ASSESSING IDENTITY AND ACCESS MANAGEMENT PROCESS MATURITY: FIRST INSIGHTS FROM THE GERMAN FINANCIAL SECTOR

Andre Schrimpf[1]
PricewaterhouseCoopers WPG GmbH, Düsseldorf, Germany

Andreas Drechsler
Victoria University of Wellington, Wellington, New Zealand
and University Duisburg-Essen, Essen, Germany [dual affiliation]
andreas.drechsler@vuw.ac.nz
ORCID: 0000-0002-7026-0241

Konstantinos Dagianis
PricewaterhouseCoopers WPG GmbH, Düsseldorf, Germany

[1] The listed affiliations reflect the authors' affiliations at the time the research was conducted.

Andre Schrimpf holds a master's degree in Information Systems from the University of Duisburg-Essen, Germany and is a Certified Information Systems Auditor (CISA). His working experience comprises auditing of information systems and IT General Controls in the financial sector within the annual audit, and special audits like ISAE 3402 as well as consulting services to comply with regulatory requirements for information systems.

Andreas Drechsler is a Senior Lecturer of Information Systems at Victoria University of Wellington, New Zealand. He holds a doctorate degree in Information Systems from the University of Duisburg-Essen, Germany and has also been a Visiting Scholar at the University of South Florida in the United States. His research interests comprise IS/IT and information security management, agility in projects and organizations, and enterprise architecture. His work has been published in the *International Journal of Project Management*, *Communications of the Association of Information Systems*, *Information Systems and E-Business Management* and other journals as well as numerous conferences.

Konstantinos Dagianis has been working for PricewaterhouseCoopers as a Risk Assurance Director in Financial Services in Düsseldorf, Germany and Los Angeles, USA and led a number of IT audit, IT consulting and digitalization projects in the financial service sector. His skills cover the digitalization of business processes, cyber-security, blockchain, information security management, IT compliance and external and internal audit and data management. Konstantinos is a Business Information Systems graduate, and is a Certified Information Systems Auditor (CISA) and a Certified Information Security Manager (CISM).

This is an Accepted Manuscript of an article published by Taylor & Francis in *Information Systems Management* on 2020-03-18, available online: https://www.tandfonline.com/doi/full/10.1080/10580530.2020.1738601

ASSESSING IDENTITY AND ACCESS MANAGEMENT PROCESS MATURITY: FIRST INSIGHTS FROM THE GERMAN FINANCIAL SECTOR

Abstract

We develop an Identity and Access Management (IAM) process maturity model and provide a first assessment of four organizations in Germany's financial industry. We find that the assessed organizations show merely average IAM maturity levels, and especially lack maturity and compliance in user registration and logging and tracking. Information technology (IT) managers, consultants, and auditors can use the model to (self)-audit, compare, or benchmark IAM process maturity, or identify weaknesses in organizations' IAM processes.

Keywords: identity and access management, IAM, maturity models, IT security, IT auditing, financial sector

INTRODUCTION

Over the recent years, organizations of all types have become increasingly exposed to information technology (IT)-related threats from the outside (e.g., hackers or cyber warfare) and the inside (e.g., fraud or employee negligence) (PWC, 2018). To defend against these threats, one key building block of effective information security is identity and access management (IAM) (Moeller, 2010; Steinberg, Rudd, Lacy, & Hanna, 2011). In a nutshell, effective IAM seeks to ensure that employees are properly identified, that they can only access the systems, functions, or data they need for fulfilling their tasks, and that the necessary checks and balances within IT-supported business processes are upheld. IAM is critical for effective information security and compliance since IAM controls the employees' basic access to IT systems and data, and thus provides the fundamental security layer for additional higher-order information security measures. However, only the various business functions can formulate concrete IAM policies (that specify which employees may or may not access particular systems, functions, or data), but it is IT's responsibility to enforce them. For this reason, effective IAM requires close collaboration between the business and IT (Kerschberg, 2011).

Among the common weaknesses that auditors have noticed within IAM's scope are conflicts arising from a lack of segregation of duties (SoD), inappropriate IAM concepts, or missing reviews of granted access rights (Singleton, 2012). One prominent example here refers to Jérôme Kerviel who caused a loss of $7.2 billion to the Société Générale bank through fraudulent actions that slipped through the net of insufficient, or insufficiently enforced, IAM controls (Sayer & Wailgum, 2008). To counteract such an improper assignment or accumulation of user rights, regulations for several industries in many countries stipulate that a sophisticated and robust IAM process be established at the intersection of business and IT. Beyond the need to comply with regulatory requirements, organizations also should have a self-interest in preventing considerable financial and/or reputational consequences from attacks or data breaches by ensuring adequate IAM process maturity.

Outside of papers with a technical focus and a few notable exceptions (Bradford, Earp, & Grabski, 2014; Rohner, 2013), IAM has not received much research attention. There are some IAM maturity models that are used in practice (Ernst & Young, 2013; Fairchild & Ribbers, 2011; Kuppinger, 2007; Maxim, Cser, Balaouras, Schiano, & Dostie, 2016; Rohner, 2013) to describe evolutionary stages and maturation paths (Becker, Knackstedt, & Pöppelbuß, 2009; Pöppelbuß, Niehaves, Simons, & Becker, 2011) for IAM. However, these IAM maturity models lack, among other things, a rigorous and transparent foundation, so that it is difficult to ascertain whether these models actually represent the current state of good IAM practices, whether they are adequate for the regulations that apply to organizations in a particular country and industry. This limits these models' usefulness for IT management, consultants, and auditors to (self)-audit, compare, or benchmark IAM process maturity or to identify common weaknesses in IAM processes. The lack of transparency also limits these models' adaptability to different contexts and their sustained utility in the light of changing legal or regulatory requirements, or the evolution of IAM practices. Moreover, the lack of academic research on IAM processes leads to little empirically-grounded insights into the state of IAM in organizations and few corresponding guidance for the afore-mentioned practitioner groups.

In this paper, we aim to provide a first step to address this situation by following a design science research (DSR) approach (Gregor & Hevner, 2013; Hevner, March, Park, & Ram, 2004) to answer the following two research questions (Nguyen Hoang, Drechsler, & Antunes, 2019) that follow two distinct knowledge goals:

RQ1: What are the elements of a comprehensive and adaptable model that can be used to assess and benchmark an organization's IAM maturity level for all IAM phases as well as regulatory compliance, and that reflects strict and good IAM practices?

RQ2: What do IAM process maturity levels and common IAM process weaknesses in organizations look like?

These two research questions combine two modes of inquiry in order to contribute to both human knowledge bases (Baskerville, Kaul, & Storey, 2015; Drechsler & Hevner, 2018): Answering the first research question contributes a rigorously designed IAM maturity model to the knowledge base containing applicable knowledge (Λ-knowledge). The model provides full transparency of its foundations and thus can be adapted to changing IAM practices or requirements. Answering the second research question does not only cover the model's evaluation regarding its practical usefulness to assess and benchmark organizations' IAM maturity levels, it also contributes first insights into the state and common weaknesses of IAM processes in organizations to the knowledge base containing descriptive and explanatory knowledge (Ω-knowledge).

Since organizations in different countries and industries are subject to different IAM-related regulatory requirements, the question arises which industry to choose as a focus for answering both research questions. In other words, what industry would allow us to 1) develop an IAM maturity model that has a high combination of applicability and utility, and 2) provide initial insights that would otherwise be difficult to achieve. As further detailed in the Research Methodology section, choosing a highly IT-dependent and heavily regulated industry has the advantage that the required IAM practices are reasonably comprehensive and strict, and the resulting model is therefore generally applicable to less or non-regulated industries as well. In such industries, overall lower maturity levels may well be found to be acceptable, both from a regulatory and an information security management perspective. For this reason, combined with the opportunity of having access to the field, the German financial industry was chosen as the context for this study. A beneficial side-effect to this industry choice is that the answers to RQ2 can provide insights that would otherwise be very challenging to gain. A consequence is, however, that an application to an industry sector with differing IAM-relevant regulations would require an adaptation of the model first.

The remainder of this paper is organized as follows: The second section covers the conceptual foundations which include the IAM process and lifecycle, relevant compliance standards, and maturity models. The third section describes our research approach in greater detail. The fourth section presents the IAM maturity model artifact itself. The fifth section gives an evaluation of the model through an application in four cases and describes our findings. In the sixth section, we discuss the theoretical and practical contributions of our study (including key implications for IAM in and beyond Germany’s financial sector organizations), as well as our research's limitations. The seventh and last section provides a conclusion and an outlook.

CONCEPTUAL FOUNDATIONS

This section covers the conceptual foundations on which we draw in the development of the IAM maturity model. These foundations comprise IAM itself, the IAM lifecycle, the relevant compliance standards affecting IAM in our chosen industry, and existing IAM maturity models.

IAM and the IAM Lifecycle

IAM consists of two components – Identity Management and Access Management – which are closely related. Summarising Moeller (2010) and Steinberg et al. (2011), Identity Management covers all relevant processes that seek to ensure the organizational identity of employees, systems, and technology components. Access Management builds on established identities in controlling and maintaining appropriate access of identities to specific areas, buildings, information systems, and technology, which includes network domains, applications, folders/directories, and data files. IAM is often closely aligned with the user account lifecycle in an organization, which comprises phases such as creating a user account, modifying account information, and eventually deleting or deactivating the account.

Neither existing research, nor the practitioner-oriented literature provides a unified picture of the exact numbers and definition of phases that typically occur within an IAM lifecycle (Bertino & Takahashi, 2011; Ernst & Young, 2013; Fairchild & Ribbers, 2011; ISO/IEC, 2013; Maxim et al., 2016; Steinberg et al., 2011). For this reason, we integrated the existing models into the following six phases:

1. *User registration*: New identities are created, access requests for normal access rights as well as privileged access rights are submitted and approved.

2. *Provisioning*: The requested access rights and the already granted access rights are checked regarding their necessity or segregation of duty conflicts. If these checks are satisfied, the requested access rights are granted.
3. *Enforce user access*: All activities pertaining to the management of the user accounts' secret authentication information, as well as authentication and authorization methods, are part of this phase.
4. *Review*: The normal and privileged access rights are systematically reviewed.
5. *Removal and adjustment*: In appropriate circumstances a phase follows in which identities and access rights are modified, unnecessary access rights are removed, and high privileged or guest access rights are automatically terminated.
6. *Logging and tracking of identities and access*: Continuously, the identity status of every user is checked and monitored, and identities and accesses are logged and tracked.

As illustrated in Table 1, this representation of the IAM lifecycle combines the theoretical and practical aspects of the existing models, and combines the traditionally recognized lifecycle phases of creation, usage, update, and deletion with an ongoing logging phase.

-- Insert Table 1 about here –

We draw on the six phases as analysis areas in our IAM maturity model later on.

IAM-related Compliance Standards

Another foundational aspect of our IAM maturity model refers to the sum of requirements prescribed by various compliance standards in our chosen context, Germany's financial sector. In this context, the regulation is quite extensive and prescribes strong IAM practices (see detailed discussion in the Research Methodology section). The standards comprise local German-specific standards, applicable international standards, industry frameworks, and de facto standards. We selected the sources of the requirements based on their relevance to the financial sector (e.g., MaRisk and PCI-DSS are specifically aimed at financial institutions), to the location (Germany as part of Europe), and to IAM. Note that regulations such as SOX, as part of U.S. law, therefore fall outside our scope. In particular, we considered the standards listed in Table 2. All of these standards and frameworks explicitly contain specific IAM requirements.

-- Insert Table 2 about here --

As these sources comprise the regulatory requirements for a strongly regulated industry, they in sum provide a comprehensive collection of strict IAM practices to inform our maturity model design. As these IAM practices do not concern the core business processes of financial institutions, they are potentially applicable to other industries as well. Note, however, that other industries may have different regulations and therefore also different requirements for IAM practices. While strict, our chosen collection of IAM practices are therefore not universally applicable.

IAM Maturity Models

Maturity models or frameworks commonly function as supportive tools for organizations that are under pressure to create competitive advantage, reduce costs and time to market, and improve quality (de Bruin, Rosemann, Freeze, & Kulkarni, 2005). Maturity models present a theory of stage-based evolution by describing stages and maturation paths for the purposes of description (an as-is assessment), prescription (how to reach a particular maturity level), and comparison (Becker et al., 2009; Pöppelbuß et al., 2011; Pöppelbuß & Röglinger, 2011).

One of the most prominent maturity models is the CMMI (Capability Maturity Model Integrated) which has evolved from the CMM (Capability Maturity Model) (Chrissis, Konrad, & Shrum, 2003). Originally, the CMM allowed the assessment of software development process maturity in five stages: initial, managed, defined, quantitatively managed, and optimizing. The CMMI as the CMM’s successor has kept the five stages but expanded the scope towards process improvement in product and service development as well as other areas. Many other maturity models have also adopted the stage-based format. Hence, Fraser et al. (2002) speak of CMM-type maturity models as one specific and popular form how a maturity model can be structured.

There are also maturity models and frameworks for IAM (Ernst & Young, 2013; Fairchild & Ribbers, 2011; Kuppinger, 2007; Maxim et al., 2016; Rohner, 2013) used in research and practice (Table 3).

-- Insert Table 3 about here --

Based on the assessment in Table 3, we find, however, that none of the extant IAM models is suitable to answer RQ1, primarily due to the lack of transparency and traceability from requirements to the models’ contents. Based on publicly available documentation, the IAM models covered in Table 3 – except for Rohner (2013) – do not give insight into their development process and none of them discuss the regulatory requirements or foundations that inform the models’ IAM coverage and content. Due to this lack of process and content transparency, neither model can be assessed as comprehensive based on their publicly available documentation. Due to the lacking traceability to the underlying IAM sources, model users can also not easily adapt any of the models, e.g. when requirements, IAM standards, or regulations change. We thus require the development of our own model.

RESEARCH METHODOLOGY

To answer RQ1, we developed our IAM maturity model as a DSR artifact (Gregor & Hevner, 2013; Hevner et al., 2004), following literature that provides requirements and processes for maturity model development (Becker et al., 2009; de Bruin et al., 2005; Mettler, 2011). In particular, we combined De Bruin et al.’s (2005) six and Becker et al.’s (2009) eight phases as outlined below. These phases also cover the phases of Peffers et al.'s (2007) generic artifact design process model and Mettler's (2011) maturity model-specific development and application phases. Combining the phases from all these sources allowed us to be as comprehensive as possible regarding our research methodology phases by covering and integrating the extant advice from the literature.

1. Scope and problem definition. We identified the problem as a lack of suitable IAM maturity models (see the section 'IAM Maturity Models' above) to answer our RQ1 and a lack of extant insight into the current state of IAM in organizations as discussed in the Introduction.

The choice of scope for the model development requires addressing the dilemma between general *applicability* across classes of contexts and high *utility* for a particular context. Iivari (2015) presents this dilemma as two general DSR strategies (either design and evaluate in a particular instance and generalize later, or design for a class of contexts and instantiate for the evaluation), but we found the problem to be more nuanced: A broad and general scope would seemingly allow the model to be *applicable* to a wide range of organizations. However, such a scope would also limit the model's *utility* to assess and benchmark IAM maturity of any organization that is required to conform to a particular set of regulatory requirements. To be able to do so, the model would require – potentially substantial – additions and revisions to include those stricter requirements. The resulting assessments would be incompatible with those derived from the application of the original model. A broad and general scope would therefore also not be of high utility for benchmarking organizations across industries.

Conversely, a narrow scope on a more strictly regulated industry increases the model's *utility* to assess and benchmark IAM maturity for that particular industry – but would seemingly limit its *applicability* to that industry in the process. However, if the model comprises good and strict IAM practices that may not be required in less regulated industries, it will still be *applicable* to organizations in those industries; its application may just yield lower maturity levels. Depending on the information security requirements and risk appetite of the respective organizations, such lower maturity levels may well be acceptable and feasible. In contrast to the previous choice of scope, the IAM maturity model could remain the same and therefore allow better benchmarking across industries. Alternatively, the model may be revised by omitting those requirements that are not necessary for a particular industry. While omitting requirements is arguably easier than adding new ones, this option would again have the downside of making the resulting IAM maturity assessments incompatible, thus preventing benchmarks between organizations across industries.

Moreover, one can assume that the general IAM maturity is higher in more strongly regulated industries. Any insights into common IAM processes weaknesses gained in such industries as answers to our RQ2 are therefore potentially generalizable to (and may be even more prevalent in) other industries. Choosing a strongly regulated industry for our research's scope therefore yields not only a widely applicable and useful IAM model but also more profound insights about the current state of IAM maturity as well. A limitation to this choice of scope, however, is the lack of an applicability to industries where a different set of regulations (and not just less) apply. For those industries, the model would have to be adapted to achieve both applicability and utility, and the results would not allow a benchmarking across industries.

Against this backdrop and combined with the opportunity of having access to the field, the German financial industry was chosen as the context and scope for this study. The financial industry heavily relies on IT and forms a key part of any country's critical infrastructure in that it is essential for the country's effective operation and survival. The exposed nature of organizations in the financial sector also means that it is usually among the most strongly regulated ones. In particular, all German organizations in this sector are legally mandated to meet a substantial number of requirements (see Table 2), and are subject to regular compliance audits (IDW AuS 330[1]; §25a(1) German Banking Act). Failure to comply with regulatory requirements can result in financial and reputational damages and, in the worst cases, can lead to mandatory closure of an organization.

2. Design and development. We followed the basic development strategy of combining two existing structures, namely the CMMI's five maturity stages introduced in the previous section and the six IAM stages outlined in Table 1. The resulting model is therefore a model of the CMM type, which is among the most complex and sophisticated forms of maturity models (Fraser et al., 2002).

3. Populate. We populated the 5x6 matrix resulting from this design with the condensed IAM requirements of standards and frameworks relevant to our chosen context. To order the numerous detailed requirements for the IAM processes and the standards and frameworks listed in Table 2 above, we first identified a number of general requirement areas for each of the six IAM phases (Table 4), based on the descriptions of the IAM phases in the relevant IAM literature (ISO/IEC, 2013; Moeller, 2010; Steinberg et al., 2011).

-- Insert Table 4 about here --

Next, we developed a definition or characterization for each requirement area. To illustrate, Table 5 lists the definition of each requirement area for the 'user registration' phase (R1.1 to R1.4). A complete list of requirement area definitions is available in the appendix.

-- Insert Table 5 about here --

[1] IDW stands for "Institut der Wirtschaftspruefer" – the German Institute of Public Auditors. AuS is the abbreviation for Auditing Standard. AuS 330 is documented in (IDW, 2013).

Note that the ‘documentation and policy’ requirement area appears in each IAM phase, due to the need for 1) comprehensive knowledge dissemination as well as strong accountability across the relevant parts of the business and IT organizations, and 2) stating grounds for the compliance assessment during audits. All other requirement areas are specific to one or more IAM phases.

Finally, we analyzed all standards and frameworks mentioned in Table 2 with respect to specific IAM requirements, in order to inform the subsequent IAM maturity model design. To illustrate this part of the process, Table 6 shows the requirements sources catalogue for the requirement area R1.1 (‘documentation and policy’ for the ‘user registration’ IAM phase) taken from Table 4.

-- Insert Table 6 about here --

To assure full transparency and traceability of the sources for each requirement in the final IAM maturity model, the complete requirements catalogue for all IAM phases is available in the appendix.

4. Test and evaluate. The test and evaluation phase comprised three iterations (see Figure 1): two as a formative and one as a summative evaluation (Venable, Pries-Heje, & Baskerville, 2016).

-- Insert Figure 1 about here --

The two formative iterations of the model’s evaluation consisted of two face-to-face discussion rounds with three experienced IT auditors each in order to ensure that we captured all important elements and requirements that organizations need to meet in order to reach a specific maturity level. The participants were all senior consultants or managers working for one of the Big 4 accounting firms with multiple years of experience in auditing and consulting on IAM and other information security-related topics. They were also certified according to CISA (Certified Information Systems Auditor, a certification offered by ISACA) or comparable industry-standard information security and audit certifications. The discussion focused on the evaluation of our IAM maturity model only; the previously analyzed existing IAM models were not discussed since they had been deemed unsuitable before (see also the section ‘IAM maturity models’ above).

In preparation for the first discussion round, the participants were provided with the initial version of the IAM maturity model. This round started with an explanation of the model’s design and the rationale behind it. Afterwards, all cells of the matrix were subjected to an open discussion. The experts’ feedback and critique were documented and informed the subsequent model revision. A key point the experts made was that the initial model version was too general, and thus we revised the model by increasing the level of detail of the provided maturity level descriptions. In addition, a few IAM process characteristics were moved up or down a maturity level, based on the experts’ feedback. The revised model was subjected to a second discussion round with the same experts. This time, they found the revised model to be sufficiently detailed and thus to be potentially useful to fulfil its purpose to assess and benchmark IAM process maturity.

The final and summative iteration of the model’s evaluation took place in four actual audit cases[2] of the same Big 4 accounting firm, in order to evaluate the model’s actual usefulness or utility to assess and benchmark IAM maturity. These four instances were selected to represent a range of typical cases (Gläser & Laudel, 2010) in our chosen context. This range comprised smaller financial industry IT service providers and banks with their own IT

[2] The first and third author were accounting firm employees at the time the research was conducted. The second author – the university representative – had no access to the actual analysis and the underlying audit data, to ensure client anonymity and auditing process compliance.

technology, as well as larger organizations from either group. The organizations in our sample have between less than a hundred and more than several hundred employees, and in revenue they range between a few million and up to several hundred million euros. The smaller firms have a few hundred IT users (such as bank employees), while the larger ones are responsible for several thousand IT users across several sets of customers. Some have a national focus, while others operate internationally as well. Anonymity and confidentiality requirements prevent us from disclosing further details.

The IAM maturity assessment was based on the documented evidence that the case organizations' IT auditors had collected during their most recent annual or special audits as of the fiscal year 2014. This evidence was analyzed with respect to the requirements of the requirements catalogue underlying the IAM maturity model. Subsequently, each IAM phase of each case was classified according to a maturity level in the model.

Beyond their purpose in the IAM maturity model's evaluation, the resulting findings also provide an initial answer to RQ2 (see the evaluation section below for further details).

5. Deploy and publish. After the evaluation, the model was deployed in the auditing service firm that conducted the evaluation for use in various kinds of client engagements as a baseline for assessing IAM processes and procedures. This publication serves as the main means of disseminating the model among the public, comprising researcher and practitioner audiences alike.

6. Maintain and take corrective actions. A future stage is envisaged, in which the maturity model is kept up-to-date, based on on-going changes in IAM requirements in the underlying standards and frameworks, as well as the ongoing development of good IAM practices.

THE IAM MATURITY MODEL

In this section, we show the end result of our design process: the final IAM maturity model (Table 7).

-- Insert Table 7 about here --

The model's vertical axis reflects the IAM lifecycle phases (Table 1). The horizontal axis contains the different maturity levels. Beyond following the established CMMI maturity levels, we expanded level 3 ('defined') to signify that an organization that completely fulfils the requirements for this level has achieved formal compliance to the existing laws and regulations for our chosen context. Each cell contains the key elements and activities that needed to be present for the corresponding maturity level, on the grounds of the requirements for the respective IAM phase as specified in the relevant standards and frameworks (see Tables 2, 4 and 6 as well as the appendix).

EVALUATION AND APPLICATION OF THE IAM MATURITY MODEL

In this section, we present key findings from the practical evaluation of our IAM maturity model in four demonstration cases regarding the process as well as the outcomes of the model's application. We conclude this section with a brief report on further uses the model has seen in actual audit and consulting practice beyond these four cases.

Generally, the level of detail in the IAM maturity model and the underlying requirements catalogue allowed a nuanced assessment of each organization's IAM maturity for each IAM phase. The IAM maturity model as depicted in Table 7 was therefore found to be overall useful and suitable to be a satisfactory answer to RQ1.

However, the process of applying the model in the demonstration cases was not without challenges. First, the documentation supplied by the audited organizations was not sufficiently detailed in all instances to allow a truly straightforward assignment of every IAM phase to a particular maturity level, when contrasted with the contents of the requirements catalogue and the IAM maturity model. This general challenge is unlikely to be resolved, however, as long as both the organizational documentation and the model are provided in a non-formal qualitative form. Second, the assessment of each aspect in each IAM phase in each organization is essentially an act of interpretation by the assessor, and there is no guarantee that – especially in 'borderline' cases – two assessors will agree on a particular assessment. Resource restrictions meant that only a single person performed a through IAM maturity assessment in the four demonstration cases. Lastly, the breadth and depth of both the IAM maturity model and the supplied documentation by an organization is considerable, and an in-depth maturity assessment for a single organization consequently represents a substantial effort. Given the 'interwovenness' of IAM aspects throughout several processes, and that one seemingly minor overlooked aspect can jeopardize the overall IAM effectiveness by unintentionally introducing an exploitable 'loophole', it is again unlikely that this task could be simplified without sacrificing the assessment's effectiveness and validity. In fact, finding these 'loopholes' is one of the main purposes of formal external audits.

Despite these challenges, applying the IAM maturity model allowed us to assess and benchmark the four organizations' IAM maturity, and thus provide some initial answers to RQ2. First, we assessed the average maturity level (AML) of the IAM phases across the organizations (see Table 8). Figure 2 is Table 8's graphical equivalent.

-- Insert Table 8 about here --

-- Insert Figure 2 about here --

We assigned a numerical value to every organization and phase according to the maturity stage (1 = initial, 2 = managed, 3 = defined, 4 = quantitative managed, 5 = optimized). If the respective organization did somewhat better than is required in a specific maturity level, we illustrated the trend towards the next phase by adding .5 to the rating in Table 8. In particular, this means that some requirements (or even a single, but key requirement) of the next phase have been met, but not to the extent of fully reaching the next phase. This allows a more differentiated assessment of AMLs.

The AMLs show that the least mature IAM phase by far, is the ‘logging and tracking user access’ phase. The other five phases are similarly mature, with the ‘user access enforcement’ phase being the most mature, and the ‘user registration’ phase the second least mature overall. The average maturity level lies, roughly, at the defined level (level 3). This value has only limited practical relevance for compliance, because every single deficiency will be reported independently. However, the AML provides an overall indication of IAM maturity in our sample.

A more detailed look at Table 8 and Figure 2 illustrates that the IAM maturity levels of the six phases differ enormously within and across the four case organizations. For instance, for organization 1, we assessed the ‘logging and tracking’ phase to be managed (level 2) without being compliant, while we assessed the ‘enforce user access’ phase to be quantitatively managed (level 4). For each phase past decisions and developments appear to give a possible explanation for the differences in assessment. In this particular case in organization 1, physical security has long been a topic of interest, which explains why the corresponding phase turned out to be more mature than other phases, which have only become important over the last few years prior to the assessment.

Across organizations within our sample, the individual IAM phase maturity levels also differ, sometimes substantially. Different organizations prove to be on different maturity levels for different IAM phases. Possible explanations for this include the necessity to comply with other international regulations (SOX, or MAS TRM), past investment of more resources in security and protection to achieve competitive advantages, or the organizations' security employees' skills and skill levels.

Finally, we assessed the compliance levels for each case and phase (see Table 9).

-- Insert Table 9 about here --

Here, the overall picture is more homogenous. All four organizations showed deficiencies in the 'user registration' and the 'logging and tracking user access' phases, to the extent that these prevented the organizations from being compliant. Note that – contrasting Figure 2 and Table 9 – even if we assessed cases 1 to 3 as being on the 'defined' maturity level, this does not automatically mean that the respective organizations were sufficiently compliant. It is possible to meet most requirements (and, therefore, to be classified as defined) and to lack a single mandatory compliance requirement, thus still to be non-compliant. Further, note that the de facto improvements necessary within the individual phases to reach the next phase, sometimes differ enormously across organizations. Whereas some organizations merely have one or two requirements that they need to meet, and that they can probably implement fairly easily, other organizations might have to restructure entire IAM phases in order to achieve compliance.

We see a possible explanation for the extensive non-compliance regarding the logging and tracking phase in the – at the time of the evaluation – relatively new requirement of having to log all accesses and identities, and other events, as well as to analyze the logs. However, we found the uniform non-compliance in the user registration phase to be more striking and severe, as the employee registration and the creation of identities, roles, and master data is the foundation of all IAM and, in turn, information security. An in-depth analysis of our assessments reveals that the main deviation from the requirements is not in the actual user registration and identity creation, but in the lack of a regular adjustment of user roles, even though almost every organization used role-based access management. In particular, we find that the organizations often implemented the various roles in a concept or policy. Over time, the role concept, or policy, has grown and is modified accordingly. However, this has been done without regular and mandated reviews regarding, for instance, SoD issues or the necessity of each role in users' daily work. This particular issue is also responsible for the first phase being rated as having the second-lowest AML in Table 8. Here, the average values for Table 8 obscure that, within this single phase, we usually found very mature user registration and creation processes combined with rather immature user and role re-adjustment processes.

Beyond the evaluation in these four demonstration cases, the model has also seen regular use in the auditing service firm in client engagements, which further underlines its practical applicability and utility. In addition to its role in determining the client organizations' current IAM maturity, the model is also used as a basis for consulting assignments, e.g. for setting up or enhancing IAM practices. Moreover, the model's practical application has repeatedly highlighted that the complexity of the IAM topic is often underestimated in practice. Here, the model provides an orientation aid that helps to gain and maintain a complete and structured view across all IAM phases.

DISCUSSION AND LIMITATIONS

Answering RQ1, we contribute a comprehensive and adaptable IAM maturity model to the knowledge base of applicable knowledge. The model's evaluation in four audit cases has demonstrated its usefulness to 1) analyze, measure, and assess the maturity of every single phase of an organization's IAM process implementation, 2) to benchmark several organizations after individual assessments have taken place, and 3) to generate insights during the assessment process into reasons for varying maturity levels in organizations beyond the quantitative maturity assessments. The model's sustained usefulness is further demonstrated by its ongoing use in an auditing service firm where it is also used beyond the audit domain in consulting assignments.

The model has a particular emphasis on assessing the extent of regulatory compliance in Germany's financial industry and it is therefore based on a particularly strict set of IAM practices. Since these practices are essentially industry-independent, however, the model can be useful both for assessment and for benchmarking in less regulated industries as well. However, the corresponding results have to be interpreted accordingly in that lower maturity levels may be acceptable in these industries. Nevertheless, there may be regulations in other countries and industries that are not covered by the model or should be contained in a different maturity level, therefore the model's range of applicability has certain limitations.

Our IAM maturity model is also superior to existing ones in several ways (Table 10).

-- Insert Table 10 about here --

Table 10 extends Table 3 and shows the advantages of our model over the others with respect to its overall comprehensiveness, transparency, and rigor. In particular, our model is more *comprehensive* in that it combines the IAM-specific requirements that are part of the many relevant compliance standards and frameworks for a particularly strongly regulated industry (see Table 2) into a single model. The complete requirements catalogue can be found in the appendix. While the other models may have been developed on similar levels of rigor, their lack of *transparency* makes it impossible to assess their rigor. Further, our model's transparency allows for a full *traceability* from requirements to model, enabling future modifications to adapt the model to sustain its utility over time in the light of changing regulatory requirements or different application contexts (industry sectors or countries, for instance) where different regulatory requirements may apply. Our model is also particularly *accessible* in that – at its highest level of abstraction – can fit on a single DIN A3 or Ledger/Tabloid-sized page (Table 7).

In turn, the model's superior comprehensiveness allows a more comprehensive (regarding the breadth and the depth) assessment and benchmark of an organization's IAM processes. The superior transparency and traceability contribute to a reasonably high level of assurance of this comprehensiveness. The superior traceability also allows the model users to adapt the IAM model to changes of and to the application context regarding the IAM-relevant standards and regulations. Finally, the superior accessibility allows someone who is knowledgeable in IAM but not intricately familiar with all the relevant standards and frameworks to use the model, perhaps for an organizational self-assessment. Overall, the IAM maturity model therefore constitutes an improvement in Gregor and Hevner's (2013) design science contribution taxonomy.

IT organizations and their IT service providers can use the model for internal audits, as well as to identify the most pressing areas requiring improvement. IT auditors can use the IAM maturity model as a standardized instrument to assess and, eventually, benchmark their clients' IAM maturity and compliance. Similarly, supervisory authorities can use the model to assess the IAM maturity for an entire sector. In case a compliance assessment for regulations in other countries and industries is sought, the model can be adapted, drawing on the tables provided in the appendix to this paper. Moreover, the model and any derivatives can easily be updated, should new good IAM practices or regulatory requirements arise – again, based on the information and transparency provided by the appendix.

Answering RQ2, we also increase our understanding of IAM in organizations by contributing preliminary insights into the current state of IAM in Germany's financial sector – a sector where one would expect particularly mature IAM processes. Based on the average maturity of, roughly, level 3, none of the four organizations we assessed proved to be particularly immature or particularly mature, however. This illustrates that achieving IAM maturity is an ongoing process. Looking at each IAM phase, our findings show that organizations find it difficult to mature evenly across all phases. Notably, all four organizations failed to meet the compliance requirements for the same two out of six IAM phases. This finding highlights the benefits of complementing traditional maturity assessments that rely on overall numbers and averages with more in-depth assessments that pay particular attention to the fulfilment of critical requirements. This finding further highlights the powerful role that law or standards-based regulatory and compliance requirements and audits can play in effectively ensuring that critical processes (such as IAM) in organizations within critical infrastructures (such as the financial sector) adhere to the key requirements. These standards often also include practical guidelines to achieve the key requirements on which organizations can draw after an assessment or audit.

Beyond the level of the individual organizations, and given that the financial sector is considered to be a critical infrastructure in a country, we consider the overall average (level 3 of 5) assessment of IAM maturity levels to be lower than expected. While it may well be possible that the four cases we analyzed were not representative of the entire sector, we nevertheless would not consider such an IAM maturity level appropriate for any organization in a critical infrastructure sector that predominantly relies on IT for its business processes. Moreover, we find the similarities across the four cases – the major weaknesses and sources for non-compliance being in the areas of user/role re-adjustment as well as logging and tracking user accesses – to be a good indication for at least a potential generalizability to other organizations. We therefore recommend that the IT and business management of German financial organizations (as also of other countries and sectors) pay special attention to these two areas, and to carefully identify and implement improvements. Similarly, we encourage auditors and regulatory institutions in Germany and beyond to pay special attention to these two areas during audits of critical infrastructure organizations. We further encourage future research to be undertaken to validate or extend our findings or to investigate possible reasons for the low maturity. For the other three identified phases, we consider the current state in our analyzed context to be a solid foundation for future continual improvement of the IAM process.

Lastly, we make a methodological contribution to DSR in providing a more nuanced perspective on the dilemma between high utility for a narrow scope or context and broad applicability across several classes of contexts than Iivari’s (2015) two general DSR strategies do. While his two strategies (either design and evaluate in a particular instance and try to generalize later, or design for a class of contexts and instantiate for the evaluation) are still valid starting points for DSR, our experience leads us to view them more as two extremes on a continuum. As a class of contexts can be chosen to be more wide or more narrow (all IT-using organizations, all financial sector organizations world-wide, all German organizations, all German financial sector organizations with their own IT department, …), we see addressing the resulting trade-off in utility and applicability early on in the design process as a crucial step, and the resolution may actually turn out to be not a trade-off. Our case provides an example for a partial resolution, since a narrow context with strict regulations allowed the model to be applicable to and potentially useful in less regulated contexts as well. The resolution is only partial however, since there can be context with a set of differing regulations ‘outside’ a continuum of more or less regulations. For such a context, the IAM model would have to be adapted on a more fundamental level – perhaps to an extent that a rebuild from scratch following our research methodology while relying on the different set of regulations would be the more efficient approach.

Of course, our research also has limitations. First and foremost, we analyzed four cases of an industry that comprised around 2,000 financial institutions at the time the research was conducted (Bundesverband deutscher Banken e.V., 2014). However, the application of the model to the four cases already successfully illustrated its utility to assess and benchmark IAM maturity beyond a single application context. In fact, based on our experience, we do not see a general limitation for the model's applicability to assess and benchmark an organization's IAM maturity. Its utility to assess compliance is limited, however, to our chosen context. A second limitation is that the organizations' IAM maturity assessments were based solely on the documented evidence that the organizations' IT auditors collected during their last annual or special audits as of the fiscal year 2014. Document-based analysis was not corroborated with direct observations within the organizations, or discussions with representatives from the organizations. Therefore, the IAM maturity assessments are to be considered 'best case' assessments, due to the potential difference between formalized policies and actual or situated information security practices (Niemimaa & Niemimaa, 2017). Lastly, due to resource restrictions, only a single person assessed the IAM maturity. It is not inconceivable that a second assessor would have come to differing assessments in some instances.

CONCLUSION AND OUTLOOK

In this paper, we developed an Identity and Access Management maturity assessment model and demonstrated its usefulness to assess and benchmark IAM maturity in four organizations in the German financial sector. We have shown our model to be superior to existing IAM maturity models regarding its comprehensiveness, its transparency and traceability to the relevant IAM frameworks it uses as sources (see appendix), and its accessibility. Further, in applying the model as IAM maturity model in four demonstration cases, we identified recurring IAM process weaknesses, namely in the areas of user registration and logging and tracking user access. These weaknesses might be prevalent in other organizations within and beyond Germany's financial sector; thus further attention to these, in research and practice, is warranted.

In particular, future research in other organizations and across industries is needed to provide a broader foundation for our initial assessment of common IAM weaknesses. Future research concerning the model itself can also assess the extent to which the model's deliberately strict foundations already meet other countries' and industries' regulatory requirements or standards. Applying the model to other, less regulated industries can extend the benchmarking scope beyond our chosen context, confirm or refute the hypothesis whether less regulated industries indeed have less IAM maturity, and identify common IAM weaknesses in those industries. Here, we advise future users, however, to check for additional regulations that may apply in the chosen industry and update the model accordingly before they use it. Lastly, further research can seek other, complementary ways to gain insight into actual organizational IAM practices and their maturity, in order to compensate for our exclusive reliance on audit documentation. A particular challenge of such empirical research would be, however, to deal with socially desirable answers that may be given in response to any of such inquiries.

DISCLOSURE STATEMENT

At the time the research was conducted, the first and third author were employed by the auditing service firm that initiated the research project, provided access to the case materials, and may use the developed maturity model as an assessment framework in their auditing practice. The second author – the university representative – had no access to the case data to ensure client anonymity and auditing process compliance.

ACKNOWLEDGEMENTS

We thank the senior editor, two reviewers, as well as the reviewers and attendees of the 'IT-Sicherheit für Kritische Infrastrukturen' [IT Security for Critical Infrastructures] track of the Multikonferenz Wirtschaftsinformatik [Multi-conference on Business Information Systems] 2016 in Ilmenau, Germany for their very helpful comments and feedback.

REFERENCES

Baskerville, R. L., Kaul, M., & Storey, V. C. (2015). Genres of inquiry in design-science research: Justification and evaluation of knowledge production. *Mis Quarterly, 39*(3), 541–564.

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management—A Procedure Model and its Application. *Business & Information Systems Engineering*, *1*(3), 213–222.

Bertino, E., & Takahashi, K. (2011). *Identity Management. Concepts, Technologies, and Systems* (1st ed.). Norwood: Artech House.

Bradford, M., Earp, J. B., & Grabski, S. (2014). Centralized end-to-end identity and access management and ERP systems: A multi-case analysis using the Technology Organization Environment framework. *International Journal of Accounting Information Systems*, *15*(2), 149–165. https://doi.org/10.1016/j.accinf.2014.01.003

Bundesverband deutscher Banken e.V. (2014). Zahlen, Daten, Fakten der Kreditwirtschaft. Retrieved April 28, 2015, from https://bankenverband.de/media/publikationen/zahlen-daten.pdf

Chrissis, M. B., Konrad, M., & Shrum, S. (2003). *CMMI Guidlines for Process Integration and Product Improvement*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc.

de Bruin, T., Rosemann, M., Freeze, R., & Kulkarni, U. (2005). Understanding the Main Phases of Developing a Maturity Assessment Model. In B. Campbell, J. Underwood, & D. Bunker (Eds.), *Proceedings of the 16th Australasian Conference on Information Systems*. Sydney, Australia.

Drechsler, A., & Hevner, A. R. (2018). Utilizing, Producing, and Contributing Design Knowledge in DSR Projects. In S. Chatterjee, K. Dutta, & R. P. Sundarraj (Eds.), *Designing for a Digital and Globalized World* (pp. 82–97). Springer International Publishing.

Ernst & Young. (2013). *Identity and access management. Beyond compliance*.

Fairchild, A., & Ribbers, P. (2011). Privacy-Enhancing Identity Management in Business. In J. Camenisch, R. Leenes, & D. Sommer (Eds.), *Digital Privacy. PRIME - Privacy and Identity Management for Europe*. Berlin, Heidelberg: Springer-Verlag.

Fraser, P., Moultrie, J., & Gregory, M. (2002). The use of maturty models / grids as a tool in assessing product development capablity. *2002 IEEE International Engineering Management Conference. Proceedings: Volume 1*, 244–249. Cambridge: IEEE.

Gläser, J., & Laudel, G. (2010). *Experteninterviews und qualitative Inhaltsanalyse* (4th ed.). Wiesbaden: VS Verlag.

Gregor, S., & Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly*, *37*(2), 337-A6.

Hevner, A., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105.

IDW (Ed.). (2013). *IDW Auditing Standard: The Audit of Financial Statements in an Information Technology Environment (IDW AuS 330)*. IDW Verlag GmbH.

Iivari, J. (2015). Distinguishing and contrasting two strategies for design science research. *European Journal of Information Systems*, *24*(1), 107–115. https://doi.org/10.1057/ejis.2013.35

ISO/IEC. (2013). *ISO/IEC 27002:2013 Information technology—Security techniques—Code of practice for information security controls*. Geneva, Switzerland: ISO/IEC.

Kerschberg, B. (2011, July 12). Data Security and Identity Access Management. Retrieved April 15, 2014, from http://www.forbes.com/sites/benkerschberg/2011/12/07/data-security-and-identity-access-management/

Kuppinger, M. (2007). Identity Management Roadmap and Maturity Levels. Retrieved February 26, 2015, from https://www.id-conf.com/files/kuppingerroadmap.pdf

Maxim, M., Cser, A., Balaouras, S., Schiano, S., & Dostie, P. (2016). *The Forrester Identity Management and Governance Maturity Model*. Forrester Research.

Mettler, T. (2011). Maturity assessment models: A design science research approach. *International Journal of Society Systems Science*, *3*(1–2), 81–98.

Moeller, R. (2010). *IT Audit, Control, and Security* (1st ed.). Hoboken, New Jersey: John Wiley & Sons.

Nguyen Hoang, T., Drechsler, A., & Antunes, P. (2019). Construction of Design Science Research Questions. *Communications of the Association for Information Systems (CAIS)*, *44*, 332–363.

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: From best practices to situated practices. *European Journal of Information Systems*, *26*(1), 1–20. https://doi.org/10.1057/s41303-016-0025-y

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Pöppelbuß, J., Niehaves, B., Simons, A., & Becker, J. (2011). Maturity models in information systems research: Literature search and analysis. *Communications of the Association for Information Systems*, *29*(27), 505–532.

Pöppelbuß, J., & Röglinger, M. (2011). What makes a useful maturity model? A framework for general design principles for maturity models and its demonstration in business process management. *Proceedings of the Nineteenth European Conference on Information Systems*. Presented at the European Conference on Information Systems, Helsinki, Finnland.

PWC. (2018). The Global State of Information Security Survey 2018. Retrieved January 11, 2019, from PwC website: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

Rohner, P. (2013). Identity Management for Health Professionals. A Method for the Integration of Responsibility, Organization and IT. *Business & Information Systems Engineering*, *5*(1), 17–33. https://doi.org/10.1007/s12599-012-0244-2

Sayer, P., & Wailgum, T. (2008, April 17). What You Can Learn about Risk Management from Societe Generale. Retrieved July 7, 2017, from CIO website: http://www.cio.com/article/2436790/security0/what-you-can-learn-about-risk-management-from-societe-generale.html

Singleton, T. W. (2012). What Every IT Auditor Should Know About Proper Segregation of Incompatible IT Activities. *ISACA Journal*, (Volume 6), 12–14.

Steinberg, R. A., Rudd, C., Lacy, S., & Hanna, A. (2011). *ITIL Service Operation. 2011 edition* (2nd ed.). Norwich: The Stationary Office.

Venable, J., Pries-Heje, J., & Baskerville, R. (2016). FEDS: A Framework for Evaluation in Design Science Research. *European Journal of Information Systems*, *25*(1), 77–89. https://doi.org/10.1057/ejis.2014.36

Figure 1

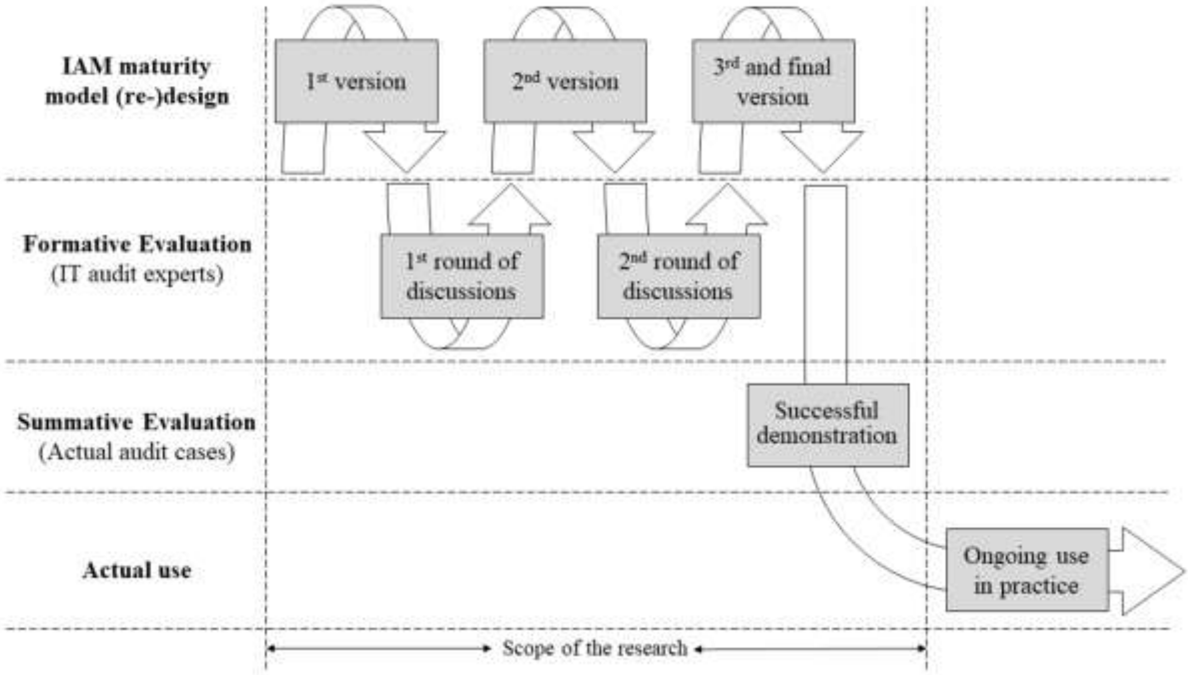
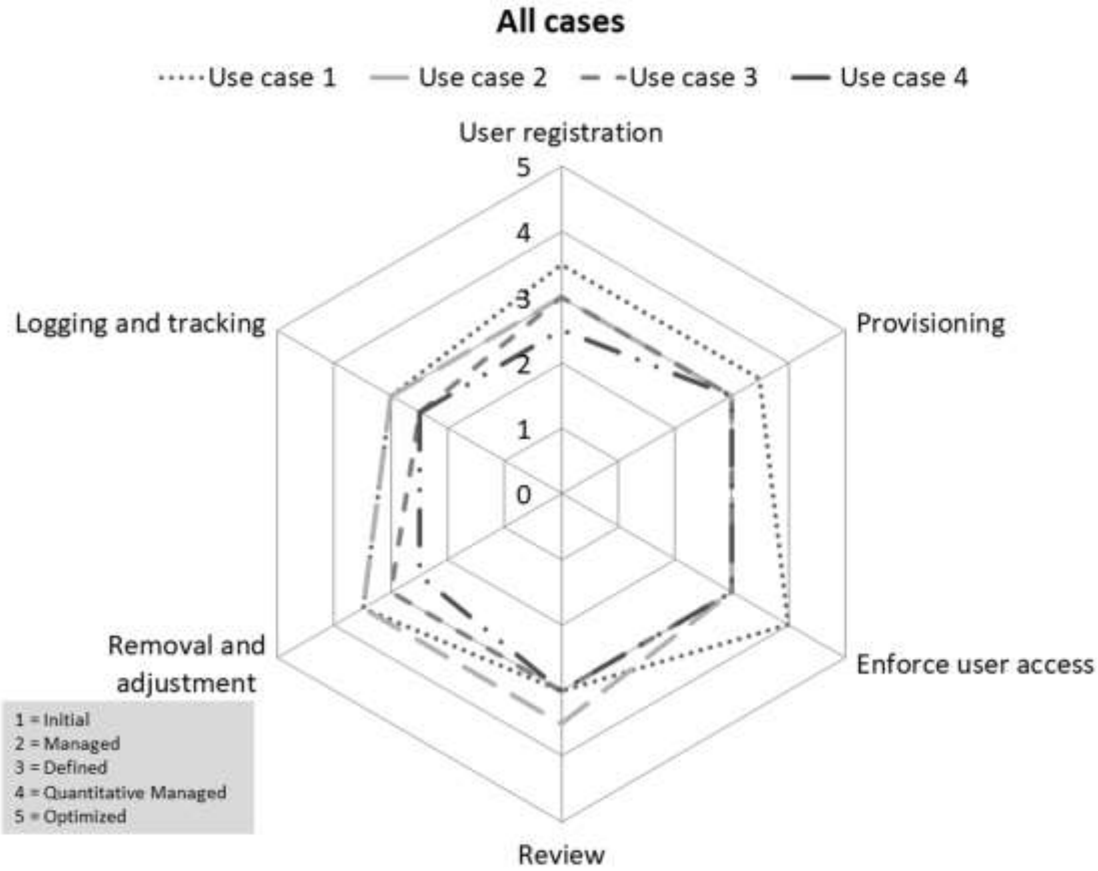


Figure 2



All cases
Use case 1
Use case 2
Use case 3
Use case 4
User registration
Provisioning
Enforce user access
Review
Removal and adjustment
Logging and tracking
5
4
3
2
1
0
1 = Initial
2 = Managed
3 = Defined
4 = Quantitative Managed
5 = Optimized

Table 1

Comparison of IAM phases across the literature

Our phases	**Bertino & Takahashi, 2011**	**Ernst & Young, 2013**	**Fairchild & Ribbers, 2011**	**ISO/IEC, 2013**	**Maxim et al. 2016**	**Steinberg et al. 2011**
1. User registration	Creation	User access request and approve	Authorization Management	User registration	Access request management	Receive request / Provide rights
2. Provisioning	-	Provision	User Management	User access provisioning	User account provisioning (‘joiner’ activities)	Valid request?
3. Enforce user access	Usage	Enforce	Authentication Management	Management of secret authentication information	Administration, Directory infrastructure, Password management	-
4. Review	-	Review and certify	Monitoring and Audit	Review of user access rights	Access recertification, Role management	-
5. Removal and adjustment	Update / Revocation	Reconcile / De-provision	User Management	User de-registration / Removal or adjustment of access rights	User account provisioning (‘mover’ and ‘leaver’ activities), Password management	Remove or restrict rights
6. Logging and tracking	Audit trail	Report and audit	Monitoring and Audit	-	Audit and reporting	Log and track access

Table 2

Laws, standards and frameworks to inform our IAM maturity model design

Name	Description and IAM relevance
Bundesdatenschutzgesetz (BDSG) **(= Federal German Data Protection Act)**	Its purpose is to protect an individual's privacy rights from being impaired through inappropriate handling of their personal data. Section 9 of the BDSG and the appendix describes the requirements for technical and organizational measures to protect data without giving concrete IAM-related options.
IT-Grundschutzkatalog **(= IT Basic Protection Catalogue)**	Published by the German Federal Office for Information Security (BSI), this is a summary of common recommendations and industry-independent information security measures for typical business processes, applications, and IT systems. It also contains several specific IAM-related measures.
Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)	The GoBD are mandatory principles of electronic archiving of accounting and tax information and electronic data access for organizations. The GoBD contain specific requirements across several sections that affect IAM.
Audit Standards (IDW AuS / IDW PS), Accounting Principles (IDW RS FAIT 1-4), IDW Standards (IDW S), Audit and Accounting Notes (IDW PH and IDW RH)	Published by the Institute of Public Auditors in Germany (IDW), several of these principles and standards contain specific requirements for IAM.
MaRisk **(Minimum Requirements for Risk Management)**	This is an important compliance standard for financial organizations published by Germany's supervisory authority (Bundesanstalt für Finanzdienstleistungsaufsicht, BaFin), which, among other things, mandates the appropriate allocation of IT access rights.
Regulations such as BASEL or the Directive 2006/43/EC (also called Euro-SOX)	These regulations do not directly specify IAM measures, but they do require organizations to implement an appropriate internal control system such as the COSO framework (see below).

ISF – The Standard of Good Practice for Information Security	Published by the Information Security Forum, this standard is a comprehensive summary of fundamental and specialized information security controls. Section CF5 describes requirements regarding customer access and the corresponding activities to manage this access. Section CF6 covers access management in general. IAM has a specific section in Section CF8.2.
ISO/IEC 2700x standards	The ISO/IEC standards family 2700x comprises several standards addressing different aspects of an Information Security Management System (ISMS). In particular, several sections of the ISO/IEC 27002 address specific IAM-related requirements (e.g., 5.1.1, 6.1.2, 9.1.1, 9.2).
PCI DSS (Payment Card Industry Data Security Standard)	The PCI DSS was developed to facilitate and improve cardholder data security and the adoption of globally consistent data security measures for all organizations which are in any way involved in payment card or cardholder data processing. Several sections in the PCI DSS contain IAM-related requirements (e.g., 7.1, 8, 9.4.4 etc.). Compared with the previously mentioned standards, these are more precise and on a more readily applicable level.
SANS Institute's Critical Security Controls	These 20 controls and their sub-controls are said to address the most prevalent information security attacks. Most relevant to IAM are CC 4 (controlled use of administrative privileges), CC 14 (controlled access based on the need to know) and CC 16 (account monitoring and control).
COBIT 5	COBIT 5 provides a comprehensive framework for enterprise IT management and governance and comprises 36 processes in five areas. Of particular interest for IAM are the APO07.06, DSS05.04, DSS05.07, and DSS06.03 processes.
COSO Internal Control – Integrated Framework	This framework aims to enable organizations to effectively and efficiently develop and maintain internal control systems, addressing matters of operations, reporting and compliance. The framework provides 17 principles, of which the principles 10 (control activities to mitigate risks), 11 (control activities over technology), and 12 (policies and procedures) are particularly relevant to IAM.
ITIL 2011	ITIL is a good practice framework for IT service management, consisting of five books. The Service Operation book contains a separate Access Management process which is of key interest to IAM.

Table 3

Assessment of extant IAM maturity models

Criterion	**Maxim et al. 2016**	**Ernst & Young, 2013**	**Fairchild & Ribbers, 2011**	**Kuppinger, 2007**	**Rohner, 2013**
Scope/focus	No specific focus, aimed at security & risk leader audience. Compliance is explicitly excluded.	No specific focus mentioned	Businesses (not further specified)	No specific focus mentioned	Hospital information systems
Foundation	Analyst experience and industry input	Not specified	Generic maturity models	Not specified	Expert interviews
Comprehen-siveness	5 maturity stages for nine functional IAM areas. Example evaluation criteria are shown, but not the full model	Five maturity stages with very general stage characteristics. The emphasis lies on steps and capabilities for moving to defined or managed maturity levels	Five maturity stages for five IAM aspects (authorization, user management, authentication, provisioning, monitoring and audit)	Four maturity stages for five IAM aspects (trusted identity, provisioning/ role management, authentication, access, auditing and compliance)	2x7 maturity stages each for responsibility, organizational, and technical IAM concerns
Rigor and Transparency	No transparency over development process, unclear rigor	No transparency over development process, unclear rigor	Only basic insights into development process given, unclear rigor	No transparency over development process, unclear rigor	Rigorous development process, well-documented

Traceability from requirements to model	No insight into the actual requirements and no explicit relations to regulations, standards or frameworks are mentioned	No insight into the actual requirements and no explicit relations to regulations, standards or frameworks are mentioned	No insight into the actual requirements and only very general relations to a few standards and frameworks are mentioned	No insight into the actual requirements and no explicit relations to regulations, standards or frameworks are mentioned	No insight into the actual requirements and no explicit relations to regulations, standards or frameworks are mentioned
Availability for users	Paid report (Forrester Research)	Free PDF white paper	Published in edited book	Free PDF	Published in academic journal
Accessibility to users	Full model not shown, only the nine aspects and the five maturity stages, as well as sample evaluation criteria and results screen	The steps for moving to defined or managed maturity levels consist of an unsorted list of several actions and capabilities for each IAM phase	Two figures along with a textual description of the five IAM aspects and the maturity characteristics for each aspect	Short descriptions for each stage and aspect and high-level roadmaps to move between the stages are given	One figure comprising all 3x2x7 stages with short descriptions, but without maturity stage names

Table 4

Compliance requirement areas for each IAM phase

IAM Phase	Requirement areas
1. User registration	R1.1: Documentation and policy R1.2: Segregation of duties R1.3: Granting process R1.4: Privileged access rights
2. Provisioning	R2.1: Documentation and policy R2.2: Segregation of duties R2.3: Provisioning process R2.4: Privileged access rights
3. Enforce user access	R3.1: Documentation and policy R3.2: Physical access control R3.3: Authentication methods R3.4: Authorization methods R3.5: Enforcement
4. Review	R4.1: Documentation and policy R4.2: Checking and auditing log files R4.3: Review process R4.4: Privileged access rights
5. Removal and adjustment	R5.1: Documentation and policy R5.2: Adjustment process R5.3: Removal process
6. Logging and tracking of identity and access	R6.1: Documentation and policy R6.2: Analyzing and auditing R6.3: Logging and tracking process R6.4: Other logging and tracking measures

Table 5

Definitions for the requirement areas R1.1 to R1.4 (as listed in Table 4)

Requirement area	Definition
R1.1: Documentation and policy	Documentation or documented policy of the user de-/registration process is published, reviewed at regular intervals, known to all and contains a concrete description of the • responsibilities and roles, • provisions, • requirements for identities like uniqueness, • and tasks, and is based on least-privilege, need-to-know and need-to-have.
R1.2: Segregation of duties	Issues pertaining to segregation of duties are appropriately considered and rules are created for handling these issues.
R1.3: Granting process	There is a central granting process for system and network access rights in which access rights and justification of non-standard access rights are assigned by a responsible specialist or senior management. The granting should be based on specific user roles, job descriptions, or activities. Approvals should be documented and archived.
R1.4: Privileged access rights	Additional consideration of privileged access rights, like root or administrator, takes place. The management of these access rights is segregated from the management of normal access rights.

Table 6

Requirement sources for the requirement area R1.1 (as listed in Table 4)

Source	**Relevant documents / sections**
BSI IT-Grundschutz Catalogue	S2.1, S2.7
FAIT 1	K 4.1 Tz. 78
FAIT 3	K 7.2 Tz. 56
MaRisk	AT5 par 3
ISO 27002	5.1.1, 6.2.1, 9.1.1, 9.2
ISF Standard of Good Practice for Information Security	CF5.1.4, CF6.2
PCI DSS	7.1.1, 7.3, 8.1, 8.5, 8.8, 9.4.1, 9.4.2, 9.4.3, 12.5.1
SANS Top 20	CSC 12-8
COBIT 5	APO 13.01, DSS 05.04, DSS 06.03
COSO	Principle 11, Principle 12
ITIL 2011	4.5.7.1

Table 7

The IAM Maturity Model

Note: The full model to be printed on DIN A3 is available as supplementary material

Maturity level **Area**	**Level 1: Initial**	**Level 2: Managed**	**Level 3: Defined and compliant**	**Level 4: Quantitatively managed**	**Level 5: Optimized**

User registration	- Local manual ad hoc registration without approvals - No documentation, no traceability - Double and inconsistent entries owing to redundancy	- Entries can be double but consistent - Sporadic requests of roles and corresponding rights - Organization-wide ID naming convention - Sporadic adjustment of roles - Sporadic segregation of duty pre-assessment - Separated process for logical and physical access controls	- Documented policy and process description - Central registration and request process, limited user group, manual procedures, justification of non-standard rights - Special consideration of privileged access rights - Regular adjustment of roles - Regular segregation of duty pre-assessment	- Central registration, controlled authorization, identification, and approval process, semi-automatic process - Use of self-service functionality to decrease time for request - Tracking all metrics of the central IAM unit e.g. Service Centre or IAM department (call volumes, costs, etc.) - Semi-automatic pre-assessment	- Centrally automated procedures in real time - Segregation of duty pre-assessments automated - Federation-wide and/or cloud-based registration process

Provisioning	- Local manual ad hoc registration without approvals - No documentation, no traceability	Locally limited automated unreliable process - Authoritative source-based provisioning for basic enterprise systems (email, badge, etc.) - Sporadic SoD assessment - Separated process for logical and physical access controls	- Documented policy and process description - Use “real-world” (business-oriented) roles to align access with real-world job function - Restrictive central manual and reliable provisioning process - SoD requirements and rules, manual checking with special measures - Timely creation of access rights - Special consideration of privileged access rights - Reduce the risk of excessive access	- Restrictive central and reliable provisioning process, semi-automatic - SoD rules and detections are semi-automatic - Limited automated process for all sources - Tracking KPIs e.g. form request to provisioning to granted	- Centrally real-time automated procedures - Automatic SoD assessments - Continuous SoD matrix improvements - Federation-wide and/or Cloud-based provisioning process

Enforcing user access	- No authentication and authorization matrices - Single authentication measures - Authorization ad hoc	- Arbitrarily formulated authentication requirements - Methods are provided, adjusted and deleted on request - Authorization matrices defined but not updated - Reduced sign-on methods - Simple measures for physical and logical access controls - Simple password requirements	- Documented policy and process description - Risk-based authentication requirements based on a regular check - Role-based access control and authorization matrices periodically updated - Password management (normal, administrative) - Single sign-on for single applications and technology groups - Enforcement measures for physical and logical access control	- Enterprise Single-Sign-On at least Desktop SSO integrating with multifactor authentication - Automated request-based password reset - Automatic locking of accounts after inactive time - Strong comprehensive enforcement measures	- Authentication requirements based on continuous risk analysis and are continuously improved - Role-based access connected to attributes to cover all possibilities - Centrally real-time control - Federation-wide and/or Cloud-based enforcement process

Review	- No review of granted access rights	- Sporadic reviews - Eventually change lists as result - Separated process for logical and physical access controls	- Documented policy and process description - Centralized review process to eliminate redundancy - Regular annual review of access rights and roles - Display roles to the access rights to increase reviewers understanding - Combined review of logical and physical access rights - Close collaboration to adjustment and removal process - Regular semi-annual review of privileged access rights	- Semi-automatic report creation - More often and semi-automatic review of access rights and roles - Review based on access records, SIEM or other activities including static access rights	- Continuous full automatic review of access rights regarding roles, responsibilities and position - Federation-wide and/or Cloud-based review process

Removal and adjustment	- Sporadic and ad hoc adjustments and removal - No standardized removal after leaving organization	- Adjustment and removal of access rights on request - Sporadic removal after termination	- Documented policy and process description - Semi-automatic reliable adjustment process in case of changes - Semi-automatic reliable removal process after termination etc. - Timely adjustment and removal of access rights	- Automatic adjustment and removal regarding specified rules and restrictions - Risk-oriented removal - Exceptions resolved by automated access adjustment should trigger a user-specific off-cycle access review - Semi-automated process to detect and disable orphan/ dormant accounts on all levels	- Rules for adjustment and removal are continuously improved and tightened - Federation-wide and/or cloud-based adjustment and removal process

Logging and tracking of identity and access	- No logging and tracking	- Logging and tracking of high privileged access rights - Sporadic review of logs if events occurred	- Documented policy and process description - Centralized review process - Logging and tracking of identity and access - Logging and tracking of visitors - Regular randomly review of logs - Logging the main systems - Other tracking measures (e.g. physical escort)	- Full automatic logging and tracking - Report creation - Semi-automatic analyzes and audits - Alert rules for critical immediate events - KPI-reports to compare performance against success criteria - Logging of all systems	- Federation-wide and Cloud-based logging and tracking of all identities and access - Automatic analyzes and audits through e.g. SIEM - Continuously analysing and alerting - Self-learning analysis tools

Table 8

Average Maturity Levels (AML) for each phase and case

	Case 1	Case 2	Case 3	Case 4	AML
User registration	3.5	3	3	2.5	3
Provisioning	3.5	3	3	3	~ 3,13
Enforce user access	4	3	3	3	~ 3,25
Review	3	3.5	3	3	~ 3,13
Removal and adjustment	3.5	3.5	3	2.5	~ 3,13
Logging and tracking user access	3	3	2	2.5	~ 2,63
AML	~ 3,42	~ 3,17	~ 2,83	~ 2,75	

Table 9

Compliance status of the cases in the IAM phases

	Case 1	Case 2	Case 3	Case 4
User registration				
Provisioning	X	X		X
Enforce user access	X	X	X	X
Review	X	X	X	X
Removal and adjustment	X	X	X	
Logging and tracking user access				

Table 10

Comparison of our model with existing IAM maturity models

Criterion	Our model	Maxim et al., 2016	Ernst & Young, 2013	Fairchild & Ribbers, 2011	Kuppinger, 2007	Rohner, 2013
Scope/focus	Organizations in a particular heavily regulated industry (German financial sector), but also applicable to less regulated industries	No specific focus, aimed at security & risk leader audience. Compliance is explicitly excluded.	No specific focus	Businesses (not further specified)	No specific focus	Hospital information systems
Foundation	15 regulatory or industry standards and frameworks	Analyst experience and industry input	Not specified	Generic maturity models and a KPMG technical report from 2001	Not specified	Expert interviews
Comprehensiveness	5 maturity stages for all six IAM phases with several aspects per phase. Each aspect in each phase is explicitly defined.	5 maturity stages for nine functional IAM areas. Example evaluation criteria are shown, but not the full model	5 maturity stages with very general stage characteristics, emphasis lies on steps and capabilities for moving to defined or managed maturity levels	5 maturity stages for five selected IAM aspects (authorization, user, authentication, provisioning, monitoring and audit)	4 maturity stages for five selected IAM aspects (trusted identity, provisioning/ role management, authentication, access, auditing and compliance)	2x7 maturity stages each for responsibility, organizational, and technical IAM concerns

Rigor and Transparency	Rigorous development process, comprehensively documented, full transparency over model foundations	No transparency over development process, unclear rigor	No transparency over development process, unclear rigor	Only basic insights into development process given, unclear rigor	No transparency over development process, unclear rigor	Rigorous development process, well-documented
Traceability from requirements to model	Full traceability from the specific sections of each relevant standard / framework to each aspect in each IAM phase	No insight into the actual requirements and no explicit relations to regulations, standards or frameworks are mentioned	No insight into the actual requirements and no explicit relations to regulations, standards or frameworks are mentioned	No insight into the actual requirements and only very general relations to a few standards and frameworks are mentioned	No insight into the actual requirements and no explicit relations to regulations, standards or frameworks are mentioned	No insight into the actual requirements and no explicit relations to regulations, standards or frameworks are mentioned
Availability for users	Academic journal (once accepted and published)	Paid report (Forrester Research)	Free PDF white paper	Chapter in edited book	Free PDF	Academic journal
Accessibility to users	Model can fit on a single DIN A3 or Ledger/Tabloid-sized page. More detailed information is available in supporting tables, if desired.	Full model not shown, only the nine aspects and the five maturity stages, as well as sample evaluation criteria and results screen	The steps for moving to defined or managed maturity levels consist of an unsorted list of several actions and capabilities for each IAM phase	Two figures along with a textual description of the five IAM aspects and the maturity characteristics for each aspect	Short descriptions for each stage and aspect and high-level roadmaps to move between the stages are given	One figure comprising all 3x2x7 stages with short descriptions, but without maturity stage names