Fallstudie: Architekturgestützter Entwicklungsansatz für IT-Compliance-Management in Regierungsbehörden – Anforderungen, Lösungsansätze, Forschungsbedarf

Dr. Silvia Knittl

Das IT-Compliance-Management hat die Aufgabe sicherzustellen, dass die IT konform zu den jeweiligen Vorgaben ist. Unternehmensarchitekturmanagement (Enterprise-Architecture-Management, EAM) beschreibt und strukturiert komplexe IT-Systeme und zeigt deren Zusammenhang zu den geschäftlichen Aufgaben in einer Organisation. In diesem Beitrag wird untersucht, inwieweit die Methoden des EAM für das IT-Compliance-Management eingesetzt werden können. Die Grundlage dazu bildet ein konkreter Fall aus der Praxis in Regierungsverwaltungen, wo in einem Identitäts- und Access-Management-Projekt bereits erfolgreich EAM-basierte Ansätze eingesetzt wurden und sich die Frage ergab, ob mit den gleichen Methoden auch die Governance entwickelt werden könnte. Der Beitrag zeigt dazu abgeleitete Anforderungen, aus der Literatur identifizierte Lösungsbausteine und weist offene Fragen bzw. möglichen weiteren Forschungsbedarf aus.

Zusätzliche Schlüsselwörter: IT-Compliance-Management, EAM, TOGAF, SABSA

1 EINLEITUNG

Compliance ist ein Querschnittsthema und betrifft alle Bereiche innerhalb einer Organisation. Die Anforderungen an Compliance umfassen laut [TÜVRheinland (2011)]: „Alle Regeln, die von der Organisation und den dort tätigen Personen zu beachten sind, unabhängig davon, ob es sich um gesetzliche oder behördliche Compliance-Anforderungen handelt oder solche, deren verbindliche Anwendbarkeit die Organisation für sich selbst oder eine andere Organisation für seine Mitglieder festgelegt hat." Abbildung 1 zeigt einen Auszug verschiedener Regeltypen, die in einem Compliance-Management-System zu berücksichtigen sind.

In diesem Beitrag wird der Fokus auf das IT-Compliance-Management gelegt. Betrachtet wird dabei ein konkreter, aber anonymisierter Fall, von Regierungsbehörden. In diesem Fall ist die Aufgabenstellung in einem IT-Sicherheitsprojekt die Einführung von Identity- und Access-Management (IAM) und die Sicherstellung der dazugehörigen Steuerungs- und Führungsprozesse einschließlich der Schaffung der notwendigen rechtlichen Rahmenbedingungen für den Einsatz dieses IAM-Systems.

Dr. S. Knittl
access GmbH, Marktstraße 47-49, 64401 Groß-Bieberau

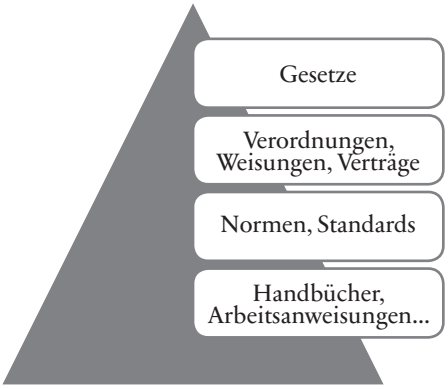

Abb. 1: Compliance: Pyramide verschiedener Regeltypen (Quelle: Eigene Darstellung)

Für das IAM wurde ein architekturgestützer Ansatz gewählt. Die Fragestellung ist nun, ob Steuerungs- und Führungsprozesse ebenfalls mittels eines architekturgestützen Ansatzes umgesetzt werden können. Betrachtet werden hierbei aus Gründen der Übersicht nicht alle möglichen Steuerungs- und Führungsprozesse, sondern das IT-Compliance-Management. Dazu wird zunächst die Fallstudie kurz beschrieben und bereits entdeckte Anforderungen aufgestellt. Im nachfolgenden Abschnitt werden mögliche Lösungsansätze dargestellt und offene Fragen bzw. weitere Forschungsfragestellungen aufgezeigt.

2 FALLBESCHREIBUNG: ARCHITEKTURGESTÜTZTES IT-COMPLIANCE MANAGEMENT IM BEHÖRDENUMFELD

In diesem Abschnitt wird der bisher gewählte Entwicklungsansatz für IT-Compliance-Management in einer Regierungsorganisation strukturiert dargestellt. Ausgangslage waren Steuerungs- und Führungsprozesse für IAM. Das IAM selbst wurde mittels eines architekturgestützten Verfahrens basierend auf TOGAF und SABSA entwickelt [Open Group (2011)]. TOGAF ist ein Architektur-Rahmenwerk und umfasst Methoden und Werkzeuge mit dessen Hilfe Unternehmensarchitekturen entwickelt werden können. SABSA ist ein Rahmenwerk zur Entwicklung risikogetriebener Unternehmenssicherheitsarchitekturen und wird aufgrund seines modularen Aufbaus oft in Teilen oder in Kombination mit anderen Sicherheits-Rahmenwerken eingesetzt (vgl. z. B. [Hoernes (2014)], [Taiwhenua (2014)], [Siedsma und Verboven (2015)]). SABSA wurde in TOGAF integriert [Open Group (2011)] und gliedert die Ergebnisartefakte eines Architekturentwicklungsprojektes in einer Matrix (siehe Abbildung 2). Für diese Matrix verwendet es in einer Dimension sechs einfache Fragepronomen und in der anderen den Grad der Vergegenständlichung von der Idee bis zur Umsetzung, der wiederum jeweils eine federführende Rolle zugeordnet ist.

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	Business Desicions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
Conceptual	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
Logical	Information Assets	Risk Management Poicies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
Physical	Data Assets	Risk Management Practices	Process Mechanism	Human Interface	ICT Infrastructure	Processing Schedule
Component	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Management Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
Service Management	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management

Abb. 2: SABSA-Matrix (Auszug aus [Open Group (2011)])

Die nachfolgende Beschreibung folgt nun in der Struktur dem SABSA-Modell und beschränkt sich aus Gründen der Übersicht auf dessen Dimensionen Organisation (Wer – „People“), Motivation (Warum), Prozessmodell (Wie) und Informationsmodell (Was – „Business Assets“) auf der Kontextebene.

2.1 Organisatorische Aspekte von IT-Compliance-Management und dessen Motivation

Die betrachteten Regierungsbehörden folgen der typischen Organisation einer Stab- bzw. Linienorganisation. Die Grundlage der Handlungen der verschiedenen Organisationseinheiten liegen als Auftrag vom Gesetzgeber im Rahmen einer Verfassung, Gesetz oder Regierungsbeschluss vor [Spektor 2005]. Zu den Aufgaben der Regierungsorganisationen gehört jedoch auch die Vorbereitung von Gesetzen. Die Prüfung von Regierungsorganisationen ist institutionalisiert durch dedizierte Kontrollorgane und ist etabliert im Bereich Datenschutz oder im Bereich der Finanzkontrolle, wie etwa auf Bundesebene der Bundesrechnungshof in Deutschland oder die Eidgenössische Finanzkontrolle in der Schweiz. Für diese beiden Prüfaufgaben, d. h. im Bereich Datenschutz und Finanzen, liegen dann auch entsprechende gesetzliche Grundlagen vor. Neben gesetzlichen Vorgaben werden im Bereich der Motivation weitere Regelungen vorausgesetzt. Zur Umsetzung von IAM in diesem Beispiel sind bewährte Methoden im Bereich der Unternehmenssicherheitsarchitektur als relevante Grundlagen identifiziert worden, wie etwa TOGAF, SABSA und Archimate [Hoernes (2014)].

IAM ist nun eine Disziplin, die alle Organisationseinheiten betrifft, die diese entsprechenden Dienste einsetzen. Das dafür umzusetzende IT-Compliance-Management-System muss nun die Rollen und Verantwortlichkeiten über eine dezentrale, verteilte Organisation hinweg konsistent festlegen. Die IT selbst ist in Regierungsorganisationen oft verteilt auf verschiedene interne und externe Organisationseinheiten. Die Komplexität der IT-Organisation, die von einem IT-Compliance-Management-System in solchen Behörden erfasst werden muss, ist u. a. in [Knittl und Wiedmer (2015)] dargestellt.

Als Anforderung ergibt sich somit im Bereich „People“ die Definition der relevanten Rollen und deren Verantwortlichkeiten. In der Abbildung 4 sind bereits drei der relevanten Rollen im Kontext Compliance dargestellt: die zuständige Rolle für den Erlass einer Vorgabe bzw. eines Gesetzes, diejenige für die Umsetzung und diejenige für die Prüfung der Konformität. Im Bereich der „Motivation“ besteht die Anforderung der Prüfung, ob die rechtlichen Grund-

lagen für deren jeweilige Aufgaben ausreichend sind und ob die weiteren methodischen Vorgaben, wie etwa die verwendeten Methoden SABSA, TOGAF oder Archimate prinzipiell für die Umsetzung geeignet sind.

2.2 Informationsmodell für IT-Compliance-Management

Die „Business-Assets", d. h. die relevanten Informationsobjekte im IT-Compliance-Management, sind in einem geeigneten Informationsmodell abzubilden. Wichtig ist hier zum einen, den eigentlichen Gegenstand von IT-Compliance, d. h. die IT selbst zu erfassen. Zum anderen sind auch die zu berücksichtigenden Vorgaben vollständig zu ermitteln und entsprechend abzubilden. Als Anforderung ergibt sich somit, dass das Informationsmodell mindestens enthält, welche Vorgaben auf welche Assets anzuwenden sind.

2.3 Prozesse für IT-Compliance-Management

Die eigentlichen Prozessaktivitäten im IT-Compliance-Management unterscheiden sich bei Behörden nicht von denjenigen anderer Organisationen und sind vereinfacht nach [FINSOZ e.V. (2014); [TÜVRheinland (2011)]:

2.3.1 Analyse und Erfassung relevanter Vorgaben

Zunächst müssen die für die Organisation relevanten Vorgaben ermittelt werden und in geeigneter Form erfasst werden. In der Abbildung 3 werden etwa auszugsweise Vorgaben dargestellt, die im Rahmen eines Identitäts- und Access-Management-Projekts im ersten Schritt als relevant identifiziert worden sind.

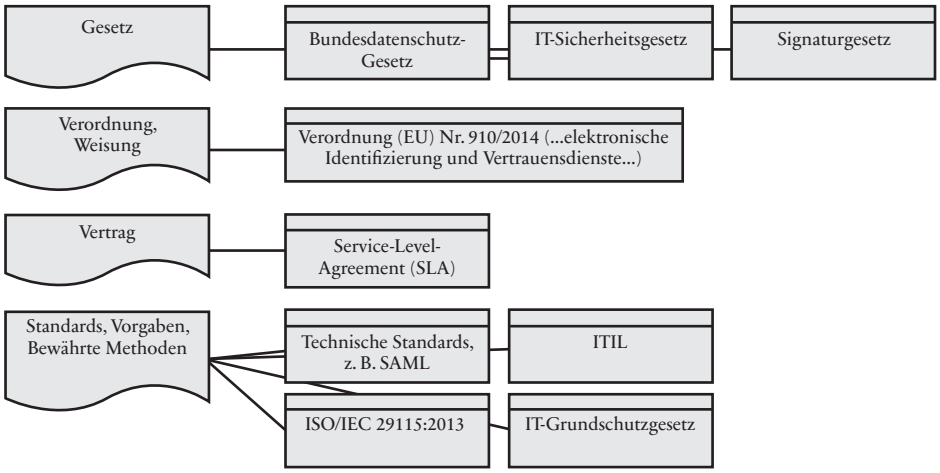

Abb. 3: Vorgaben: Auflistung für ein IAM-Projekt (Auszug) (Quelle: Eigene Darstellung)

2.3.2 Ableiten von Anforderungen

Im nächsten Schritt sind dann je Vorgabe, die aus der Vorgabe zu berücksichtigenden Anforderungen und entsprechende Kontrollmerkmale abzuleiten.

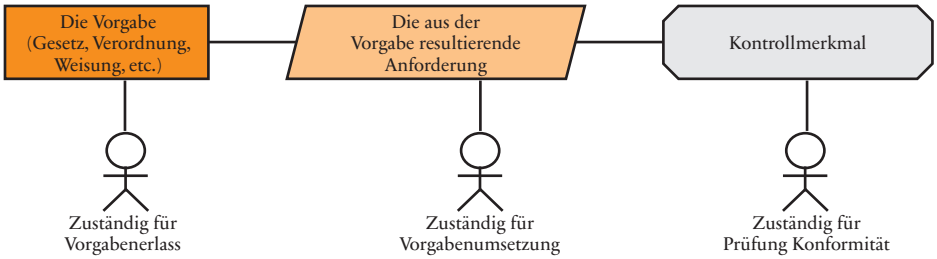

Abb. 4: ArchiMate-Notation: Vorgabe – Anforderung – Kontrollmerkmal (Quelle: Eigene Darstellung)

Die Abbildung 5 zeigt dazu auszugsweise Anforderungen aus dem Bundesdatenschutzgesetz visualisiert mit Hilfe der ArchiMate-Notation [OpenGroup (2013)]. Eine aus §4 resultierende Anforderung ist, dass die Zulässigkeit der Datenverarbeitung per Gesetz oder durch die Einwilligung des Nutzers erlaubt worden sein muss. Aus dieser Anforderung ergeben sich dann mögliche Kontrollpunkte, wie die Prüfung der rechtlichen Grundlage oder die der Nutzereinwilligung.

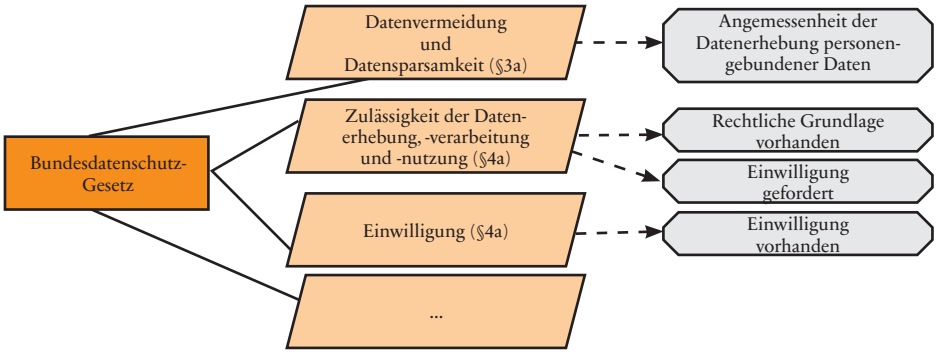

Abb. 5: Bundesdatenschutzgesetz – Auszug Anforderungen und Kontrollmerkmale in ArchiMate-Notation (Quelle: Eigene Darstellung)

2.3.3 Integrieren

In dieser Phase wird entschieden, welche der vorher ermittelten Anforderungen wie und zu welchem Grad umgesetzt werden. Dazu können Arbeitsabläufe so gestaltet werden, dass diese die Erfüllung der Compliance-Anforderungen erleichtern oder ermöglichen oder es können Kontrollmechanismen festgelegt werden, um etwaige Nichtkonformität erkennen zu können.

2.3.4 Prüfen

In der letzten Phase erfolgt eine gem. Prüfplan durchgeführte Prüfung der Konformität. Wichtig ist dabei auch das nachhaltige Dokumentieren und stufengerechte Kommunizieren der Ergebnisse. Diese erstellten Dokumente bilden dann auch die Grundlage für die Evaluation der Wirksamkeit des gesamten Compliance-Management-Systems.
Die Anforderung im Prozessbereich ist hier die geeignete Abbildung auf die betrachtete Organisation. Als Grundlage dazu müssen vorab die oben geforderten Rollen und Verantwortlichkeiten festgelegt worden sein.

3 LÖSUNGSANSÄTZE UND FORSCHUNGSBEDARF BEI ARCHITEKTURGESTÜTZTEN ANSÄTZEN IM BEREICH IT-COMPLIANCE-MANAGEMENT BEI BEHÖRDEN

Im vorherigen Teil wurden Anforderungen an IT-Compliance-Management basierend auf der betrachteten Fallstudie ermittelt. In diesem Abschnitt wird nun aufgezeigt, inwieweit und bei welchen Aspekten architekturgestützte Ansätze das IT-Compliance-Management in Regierungsbehörden unterstützen können und wo es weitere offene Fragen bzw. weiteren Bedarf an Forschung geben könnte.

3.1 Organisation und Motivation

Wie oben dargestellt, benötigen Verwaltungen als Grundlage für ihre Handlungen eine gültige Rechtsgrundlage. In der Schweiz etwa wurde in der Bundesinformatikverordnung die Grundlagen für eine IKT-Steuerung und -Führung gelegt. In den USA hat der Clinger-Cohen Act bereits 1996 eine formelle Grundlage dafür geschaffen, dass bewährte Praktiken im IT-Management auch für Behörden eingeführt werden können. Festgelegt wurde dazu die CIO-Position in jeder größeren Einheit und die Forderung nach der Erstellung von Unternehmensarchitekturen [Congress of United States of Amerika (1996)]. In weiteren Analysen wäre daher zu prüfen, ob die bestehenden rechtlichen Grundlagen ausreichend sind.

Eine notwendige Voraussetzung zur Umsetzung von Unternehmensarchitektur-Management und daher auch für ein architekturgestütztes Compliance-Management in Verwaltungsorganisationen ist laut [Obermeier (2014)] die Festlegung von Rollen und Verantwortlichkeiten unter der Berücksichtigung der spezifischen Rahmenbedingungen der öffentlichen Verwaltung. Hierzu sind weitere Analysen notwendig, welche spezifischen Rollen und Verantwortlichkeiten es in der jeweiligen Verwaltungsorganisation sind. Möglicherweise könnte der Multi-Level-Governance-Ansatz der OECD hier auch für IT-Compliance entsprechenden Input liefern [Rodrigo, Allio und Andres-Amo (2009)]. In [Schultis, Elsner und Lohmann (2014)] werden drei verschiedenen Kollobarationsmodelle für große, dezentrale Architekturprojekte vorgestellt. Weitere Fragestellungen könnten sich damit beschäftigen, ob und welche der dort ermittelten Herausforderungen in der Organisation von Architekturprojekten in großen, dezentralen Umgebungen von der Industrie- auf Verwaltungsumgebungen übertragbar sind.

3.2 Prozess

Es gibt bereits viele Ansätze im Bereich Compliance von Unternehmensarchitekturen, die sich damit beschäftigen, wie die Unternehmensarchitekturen selbst konform zu verschiedenen Vorgaben gestaltet werden können. In [Obermeier (2014)] werden etwa explizit Anforderungen für öffentliche Verwaltungen postuliert, wie etwa dass das EAM-Konzept die Prüfung von Prinzipien und Richtlinien erzwingen und dass es in bestehende Managementprozesse eingebettet werden muss. IT-Compliance-Management wäre so ein bestehender Managementprozess, es wird jedoch hierzu keine dedizierte Lösung entwickelt. In [Liimatainen, Heikkilä und Seppänen (2008)] werden Ansätze aufgestellt, wie in Behörden Entwicklungsprogramme konform zur Architektur gestaltet werden können, in [Knodel und Popescu (2007)] wird dargestellt, welche Mechanismen es gibt, um Architektur-Compliance festzustellen. Im Artikel von [Lohmann (2011)] werden Ansätze zur Compliance von Geschäftsprozessen dargelegt.

Nur wenige Ansätze beschäftigen sich jedoch damit, wie mittels architekturgestützer Verfahren das IT-Compliance-Managment selbst effektiv entwickelt sowie eingesetzt werden kann. In [Vicente (2011)] beschreibt der Autor in seinem Ansatz eine Referenzarchitektur für ein integriertes Governance-, Risiko- und Compliance-Management unter Verwendung der

Architekturentwicklungsmethode (ADM) von TOGAF und ArchiMate. Bei diesem Ansatz wären weitere Assessments notwendig, inwieweit diese in Verwaltungsorganisationen eingesetzt werden können. [Foorthuis, et al. (2009)] beschreiben, wie Organisationen (Business) und IT-Projekte auf Compliance überprüft werden können mit Hilfe von Unternehmensarchitektur. Sie beschreiben in ihrer Arbeit verschiedene Arten von Compliance-Checks, wie etwa für Korrektheit, Konsistenz oder Vollständigkeit. Der Beitrag von [Julisch et al. (2011)] verfolgt einen ähnlichen Ansatz mit Pattern-basierten Kontrollen. Bezogen auf obiges Funktionsmodell ist zu prüfen, wie diese Ansätze im IT-Compliance-Management bei Behörden verwendet werden können

3.3 Informationsmodell

Die obige Anforderung nach Erstellung von Informationsmodellen für IT-Assets in verteilten, dezentralen Umgebungen wurden u. a. in [Knittl (2012)] gezeigt. Dort wurde auch der Zusammenhang zwischen dem ITIL-basierten Konfigurationsmanagement und dem Unternehmensarchitekturmanagement dargelegt. Eine interorganisationale CMDB kann somit als Werkzeug eine Basis für organisationsübergreifendes Architekturmanagement bilden. Wie die ioCMDB für das IT-Compliance-Management verwendet werden könnte, wäre in weiteren Analysen zu prüfen. Der Ansatz von [Sillaber und Breu (2012)] zeigt auf, dass in einem Provider-Netzwerk die jeweiligen Compliance-Anforderungen über das gesamte Netzwerk entsprechend abgebildet werden müssen. Sie liefern hierzu ein Metamodell, dessen Verwendung in einer ioCMDB zu testen wäre. Prinzipiell ist die Unterstützung der Prozessaktivitäten durch architekturgestützte Verfahren möglich. Die Modellierungskonvention ArchiMate [OpenGroup (2013)] kann dazu verwendet werden, wie z. B. [Waltl, Schneider und Matthes (2014)] in ihrer Arbeit beschreiben. Dort zeigen die Autoren explizit die Machbarkeit der Modellierung von Compliance-Anforderungen mittels ArchiMate. ArchiMate wurde daher auch für die Darstellung der obigen Abbildungen verwendet. Jedoch setzt diese Aufgabe voraus, dass die entsprechenden Anforderungen einfach aus dem Gesetz bzw. der Vorgabe extrahiert werden können. Aktuelle Untersuchungen zeigen jedoch, dass die Komplexität der Gesetzestexte und deren Zerlegung selbst noch ein eigener Forschungsgegenstand sind [Waltl und Matthes (2015)]. Hierbei stellt sich die Frage, ob relevante Vorgaben und Gesetze, zumindest solche, die die IT betreffen, nicht von vornherein selbst mittels modellbasierter Verfahren entwickelt werden könnten, um deren Übertragbarkeit und damit Anwendbarkeit im Bereich der IT-Compliance zu erleichtern. Im Vorgehensmodell zur Erstellung von Gesetzen etwa dürfen bereits bei Bedarf kausale Modelle zur Illustration der Zusammenhänge von Ursachen und Problemen verwendet werden (vgl. z. B. [Bundesamt für Justiz (2014)]), der daraus entwickelte eigentliche Gesetzestext darf dann allerdings nur in natürlicher Sprache formuliert werden (z B. [Schweizerische Bundeskanzlei (2015)], [Bundeskanzleramt Österreich (2004)]) und soll möglichst knapp und einfach formuliert werden [Bundeskanzleramt Österreich (1990)]. Weiterer Forschungsbedarf wäre daher notwendig zur Untersuchung, inwieweit die Methoden der Rechtserzeugungsprozesse zumindest für die IT betreffende Gesetze auf architekturbasierte Verfahren umgestellt werden könnten, um deren Anwendbarkeit für die IT-Compliance zu vereinfachen.

4 ZUSAMMENFASSUNG

In diesem Artikel wurde anhand eines Fallbeispiels vorgestellt, welche Herausforderungen es beim Einsatz architekturgestützter Methoden im IT-Compliance-Management gibt. Die Ausgangslange war ein Projekt im Sicherheitsbereich im Verwaltungsumfeld in der Domäne Identitäts- und Access-Management (IAM). Dort wurden erfolgreich die Methoden des Architekturmanagements, wie etwa TOGAF, SABSA und ArchiMate, für dessen Entwicklung eingesetzt. Es ergab sich daher die Fragestellung, ob diese Methoden nicht ebenso erfolgreich zur Entwicklung von Steuerung und Führung von IAM, am Beispiel des IT-Compliance-Managements, verwendet werden können. Beleuchtet wurden daher die Anforderungen an ein architekturgestütztes IT-Compliance-Management anhand verschiedener Dimensionen und es wurde gezeigt, dass es in jeder der betrachteten Dimensionen bereits einzelne, teils isolierte Lösungsbausteine für eine Umsetzung gibt. Es sind nun jedoch weiteren Analysen oder Forschungsarbeiten notwendig, die prüfen, ob und inwieweit die hier identifizierten Ansätze für eine integrierte Lösung dienen können. Eine identifizierte Fragestellung ist es, ob die Methoden der Rechtserzeugungsprozesse selbst bereits mittels architekturbasierter Verfahren entwickelt werden könnten, damit die eigentliche Grundlage der IT-Compliance, nämlich Gesetze, unmittelbar, d. h. ohne nachträgliche Interpretation und Umsetzung in einer Unternehmensarchitektur angewendet werden können.

Methoden des Architekturmanagements für das IT-Compliance-Management zu verwenden, scheint nach obigen Analysen ein möglicher Weg zu sein. Die gewählte Fallstudie zeigt die Komplexität dieser Aufgabe in verschiedenen Bereichen: dezentrale Organisation, verteilte Verantwortlichkeiten, IT-Provider-Netzwerke, verschiedenartige, teils kontextabhängige zu berücksichtigende Vorgabetypen. Aus diesem Grund sollten zukünftig weitere Fallstudien zu diesem Thema durchgeführt werden. Dadurch können die hier aufgestellten Anforderungen auf deren Übertragbarkeit getestet und ggf. weitere neue Anforderungen ermittelt werden.

REFERENZEN

Bundesamt für Justiz (2014): Gesetzgebungsleitfaden – Module Gesetz, Verordnung und Parlamentarische Initiative, Bern, 2014.

Bundeskanzleramt Österreich (1990): Handbuch der Rechtssetzungstechnik – Teil 1: Legistische Richtlinien, Wien, 1990.

Bundeskanzleramt Österreich (2004): Richtlinien für die Erarbeitung und die Gestaltung von Rechtstexten und Muster, http://www.bundeskanzleramt.at/DocView.axd?CobId=1649, zuletzt aufgerufen am 17. Oktober 2015.

Congress of United States of Amerika (1996): Information Technology Management Reform Act (Clinger-Cohen Act of 1996), http://www.gpo.gov/fdsys/pkg/PLAW-104publ106/pdf/PLAW-104publ106.pdf, zuletzt aufgerufen am 8. Juli 2015.

FINSOZ e.V. (2014): IT-Compliance-Guideline für die Sozialwirtschaft – Richtlinienpapier FINSOZ e.V., https://www.finsoz.de/sites/default/files/dokumente/IT-Compliance-Guideline_V1f.pdf, zuletzt aufgerufen am 24. November 2015.

Foorthuis, R., Hofman, F., Brinkkemper, S. und Bos, R. (2009): Assessing Business and IT Projecs on Compliance with Enterprise Architecture, http://ceur-ws.org/Vol-459/paper6.pdf, zuletzt aufgerufen am 24. November 2015.

Hoernes, P. (2014): Ein IAM Grossprojekt aus der Perspektive des Enterprise Architekten – Erfahrungen aus der Schweizer Bundesverwaltung, Vortrag i. Rahmen d. GI Arbeitskreises EAM, 2014.

Julisch, K., Suter, C., Woitalla, T. und Zimmermann, O. (2011): Compliance by Design – Bridging the Chasm between Auditors and IT Architects, in: Computers & Security, Volume 30, Ausgabe 6-7, 2011, S. 410-426.

Knittl, S. (2012): Werkzeugunterstützung für interorganisationales IT-Service-Management – ein Referenzmodell für die Erstellung einer ioCMDB, 2012.

Knittl, S. und Wiedmer H. U. (2015): Dienste und IT-Governance in der Bundesverwaltung – Bedarf, Nutzen und Potenzial, in: eGov Präsenz, 01, 2015, S. 50-51.

Knodel, J. und Popescu D. (2007): A Comparison of Static Architecture Compliance Checking Approaches, in: Conference on Software Architecture (WICSA ,07), Mumbai, 2007, S. 12.

Liimatainen, K., Heikkilä J. und Seppänen V. (2008): A Framework for Evaluation Compliance of Public Service Development Programs with Government Enterprise Architecture, in: The 2nd European Conference on Information Management and Evaluation (ECIME 2008), London, 2008, S. 269-276.

Lohmann, N. (2011): Compliance by design for artifact-centric business processes, in: 9th International Conference, BPM, Clermont-Ferrand, 2011, S. 99-115.

Obermeier, M. (2014): Enterprise Architecture Management in der öffentlichen Verwaltung: Design, Einführung und Evaluation, München, 2014.

Open Group (2011): TOGAF® and SABSA® Integration – How SABSA and TOGAF complement each other to create better architectures, http://www.vanharen.net/Player/eKnowledge/togaf-and-sabsa-integration.pdf, zuletzt aufgerufen am 24. November 2015.

Open Group (2013): ArchiMate® 2.1 Specification, https://www2.opengroup.org/ogsys/publications/viewDocument.html?publicationid=13363&documentid=12366, zuletzt aufgerufen am 7. Juli 2015.

Rodrigo, D., Allio, L. und Andres-Amo, P. (2009): Multi-Level Regulatory Governance: Policies, Institutions and Tools for Regulatory Quality and Policy Coherence, in: OECD Working Papers on Public Governance, Nr. 13, 2009.

Schultis, K., Elsner, C. und Lohmann, D. (2014): Architecture challenges for internal software ecosystems: a large-scale industry case study, in: Proceedings of the 22nd ACM SIGSOFT International Symposium on Foundations of Software Engineering (FSE 2014), New York, 2014, S. 542-552.

Schweizerische Bundeskanzlei (2015): SCHREIBWEISUNGEN – Weisungen der Bundeskanzlei zur Schreibung und zu Formulierungen, Bern, 2015.

Siedsma, P. und Verboven, M. (2015): Practical Experiences of SABSA Domain Modelling at ING, in: 7. SABSA World Congress, Naas, 2015.

Sillaber, C. und Breu, R. (2012): Managing legal compliance through security requirements across service provider chains: A case study on the German Federal Data Protection Act, in: Informatik 2012: Proceedings der GI/GMDS-Jahrestagung, Gesellschaft für Informatik, 2012, S. 1306-1317.

Spektor, I. (2005): Die Organisation der öffentlichen Verwaltungen, http://www.organisation-oeffentliche-verwaltung.de, zuletzt aufgerufen am 3. August 2015.

Taiwhenua, T. (2014): All-of-Government Risk Assessment Process: Information Security, https://www.ict.govt.nz/assets/ICT-System-Assurance/Risk-Assessment-Process-Information-Security.pdf, zuletzt aufgerufen am 17. Oktober 2015.

TÜV Rheinland (2011): TR CMS 101:2011 – Standard für Compliance Management Systeme, https://www.tuv.com/media/germany/60_systeme/csr_nachhaltigkeit_compliance/compliance/faktenblaetter/compliance_standard_tr.pdf, zuletzt aufgerufen am 24. November 2015.

Vicente, P. F. O.(2011): A Reference Architecture for Integrated Governance, Risk and Compliance, Lissabon, 2011.

Waltl, B. und Matthes, F. (2015): Comparison of Law Texts: An Analysis of German and Austrian Legislation regarding Linguistic and Structural Metrics, in: Internationales Rechtsinformatik Symposium (IRIS), Salzburg, 2015.

Waltl, B., Schneider, A. W., und Matthes, F. (2014): Deriving and Modelling Compliance Requirements from Legal Audits, in: EICAR: Trust and Transparentcy in IT Security, Frankfurt am Main, 2014.