

GRUNDLEGENDES ZUR VERFAHRENS- UND COMPLIANCE DOKUMENTATION I

Siegfried Mack

1. Motivation

Beim Sprechen oder Schreiben über Aspekte der Verfahrensdokumentation (VFD nach GoBS oder GoBit) geraten wir, um zu verdeutlichen was jeweils gemeint ist, fast unweigerlich in die Versuchung, das fraglichen Objekt durch eine zugeordnete Aufzählung von Begriffen schärfer einzugrenzen. Die Ursache dieses Phänomens ist bekanntlich auf das Fehlen eines verbindlichen Begriffsapparates zurückzuführen. Eine Folge dieses Phänomens besteht darin, dass die Bildung von Modellen zur VFD sich sehr schwierig und immer als individuelle Interpretation gestaltet. Ganz beeindruckend zeigen das die unterschiedlichen IT-Anwendungen zur elektronisch geführten VFD. Nachfolgend möchte ich die Entwicklung eines Begriffsapparates mit taxonomischen Hilfsmitteln beschreiben; in weiteren Aufsätzen soll dann gezeigt werden, wie dieser zur Modellkonstruktion genutzt werden kann. Kritiken, Kommentare, Vorschläge und Beiträge sind mir jederzeit willkommen.

1.1. Situation

Durch das Fehlen genauerer Vorgaben durch den Gesetzgeber wird der Erstellung und Pflege einer VFD nach dem Wissens- und Erfahrungsstand der zufällig Beteiligten bewältigt. Der so genannte Standard, der von TÜVIt/VOI publiziert wurde, spiegelt in seiner Struktur zwar die GoBS wieder und greift sehr gründlich fast alle Kriterien auf, die aus DMS-Sicht sinnvoll und notwendig, doch fehlen zahlreiche Elemente der Governance z.B. IKS), die Gesamtstruktur ist mit etablierten Konzepten (BSI/Grundschutz, Coso/Cobit) nicht verträglich und bei zahlreichen Objekten nur schwer zu handhaben.

Für den Betreiber sind oft völlig unterschiedlich gebaute Teilmengen von Dokumentation, die von den Lieferanten der ERP-, Buchhaltungs-, Archivierungs- und Workflow-Anwendungen geliefert werden, zu „homogenisieren“, d.h. unter einem „Informationsdach“ einzubinden. Die Folgen treffen die Prüfer - Wirtschaftsprüfer und Prüfer der Finanzbehörden: In jedem Unternehmen hat die VFD ein anderes Gesicht.

1.2. Ansatz

Zur Erstellung und Pflege der Compliance Dokumentation wäre es für die Unternehmen hilfreich, ein Modell zur Hand zu haben, der es den Beteiligten erlaubt, zielgenau und unabhängig voneinander die nötigen Informationen zu sammeln und in die passenden „Schubladen“ des Modells einzufügen.

Ein solches Modell lässt sich in Anlehnung an die Konzepte der Objektorientierung konstruieren. Identifiziert man die Klassen aller Elemente, die für Darstellung der Compliance eine Rolle spielen, und modelliert diese Elemente durch Bestückung mit passenden Attributen, findet sich ein systematischer Ansatz, bei dem die Ergebnisse anderer Ansätze berücksichtigt bzw. genutzt werden können.

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 wird der Begriff des Compliance-Universums (bzw. Verfahrenswelt) eingeführt; ausgehend hiervon erfolgt die Identifikation der Objekte.

2.1. Taxonomie

Das *Compliance-Universum* enthält die Compliance-relevanten Objekte eines Unternehmens: Ressourcen und Aufzeichnungen.

Im *Compliance-Universum* finden die Compliance-relevanten Ereignisse statt.

Die *Compliance-Dokumentation* beschreibt das Compliance-Universum.

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

Daten, die im Zusammenhang mit einem Ereignis auftreten, werden nachfolgend als Daten-Objekt bezeichnet; z. B. gehören zu einem Geschäftsvorfall Daten-Objekte wie: Buchungsbeleg, Rechnung, Konten, Steuertabelle, Journal etc.) um nicht den zu allgemeinen Begriff Data (wie in Cobit und anderen Modellen) zu verwenden.

Aufzeichnung bezieht sich ausschließlich auf Ereignisse, die Elemente der Unternehmensaktivitäten bilden; Aufzeichnungen treten als Daten-Objekte in Erscheinung: Bewegungsdaten, Journale, Log-Files, Protokolle, Berichte etc. und unterliegen der Beschreibung. Bei der Einteilung spielt es keine Rolle, ob diese Aufzeichnungen durch eine IT-Anwendung entstehen oder manuell erfolgen. Die Aufzeichnung über ein Ereignis wie z.B. ein Monitoring-Protokoll, das als dokumentierendes Daten-Objekt aufzeichnet, wann, durch wen welcher Geschäftsvorfall durchgeführt wurde, ist zu unterscheiden von der Aufzeichnung, die durch die operative Anwendung erfolgt wie z. B. Erfassung eines Kreditors. Im Zweifelsfalle wird die Aufzeichnung „über“ ein Ereignis mit „D-Aufzeichnung“ unterschieden von der operativen Aufzeichnung (O-Aufzeichnung).

Die Beschreibung dient Darstellung von Sachen, Sachverhalten und Ereignismustern. Die Beschreibung zerfällt ihrerseits in zwei Klassen, nämlich Beschreibungen, die sich auf reale oder abstrakte Objekte beziehen.

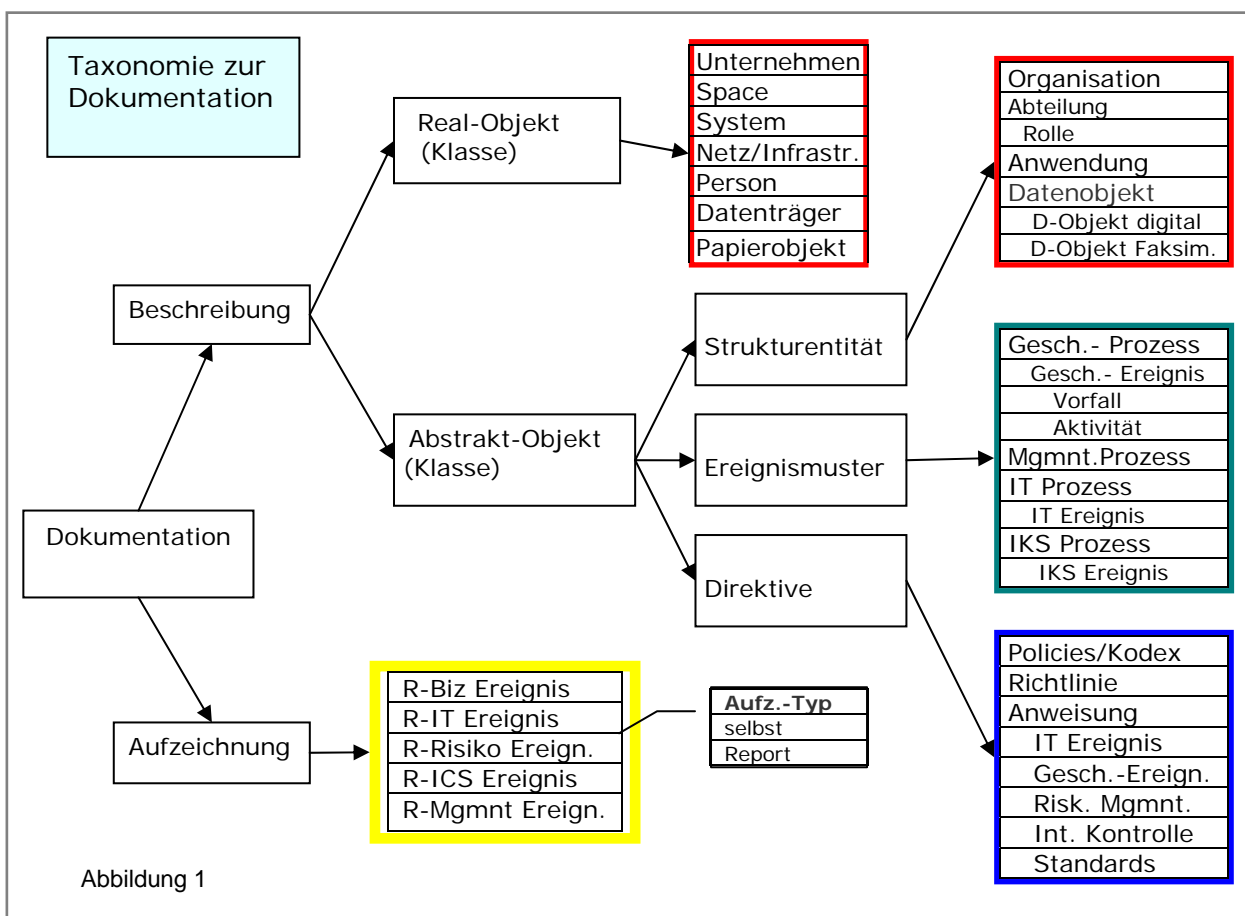


Abbildung 1

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 Beschreibung der Ressourcen ergibt sich aus der Vereinigung der Beschreibung der Real-Objekte und der Struktur-Objekte (rot umrandete Kasten in *Abbildung1*, mit Ausnahme von Unternehmen). Die Governance wird in den *Direktive* 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 (D- und O-Aufzeichnungen) umfasst, führt das zu einer dreischichtigen Gliederung der Beschreibungen des Dokumentations-Universums (D-Universum in *Tabelle 1*). Da zur Identifikation des jeweiligen D-Universums die Firmendaten notwendig sind, wird als Informationsdach die Schicht Unternehmen darüber gesetzt.

C-Universum
Unterneh-
Governance
Ereignisse
Ressourcen

Tabelle 1

3. Realisierung des Documentation Framework

Mit den hier vorgestellten Einteilungen und den identifizierten Klassen lässt sich ein universeller äußerer Rahmen (Company Documentation Framework) für die Dokumentation entwickeln. Vor der Ausgestaltung des Rahmens durch die Einordnung der Klassen in die vier Abschnitte von Tabelle 1 sollen im nächsten Teil des Aufsatzes zunächst das Darstellungsmodell und die Darstellungsmittel für die Objekte festgelegt werden.

S. Mack, Dortmund, 05.12.2010

Plan der weiteren Aufsätze

- (II) Darstellungsmodell und -mittel
Gestalt des Beschreibungs-Objekts
Meta-Meta-Objekt der Beschreibungen
Gestaltung des Dokumentationsrahmens
Typisierung von Beschreibungs-Objekten

- (III) Verfeinerung des Modells I
Modellierung spezieller Objekte
Geschäftsvorfall / IT-Anwendungen
Historisierung von Objekten

- (IV) Verfeinerung des Modells II
Attributbildung in Ressourcen
Attributbildung in Ereignisse
Beschreibungsmodell des IKS
Rahmen Governance

- (V) Beschreibungsrahmen & Umsetzung
Darstellung des Beschreibungsrahmens
Methoden und Mittel der Umsetzung
Papier/HTML/Intranet/Anwendung

- (VI) Nutzung des Modells
HTML-Reporting Jahresabschluss
PDF-Wandlung Jahresabschluss
XML-Schema des Rahmen/Objekte