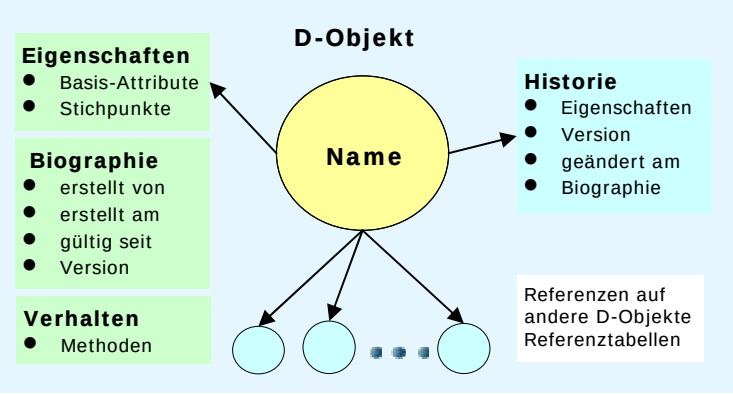
Modell für die Verfahrensdokumentation nach GoBS III

Siegfried Mack

Mit den bisher in den letzten Tabellen verwendeten Basis-Attributen, die sich auf die Angabe eines „einfachen“ Attributwertes beschränkten, lassen sich die Forderungen der GoBS in Sachen Verfahrensdokumentation noch nicht erfüllen. Die Beantwortung eines Themenpunktes wie „Konzept zur Sicherstellung des Zugriffs über einen eindeutigen Index“ verlangt nach der Darstellung eines Sachverhaltes. Hierfür werden einige Sätze und evtl. eine Grafik benötigt.

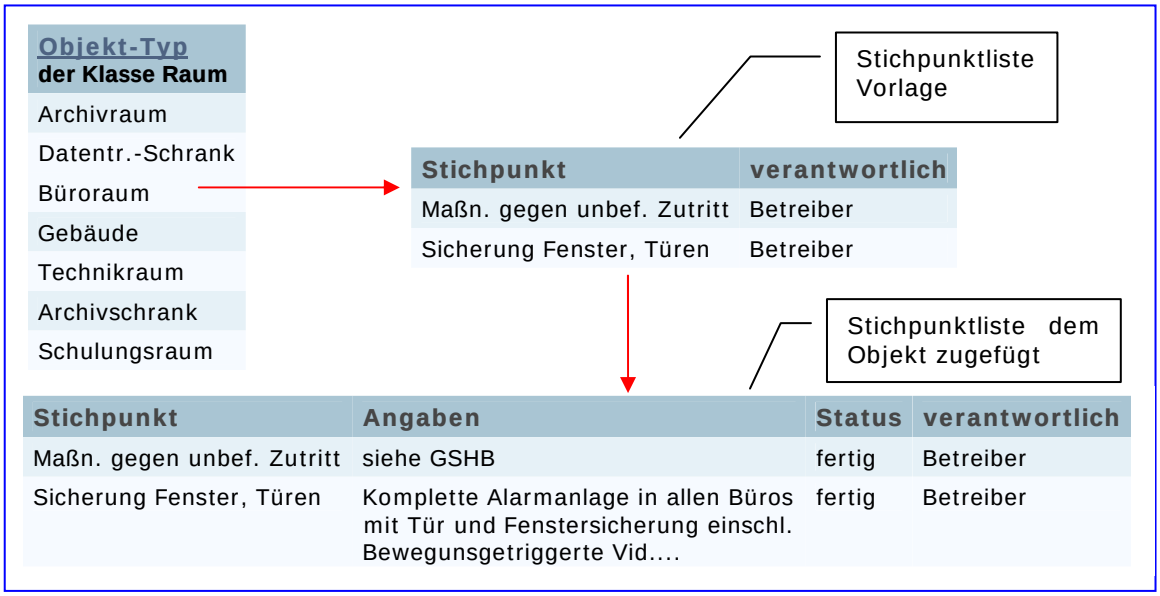


Stichpunkte: Werfen wir noch einen Blick auf den Block „Eigenschaften“ des D-Objekts, so finden sich hier die „Stichpunkte“, die jeweils als Paar „Stichpunkt – Angaben“ bzw. Fragestellung - Stellungnahme auftreten.

Diese Stichpunktlisten sind spezifisch für den jeweiligen Objekt-Typ und lassen sich einfach anhand einer Tabelle auswählen; jedem Objekt-Typ ist eine „leere“ Stichpunktliste zuzuordnen, die nur den Stichpunkt-Text und das Attribut „verantwortlich“ mit den zugehörigen Attributwert (Hersteller, Betreiber, Integrator oder Kombinationen hiervon) enthält. Beim Hinzufügen der rudimentären Stichpunktliste (Vorlage) zum D-Objekt wird jeder Eintrag mit weitere Attributen versehen:

- Angaben: Textfeld zur Bearbeitung des Stichpunktes;
- Status: offen / fertig;
- Datei: Wahlweise ein Datei-Auswahlfeld zur Verknüpfung mit einer Datei;

Hier als Beispiel das Fragment einer Stichpunktliste für ein Objekt der Klasse Raum vom Typ „Büroraum“ :



Nach diesem Verfahren lassen sich für alle Objekt-Typen des IT-Verbundes entsprechende Stichpunktlisten erstellen. Hierzu nimmt man entweder den Text der GoBS zu Hilfe oder diverse andere Veröffentlichungen, die solche Themen-Stichpunkte diskutieren (u.a. EDV-Checklisten der OFDs, die leider föderalistische Unterschiede und tragische Ungereimtheiten aufweisen).

Das Konzept der Stichpunktliste im D-Objekt eignet sich gut dafür, Themenkataloge im Sinne eines GoBS-Checks den Elementen des IT-Verbundes zuzuordnen. Auch Elemente der oben genannten Fragenkataloge, sofern die Fragen heute nicht aktuell sind, lassen sich einfach in das D-Objekt integrieren.

Fassen wir die bisher gewonnen „statischen“ Objekte der „Verfahrenswelt“ im Unternehmen nochmals zusammen:

IT-Verbund	
	1) Räume(Gebäude/Raume/Schrank)
	2) IT-Systeme (nach der Nomenklatur gem. BSI/GSHB: Client, Server, aktive Netzelemente, Einplatzrechner etc.)
	3) Netzwerk-Verbindungen (galvanisch oder drahtlos)
	4) IT-Anwendungen
Organisation	
	1) Abteilungen
	2) Rollen
	3) Personen
Daten-Objekte	
	1) Stammdaten
	2) Dokumente (auch Steuerdaten und Data Sets)
	3) Belege
	4) Konten
	5) Journale

und sehen uns die Möglichkeiten der Attributbildung der Daten-Objekte vom Typ Dokumente/Belege wie versprochen etwas näher an. Zunächst ein Beispiel:

Bezeichnung: Liste Zahlungseingänge	
Beschreibung	elektronische übermittelte Überweisungliste
Eigenschaften	
IT- Anwendung	FIBU-Navision
Klasse	Dokument
Format	----------
Aufbew.-Typ	digital
	inhaltlich
	Original
GDPdU-relevant	GDPdU=ja
Aufbew.-Frist	10
AWV-Name	Eingangsüberweisungsträger
XML (Beschreibungsstd.)	b-list-ein.xml

Schutzbedarf	
Vertraulichkeit	sehr hoch
Integrität	sehr hoch
Verfügbarkeit	sehr hoch
PBZ-Data	ja
Methoden	
Ordnung	Datum
Ablage	Archiv-2
Zugriff	DMS/Docs/Menu
Export	DMS/Docs/Menu
Signatur	---
Vernichtung	automatische Löschung
Biographie	
Version	4

Die Attribute unter **Eigenschaften** sind selbsterklärend: Die das Dokumente führende Anwendung, der Aufbewahrungstyp nach der Terminologie der GoBS, ein Hinweis auf die GDPdU-Relevanz, der offizielle Name nach der Liste des AWV, die Aubewahrunsfirst usw. Der Schutzbedarf ist nur für den Fall der Anwendung des GSHB interessant, weil im GSHB empfohlen wird, den Schutzgrad der Anwendung ausgehend von den von dieser geführten Daten zu bestimmen.

Methoden: Diese Art von Attribut ist etwas interessanter. Übernehmen wir, wenn auch vielleicht nicht ganz streng im Sinne der Objektorientierung, den Begriff der Methode. Damit lassen die Attribute zusammenfassen, die erläutern, welche Operationen auf das Dokument anwendbar sind bzw. angewendet werden. Damit lassen sich eine Vielzahl von Dokumentoperationen ordnend zusammenfassen. Die Einträge sollten generisch über eine Tabelle erzeugt werden und mitwachsen, damit nur die für das Unternehmen spezifischen Angaben gesammelt werden. Mit Stammdaten, Journalen/Protokollen und Konten wird entsprechend verfahren.

Damit sind die wahrnehmbaren Objekte erfasst, die in der „Welt" der Verfahrensereignisse als „Ressourcen" in Erscheinung treten können und es ist gezeigt, wie sich die Attribute kategoriell geordnet unterbringen lassen. Die Objekte der Verfahrenswelt stehen jetzt bereit, um nachzubilden, was im Unternehmen „geschieht". Hierbei werden die Geschehnisse der Verfahrenswelt durch Ereignisse identifiziert, die wiederum als Dokumentations-Objekt modelliert werden sollen - anwendbar für GoBS und SOX.

Ereignisse: Die Ereignisse zerfallen in drei Klassen: Allem voran der Geschäftsvorfall und der „interne Leistungsprozess" (Bezeichnung in den GoBS); beim Leistungsprozess handelt es sich in Bezug auf den Geschäftsvorfall durchweg um eine Vor- oder Nachverarbeitung von Daten (z.B. Scannen von Faksimiles, OCR etc.) oder um Prüf- oder Kontrollhandlungen, die dem IKS unterliegen, d.h. IKS-Instrumente darstellen. Nachfolgend solle die Bezeichnung „Prozess" für den internen Leistungsprozess aus den GoBS benutzt werden. Achtung!: Der „Prozess" ist nicht mit dem „Geschäftsprozess" zu verwechseln.

Ereignisse
Geschäftsvorfälle
Prozesse (GoBS)
IT-Ereignisse

Die nächst wichtige Klasse von Ereignissen sind die IT-Ereignisse, die ihrerseits Elemente von IT-Prozessen sind - analog den Geschäftsvorfällen, die als Elemente von Geschäftsprozessen auftreten. Damit erhalten wir drei Klassen von Ereignissen in der Verfahrenswelt (Tabelle links). Diese Ereignisse werden nun als D-Objekte modelliert.

Streng genommen sollten die IT-Ereignisse an oberster Stelle stehen; dies entspräche eher unserer heutigen Auffassung des IT-Enabling. Denn erst nach dem Bereitstellen des Betriebssystems, Installation der Anwendung usw. sind IT-gestützte Ereignisse wie Geschäftsvorfälle etc. erst möglich.

Geschäftsvorfall: Das Modell für den Geschäftsvorfall wurde bereits im Teil II, Abb.7 skizziert. Die nächsten Tabellen zeigen beispielhaft einige Basisattribute:

Aktion	Kauf eines Geländes (buchen)
Art	fachlich-intern
Rolle	Datenschutzbeauftragter
IT-Anwendung	FIBU-Navision
Anwndg.-O-ID	A4
Owner	Einkauf
Spez. Anweisung	nur aus notariellem Original
Anmerkungen	keine
Klasse (GP)	Anlagen-Zugang
Biographie	
erstellt von	Administrator
erstellt am	20.10.2005
Version	4

IKS-Parameter	
IKS-Objekt	ja
Funktionstrennung	Genehmigung Durchführung
Begründung	--------
unterliegt Richtlinie	keine Annahme von Bakschisch
Prüfungen	
Eingabeprüfung	System
Ergebnisprüfung	intellektuell
Schutzbedarf	
Vertraulichkeit	hoch
Integrität	hoch
Verfügbarkeit	niedrig
SBmax	hoch

Zur Erfüllung der Beleg-, Journal- und Kontenfunktion sind als Attribute dementsprechend mindestens ein Beleg, Journal und Konto zuzuordnen. Bei Nutzung von Stammda-

ten oder anderen Daten-Objekten, sind diese ebenfalls anzugeben. Falls innerhalb der Abwicklung des Geschäftsvorfalls andere Anwendungen involviert sind (simultane Weiterleitung von Daten an oder holen Daten von anderen Anwendungen), werden diese in der dem Geschäftsvorfall zugeordneten Tabelle vermerkt. Etwa in folgender Form:

Daten-Objekte / Sekund.-Anwendungen		
Bezeichnung	**Art**	**I/O-Typ**
Büromaterial	Sachkonto	Output
Direkt	Personenkonto	Senke
FIBU-Navision	Anwndg. Std.	Output
F-Stamm	Stammdaten	DB
Kontoauszug	Beleg	Input

Damit ist auch der Datenfluss von und zu anderen Anwendungen erfassbar; die Einträge zur Erfüllung der Beleg-, Journal- und Kontenfunktion sind klar. Falls mehrere Konten involviert sind, lassen sich diese ebenfalls eintragen.

Mit dieser Darstellung wird das oben genannte Modell des Geschäftsvorfalls als D-Objekt nachgebildet. Die bereits definierten Ressourcen erleichtern die Konstruktion des Komplexobjekts.

Der übergeordnete Geschäftsprozess wird durch die Klasse (GP) erfasst, um deutlich zu machen, falls GP-Diagramme vorliegen, welchem Geschäftsprozess der Geschäftsvorfall zuzuordnen ist. Die Basis-Attribute sind nur beispielhaft und nach Ermessen zu definieren. So ließen sich noch Hinweise auf das passende Menü der führenden Anwendung unterbringen usw. Die Übersicht stellt sich dann als Tabelle dar:

Bezeichnung	IT-Anwendung	Owner (Abtlg.)	erstellt von	erstellt am	Version
Eingang Zahlung	FIBU-Navision	Controlling	sm	20.7.2006 17:34	4
Einkauf-Metalle	Warenwirtschaft II	Einkauf	Administrator	19.7.2006 18:13	1
Grundst.Kauf	FIBU-Navision	Einkauf	Administrator	26.6.2006 03:36	3
KFZ-Kosten erf.	FIBU-Navision	Controlling	Administrator	20.7.2006 16:00	2
Kreditaufnahme	FIBU-Navision	Geschäftsleitung	sm	2.7.2006 13:12	1
Kreditvergabe	Lohn & Gehalt	Personal	Administrator	2.7.2006 13:23	1
Mahnung	FIBU-Navision	Buchhaltung	Administrator	19.7.2006 16:14	1
Materialeinkauf	Warenwirtschaft II	Einkauf	Siegfried Mack	2.7.2006 13:11	1
Verkauf-Anlage	Personaldatenverw.	Controlling	Administrator	29.6.2006 11:40	11

Der Prozess (gem. GoBS) unterscheidet sich vom Geschäftsvorfall lediglich dadurch, dass hier kein Konto nötig ist und statt des Journals eine typisches Protokoll erstellt wird (bzw. werden sollte). In beiden Fällen erfolgt die Feststellung der Identität eines durchführenden Mitarbeiters über die Rolle in Verbindung mit dem konkreten Journal bzw. Protokoll. Durch die Rolle wird der Kreis der Mitarbeiter eingeschränkt und im konkreten Journal/Protokoll findet sich ein Hinweis auf dem Mitarbeiter.

IT-Ereignisse: Die Darstellung der IT-Ereignisse gestaltet sich wesentlicher einfacher. Das liegt daran, dass für IT-Prozesse etablierte Klassifizierungsrahmen vorliegen (ITIL, COSO/CObIT…). Bei einem personengebunden IT-Ereignis werden von einem Mitarbeiter Handlungen durchgeführt, die auf Objekte des IT-Verbundes einwirken. Das Vorgehen entspricht im übrigen dem beim Geschäftsvorfall. Das IT-Ereignis wird als Klasse definiert und die Attribute ergeben sich von selbst: Bezeichnung, Rolle, betroffenes Elemente aus dem IT-Verbund, eine sprechende Bezeichnung über die Art der Handlung, Zuordnung des Prozesses nach COSO/CObIT mit der entsprechenden Prozessklasse und evtl. zusätzlich eine Kategorisierung nach dem Sprachgebrauch des Unternehmens.
Hierbei empfiehlt es sich, Möglichkeiten der Gruppenbildung oder Zusammenfassung zu nutzen, wie sie im GSHB bei der Darstellung des IT-Verbundes gebraucht werden.
Da bei jedem IT-Ereigniss Protokolle, Testate oder Berichte entstehen können, die zur Kontrolle bzw. dem Nachseis der Durchführung Verwendungen finden, werden diese in einem separaten IT-Journal geführt, das später besprochen werden soll, da es im wesentlichen ein Kontrollinstrument im Sinne des IKS darstellt, das Nachweise für die einzelnen IT-Ereignisse verlangt (wie auch SOX).

Die Ereignisse der Verfahrenswelt sind damit ausgeschöpft bis auf solche, die der Governance bzw. dem IKS bzw. als Maßnahme gegen Gefährdungen (GSHB) ergriffen werden.

Governance: Wenden wir uns nur der obersten Schicht der D-Objekte zu, der Schicht der Governance. Hier wird gestaltet, gelenkt, kontrolliert usw. Dies ist der Brutstätte der Ideen für die Gestaltung der Verfahrenswelt. Unter Lenkung und Kontrolle finden hier die Veränderungen ihren Anfang.

Verfahrenswelt
Governance
Ereignisse
Ressourcen

In der Governance finden sich die folgenden D-Objekte: Das IKS, das IT-Journal und der IT-Grundschutz als Analyse- und Gestaltungsaufgabe der IT-Ereignisse des IT-Verbundes. Abschließend werden die wichtigsten Unternehmensdaten, Hinweise zur Abrechnungsperiode usw. aufgeführt.

Im nächsten Aufsatz soll der Aufbau der Governance und die Abbildung in D-Objekte besprochen sowie die Gesamtdarstellung der Verfahrenswelt abgeschlossen werden; abschließend werden die Integration von IT-Grundschutz, Risikomanagement, IKS etc. erläutert.

Dortmund, November 2006

Autorenhinweis
Siegfried Mack
pragma@best-quotation.de
www.aufbewahrungspflicht.de