

TAXONOMIE UND STRUKTURMODELL FÜR DIE COMPLIANCE DOKUMENTATION

Siegfried Mack HD

Kurzfassung

Compliance Dokumentation als Disziplin: Vorstellung eines Strukturrahmens für die Compliance Dokumentation zur Erleichterung und Systematisierung des Prüfwesens; mit einer einfachen Taxonomie und zugehörigen Begriffsklärungen lässt sich ein universelles, leicht handhabbares Modell der Enterprise Compliance Dokumentation für die gesetzlichen Dokumentationsforderungen gewinnen, das sich bei der Erstellung und Prüfung als nützliche Navigationshilfe erweisen kann.

1. Motivation

1.1. Situation

Unternehmen in Europa und den USA sehen sich zur Erfüllung gesetzlicher Vorschriften dazu gezwungen, ihre Geschäftsaktivitäten umfassend zu dokumentieren, um deren Prüfbarkeit und Zuverlässigkeit sicherzustellen. In Amerika treffen wir auf SOX, FISMA u.a.; in Europa finden sich in fast allen Ländern Vorschriften im Finanz- und Steuerwesen, die sich inhaltlich stark überschneiden. Die Europäer ziehen nach mit EUROSOX und speziellen Vorlagen wie MIFID. Im Gegensatz zur klaren Strukturierung, ja Standardisierung des Financial Reporting (XBRL Europe) gibt es für die darunter liegende Schicht, nämlich die Dokumentation der Geschäftsaktivitäten, außer Best Practice Vorschlägen keine standardisierbaren Strukturierungsrahmen.

1.2. Folgen

Durch ein Fehlen granularer Vorgaben wird die interdisziplinäre Aufgabe der Compliance Dokumentation nach dem Gusto und Erfahrungsschatz der zufällig Beteiligten bewältigt. Hierbei sind oft völlig unterschiedlich gebaute Teilmengen von Dokumentation, die von den Lieferanten der ERP-, Buchhaltungs-, Archivierungs- und Workflow-Anwendungen geliefert werden, zu „homogenisieren“ und in die Dokumentation einzubinden. Da auch die Aufzeichnungen von und über Geschäfts- und IT-Aktivitäten zur Dokumentation zu rechnen sind, und die Aufzeichnungen selbst ebenfalls zu dokumentieren sind, steigert das die Schwierigkeiten für die Beteiligten. Die Strukturierung der Governance Dokumentation, mit IKS, Policies, IT-Management und Risikomanagement tut dann ihr Übriges. Die Folgen treffen die Prüfer - Wirtschaftsprüfer und Prüfer der Finanzbehörden: In jedem Unternehmen hat die Compliance Dokumentation ein anderes Gesicht.

1.3. Ursachen

Die stark variierenden Erscheinungsbilder der Compliance Dokumentation scheinen je nach Disziplin (IT, Recht, Branche, Buchhaltung, SW-ProduktHersteller etc) in folgenden Ursachen begründet.

- Interpretation der Begriffe Compliance und Compliance Dokumentation
- Sicht-spezifische Auffassungen

So finden sich auf dem amerikanischen Markt zahlreiche „Compliance Produkte“, die zu Monitoring- und Aufzeichnungszwecken als operative Elemente in bestehende ERP-, Buchhaltungs-, Workflow-, Archivierungs- und andere Anwendungen als ICS-Elemente „eingeflochten“ wer-

den. Die deskriptive Darstellung der Geschäftsaktivitäten und der teilnehmenden Elemente wird hier oft vernachlässigt oder ganz außer Acht gelassen.

Im deutschsprachigen Raum wird Compliance Dokumentation durch den Begriff der Verfahrensdokumentation, die bereits in den seit 1995 in Deutschland gültigen Steuervorschriften (GoBS) gefordert wird, in vielen Unternehmen auf Verfahrensdokumentation eingeeengt. Da die GoBS von den Finanzbehörden und Unternehmen bezüglich der Verfahrensdokumentation in gleicher Weise ignoriert werden, überträgt sich diese Haltung offenbar auf die Compliance Dokumentation.

1.4. Fragestellung

Zur Konzeption, Erstellung und Pflege der Compliance Dokumentation wäre es für die Unternehmen hilfreich, einen generischen Strukturierungsrahmen zur Hand zu haben. Bezeichnen wird diesen noch undefinierten Rahmen als Compliance Dokumentations-Modell, sollte dieses Modell drei Aufgaben erfüllen:

- a) Systematische Identifikation und Einordnung der zu dokumentierenden Objekte
- b) Integration von Fragen zur Erkennung von Compliance/Non-Compliance
- c) Nutzung als (Strukturstandardisiertes) „Navigationssystem“ für den Prüfer

Ist es möglich, ausgehend von einem naiv-taxonomischen Ansatz, ein solches Dokumentations-Modell zu entwickeln? Ein Modell, das den Größten Gemeinsamen Teiler der unterschiedlichen Anforderungen an eine beliebige Compliance Dokumentation liefert und sich um Branchen- und Vorschriftenspezifische Elemente erweitern lässt?.

Die nachfolgende Diskussion eines ersten Ansatzes fokussiert auf Dokumentationsforderungen wie sie *gemeinsam* durch SOX, FISMA, GoBS u. a. m. gestellt werden.

2. Modellgewinnung

Zur pragmatischen Gewinnung der Taxonomie werden Begriffe aus dem Sprachgebrauch der Objekt-Orientierung genutzt und der Begriff des Compliance-Universums eingeführt; ausgehend hiervon erfolgen die schrittweise begriffliche Verfeinerung und Identifikation der Objekte.

2.1. Taxonomie

Das *Compliance-Universum* enthält alle Compliance-relevanten Objekte eines Unternehmens; die *Compliance-Dokumentation* beschreibt das Compliance-Universum und *enthält* alle Aufzeichnungen, die nach den für das Compliance-Universum gültigen Vorschriften aufzubewahren sind.

Compliance Dokumentation wird in zwei Klassen zerlegt: *Aufzeichnung* (Recording) und *Beschreibung* (Description).

Aufzeichnung bezieht sich ausschließlich auf Ereignisse, die Elemente der Unternehmens- bzw. Geschäftsaktivitäten bilden; Aufzeichnungen treten als Daten-Objekte in Erscheinung: Bewegungsdaten, Journale, Log-Files, Protokolle, Berichte etc.; bei der Einteilung spielt es keine Rolle, ob diese Aufzeichnungen durch eine IT-Anwendung oder manuell erfolgen.

Die Beschreibung dient Darstellung von Sachen, Sachverhalten und Ereignissen. Die Beschreibung zerfällt ihrerseits in zwei Klassen: Reale und abstrakte Objekte, d.h. nicht tangible Objekte.

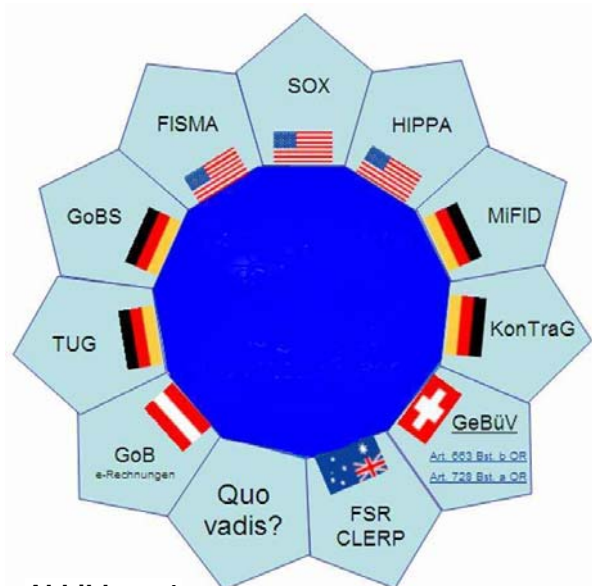


Abbildung 1

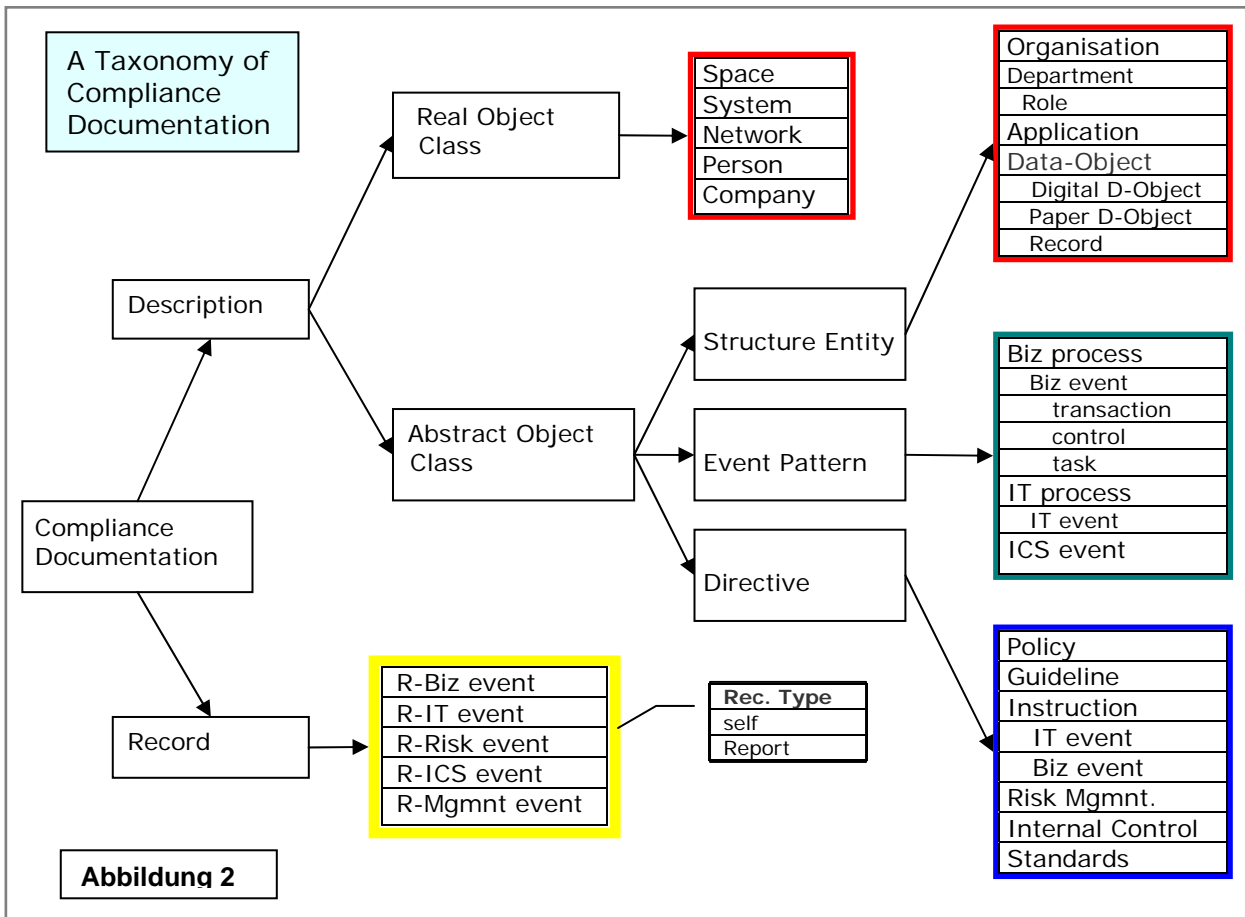


Abbildung 2

Die Real-Objekte (Raum, System, Netzwerk, Anwendung, Person) bilden eine Teilmenge der Ressourcen. Jedes Objekt wird durch eine typisierte Beschreibung repräsentiert. Die Beschreibung der Abstrakt-Objekte zerfällt in drei Klassen: Beschreibung von Strukturen, Mustern und Direktiven. Die Strukturen umfassen die Organisation und alle Daten-Objekte. Die Muster stellen Strukturvorgaben für Ereignisse dar. Die Direktiven umfassen alle Anweisungen, Richtlinien, Policies usw. einschl. alle Instruktionen bzgl. der Durchführungsmodalitäten für Ereignisse. Die eingeführten Begriffe erläutert die nachfolgende Tabelle:

Name	Meaning	Class	Instance
Real object	Representation of a real Enterprise-Object	x	
Abstract object	Representation of an abstract Enterprise-Object	x	
Event pattern	Event Structure definition (action template)	x	
Structure entity	Representation of a structured entity	x	
Directive entity	Standards, guidelines to be followed	x	
Space	Area, building, room, cabinet		x
System	Representation of hardware object		x
Application	IT-Application		x
Biz event	Biz process embedded task/activity	x	
Biz transaction	Biz-supporting task/activity	x	
Biz task	Biz process embedded activity, task	x	
Biz control	Biz process embedded control/check/release	x	
R-Biz event	Real world Biz event (instance)		x
R-IT event	Real world IT event (instance)		x
R-Risk event	Real world Risk Management event (instance)		x
R-ICS event	Real (world) Internal Control System activity		x
R-Mgmnt. event	Real (world) Management activity		x
Biz process	Pattern defining flow of Biz events	x	
IT process	Pattern defining flow of IT events (task, activity)	x	
IT event	IT activity, task	x	
Ctrl event	Process embedded Ctrl event (task, activity)	x	

Tabelle 1

Die Beschreibung der Ressourcen ergibt sich aus der Vereinigung der Beschreibung der Real-Objekte und der Struktur-Objekte (rot umrandete Kasten in *Abbildung 2*). Die Governance wird in den Directive Beschreibungen manifest, das Unternehmen verändernde Handlungen werden komplett unter R-Management-Event zusammengefasst. Da die Beschreibung der Struktur-Entitäten alle Daten-Objekte einschl. der Aufzeichnungen umfasst, führt das zu einer dreischichtigen Gliederung der Beschreibungen des Dokumentations-Universums (D-Universum in *Tabelle 2*). Auf dieser Grundlage wird die Modellgewinnung fortgeführt.

D-Universum
Governance
Ereignisse
Ressourcen

Tabelle 2

2.2. Dokumentations-Objekt – Repräsentation der Beschreibung

Nach Aufteilung der Beschreibung in drei aufeinander aufbauende Schichten wird festgelegt, mit welchen Mitteln die Objekte des Compliance-Universums im D-Universum nachgebildet werden; die Nachbildungen werden als Dokumentations-Objekte bezeichnet. Für jedes Element aus den Schichten Ressourcen, Ereignisse und Governance wird eine Beschreibung in Form eines D-Objekts erzeugt. D-Objekte werden dargestellt durch Name, Typ, Basis-Attribute, Stichpunkte, Referenzen und Methoden; die Biographie durch Klassen-Attribute.

Name: Bezeichnung des Objekts

Basis-Attribute: Elementareigenschaften, die in der Form Name/Wert dargestellt werden.

Biographie: Autor, Erstellungsdatum, Änderungsdatum, Version

Typ: Bestimmt die Unterlassenzugehörigkeit und damit spezifischere Attribute.

Stichpunkte: Thematische Fragestellung bzw. Kriterium in Form eines Satzes; hierzu werden Angaben verlangt. Zu jedem Typ gehören spezifische Stichpunkt-Tabellen.

Referenzen: Bezüge auf andere, bereits erzeugte D-Objekte. Die Referenzierung erfolgt ohne referenzielle Integrität, um den Papiercharakter der Dokumentation aufrechtzuerhalten.

Methoden: Erklärung, was mit dem durch das D-Objekt repräsentierte Objekt "gemacht" werden kann; erscheinen als Methoden-Name: Methodenwert(Text). Methoden werden nur im Zusammenhang mit Daten-Objekten verwendet. Beispiele: Import: ODBC/mdb; Ablage: chronologisch mit Datum/Uhrzeit. Die Repräsentation kann durch Auswahllisten oder Multi-Selektionslisten erfolgen.

Datentypen: Als Datentypen werden zugelassen: Boolean, String, Text, Datum (gDate), Zahl, URI und Tabelle, die Elemente dieser Datentypen enthält. Damit ist das Meta-Modell des D-Objekts gewonnen. Die Modellierungsaufgabe besteht darin, D-Objekt-Modelle für die Klassen der Compliance-Objekte durch passende Bestückung mit Basis-Attributen, Stichpunkten, Methoden und Referenzen auf andere D-Objekte zu erzeugen; die Biographie bleibt als Klassenvariable für alle Unterklassen bestehen.

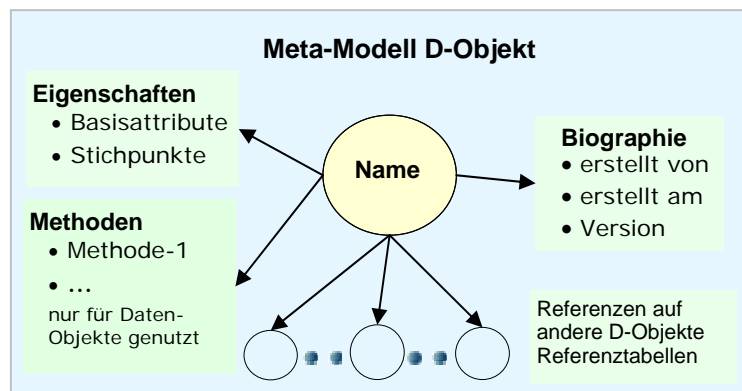


Abbildung 3

3. Realisierung

Mit den hier vorgestellten Mitteln lassen sich unterschiedlichste Compliance-Dokumentationen realisieren, die alle denselben Strukturrahmen und dieselben Objektklassen aufweisen. Die Umsetzung kann auf Papier, mit einfachsten Office-Mitteln, über HTML-Seiten oder als Intranet-Anwendung erfolgen. Das Modell kann bei bestehenden Teil-Dokumentationen als zentrale Navigationsoberfläche genutzt werden. Wichtig ist, dass der Benutzer immer das gleiche „Navigationssystem“ nutzen kann.

S. Mack, Dortmund, 8.7.08