die beide durch die Deutsche Akkreditierungsstelle GmbH (DAkkS) akkreditiert sind.

Das Vorgängermodell ISIS12 wurde insbesondere für die öffentliche Verwaltung und KMU entwickelt und mit CISIS12 um Compliance-Aspekte ergänzt. ISIS12 umfasst ein Vorgehensmodell mit 12 Schritten zur Einführung eines Informationssicherheits-Managementsystems (vgl. im Einzelnen [Dikau & Gebhardt 2021]). Nachfolgend soll die Auffassung des Autors begründet werden, dass CISIS12 wie BSI IT-Grundschutz oder ISO 27002 zur Konkretisierung aufsichtsrechtlicher Vorgaben an die IT herangezogen werden kann.

Die Vorgängerversion ISIS12 und CISIS12 unterscheiden sich in zwei Bereichen von den weiter oben genannten Standards und Normen, was einer Anerkennung als »gängiger Standard« zunächst im Wege stehen könnte. Zum einen handelt es sich bei dem Verfasser von CISIS12 um einen privatwirtschaftlichen Verein, der den Ansprüchen an einen allgemein anerkannten Standardsetter nicht genügen kann. Zum anderen basierte der Vorgänger ISIS12 noch auf einem generischen Risikomodell, d.h., die im Maßnahmenkatalog beschriebenen technischen und organisatorischen Maßnahmen differenzieren nicht zwischen unterschiedlichen Risiko- bzw. Schutzbedarfskategorien. In CISIS12 ist das Risikomanagement als expliziter Schritt 8 in die Vorgehensweise integriert und dieser Punkt somit obsolet. Gleichwohl gehen die vorgeschlagenen Bausteine und Maßnahmen noch von einem einheitlichen Risikoprofil aus, was etwa einem normalen Schutzbedarf entsprechen würde. Für Objekte mit einem höheren Schutzbedarf dürften die von CISIS12 vorgeschlagenen Maßnahmen nicht mehr ausreichend sein; hier muss dann auf weitere Standards zurückgegriffen werden. Hilfreich ist dabei der Verweis in den Maßnahmenkatalogen von CISIS12 auf die entsprechenden Kapitel in ISO/IEC 27001, BSI IT-Grundschutz und BSI IT-Grundschutz-Kompendium. Allerdings sollte der normale Schutzbedarf der Risikolage vieler kleiner und mittlerer Institute entsprechen.

Zum erstgenannten Thema einer Akzeptanz von CISIS12 als »gängigem Standard« kann neben der Verbreitung von CISIS12 in der öffentlichen Verwaltung (vgl. etwa den Erfahrungsbericht von [Kraus & Plehn 2020]) auch ein Gutachten eines Fraunhofer Instituts herangezogen werden, unter welchen Umständen ISIS12 zu vergleichbaren Ergebnissen wie der BSI IT-Grundschutz oder ISO 27001 führt.

Das Fraunhofer AISEC[3] hat im Jahre 2014 untersucht, ob ISIS12 (Vorgänger von CISIS12) geeignet ist, die Vorgaben des IT-Planungsrats[4] für das Informationssicherheitsmanagement in öffentlichen Verwaltungen zu erfüllen. In seinem Gutachten kommt das Fraunhofer AISEC zu dem Ergebnis, dass ISIS12 eine geeignete Vorgehensweise für eine sogenannte »Standardbehörde« darstellt, die durch folgende Eigenschaften charakterisiert werden kann [Fraunhofer 2014, S. II, 16]:

- Bis ca. 500 Mitarbeitern
- Homogene IT-Basisinfrastruktur
- Keine über öffentliche Netze ungeschützt angebundenen Außenstellen
- Überwiegend normaler Schutzbedarf
- Keine Hochverfügbarkeitsanforderungen
- Keine kritische Infrastruktur im Sinne der BSI-KritisV[5]

Diese Merkmale einer »Standardbehörde« dürften auch für viele kleine und mittlere Finanzinstitute zutreffend sein.

Zusammenfassend ist festzustellen, dass jedes Institut vor Anwendung des Standards die Eignung von CISIS12 vorab evaluieren und dokumentieren sollte. Bei einem positiven Ergebnis steht nach Ansicht des Autors der Verwendung von CISIS12 als »gängigem Standard« nichts im Wege.

Abschließend sei noch an einem Beispiel die Verwendung von CISIS12 bei der Erfüllung aufsichtsrechtlicher Anforderungen demonstriert.

Auf der linken Seite der Abbildung 4 sind die von Tz. 1.2 der BAIT genannten Mindestbestandteile einer IT-Strategie aufgeführt. Hierzu zählen auch die Ziele, Zuständigkeiten und die Einbindung der Informationssicherheit in die Organisation. Um diese generellen Vorgaben zu interpretieren, kann auf den Baustein B2.020 Sicherheitsziele und -strategien aus dem CISIS12-Maßnahmenkatalog zurückgegriffen werden. Dieser Baustein sieht die Initiierung eines Sicherheitsprozesses, die Festlegung der Sicherheitsstrategie, den Aufbau von Rahmenbedingungen für die Informationssicherheit und die entsprechenden Verpflichtungen für die Leitungsebene vor.

5 Fazit

Die gesetzlichen und aufsichtsrechtlichen Anforderungen an die Ausgestaltung einer angemessenen Geschäftsorganisation stellen die IT kleiner und mittlerer Institute vor große Herausforderungen. Mangelnde personelle Ressourcen, fehlendes Know-how im Kontext von Governance, Risk und Compliance sowie begrenzte finanzielle Mittel erschweren eine umfassende Befassung und Implementierung der nach MaRisk und BAIT verlangten Prozesse, Maßnahmen und Verfahren. Allerdings haben viele kleine und mittlere Institute eine Risikolage, die nicht mit der Risikolage großer Institute vergleichbar ist.

In diesem Beitrag wurden die Bausteine aufgezeigt, die auch kleine und mittlere Institute befähigen sollen, aufsichtsrechtlichen Anforderungen unter Beachtung ihrer individuellen Risikosituation und ihres Geschäftsmodells zu erfüllen. Bei der Analyse der aufsichtsrechtlichen Anforderungen ist stets der Kontext zwischen dem Gesetz (hier insbesondere § 25a Abs. 1 KWG) sowie den das Gesetz interpretierenden MaRisk und BAIT zu beachten.

Einem Projekt zur Umsetzung bzw. Vervollständigung aufsichtlicher Anforderungen sollte stets eine Statusanalyse vorausgehen. Vor der Befassung mit einzelnen Themenbereichen der BAIT müssen die grundlegenden Bausteine wie die Doku-

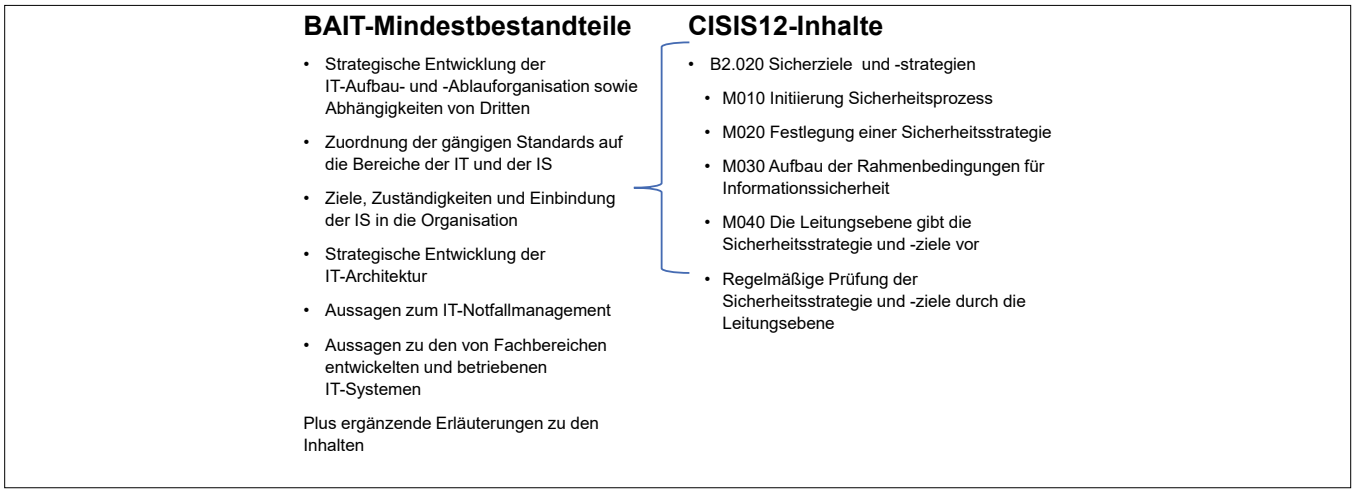


Abb. 4: Verwendung von CISIS12 für die Prozessgestaltung

3 Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC, Garching bei München.

4 Der IT-Planungsrat ist das zentrale politische Steuerungsgremium zwischen Bund und Ländern in Fragen der Informationstechnik und der Digitalisierung von Verwaltungsleistungen. Zu seinen Aufgaben gehört gemäß § 1 IT-Staatsvertrag auch die Festlegung übergreifender IT-Interoperabilitäts- und Sicherheitsstandards *(https://www.it-planungsrat.de/der-it-planungsrat/aufgaben)*.

5 Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) vom 22. April 2016 (BGBl. I S. 958), zuletzt geändert durch Art. 12 G vom 23.6.2021 I 1858.

mentation des Informationsverbunds, die Erhebung und Bewertung der zu steuernden Risiken sowie die Schutzbedarfsanalyse vorangestellt und abgeschlossen sein. Die Definition von Sollmaßnahmen, die GAP-Analyse zwischen Soll- und Istmaßnahmen und die Handlungsfelder aus der Statusanalyse bilden dann den Rahmen für das folgende Umsetzungsprojekt.

Dem Proportionalitätsgedanken werden die MaRisk und die BAIT gerecht, indem für die Ausgestaltung von IT-Prozessen keine konkreten Vorgaben gemacht werden, sondern auf »gängige Standards« verwiesen wird. Die benannten Standards wie BSI IT-Grundschutz oder ISO 27002 sind für kleine und mittlere Institute aber in der Handhabung zumeist zu umfangreich und zu komplex. Für den Standard CISIS12 wurde begründet, dass kleine und mittlere Institute nach einer bewussten Entscheidung die Bausteine und Maßnahmen bei der Entwicklung von IT-Systemen und Prozessen berücksichtigen können. Ausdrücklich nicht im Fokus stand dabei die Verwendung der Vorgehensweise von CISIS12 als Blaupause für die Einführung eines institutsweiten Informationssicherheitsmanagements.

Literatur

[BaFin 2012] *Bundesanstalt für Finanzdienstleistungsaufsicht:* Die Erfolgsgeschichte der MaRisk, veröffentlicht unter *https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2012/fa_bj_2012_08_marisk.html, Zugriff am 09.09.2022.*

[BaFin 2021a] *Bundesanstalt für Finanzdienstleistungsaufsicht:* Mindestanforderungen an das Risikomanagement – MaRisk, Erläuterungen zum Rundschreiben 10/2012 (BA), Stand 16.08.2021, veröffentlicht unter *https://www.bundesbank.de/resource/blob/600230/2e49e0b947cc6588689ab41561b1dde3/mL/2021-08-16-erlaeuterungen-data.pdf*, Zugriff am 09.09.2022.

[BaFin 2021b] *Bundesanstalt für Finanzdienstleistungsaufsicht:* Rundschreiben 10/2017 (BA) in der Fassung vom 16.08.2021 Bankaufsichtliche Anforderungen an die IT (BAIT), veröffentlicht unter *https://www.bundesbank.de/resource/blob/863264/6e6c87e41efd6d70b48b587ec899b89b/mL/2017-10-bait-2021-data.pdf*, Zugriff am 09.09.2022.

[BaFin 2021c] *Bundesanstalt für Finanzdienstleistungsaufsicht:* Rundschreiben 10/2021 (BA) Mindestanforderungen an das Risikomanagement – MaRisk, Stand 16.08.2021, geändert am 04.05.2022, veröffentlicht unter *https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2021/rs_1021_MaRisk_BA.html*, Zugriff am 09.09.2022.

[BaFin 2021d] *Bundesanstalt für Finanzdienstleistungsaufsicht:* Sonderprüfung (Stand 17.09.2021), veröffentlicht unter *https://www.bafin.de/DE/Aufsicht/BankenFinanzdienstleister/Massnahmen/Sonderpruefung/sonderpruefung_node.html*, Zugriff am 09.09.2022.

[Bretz 2012] *Bretz, J.:* Anforderungen der Aufsicht. In: Bretz et al.: Prüfung IT im Fokus von MaRisk und Bundesbank – Verstärkter IT-Fokus in Sonderprüfungen. Finanz Colloquium, Heidelberg, 2012, S. 1-50.

[Dikau & Gebhardt 2021] *Dikau, J.; Gebhardt, T.:* ISIS12 – das ISMS für KMU und Behörden. IT-Governance 15 (2021), 33, S. 18-24.

[DIN EN 45020] *DIN Deutsches Institut für Normung e. V.:* DIN EN 45020 – Normung und damit zusammenhängende Tätigkeiten – Allgemeine Begriffe (ISO/IEC Guide 2:2004), März 2007.

[Fraunhofer 2014] *Fraunhofer AISEC:* Gutachten zur Anwendbarkeit von ISIS12 in der öffentlichen Verwaltung (Stand 11.2014), veröffentlicht unter *https://www.it-planungsrat.de/fileadmin/beschluesse/2015/Beschluss2015-05_Gutachten_ISIS12.pdf*, Zugriff am 10.09.2022.

[ISACA 2013] *ISACA Germany Chapter e. V. (Hrsg.):* ISACA-Leitfaden – IT-Risikomanagement – leicht gemacht mit COBIT, veröffentlicht unter *https://www.isaca.de/sites/default/files/attachements/2012-isaca-leitfaden-it-risikomanagement_0.pdf*, Zugriff am 09.09.2022.

[IT-Sicherheitscluster 2021a] *IT-Sicherheitscluster e. V.:* CISIS12 (ISIS12 V3.0) Compliance und Informationssicherheit in 12 Schritten – Baustein- und Maßnahmenkatalog (Stand 06.2021), kostenpflichtig zu beziehen unter *https://cisis12.de/cisis12-dokumente/*, Zugriff am 10.09.2022.

[IT-Sicherheitscluster 2021b] *IT-Sicherheitscluster e. V.:* CISIS12 (ISIS12 V3.0) Compliance und Informationssicherheit in 12 Schritten – Handbuch (Stand 06.2021), kostenpflichtig zu beziehen unter *https://cisis12.de/cisis12-dokumente/*, Zugriff am 10.09.2022.

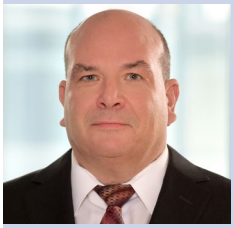
[IT-Sicherheitscluster 2021c] *IT-Sicherheitscluster e. V.:* CISIS12 (ISIS12 V3.0) Compliance und Informationssicherheit in 12 Schritten – Ein Vorgehensmodell zum strukturierten Aufbau und der Etablierung von Managementsystemen in beliebigen Organisationen (Stand 06.2021), kostenpflichtig zu beziehen unter *https://cisis12.de/cisis12-dokumente/*, Zugriff am 10.09.2022.

[Klotz 2020] *Klotz, M.:* IT-Compliance. In: Tiemeyer, E. (Hrsg.): Handbuch IT-Management – Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis. 7. Auflage, Hanser, München, 2020, S. 841-884.

[Knoll 2019] *Knoll, M.:* Praxisorientiertes IT-Risikomanagement – Konzeption, Implementierung und Überprüfung. 2., überarb. und erw. Auflage, dpunkt.verlag, Heidelberg, 2019.

[Kraus & Plehn 2020] *Kraus, C.; Plehn, H.:* ISIS 12 – In 12 Schritten zu mehr Informationssicherheit – Einführung des Informationssicherheitssystems ISIS 12 an der Otto-Friedrich-Universität Bamberg, veröffentlicht unter *https://www.uni-bamberg.de/fileadmin/rz/it-sicherheit/DFN-Konferenz_2020_ISIS12-Beitrag.pdf*, Zugriff am 09.09.2022.

[Kühn 2012] *Kühn, R.:* Ausgestaltung eines IT-Risikomanagement-Systems. In: Bretz et al.: Prüfung IT im Fokus von MaRisk und Bundesbank – Verstärkter IT-Fokus in Sonderprüfungen. Finanz Colloquium, Heidelberg, 2012, S. 51-118.



Martin Fröhlich

ist selbständiger IT-Berater und betreut Unternehmen rund um die Themen IT-Governance und IT-Compliance. Er verfügt über jahrzehntelange Erfahrung in der IT-Prüfung und IT-Beratung und war 20 Jahre Partner bei einer der Big4 mit Verantwortung für die Prüfung und Beratung von Finanzdienstleistungsunternehmen. Martin Fröhlich ist CISA, IT-Auditor[IDW], Mitglied des FAIT beim IDW und Vizepräsident des ISACA Germany Chapter e.V.

Dr. Martin Fröhlich
IT-Compliance Solutions
Kerkmannstr. 6
46535 Dinslaken
mf@martin-froehlich.de
https://martin-froehlich.de/

Vorschau* auf Heft 37 der »IT-Governance« (Juni 2023)

Für Heft 37 der »IT-Governance« sind Fach- und Praxisbeiträge zu den Themen Informationssicherheit und Risikomanagement, Prüfung digitaler Geschäftsmodelle, COBIT® for Small and Medium Enterprises using COBIT 2019 und Herausforderungen des Einsatzes von KI geplant sowie Artikel für die Rubriken »Zum Thema«, »Standards« und »IT-Prüfung« und Buchbesprechungen.

Wenn Sie zu einer der nächsten Ausgaben der »IT-Governance« einen Beitrag leisten möchten oder Anregungen haben, wenden Sie sich bitte an red-itgov@dpunkt.de.

Um sicherzugehen, dass Ihr Vorschlag bei entsprechender Eignung berücksichtigt werden kann, sollte dies bitte spätestens ca. 4 Monate vor Erscheinungstermin des jeweiligen Heftes erfolgen.

* Änderungen vorbehalten.

Dieser Ausgabe der IT-Governance liegt eine Beilage »Grundlagen der IT-Revision für den Einstieg in die Praxis« (2., akt. u. überarb. Aufl. Sept. 2022) des ISACA Germany Chapter e. V. bei.

Inserentenverzeichnis

adesso SE, Dortmund – Umschlaginnenseite hinten

ADVISORI FTC GmbH, Frankfurt am Main – 26

Audicon GmbH, Düsseldorf – 31

IBS Schreiber GmbH, Hamburg – 9

ISACA Germany Chapter e. V., Berlin – Umschlaginnenseite vorne

IT-Compliance Implementation GmbH, Essen – 33

Protiviti GmbH, Berlin – 35

SIGS DATACOM GmbH, Troisdorf – 36

Software Quality Experts GmbH, Linz – Umschlagaußenseite hinten

Versio.io, Berlin – 24

Anzeige

oop DIGITAL
software meets business

KONFERENZ FÜR SOFTWARE ARCHITEKTUR

06.–09. FEBRUAR 2023

PROGRAMM ONLINE

WWW.OOP-KONFERENZ.DE

Impressum

IT-Governance
Fachzeitschrift des Germany Chapter of »The Information Systems Audit and Control Association« e.V. (ISACA)

http://it-governance.dpunkt.de/

16. Jahrgang – Heft 36 – Dezember 2022
ISSN: 1864-6557
© dpunkt.verlag GmbH
Wieblinger Weg 17, 69123 Heidelberg
Tel. 06221 1483-0, Fax 06221 1483-99
www.dpunkt.de

Vertrieb:
Evelin Wilbert
Tel. 06221 1483-40, wilbert@dpunkt.de

Redaktion:
Christa Preisendanz,
red-itgov@dpunkt.de

Anzeigen:
Julia Griebel
Tel. 06221 1483-50, anzeigen@dpunkt.de

Satz + Herstellung: Frank Heidt
Copy-Editing: Ursula Zimpfer, Herrenberg
Umschlaggestaltung: Helmut Kraus, www.exclam.de
Druck: Wörmann PRODUCTION CONSULT, www.wp-consult.eu

Bezugsbedingungen (Stand 1.1.2023): Erscheinungsweise: 2 Ausgaben pro Jahr, Preis: €28,50 zzgl. Versandkosten (Inland: €4,00/Ausland: €8,10). GI-, OCG-, ASQF- und swissICT-Mitglieder erhalten eine Ermäßigung von 25%. Das Studenten-Abo kostet €18,00 zzgl. der Versandkosten (gegen Vorlage der Immatrikulationsbescheinigung). Das Einzelheft kostet €17,20 zzgl. Versandkosten.

Das Abonnement ist 8 Wochen vor Ablauf des Bezugszeitraums schriftlich kündbar.

Die Zeitschrift sowie alle in ihr enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Fotokopien für den persönlichen und sonstigen eigenen Gebrauch dürfen nur von einzelnen Beiträgen oder Teilen daraus als Einzelkopien hergestellt werden. Jede im Bereich eines gewerblichen Unternehmens hergestellte oder benützte Kopie dient gewerblichen Zwecken gemäß § 54 (2) UrhG und verpflichtet zur Gebührenzahlung an die VG WORT, Abteilung Wissenschaft, Goethestraße 49, 80336 München, von der die Zahlungsmodalitäten zu erfragen sind. Die Wiedergabe von Warenbezeichnungen in dieser Zeitschrift berechtigt auch ohne Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutzgesetzgebung als frei zu betrachten wären.

»IT-Governance« – Aims & Scope

»IT-Governance« adressiert die Herausforderungen des modernen IT-Managements und vermittelt aktuelles Wissen über wegweisende und beispielhafte Methoden, Konzepte und Erfolgsfaktoren der IT-Governance für Management, Berater, Auditoren und Wissenschaftler. Die Artikel umfassen Überblicksdarstellungen, Analysen, Forschungsergebnisse, Fallstudien, Success Stories und Tutorials. Sie sind praxisorientiert und reflektieren theoretische Konzepte sowie den aktuellen Stand der Forschung. Einen Schwerpunkt der Beiträge bilden einerseits Informationen rund um das Referenzmodell »Control Objectives for Information and related Technology« (COBIT), andererseits Ergebnisse, die in den ISACA-Arbeitskreisen erzielt werden.

Ein Serviceteil enthält außerdem Informationen zu Standards, IT-Prüfung und neuen Büchern aus dem Themenumfeld der IT-Governance.

»IT-Governance« ist die Fachzeitschrift des Germany Chapter der »Information Systems Audit and Control Association« e.V. (ISACA).

»IT-Governance« wird herausgegeben von
Dr. Martin Fröhlich
Prof. Dr. Matthias Goeken
Prof. Dr. Michael Klotz
Ingo Struckmeyer
(verantwortlicher Schriftleiter)
Marc Weber
(hrsg-itgov@dpunkt.de)