Building a Reference Model for Anti-Money Laundering in the Financial Sector

Felix Timm[1], Andrea Zasada[1], Felix Thiede[1]

[1]University of Rostock, Institute of Computer Science, Rostock, Germany
`{felix.timm,andrea.zasada, felix.thiede}@uni-rostock.de`

Abstract. Anti-Money Laundering (AML) can be seen as a central problem for financial institutions because of the need to detect compliance violations in various customer contexts. Changing regulations and the strict supervision of financial authorities create an even higher pressure to establish an effective working compliance program. To support financial institutions in building a simple but efficient compliance program we develop a reference model that describes the process and data view for one key process of AML based on literature analysis and expert interviews. Therefore, this paper describes the customer identification process (CIP) as a part of an AML program using reference modeling techniques. The contribution of this work is (i) the application of multi-perspective reference modeling resulting in (ii) a reference model for AML customer identification. Overall, the results help to understand the complexity of AML processes and to establish a sustainable compliance program.

Keywords: Reference Modeling, Compliance Management, Anti-Money Laundering, Financial Sector

1 Motivation and Introduction

The financial industry offers services for individuals and companies to realize money transactions and grant access to numerous financial products such as accounts, shares or credits. Typical financial institutes are banks, insurance and leasing companies. The economic impact of financial activities is enormous. For example, in 2013 the insurance, reinsurance and pension funding in Germany reaches an annual turnover of 251,140 million Euro achieved by only 158,308 employees of 848 companies [1].

The size and structure of the financial industry does not only leave a multitude of financial perspectives but also openings for criminal activities such as money laundering. Money laundering can be described as the process of transforming illegal into legal assets [2]. The *German Institute of Economic Research* (DIW) estimates that about 100 billion Euros are laundered in Germany per year. The observance of regulations that prevent illegal activities like money laundering is ensured by business process compliance management [3]. However, different asset classes and trading platforms make real-time risk and compliance monitoring a challenging and expensive task [4]. The monetary resources that companies need to invest in their compliance management include

implementation, remediation, and penalty associated costs [5]. A global survey with 200 hedge fund managers reveals that almost two thirds (64 percent) of respondents were spending over 5 percent in 2013 of their total operating costs on meeting compliance requirements [6].

The implementation of compliant business processes requires the collaboration of all involved stakeholders, such as compliance officers, IT and legal experts to build a reference model including necessary compliance requirements. The formal description of compliance requirements can be effectively supported by conceptual modeling techniques. These techniques are applied to improve the understanding and communication among stakeholders, which helps to prevent legal violations and reduces the operating costs of compliance management. An essential part of the compliance management of financial institutes is constituted by *anti-money laundering* (AML) regulations. In literature, the term reference model is often related to the *Enterprise Architecture Management* (EAM). EAM is used to reduce the complexity of business activities to create reference models abstracted from reality [7]. Current approaches tackle single information systems disciplines like e-government and miss so far a documented procedure to build the corresponding reference model [8]. With this paper, we drive attention to AML regulations and the necessity to develop a reference model that facilitates the application of compliance requirements in the financial industry. The research questions (RQs) are:

RQ1: *Which compliance regulations have to be adopted for AML prevention?*
RQ2: *How should a reference model for the AML CIP be constituted?*

The paper is structured as follows. In Section 2 we discuss the process of money laundering and give an overview on AML regulations and best practices. After presenting the research method in Section 3, we introduce the reference model for AML customer identification in Section 4. In the end, we discuss the evaluation approach in Section 5 before we conclude our work in Section 6.

2   Anti-Money Laundering Regulations

In general, the money laundering process consists of three stages: placement, layering and integration [9]. At the first stage illegal money is placed at a bank account. By using an account with a low risk, the money launderer avoids to be detected by authorities. At the layering stage the money is transferred from one to several other accounts, which lowers the chance that law enforcement detects and follows the money flow. At the last stage the money is actually laundered by investing in legal businesses like property or luxury articles [10]. Research indicates that effective AML is a resource-intensive quest and benefits from the collection, maintenance and dissemination of customer related information [11]. Another positive impact on AML can be observed regarding the employee work attitude and training [12].

Laws and guidelines are describing general principles and criteria to establish an AML process and to assign appropriate control activities. This paper covers the German *Money Laundry Law* (GwG) [13], the guidelines published by the *Federal Financial*

Supervisory Authority (BaFin) [16] and the two international financial supervision committees namely *Financial Action Task Force* (FATF) [14] and the *Wolfsberg Group* [15]. The GwG explains various levels of diligence that can be used by financial institutions to identify the customer or guarantee the *Know Your Customer* (KYC) principle. KYC means that financial institutions have to implement a suitable system of internal controls and policies to identify their customers and suspicious transactions [17]. It describes fines for financial institutions if their money laundering detection fails or AML mechanisms have not been implemented [18]. The BaFin publishes lists of non-cooperative countries and territories that can be used to identify single financial institutions which follow the law. Moreover, BaFin suggests guidelines that support the customer identification and the ascertainment of the beneficial owner of a company. The FATF recommends that financial institutions should establish compliance programs to prevent money laundering and counter terrorism [19]. The Wolfsberg Group, an association of eleven global financial institutions, built an industrial standard for compliance [20]. It is known as the Wolfsberg principles and motivates financial institutions to exchange information on AML cases [21]. Financial institutions that cannot establish these principles are disclosed [22]. To ensure that laws and guidelines are met, financial institutions have to establish an organizational framework to identify money laundering cases [23]. The steps of building an AML program are described in Table 1. After identifying and adapting financial regulations and guidelines, risk phenomena are measured [20]. Depending on the results, the AML process is defined usually supported by appropriate software [20]. Many guidelines also suggest to install organizational structures, which should at least encompass a compliance officer, whose task is to decide which countermeasures to take [12].

Table 1. AML program for financial institutions

Phase	Step	Name	Description	Example
Planning	1	Identify regulations	Compliance with legal requirements and official guidelines.	Wolfsberg principles
	2	Derive company guideline	Internal rules for handling money laundering cases.	Code of conduct
	3	Conduct risk analysis	Risk analysis for risk classes related to customer, product or location.	Money transaction
	4	Define process and control activities	Specification of the anti-money laundering process and control activities.	Customer identification
	5	Implement control system	Establishing of working routines and software for monitoring and reporting.	Business application
	6	Define control structure	Organizational function for money laundering reports to top management.	Report
Controlling	7	Define organ. function	Department for handling money laundering cases and conducting risk analyses.	Department
	8	Appoint representative	Head of the anti-money laundering department.	Agent
	9	Conduct employee training	Regular trainings and briefings on relevant regulations and the compliance program.	Seminar
	10	Conduct internal and external audits	Identification of deficiencies of the established compliance program.	Consultant

3 Methodological Approach

This approach integrates the process and data perspective in one reference model for a central AML process. The aim is to develop a reference model for AML exemplified for the CIP. We therefore conducted a literature analysis on common AML regulations as described in Section 2. To holistically capture the CIP and the data-centric nature of its related KYC paradigm a reference model should consider different perspectives. For developing such a multi-perspective reference model we adapted the procedure model by Rosemann and Schütte (1999) [24] because it explicitly defines different perspectives on the problem domain. The model consists of five phases: (1) Problem identification, (2) Design of the reference model frame, (3) Design of the reference model structure, (4) Finalization of the reference model and (5) Application of the reference model. The scope of this paper comprises phase (1) to (4) which are described in Section 4.

In the first phase a problem definition is given to determine modeling objectives, e.g. reducing the model complexity or improve the process efficiency. This requires a detailed process description including relevant regulations, stakeholders and modelling perspectives, e.g. process, data, application or technology [25]. As we are addressing customer identification and KYC in our approach, we will focus on the process and data perspective. The second phase is dedicated to the method applied for process modeling and a first sketch of the process, for which we propose the common *Business Process Model and Notation* (BPMN 2.0) standard. The third phase deals with the actual design of the process model, while phase four is used to enrich the process model with business data and evaluate the model constraints, for which we used the literature analysis. In phase four we conducted two expert interviews with senior IT consultants to complete the process information that has been gained from literature. The experts work for different IT vendors specialized for compliance software in the financial sector. Given their longtime experiences in supporting their customers (i.e. financial institutes) in implementing a successful AML program, we consider them as appropriate experts for our purpose.

4 Reference Model for Anti-Money Laundering

The processes of an institute's AML program can be seen as supporting processes related to the daily routines of the banking business, such as account opening, payments or account management. For instance, each transaction made by a customer will be monitored in terms of AML parameters like the transaction's amount. Further, the AML program can be divided into four different activities. The (i) AML hazard analysis is an upstream process, which analyzes all risks that are related to AML such as customer- or location-related risks. It results in a risk matrix used to assess a certain customer's likelihood to launder money. The (ii) CIP is triggered every time the institute enters a new business relationship with a customer [20]. This implies to follow the KYC principle discussed earlier. Every transaction is monitored during the (iii) *transaction monitoring process* and checked against threshold values depending on the customer's risk

assessment. Every suspicious activity triggers the (iv) *AML case handling* [20]. According to the experts, process (iii) is usually automated. Thus, we excluded it from our reference model. Process (i) is often performed with a global perspective on the institute, where AML risks are a subset of the holistic risk scheme. Although we consider process (i) vital for correct AML, we excluded it due to space limitations. In consequence, we focused on the processes (ii) and (iv) when performing reference modeling. In the following section, we will present the (ii) CIP of an AML program in BPMN and the KYC principles from a data perspective.

4.1 Reference Process Perspective on AML

The main source of information is a literature analysis we performed. On basis of the identified literature the first version of the reference models emerged. Then, two expert interviews were conducted. The resulting models are presented in the following section.

The AML CIP is triggered every time a new customer enters a relationship with the institute. Next to the usual customer data handling, on the one hand financial institutes face strict requirements by law in terms of data complexity, validation and screening. On the other hand, institutes have to assess the customer's risk regarding money laundering in order to adjust their AML monitoring systems and research activities. Three types of sources were used to model the reference process model. First, results from the literature analysis [20, 22, 26, 27] served as a process foundation. Second, laws and directives from different authorities were analyzed [13, 28, 29]. Third, known recommendations and best practices were incorporated into the reference model [14, 15, 30]. For the final reference model we use the BPMN 2.0 notation for the process perspective, which is visualized in Fig. 1.

There are five roles acting in the process, which are represented by the BPMN 2.0 swim lanes. While the customer and a service provider are modeled as a black box lane, the collaboration between three generic departments is modeled. First, the customer's account representative (AR) receives several sources of data from the customer during the *customer identification*. The amount of data depends on the customer's type (see Section 4.2). The institute needs defined internal guidelines for correct and complete customer data collection derived from national or international law. The guidelines also define how to *validate the customer's identity* by using official service providers like *Office of Foreign Assets Controls* (OFAC) or internal identity list. The next step *identify customer's purpose of usage* is important to predict future account movements and relate the customer to a risk cluster. Subsequently, the *AML employee* (AE) uses the validated customer data to assess her or his risk profile. Therefore, the *customer screening* compares the customer's identity with existing AML lists. For instance, the institute has to be aware whether the new customer is a *political exposed person* (PEP) or named in an official sanction list. Most of these lists can be accessed by service providers such as OFAC or *World Check by Thomson Reuters*. The institute should define against which lists the customer has to be checked. Afterwards, the AE *assesses the customer's risk* based on the risk matrix defined by the AML hazard analysis. The results of this risk assessment are then integrated into the monitoring system. The monitoring sys-

tem's threshold values are set depending on the customer's risk profile. The more precise and diligent the customer data is assessed, the more exact the monitoring system works. For instance, when a PEP, whose AML risk is set as high, receives a transaction from a country, which AML list providers rate as highly corrupt, the transaction can be identified as a possible AML case. This case will then be handled by the process (iv) *AML case handling*. The reference model in Fig. 1 also includes a BPMN 2.0 model of the AML hazard analysis with a low level of detail to highlight the dependencies with the customer identification. It is performed by an employee of the risk management department. In general, the institute has to decide which risk phenomena related to the institute contain AML risk and can be measured. For each of these phenomena values are defined, from which scenarios are derived instantiating the different values. These scenarios are assessed regarding their likelihood to represent an AML case. Usually, this is done by defining an AML risk of a scenario from low over medium and high to unacceptable. When a customer's risk is assessed, his profile is related to these scenarios.
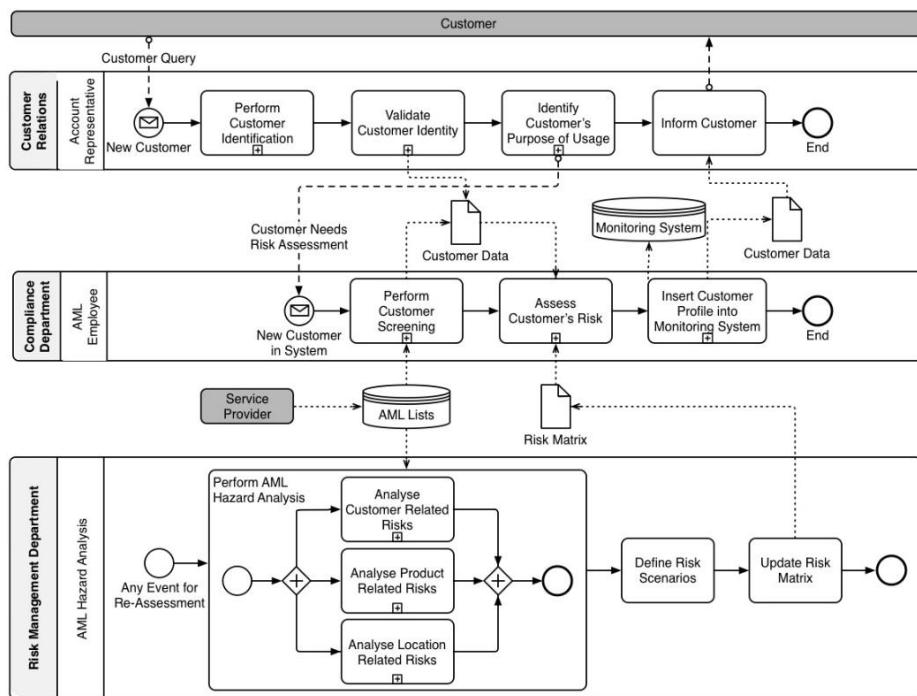

Fig. 1. The CIP reference process in an AML program

4.2 Reference Data Perspective on AML

In the CIP the processes data is customer data, risk matrix and AML lists. After structuring the identified data into these clusters, more detailed data structures were built. This was discussed within the expert interviews, which also served as an information source. Table 2 summarizes the data structure. The findings reveal that most of the analyzed data is related to the customer. Depending on the type of customer (natural or corporate) the required data fields differ. While the identification of private customers is primarily limited to personal information, the research activities of the AR and AE from Fig. 1 are very complex and cost-intense (e.g. to identify the beneficial owners). Furthermore, the type of relationship the customer enters with the institute needs to be distinguished in the stated data fields. The data about the customer and her or his business relationship with the institute are used to assess the customer's risk level. This is based on the prior developed risk matrix. Table 2 shows which risk phenomena should be captured in order to build AML risk categories, e.g. risks related to the customer, countries or even the institute's employees. The AML lists that are used for customer identification are usually provided by third parties (see Section 4.1). The structure in Table 2 serves as a general data view on the CIP. The elaboration of the concrete data objects exceeds the scope of the paper. In general, the complexity of data used for customer identification depends on its context, i.e. the type of customer and its environment. The authors derive a strong dependency between the process and data perspective in the CIP. For instance, the sub-tasks of *validate customer identity* changes with the type of customer. We identify the need to incorporate these dependencies within the reference model. The current reference model uses BPMN 2.0, which is restricted to model the control flow and lacks profound data modeling. Therefore, we suggest the *Enterprise Architectures* (EA) concept as a possible alternative to the current model structure. EAs capture the structure of an organization from different perspectives (e.g. business, data, application and technology layer) and reveal their interdependencies [25]. This would add value for institutes to identify the dependencies not only regarding AML but their whole compliance organization.

5 Evaluation of the Reference Model

The development of a reference model is an iterative process. This process is characterized by different versions of the considered model. The reference model should be evaluated using a validation method, which may lead to adjustments of the reference model [24]. In this work two iteration loops were traversed. Therefore, semi-structured telephone interviews with experts of two different vendors for financial compliance software were conducted [31]. While the first iteration loop concentrated on the process perspective, the second iteration loop focused on the data perspective of the AML program. The experts assessed the reference model as content wise correct, mentioning that the detailed sub-tasks may differ among different institutes. Furthermore, they pointed out that the usage of a complete data structure inside the institutes has a significant influence on the AML program's success. The expert interviews provided most input for the data perspective, which most literature did not discuss in detail.

Table 2. Data perspective of the CIP

Data Object	Contained Information	
Customer Data	A) Natural Person: • Personal data (e.g. name and nationality) • Occupation and industry • Sources of wealth • Relationships to other clients • Data of business relationship	B) Corporate Identity: • Industry and legal form • Places of business (national vs. global) • Beneficial owners • Organizational structure • Data of business relationship
Business Relationship	• Purpose of account or product • Total assets	• Type of account, currency and account opening • Predication of transactions
Risk Matrix	• Customer related • Product related • Country related • Business process related	• Employee related • Transaction related • Information systems related • Derived risk categories
AML Lists	• PEP and related lists • Sanction lists • Black lists	• Internal lists • Country risk lists

6 Conclusion

This work addresses the need of financial institutes to meet regulatory requirements defined on national and international level. Therefore, we present the results of applying multi-perspective reference modeling by Rosemann and Schütte for an AML program based on a literature analysis and expert interviews [24]. By analyzing related literature, legislative texts and recommendations from practitioners' working groups, requirements for an AML program have been derived (RQ1). On the basis of these results and two expert interviews, a reference model was developed capturing process and data perspectives of the CIP in an AML program (RQ2). From theoretical point of view this work contributes how to apply reference modeling. Further, practitioners can benefit from this approach in terms of evaluating their current practice of an AML program. Nevertheless, the authors want to point out that the used data base may not be complete in order to provide a sufficient level of detail of the reference model. Moreover, the interviewed experts may be biased since they represent the interests of their respective enterprise. In consequence, the authors see multiple areas for future research in this topic. First, the data base could be enriched by conducting interviews or workshops at the institutes' in order to gather their current state and identify practitioners' best practices, which would result in applying inductive reference modeling [32]. Second, the proposed reference model could be extended by concepts of EA. Finally, broadening the horizon to other domains of financial compliance like regulatory reporting might identify synergies among different data models, which then would be represented by a holistic reference model.

References

1. Statistisches Bundesamt. (2016) Statistisches Jahrbuch 2015: Kapitel 27: Weitere Dienstleistungen

2. Friedrich Schneider, Ursula Windischbauer. (01/01/10) Money Laundering: Some Facts. Economics of Security Working Paper Series

3. Steffen Höhenberger, Dennis M Riehle, Patrick Delfmann. (2016) From Legislation to Potential Compliance Violations in Business Processes. Simplicity Matters. In: Proceedings of the European Conference on Information Systems (ECIS 2016), Instanbul, Turkey

4. Deloitte Center for Financial Services (2016) Banking reimagined: How disruptive forces will radically transform the industry in the decade ahead

5. Abdullah NS, Indulska M, Sadiq S (2016) Compliance management ontology – a shared conceptualization for research and practice in compliance management. Inf Syst Front. doi: 10.1007/s10796-016-9631-4

6. KPMG International The Cost of Compliance: 2013 KPMG/AIMA/MFA Global Hedge Fund Survey

7. ten Harmsen van der Beek,Wijke, Trienekens J, Grefen P (2012) The Application of Enterprise Reference Architecture in the Financial Industry. In: Aier S, Ekstedt M, Matthes F et al. (eds) Trends in Enterprise Architecture Research: 7th Workshop, TEAR 2012, Barcelona, Spain, October 23-24, 2012. Proceedings, vol 131. Springer, Berlin, Heidelberg, pp 93–110

8. Tambouris E, Kaliva E, Liaros M et al. (2014) A reference requirements set for public service provision enterprise architectures. Softw Syst Model 13(3): 991–1013. doi: 10.1007/s10270-012-0303-7

9. Reuter P, Truman EM (2004) Chasing dirty money: The fight against money laundering. Inst. for Internat. Economics, Washington, DC

10. Angela Samantha Maitland Irwin, Kim-Kwang Raymond Choo, Lin Liu (2012) Modelling of money laundering and terrorism financing typologies. Journal of Money Laundering Control 15(3): 316–335. doi: 10.1108/13685201211238061

11. Kemal MU (2014) Anti-money laundering regulations and its effectiveness. Journal of Money Laundering Control 17(4): 416–427. doi: 10.1108/JMLC-06-2013-0022

12. Hung Kwok TS Anti money laundering ("AML") management and the importance of employees' work attitude. In: 2013 International Conference on Engineering, Management Science and Innovation (ICEMSI), pp 1–4

13. German Goverment (2008) Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz - GwG). https://www.gesetze-im-internet.de/bundesrecht/gwg_2008/gesamt.pdf

14. Financial Action Task Force (2013) National money laundering and terrorist financing risk assessment.http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf

15. Wolfsberg Group (2009) Wolfsberg AML Guidance on Credit/Charge Card Issuing and Merchant Acquiring Activities. http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_Credit_Cards_AML_Guidance_(2009).pdf

16. Federal Financial Supervisory Authority (since 2011) Circulars on Anti-Money Laundering.

https://www.bafin.de/EN/Aufsicht/Geldwaeschebekaempfung/geldwaeschebekaempfung_node_en.html

17. Olatunde Julius Otusanya, Solabomi Omobola Ajibolade, Eddy Olajide Omolehinwa (2011) The role of financial intermediaries in elite money laundering practices: Evidence from Nigeria. Journal of Money Laundering Control 15(1): 58–84. doi: 10.1108/13685201211194736

18. Bundesverband Deutscher Leasing-Unternehmen (2012) Anwendungsempfehlungen zur Geld- wäschebekämpfung bei Leasing-Unternehmen

19. Lagzdins A, Sloka B (2012) COMPLIANCE PROGRAM IN LATVIAS' BANKING SECTOR: THE RESULTS OF A SURVEY. EurInsStud 0(6). doi: 10.5755/j01.eis.0.6.1612

20. Sullivan K (ed) (2015) Anti-money laundering in a nutshell: Awareness and compliance for financial personnel and business. Apress, Berkley

21. Pieth M, Aiolfi G (2003) Anit-Money Laundering: Levelling the Playing Field

22. Verhage A (2009) Between the hammer and the anvil?: The anti-money laundering-complex and its interactions with the compliance industry. Crime Law Soc Change 52(1): 9–32. doi: 10.1007/s10611-008-9174-9

23. Basel Commitee (2005) Compliance and the compliance function in banks.

24. Rosemann M, Schütte R (1999) Multiperspektivische Referenzmodellierung. In: Becker J, Rosemann M, Schütte R (eds) Referenzmodellierung: State-of-the-Art und Entwicklungs-perspektiven. Physica-Verlag HD, Heidelberg, pp 22–44

25. Ahlemann F, Stettiner E, Messerschmidt M et al. (2012) Strategic Enterprise Architecture Management. Springer Berlin Heidelberg, Berlin, Heidelberg

26. Smet D de, Mention A (2011) Improving auditor effectiveness in assessing KYC/AML practices. Managerial Auditing Journal 26(2): 182–203. doi: 10.1108/02686901111095038

27. Tang J, Ai L (2013) The system integration of anti-money laundering data reporting and customer relationship management in commercial banks. J of Money Laundering Control 16(3): 231–237. doi: 10.1108/JMLC-04-2013-0010

28. European Union (2015) DIRECTIVE (EU) 2015/849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=DE

29. US Government (2001) USA Patriot Act. https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

30. Financial Action Task Force (2012) International standards on the combating of money launder- ing and the financing of terrorism and proliferation. The FATF recommendations. http://www.fatf-gafi.org/media/fatf/documents/recommenda-tions/pdfs/FATF_Recommendations.pdf

31. Runeson P, Höst M (2009) Guidelines for conducting and reporting case study research in software engineering. Empir Software Eng 14(2): 131–164. doi: 10.1007/s10664-008-9102-8

32. Loos P, Fettke P, Walter J et al. (2015) Identification of Business Process Models in a Digital World. In: Vom Brocke J, Schmiedel T (eds) BPM - driving Innovation in a digital world. Springer, Cham, pp 155–174