Modell für die Verfahrensdokumentation nach GoBS II

Siegfried Mack

Vor der Fortsetzung der Entwicklung eines Dokumentationsmodells für die GoBS soll noch einmal das zu verwendende Dokumenationsobjekt (D-Objekt) in Gedächtnis gerufen werden:

Darstellungsmittel: Mit Hilfe des rechts gezeigten D-Objektes sollen die Objekte der Realität im Modell repräsentiert werden.

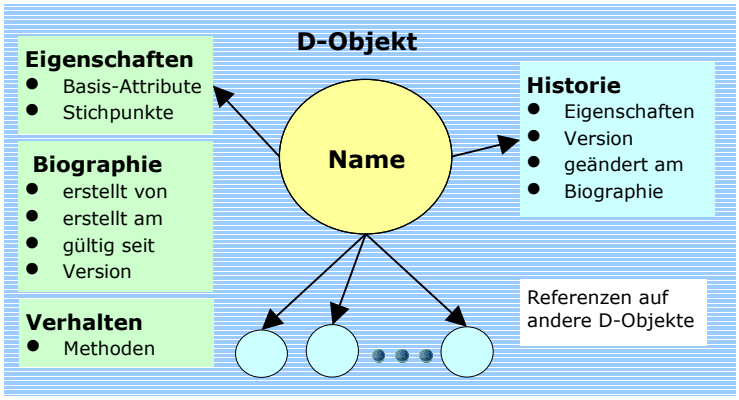

Abb. 1

Der Weg zum D-Objekt: Beginnen wird die Objektfindung mit einer phänomenologischen Annährung an die IT-Objekte. Wer IT-Objekte identifizieren will, muss zunächst in ein Gebäude und dann in verschiedene Räume eintreten. In den Räumen finden sich IT-Systeme: Server, Clients, Peripherie usw. Der kleinstmögliche Container, der IT-Objekte enthalten kann, wäre der Schrank (Schutzschrank, Archivschrank, etc.). Ein Blick in die GoBS bestätigt: Gebäude, Räume etc., die IT- oder GoBS-relevante Objekte (z.B. IT-Komponenten, Datenträger usw.) enthalten, unterliegen Sicherheitsanforderungen und sind damit schutzbedürftig: Gebäude, Räume und Schränke.

O-Id	Bezeichnung	Raum-Typ	Inhalt IT-Objekte
R01	Buchhaltung	Büroraum	9 PC, 2 Hubs 1 Server; nach Büroschluss und Reinigung wird der Raum abgeschlossen. Kabelanschlüsse über Bodentanks.
R0-14	Meeting-RII	Schulungsraum	Projektor, stat. PC
R0-18	Buchhaltung II	Büroraum	8 PCs, 1 Hub
R02	Lager	Gebäude	im Lager werden Produkte der Serienfertigung vorgehalten. Seit Januar auch Gabelstapler
R02-25	Personal-Büro	Büroraum	6 PCs, 1 Switch, 2 Netzdrucker, 1 Scanner
R04	Controller-Raum	Büroraum	4 PC, Plotter, 3 lokale Drucker
R05	Vertrieb-II	Büroraum	4 PC, 2 Hubs 1 Server; nach Büroschluss Kabelanschlüsse über Bodentanks. und Reinigung wird der Raum abgeschlossen.
R05/SR	Marketing	Büroraum	Datenträger Rev.; Datenträger Wochensicherung S1,s3,4

Damit haben wir in erster Näherung eine Übersichtdarstellung der Räume gefunden. Jeder „Raum", hier im Sinne von umschließendem Raum gebraucht, erhält eine Objekt-ID, eine Bezeichnung (Name), eine Typisierung (Raum-Typ) und eine kurze Beschreibung des Inhalts als Basis-Eigenschaften.

Vordenker und Wandel: An dieser Stelle erscheint es angebracht, auf einige Entwicklungen seit dem Erscheinen der GoBS im Jahre 1995 einzugehen. Von Unternehmensberatern, dem TüVit Essen, dem VOI und Beratungsunternehmen wurden Fragenkataloge für die Verfahrensdokumentation entwickelt. Ein wesentlicher Teil dieser Fragen beschäftigte sich mit IT-Sicherheit. Durch das BSI wurde mit dem Grundschutzhandbuch zur IT-Sicherheit im Verlauf der letzten Jahre ein Standard etabliert. Dieser Standard verbindet eine wohldefinierte Nomenklatur mit einem klaren Betrachtungsmodell und einer straffen

Vorgehensweise bei der Behandlung des Themas IT-Sicherheit bzw. ISMS (it-security management system).

Die durch ihre Allgemeinheit sehr umfassende Darstellung der GoBS erlaubt ohne weiteres die Integration der grundlegenden Elemente dieses Standards; in Anbetracht der heute grundlegenden Bedeutung der IT-Sicherheit ist diese Integration im GoBS-Sinne faktisch zwingend. Das bringt den Vorteil mit sich, dass auf ein gewaltiges Volumen an „Denkarbeit" und Standardisierung aufgebaut werden kann; zudem wird das Grundschutzhandbuch des BSI laufend aktualisiert.
Das Konzept des D-Objektes eignet sich sehr gut dafür, das Gerüst des BSI Grundschutzhandbuches abzubilden. Auch Elemente der oben genannten Fragenkataloge, sofern die Fragen heute nicht aktuell sind, lassen sich strukturell durch das D-Objekt integrieren.

Harmonisierung: Um nun die Sichtweisen der GoBS und des BSI GSHB auf die IT-Welt zu harmonisieren, müssen grundlegende Einteilungen der IT-Welt aus dem GSHB für die Verfahrensdokumentation übernommen werden.
Besteht die IT-Welt in der Sicht der GoBS aus IT-Komponenten (d.h. Hardware und Software), geht das GSHB vom IT-Verbund aus. Der IT-Verbund wird eingeteilt in Räume, IT-Systeme, Infrastruktur und IT-Anwendungen. Diese vierteilige Gliederung des IT-Verbundes soll nach der oben begonnen „phänomenologischen Begehung" weiter verfolgt werden. Auf die notwendigen Harmonisierung wird dann jeweils beim Konstruieren der D-Objekte eingegangen und es wird möglichst die Nomenklatur des BSI GSHB verwendet.

IT-Systeme: Hierzu zählen alle Rechner und die aktiven Netzwerkelement wie Hubs, Switches, Router etc. und weil ebenfalls aktiv im Netzwerk, TK-Anlagen und Netzwerkdrucker.

O-Id	Bezeichnung	Typ	Plattform/BS	Architektur	Anz.	IT-Raum	Benutzer
A-IT	Alle Systeme	All-Systems	--------	-------	1		Alle IT-Benutzer
C12	wartung kfz	Client	SOLARIS II	Intel Pent.	1	Raum-A13	
C2	Laptops in Verw..	LAPTOP		titanium	7		GL/FIBU/PERS
C3	CLTs/Buchhaltung	Client	SOLARIS II	Intel Pent.	4		Anlagenbuchahltung
C4	Vertrieb	Client			6	Lager	Vertr./marktng./Cont.
C7	PC f. stud. Hilfskr.	Client	XP/PRO-C	Intel Pent.	3	Raum-A13	
C8	PCs - Controlling	Client	XP/PRO-C		5	Raum-A13	Controlling
IO1	Scanner	Scanner	MD397	Fuijitsu	1	Raum-ZX14	
N1	HUB -ersteEtage	HUB	--------	3COM	3		Administrator-1
N2	Switch-CAD	Switch	D-Link	D-Link	1	Raum-A13	CAD-men
N3	Web-Router	Router	--------	Cisco	1		Geschäftsleitung
N4	R-Dlink-1	Router	--------	D-Link	4		Administrator-1
PR1	Netzdrucker Buchh.	Netzdrucker	--------	Fuijitsu	1	Buchhaltung	
PR2	HP-Drucker Eink....	Netzdrucker	--------	HP	1	Controller-R.	Geschäftsleitung
S1	Faxserver Perso....	Server	WIN/NT-Server	Intel Titan.	1		GL/CON
S2	Domain Controll....	Server		???	2		Administrator-1
S24	Server-Warenwir....	Server	WIN/NT-Server	Intel Titan.	1	Raum-ZX14	CADMAN
S3	Server Personal....	Server		RISC6000	1		
S6	Fibu-Server	Server	MACOS-SERVER	RISC6000	1	Raum-A13	Anlagenbuchhaltung
T01	TK Highcom/S	TK-Anlage	--------	HighCom	1		

Wiederum erhält jedes IT-System eine Objekt-ID, einen Namen usw. Die bereits oben erzeugten D-Objekte für Räume lassen sich hier bereits verwenden.
Das wichtigste an dieser Tabelle ist der „Typ". Der Typ bestimmt einerseits, welcher Baustein (ganz wie ein Operator in der Mathematik) auf das jeweilige D-Objekt anzuwenden ist; andererseits wird dadurch auch festgelegt, welche Attribute und welche Fragestellungen für das fragliche Objekt bei der Darstellung im Sinne der Verfahrensdokumentation nach den GoBS in Frage kommen. Um die Arbeit der Dokumentation zu vereinfachen, wird für alle Elemente des IT-Verbundes der Typ „Alle-…" eingeführt. Damit können Ei-

genschaften, die für alle Elemente dieser Kategorie gelten, den einzelnen Elementen „vererbt" werden; das spart an vielen Stellen unnötigen Dokumentationsaufwand.

Ein weiterer Aspekt ist bei der tabellarisch geordneten Erfassung dieser Daten wichtig. Sie sollen sowohl für das GSHB als auch für die Verfahrensdokumentation nutzbar sein. Deshalb sind die Basis-Attribute so gewählt, dass sie für beide Zwecke verwendet werden können.

Infrastruktur - Netzwerk – IT-Verbindungen: Als nächstes erschließen sich der Wahrnehmung die Kabelverbindungen zwischen den IT-Systemen. Die drahtlosen Verbindungen lassen sich nur postulieren z.B. durch Antennen von WLAN-Elementen. Wählen wir für das Netzwerk mit Draht- oder Funkverbindungen zwischen den aktiven Netzwerkkomponenten wie Hubs, Switches, Routern, DSL-Modems etc. die passenden Attribute aus und stellen diese tabellarisch dar:

O-Id	Bezeichnung	linkt IT-System	O-Id-A	mit IT-System	O-Id-B	via
L01	Domain-zu Fibu	Finanzbuchhaltung	S6	Web-Router	N3	LAN/100 MBit
L02	FicuCls an Server	PCs Personalverw.	C1	Server-Warenwirt.	S24	Bluetooth
L03	Fibu-Serv an Hub4	Finanzbuchhaltung	S6	HUB -ersteEtage	N1	WLAN
L04	Switch-to-Hub5	R-Dlink-1	N4	HUB -ersteEtage	N1	LAN/100 MBit

Die bereits erzeugten D-Objekte für die IT-Systeme lassen hier sofort in Form der Platz sparenden O-IDs dank GSHB-Disziplin verwenden.

IT-Anwendungen: Zum Schluss ergibt sich zwingend die Existenz der IT-Anwendungen, die den IT-Systemen das „Leben einhauchen" und ohne die Systeme und Netzwerke keinen Sinn machten. Damit kommen wir zu den letzen Objekten des IT-Verbundes.

O-Id	Bezeichnung	Typ	auf IT-System	Fachaufgabe
A1	OrgPläne	OFFICE-SW	Laptops in Verwaltung	Organisation
A10	Anlagenbuchhaltung	Anwndg. indiv.	Fibu-Server	Führung Anlagenbestand
A11	E-Shop	Anwndg. indiv.	Vertrieb	Angebot und Bestellung elektronisch
A12	Fuhrparkmngmnt.	Anwndg. indiv.	Server-Warenwirtsch.	Kostenkontrolle Fuhrpark; Alterung, Rentabilität, RW-Kontro....
A2	Personaldatenverw.	Anwndg. indiv.	Server Personalverw.	Erhebung/Verwaltung Personaldaten
A3	Kundendaten	Datenbank	Server-Warenwirtsch.	Erfass und Pflege Kundendaten
A4	FIBU-Navision	Anwndg. Std.	Fibu-Server	Finanzbuchhaltung und Hauptbuch
A5	Lohn & Gehalt	Anwndg. indiv.	Fibu-Server	Erstellung GEhalts- und Lohnabrechnung inkl. automatisher....
A6	Produktdatenverw.	Datenbank	Server-Warenwirtsch.	....
A7	Warenwirtschaft II	Anwndg. Std.	Server-Warenwirtsch.	....
A8	Scan-Archive-Mail	Anwndg. indiv.	Server Personalverw.	....
ALL	Alle Anwendungen	Alle-Software	Alle Systeme	....
Ax-1	Zugang/Authentifiz.	Anwndg. Std.	Alle-Clients	...

Damit ist die reine Erfassung des IT-Verbundes mit den wichtigsten Basis-Attributen abgeschlossen.

Organisation ist alles: Als nächstes stehen wir vor der Aufgabe, Angaben zur Organisation, den Mitarbeitern und deren Funktion im Zusammenhang mit IT-Anwendungen in die Kleider von D-Objekten zu packen. In den GoBS wird Wert auf die Funktionstrennung bei Aufgaben und Abteilungen gelegt. Auf der untersten Ebene der Abteilungshierarchie soll die Funktionstrennung zwischen „fachlichen" und „technischen" Aufgaben für die gesamte Abteilung gegeben sein. Diese scharfe Trennung zwischen IT-Enabling und Durchführung der Geschäftsvorfälle ist ein unabdingbares Element der IT-Sicherheit. Zudem wird ver-

langt, dass klar dokumentiert wird, welche Abteilung für welche Aufgaben zuständig ist. Da die Abteilung durch eine Zusammenfassung von Individuen oder Unterabteilungen repräsentiert wird, sind die Abteilungen zu typisieren, zu benennen.
Lässt sich eine Abteilung klar als entweder rein fachlich oder technisch klassifizieren, ist die Funktionstrennung vordergründig gegeben. Das Bild der Abteilungsübersicht wird damit sehr einfach:

Name	Klasse Abtlg.	Version
Vertrieb-Hamburg	Abtlg. kaufm.	1
WEB-SERVICE	Abtlg. kaufm.	1
CAD	Abtlg. techn.	1
Zentrale Godesberg	ADM/Org.-Ber.	1
Verwaltung	ADM/Org.-Ber.	1
Lager/Logistik	ADM/Org.-Ber.	1
Geschäftsleitung	ADM/Org.-Ber.	2
Firma	Gesch.-Bereich	3
Marketing/Vertrieb	Hauptabteilung	1
Produktion	Hauptabteilung	1
Versand	kaufmännnisch	1
Einkauf	kaufmännnisch	1
Vertrieb-Berlin	kaufmännnisch	1
….	….	….

Die hierarchisch übergeordneten Abteilungen werden dann um die Angabe der unmittelbar darunter liegenden ergänzt. Etwa wie folgt:

Unterabteilung	Art der Abteilung
Buchhaltung	kaufmännnisch
Haus- & Gebäudetechnik	technisch
Informationstechnik	technisch
Personal	kaufmännnisch

Rollenspiel: Etwas aufwändiger wird die Darstellung der Tätigkeiten eines Mitarbeiters, die dieser in Verbindung mit einer IT-Anwendung durchführen kann, bzw. welche Arten von Tätigkeiten durch ihn erlaubt bzw. zugelassen sind. Dargestellt wird dieser Satz von erlaubten Tätigkeiten durch eine Rolle, die in etwa einem „Rechteprofil" entspricht, aber zusätzlich GoBS-spezifische Parameter enthält. Diese Rollen sind notwendig, um aufgrund von Journal-Daten oder Protokollen einen Geschäftsvorfall oder die zugehörige Buchung (buchungspflichtiger Geschäftsvorfall) rekonstruieren zu können. Wichtig ist, dass die Rolle unabhängig von einer Person ganz abstrakt definiert wird, da ja einzelnen Personen mehrer Rollen auf sich vereinigen können.

Rolle	Art	IT-Anwendung	Beschreibung
Abgang Waren	fachlich	Anlagenbuchhaltung	…
Auftragsabwicklung	fachlich	FIBU-Navision	…
Auftragsannahme	fachlich	FIBU-Navision	…
Banküberweisungen	fachlich		…
Datenschutzbeauftragter	fachlich	Alle Anwendungen	…
F-Buchhalter	fachlich	Anlagen-Buchhaltung	…
……..	…	…..	….

Die spezifischen Attribute der Rollen sollen definiert werden, wenn alle für die GoBS wichtigen D-Objekte in der Tabellensicht erfasst worden sind.

Wer hat wann was getan? Das ist die Frage, die in den GoBS gestellt wird, wenn es um Geschäftsvorfälle oder interne Leistungsprozesse geht. Zur Rekonstruktion des Geschäftsvorfalls ist die Identifikation des verantwortlichen Mitarbeiters eine Grundnotwendigkeit.

Titel/Anrede	Vorname	Name	Abteilung
Dr.	Johann	Datendieb	Controlling
Dress	Julia	Nixgut	Entwicklung
Frau	Tulip	Fletcher	Firma
MBA	Mirko	Nodollar	Firma
Herr Dr.	Jonny	Cash	Lohnbuchhaltung
Herr	Klaus	Zuverlässig	Zentrale Godesberg

Die Ergänzung um die passenden Basisattribute ist jedem vertraut. Wichtig anzumerken ist, dass mit jedem Eintrag eine weitere Tabelle verknüpft ist, die die jeweiligen Rollen zusammenfasst und für jede Rolle einen Gültigkeitszeitraum angibt.
In einer zweiten Tabelle empfiehlt sich die Angabe von Vertretern mit Zeiträumen, damit auch der Forderung nach einer Vertreterreglung genüge getan wird. Die erste Untertabelle etwa in folgender Form:

Rolle	System	Zeitraum von	bis
Auftragsabwicklung	FIBU-Navision	2.8.2006	
Banküberweisungen	Buchhaltung	1.7.2006	
Datenschutzbeauftragter	Alle Anwendungen	1.7.2006	

Der Aufbau der zweiten Tabelle versteht sich von selbst.
Damit sind die D-Objekte der Organisation grob identifiziert.

Nun kommt ein Abschnitt an die Reihe, der vor allem für das Thema GDPdU von Bedeutung ist und die Definition der Objekte abschließt, die für die Konstruktion der Modelle von Geschäftsvorfällen und internen Prozessen benötigt werden: Die Identifikation der Daten-Objekte.

Die GoBS unterscheiden zwischen Stammdaten, Steuerdaten, Dokumenten, Belegen, Journalen und Konten. Da Steuerdaten meist den Charakter eines elektronischen Dokuments aufweisen, soll folgende Kategorisierung genutzt werden:
Stammdaten, Dokumente, Journale und Konten. Unter Dokumente erfolgt eine Typisierung nach Dokument/Beleg/Steuerdaten. Unter Dokumenten können danach sowohl Papiervorlagen als auch beliebige digitale Data Sets verstanden werden. Nun zur ersten Übersicht, den Stammdaten:

Stammdaten					
Name	**Führ. IT-Anwendung**	**O-Id**	**GDPdU**	**PBZ-Data**	**Version**
Autos	FIBU-Navision	A4	GDPdU=ja	PBZ=nein	11
F-Stamm	Warenwirtschaft II	A7	GDPdU=ja	PBZ=ja	10
Gehaelter	Lohn & Gehalt	A5	GDPdU=ja	PBZ=ja	4
Kfz-Verbrauch	FIBU-Navision	A4	GDPdU=ja	PBZ=nein	1
Produkte	Produktdatenverw.	A6	GDPdU=ja	PBZ=nein	1
produktepreise	Anlagenbuchhaltung	A10	GDPdU=nein	PBZ=nein	4
WEB-Kunden	Kundendaten	A3	GDPdU=ja	PBZ=ja	2

Und entsprechend für die Belege/Dokumente und Steuerdaten:

Dokumente - Belege - Steuerdaten						
Name	**Art**	**IT- Anwendung**	**O-Id**	**GDPdU**	**PBZ-Data**	**Version**
Bankliste Zahlungs-eingänge	Papierbeleg	FIBU-Navision	A4	GDPdU=ja	PBZ=ja	4
Gutscheine	Beleg	Kundendaten	A3	GDPdU=ja	PBZ=ja	5
Kontoauszug	Beleg	Anlagenbuchhal-tung	A10	GDPdU=ja	PBZ=ja	1
Scheine	Beleg	Lohn & Gehalt	A5	GDPdU=ja	PBZ=nein	2
Tabelle Umrechnung RAND 2001	Steuerdaten	OrgPläne	A1	GDPdU=ja	PBZ=nein	2
Wareneingangsschein	Beleg	Warenwirtschaft II	A7	GDPdU=ja	PBZ=ja	1

Die Übersichten für die Konten und Journale ergeben sich dann von selbst.

Der nächste Schritt besteht nun darin, für alle bisher nur grob definierten Objekte die „feineren" Attribute zu bestimmen. Diese Bestimmung erfolgt im nächsten Teil der Aufsatzreihe.