Enterprise Architecture Management Patterns for Company-wide Access Views on Business Objects

Sabine Buckl, Florian Matthes, Ivan Monahov,
Sascha Roth, Christopher Schulz, Christian M. Schweda
Chair for Informatics 19
Technische Universität München
{buckls, matthes, monahov, rothsa, schulzc, schweda}@in.tum.de

September 1, 2011

Abstract

Modern application landscapes consist of a multitude of inter-connected business applications exchanging data in many ways. These business applications are used by employees who take on several organizational roles. However, when broadening the scope to an enterprise-wide perspective, lack of clarity prevail with respect to the questions which roles have access to which business applications as well as the business objects managed by them. This paper focuses on challenges related to enterprise-wide availability of business objects and compliance and associated confidentiality aspects.

Motivated by best practices from industry, this paper describes patterns to develop, analyze, and justify an enterprise-wide access matrix. The paper presents three enterprise architecture management (EAM) patterns. The *methodology pattern* describes the steps to be performed to document, analyze, and manage the access on business objects; the *viewpoint pattern* provides respective graphical models facilitating a business object access management on enterprise-level; the *information model pattern* defines the concepts and relationships that need to be documented in order to create the graphical model.

1 Introduction and Overview

Today, a typical application landscape is characterized by a large number of business applications interlinked via different interfaces. Over time, the amount of data stored in these business applications continuously increases as a result of the broadening business support and the age of operation of these applications. As a matter of fact, these applications are used by employees with different organizational *roles*. When broadening the scope to an enterprise-wide perspective, lack of clarity and uncertainty prevail regarding the question

> 'Which roles have read and/or write access to which business applications as well as the data managed by them?'.

Supporting new business requirements (e.g. electronic discovery as described in [Gei08, Sch09]) inevitably means that employees are granted access to ever-increasing amount of data that 'they need to know'. Thereby, role-based access mechanisms enable reading and writing permissions for both, the selection of available data, i.e. instances of *business objects*, and the distinctive set of the respective business objects' attributes. At the same time, this access should consider time-related aspects, e.g. an employee not longer employed in a certain department should be revoked access rights no longer needed. Therefore the concept of roles, groups, and access rights to logical units comprises a temporal dimension, which represents the time period of validity for a certain right. Due to the increasing interconnectivity of business applications, the mechanisms of role-based access control deserve further analysis. Especially the question of

> 'whether a role may transitively access confidential information at a specific moment in time'

is of high interest.
This article includes patterns on Enterprise wide access views, being part of the *EAM Pattern Catalog*, a pattern language for enterprise architecture management [BEL$^+$07, Ern08, Ern10], which employs a pattern-based approach to EA management. The complete *EAM Pattern Catalog* is available online at http://eampc-wiki.systemcartography.info [Cha09] and currently includes more than 150 EAM Patterns. For a detailed explanation of the concept refer to [Ern10]. The intention behind this article is to further extend and enhance the already documented EAM Patterns by providing dedicated patterns which deal with the challenge of enterprise-wide access on business objects in particular. In doing so, the present contribution documents not yet described EAM patterns in order to advance the EAM pattern language. The second part of this section lists some remarks to writer's workshop participants, gives a short overview on the intended audience, and provides definitions of pattern types presented in the course of this paper.

1.1 Intended Audience

This article and the herein included patterns are intended for people concerned with governing the information technology (IT) of a company, aligning business and IT, as well as people concerned with challenges regarding IT compliance.

Potential readers for this article are: people concerned with IT related business risk and IT security, enterprise architects, business application owners, and legal department members which possess a basic understanding of IT.

1.2 Pattern types

The previously mentioned *EAM Pattern Catalog* introduces four types of patterns:

- **Methodology patterns (M-Patterns)**: specify a methodology to address management problems in a stepwise manner. The procedures defined by the M-Pattern can be very different, ranging from visualizations and group discussions to more formal techniques as e.g. metrics calculations [LS08]. M-Patterns explicate the methodologies in order to complement activities carried out in an ad-hoc manner or relying on implicit knowledge with activities carried out more systematically,

- **Viewpoint patterns (V-Patterns)**:provide visualizations like diagrams, reports, etc., which are practically proven to be adequate to address problems in EA management. The data required to produce the visualization is documented in one or more I-Patterns,

- **Information model patterns (I-Patterns)**:supply best-practice information model fragments, including definitions and descriptions of the used concepts, which can be used to collect information to address a certain problem in EA management and
- **Anti patterns**: document typical mistakes made in the context of EA management, and provide revised solutions in order to support the pattern user to prevent these pitfalls.

This article focuses on proven practices in the context of enterprise-wide access to business objects, therefore it presents patterns of the former three types but abstains from discussing anti-patterns. The remainder of this article is structured as follows: Section 2 presents an M-Pattern for creating enterprise-wide access views on business objects. Subsequently, Section 3 presents a V-Pattern visualizing enterprise-wide access matrices. Finally, Section 4 introduces an I-Pattern for an enterprise-wide access management. Anti patterns are not considered by the article.

2 M-Pattern: Managing company-wide access to business objects

2.1 Example

The need for an transparency regarding the access permissions role level in a comprehensive manner enabling the analysis and management thereof is confirmed by one of our German industry partners acting in the car manufacturing industry [BMR^{+}10]. Recent economic development has prompted this partner to construct a car production plant in the United States to assemble and sell mid-sized passenger cars directly on site. From an IT perspective, this means that 170 business applications hosted in Germany will also provide business support for the new plant. Due to *Federal Rules of Civil Procedure*[1] as well as the amendments made on federal state level[2], an attorney filing a lawsuit is possibly granted access to electronically stored information retrievable by making use of business applications. In case of the car manufacturer, claims considering specific automotive parts (e.g. cylinder head gasket, or gear drive) may allow the plaintiffs counsel in certain circumstances to conduct detailed on site investigations to identify additional evidence. These investigations, which are subsumed by the term *electronic discovery* [Gei08, Sch09], may also encompass data about parts which were not in scope of the initial lawsuit. From the perspective of the industry partner, these parts are denoted *critical products.* Translated into the terminology of *business objects* encapsulating data, one critical product is mapped to one business object which in turn is stored within an business application. Hence, if a product is deemed critical since it may become subject to a litigation, the according business object in addition to the storing business applications are marked as critical, too.

The problem motivating the development and usage of business object access viewpoints which increase transparency by documenting the current status quo can be described as follows: In the event of *substantiated suspicion*, a lawyer investigating on a critical product may legally have the right to undertake the role of those employees, who were dealing with the according business object. This in turn may allow the legal representative to gain access on additional business objects and related business applications which were not in the initial scope of the litigation. Once access is provided to a business application, the lawyer would be able to retrieve data (represented by business objects) in neighboring systems possibly leading to follow-up claims. As a necessary result, concrete links between roles, business objects, and business applications should be systematically identified, documented, and later on adjusted, mitigating the risk which would be emanated by a lawyer who has comprehensive access rights.

2.2 Context

A company intents to gain transparency on the interlinking of business applications, their managed business objects, as well as the (transitive) access rights on these applications and objects. In this vein, the company wants to ensure that in the event of an on site investigation the access is restricted to those business objects only which a certain role would actually require to fulfill the assigned task.

[1] see http://www.uscourts.gov/rules/newrules4.html for details.

[2] see http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf for details.

2.3 Problem

To prevent misuse of information, you want to know which role has permission to access business objects stored in a specific business application. Furthermore, you are interested in the interconnections between those applications in addition to the detailed access rights a role has on a certain point in time on either a selection of business objects or an object's distinctive attribute. In doing so, you would like to find out which role may have transitively access on parts of business objects that where originally not considered to be accessible by this role.
The following *forces* influence the solution:

- *Detailed analysis vs. time effort and amount of work spent* The current state documentation can cover information on different level of abstractions. For instance, interfaces can be considered as bidirectional connections between two business applications without taking the direction of access, the type of access (read/write), or additional security mechanisms into account.

- *On-demand update of current documentation vs. defined maintenance process* The current state description can either be updated on a regularly basis, which requires the establishment of a dedicated maintenance process or can be triggered on demand. If on demand is chosen, the risk is taken of being too late to avoid legal damage caused by a complaint successfully filed by a lawyer.

- *External experts vs. cost savings* To document the current state external experts could be consulted. While these experts typically have insights into multiple companies and possess expertise regarding the legal regulations in different countries, the labor costs spent for these experts are typically above average. A cheaper solution would be to use internal experts, who know the internal processes and workflows very well.

2.4 Solution

A method for constructing enterprise-wide access matrices on business objects is illustrated in Figure 1 employing the Business Process Modeling Notation (see [Obj08]). Subsequently, the method steps are explained in detail.

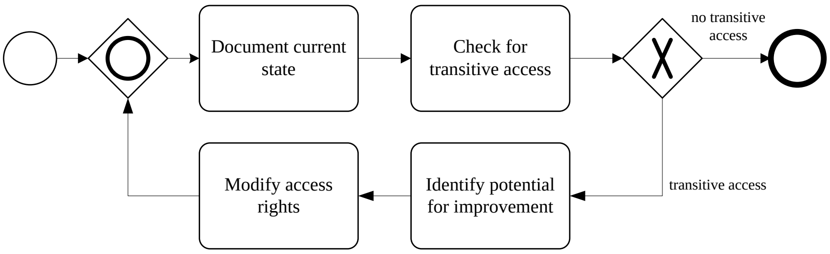

Figure 1: A method for creating company-wide access views on business objects (in BPMN [Obj10]

Document current state gathers information about current access rights, hence documenting which business objects are stored in a specific business application which in turn may be accessed by one to many roles. Thereby, viewpoints making use of a matrix form can be leveraged to express read/write-relationships between two of these concepts. The resulting views (cf. Section 3) are filled with information gathered from different business units within the company which have information on the access permissions. This documentation task can be performed in various ways, e.g. interviewing the respective stakeholders in the business units or observing actors during their IT-supported work. While the former method is top-down, hence from a user's point of view, bottom-up approaches from a business application perspective can also be applied such as automatic logging the users accessing a certain business application.

Check for transitive access involves an expert-based analysis for transitive access on business objects. In a first step, the access rights of roles via intermediary business applications on corresponding business objects are determined and visualized using a tabular viewpoint. Secondly, the resulting view is enriched with information on transitive access, i.e. with information on business objects that may be reached from a role via exploiting the interrelations between the according business applications.

Identify potential for improvement is conducted by experts, who analyze transitive access relations, and identify the subset violating enterprise policies or legal rights. In using the views and the knowledge contained therein, concrete action items can be derived aiming at restricting the access on specific business objects.

Modify access permissions calls on well-known methods ranging from location-based restrictions of network access to role-based application layer access control. Thus, access permissions are modified to incorporate the improvements identified before by experts. Afterwards, a new current state of the access permissions is documented (cf. Figure 1).

2.5 Implementation

Usually, a high degree of stakeholder involvement is required to implement above described method. Put it more simply, it is essential that a defined set of roles participates in the endeavor to ensure an up-to-date view on the company-wide access to business applications and objects in case of an imminent on site investigation. Critical for the success of the M-Pattern are the following participants:

business application owners need to provide information on the business applications and the interfaces offered and used.

data stewards are responsible for business objects and provide information on their relations to other business objects.

administrators are concerned with the roles, groups, and access rights and the implementation of access rules.

domain expert provide information regarding the business context where a certain business object is actually needed.

lawyers are experts for laws and the impact of information access. They detail on the judicial consequences an access permission on a certain business object for a specific role brings along.

2.6 Variants

2.7 Known Uses

The approach documented in Managing company-wide access to business objects is in use in the following companies:

- Volkswagen AG
- Allianz SE

2.8 Consequences

The documented access to business objects needs to be updated regularly in order to ensure that the documentation does not become obsolete. This can be achieved e.g. by enhancing the project management process by an additional step which requires the compilation of a report after a project's termination. The report includes performed changes with respect to business objects, business applications, and interfaces. Similarly, the administrators have to update the current state, if they perform changes with respect to the access rights of certain roles.

2.9 See Also

In order to support the implementation of M-Pattern Managing company-wide access to business objects the V-Pattern Enterprise wide access views should be considered.

3 V-Pattern: Enterprise wide access views

3.1 Example

First, the car manufacturer documents which roles have direct access to which business applications (see Figure 2(a)) and which business application stores particular business objects (see Figure 2(b)). In a next step, the car manufacturer documents which business application exports interfaces to other business applications (cf. Figure 2(c)). For instance, system administrators reported that they send a nightly database dump of the *CRM* to the *ERP* business application.

		Business application		
		CRM	*ERP*	*Portal*
Role	*HR*	rw	-	rw
	Sales	rw	-	rw
	R&D	-	rw	-

(a) Role ⇒ Business application

		BA		
		CRM	*ERP*	*Portal*
BO	*Customer*	rw	-	rw
	Construction plan	-	rw	-
	Contract	-	-	rw

(b) Business object (BO) ⇒ Business application (BA)

		BA2		
		CRM	*ERP*	*Portal*
BA1	*CRM*	rw	-	-
	ERP	rw	rw	-
	Portal	-	-	rw

(c) Business application (BA1) ⇒ Business application (BA2)

Legend	
-	no access
r	read
w	write

Figure 2: Enterprise-wide access matrices

Figure 3 depicts the results of the step checking for transitive access. This view is taken into account by experts from the car manufacturer, who assess the criticality of the corresponding direct and transitive access permissions.

		Business object		
		Customer	*Construction plan*	*Contract*
Role	*HR*	rw	-	rw
	Sales	rw	-	rw
	R&D	- [rw]	rw	- [rw]

Legend	
-	no access
r	read
w	write
[r]	transitive read
[w]	transitive write

Figure 3: Role ⇒ Business object (current state) including transitive permissions

Access violations are identified by the legal department at the car manufacturer, i.e. the role *R&D* accessing the *ERP* business application is also allowed to read the business objects *Customer* and *Contract* violating enterprise policies. According to Figure 3 the documented transitive properties represent access violations since the role *R&D* should not be allowed to read the *Customer* and *Contract* business object. Consequently, a root cause analysis is performed at the car manufacturer, revealing that the connection between *CRM* and *ERP* causes this access violations. Since business processes were improved, the *ERP* system required information on the business object *Customer*, and for this reason, a nightly database

dump of the *CRM* is transfered to the *ERP*.
While the business object *Customer* is not categorized as *critical product*, the business object *Contract* is. Thus, the car manufacturer immediately restricts access to the *CRM* business application and contacts the owners of the *ERP* and *CRM* business applications in order to conjointly work out a solution which prevents the *ERP* business application to access the data of the *CRM* while bewaring business functionality.

3.2 Context

According to [Int07] a *view* is “a representation of a whole system from the perspective of a related set of concerns”, whereas a *viewpoint* is “a specification of the conventions for constructing and using a view.” That means, a viewpoint is “ pattern or template from which to develop individual views by establishing the purposes and audience for a view and the techniques for its creation and analysis.” In order to analyze access permissions on business objects, viewpoints are used. Commonly, employees are granted access to information systems including any business objects shared by the information system. Those access permissions are commonly set per business application disregarding permissions of the employee’s role to business objects. In particular, due to interconnectivity of information systems, it may happen, that an employee gets access to business objects via transitive access to business objects of information systems the employee does not have access to.

3.3 Problem

An organization wants to visualize a holistic overview which roles have permissions to read and write information of enterprise-wide available business objects (cf. [BMR+10]). The following *forces* influence the solution:

- You want to visualize existing permissions of business objects of an application landscape.
- You want to analyze permissions for legal reasons, e.g. compliance.
- You want to analyze permissions for a carve-out, offshoring, or outsourcing.

3.4 Solution

Figure 4 illustrates a holistic view, which roles should have access to the business objects, i.e. describes the target state. Another view shows, which roles actually have access to the business objects, i.e. it describes the current state. According to M-Pattern Managing company-wide access to business objects (see Section 2), after a gap analysis, access permissions are refined (cf. transitive access in Figure 3). To get the relevant information, which business objects are accessible transitively, intermediate information may be necessary (cf. Figure 2). Note that the underlying information model of Figure 2 is given by I-Pattern Capture company-wide access information in an information model.

3.5 Implementation

Views according to the afore presented viewpoint can be created manually by any ‘drawing tool’, like e.g. Microsoft PowerPoint or spreadsheet applications like Microsoft Excel. As

		Business object		
		Customer	*Construction plan*	*Contract*
Role	*HR*	rw	-	rw
	Sales	rw	-	rw
	R&D	-	-	-

Legend	
-	no access
r	read
w	write

Figure 4: Role ⇒ Business object (current state)

manual creation is time consuming and error prone it is advised to use a tool (see e.g. [seb05, Sch06, MBLS08]), which can automate the creation of such visualizations, e.g. SyCaTool[3].

3.6 Variants

Based on I-Pattern Capture company-wide access information in an information model (see Section 4), the following variants exist.

Types of access permissions: Depending on the access permission granularity, the viewpoint may differ in terms of changed legend symbols, i.e. different types of access permissions. For instance, read only, write, or read/write permissions have been observed.

Time-reference of access permissions: More complex types include a period in time when the access permission is actually valid, i.e. the access permission is only valid for an employee working in a specific project for a defined task lasting a specified period of time.

Selections: Business objects may be partially visible to roles, e.g. an attribute is only visible for special interests.

Projections: Business objects may contain others.

Note that these variants can also be combined, i.e. all types of access permissions can be time-referenced. Benefits: A top-down approach typically means less effort due to the number of ratio of analyzed business processes and business applications deployed. However, analyzing business objects via a top-down approach will also include business objects without IT support.

3.7 Known Uses

- Buckl et al. employed this visualization in the automotive industry at Volkswagen AG (cf. [BMR+10]).
- Matthes et al. [BELM08]
- Allianz SE

[3] See `http://wwwmatthes.in.tum.de/wikis/sebis/sycatool`, last accessed 2011-04-18.

3.8 Consequences

- Hidden access permissions of roles become visible.
- Counteractions can be taken.
- Implicit/undetected law violations become visible.
- Compliance can be measured.

3.9 See Also

This V-Pattern may be useful when using M-Pattern Managing company-wide access to business objects (see Section 2). The visualized information is based on I-Pattern Capture company-wide access information in an information model (see Section 4).

4 I-Pattern: Capture company-wide access information in an information model

Subsequent information model can be employed to store information on the company-wide access model, i.e. the access restrictions of certain user roles to the business applications and the therein contained business objects.

4.1 Example

A car manufacturer operates multiple business applications via which its users can access business objects of different criticality. As part of a management process for setting the appropriate access rights the car manufacturer wants to store the current access policies of the business applications together with information on the business objects, to which the applications grant access.

4.2 Context

An organization has established a dense web of interconnections between its business applications, such that different business applications have and may grant access to key business objects.

4.3 Problem

You want to model the business applications that you operate, the user roles that access these business applications, and the business objects on which the according applications provide access. The following forces apply in the given context:

- **coarse-grained** vs. **fine-grained business objects**: being element on a conceptual level, the organization has freedom to choose the level of detail on which the business objects are modeled. Especially when critical information is considered, a more fine-grained model may help to understand discouraged access more clearly. Contrariwise, detailed modeling can be by far more resource consuming.

- **contextualized permissions** vs. **worst-case access**: additional constraints may apply on the access permission of a specific user role on a business application. This may describe that the role can only access a part of the business objects available in the business application. Modeling these constraints may help to reduce *false positives*, i.e. wrong indications to potentially discouraged access, but this information may be hard to collect.

4.4 Solution

Figure 5 presents an information model for storing access related information. It contains the three main concepts: role, business application, and business object. As described in the model, roles have access to business applications storing different business objects. Furthermore, business applications are connected via interfaces to other business applications, whereas interfaces may constitute of database dumps of another business applications, i.e. business objects are transfered without any access control leading to transitive access for roles.

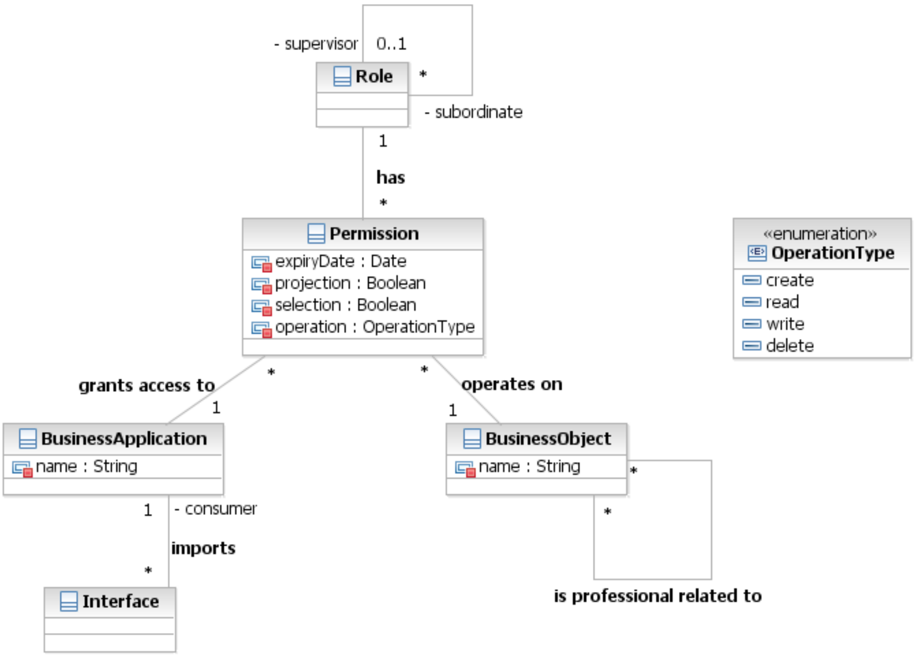

Figure 5: Information model for an enterprise-wide access management

The information model provides a relationship (is professional related to) for expressing that two business-objects hold closely related information. In particular, the relationship covers more expressive relationships such as:

- *projection* meaning that one business object contains only parts of the information available in the business object, it is projected from. This can be identified with a kind of generalization relationship with the projected business object being the generalized one.

- *selection* meaning that one business object covers only parts of the information available in the other business object with respect to the actual instances.

The instances of the class BUSINESS OBJECT together with the links established by the SUBSUMES-relationship are expected to form a directed, acyclic graph. This graph mirrors relationships with respect to the degrees of information richness as embodied in the business objects. A cycle in such graph would indicate that at least two business objects are understood to subsume each other, which in turn hints towards these objects being to similar to distinguish in the context of the access model. Having discovered such circular relationship, a model user is strongly advised:

- either to *merge* the business objects participating in such circle into a single one, or

- to *introduce* another, more detailed business object, subsuming at least two participants of the circle, thus removing the circular relationship.

4.5 Implementation

The information model displayed in Figure 5 can be implemented using different EA management tools. In particular, the tool planningIT of alfabet AG and Adaptive EAM of Adaptive Inc. provide sophisticated mechanisms for appropriately modeling business objects [MBLS08]. Due to the central nature of these objects, any supporting tool must supply appropriate modeling facilities.

4.6 Known Uses

The I-Pattern Enterprise wide access viewsis in use in the following companies:

- Volkswagen AG
- Allianz SE

4.7 Consequences

Part of the information as required by the information model presented above may be drawn from access control lists available in the sign-on infrastructure of the organization. For the information on the accessible business objects nevertheless, manual effort in collecting and maintaining this information is required. To achieve consistent and actual modeling, the information model has to be linked to enterprise-wide business object management endeavors or – in case such endeavors do not exist – each business application owner may be required to supply the needed information. In the latter case, the difficulty of terminological ambiguities exists. In particular without relying on an enterprise-wide business object management, no consistent naming for the business objects may exist, leading to ambiguities in the access model.

4.8 See Also

V-Pattern Enterprise wide access views(see Section 3) may be utilized to perform analyzes on information stored according to this I-Pattern.

5 Acknowledgment

We want to thank all participants of the writer's workshop of EuroPloP11 and especially our shepherd Hugo Sereno Ferreira for the time they spent for reading, commenting, and discussing this article.

6 Future Work

The *EAM Pattern Catalog*is currently available at http://eampc-wiki.systemcartography.info, based on the results of an extensive online survey. Certainly, the EAM patterns should continually be revised for readability and understandability and be extended to provide more detailed guidance in addressing the problems of EA practitioners, preferably by an EAM Pattern community. In order to improve the current version and to further exploit the advantages of patterns for EA management, an excerpt of the *EAM Pattern Catalog*had been included in this document to be discussed in the pattern community.

References

[BEL+07] Sabine Buckl, Alexander M. Ernst, Josef Lankes, Kathrin Schneider, and Christian M. Schweda. A pattern based approach for constructing enterprise architecture management information models. In A. Oberweis, C. Weinhardt, H. Gimpel, A. Koschmider, V. Pankratius, and Schnizler, editors, *Wirtschaftsinformatik 2007*, pages 145–162, Karlsruhe, Germany, 2007. Universitätsverlag Karlsruhe.

[BELM08] Sabine Buckl, Alexander M. Ernst, Josef Lankes, and Florian Matthes. Enterprise Architecture Management Pattern Catalog (Version 1.0, February 2008). Technical report, Chair for Informatics 19 (sebis), Technische Universität München, Munich, Germany, 2008.

[BMR+10] Sabine Buckl, Florian Matthes, Sascha Roth, Christopher Schulz, and Christian M. Schweda. A method for constructing enterprise-wide access views on business objects. In Klaus-Peter Fähnrich and Bogdan Franczyk, editors, *GI Jahrestagung (2)*, volume 176 of *LNI*, pages 279–284. GI, 2010.

[Cha09] Chair for Informatics 19 (sebis),Technische Universität München. EAM pattern catalog wiki. `http://eampc-wiki.systemcartography.info` (cited 2010-02-25), 2009.

[Ern08] Alexander M. Ernst. Enterprise architecture management patterns. In *PLoP 08: Proceedings of the Pattern Languages of Programs Conference 2008*, Nashville, USA, 2008.

[Ern10] Alexander M. Ernst. *A Pattern-Based Approach to Enterprise Architecture Management.* PhD thesis, Technische Universität München, München, Germany, 2010.

[Gei08] Ivo Geis. eDiscovery und Datenschutz. Website, 2008. http://www.ivo-geis.de/veroeffentlichungen/eDiscovery_und_Datenschutz.pdf, visited on April 20th, 2010.

[Int07] International Organization for Standardization. ISO/IEC 42010:2007 Systems and software engineering – Recommended practice for architectural description of software-intensive systems, 2007.

[LS08] Josef Lankes and Christian M. Schweda. Using metrics to evaluate failure propagation and failure impacts in application landscapes. In M. Bichler, T. Hess, H. Krcmar, U. Lechner, F. Matthes, A. Picot, B. Speitkamp, and P. Wolf, editors, *Multikonferenz Wirtschaftsinformatik*, Berlin, Germany, 2008. GITO-Verlag.

[MBLS08] Florian Matthes, Sabine Buckl, Jana Leitel, and Christian M. Schweda. *Enterprise Architecture Management Tool Survey 2008*. Chair for Informatics 19 (sebis), Technische Universität München, Munich, Germany, 2008.

[Obj08] Object Management Group (OMG). Software & systems process engineering meta-model specification (formal/2008-04-01), 2008.

[Obj10] Object Management Group (OMG). Business process model and notation (bpmn) – version 2.0, 2010.

[Sch06] Christian M. Schweda. *Architektur eines Visualisierungswerkzeuges für Anwendungslandschaften – Anforderungsanalyse und prototypische Realisierung*. Diplomarbeit, Fakultät für Informatik, Technische Universität München, 2006.

[Sch09] Claus Schmid. Electronic discovery – kaum bekannt aber wichtig. *WIRTSCHAFTSINFORMATIK & MANAGEMENT*, 1(3):40–48, 2009.

[seb05] sebis. Enterprise architecture management tool survey 2005. Technical report, Chair for Informatics 19 (sebis), Technische Universität München, Munich, Germany, 2005.