

Identity and Access Management Metrics: A Systematic Review

THOMAS BAUMER, University of Regensburg, Regensburg, Germany and Nexis GmbH, Regensburg, Germany

SASCHA KERN, Nexis GmbH, Regensburg, Germany

LUDWIG FUCHS, Nexis GmbH, Regensburg, Germany

GÜNTHER PERNUL, University of Regensburg, Regensburg, Germany

Identity and Access Management (IAM) challenges organizations, requiring carefully orchestrated processes, technologies, and authorizations. Despite its strategic relevance, we lack a consolidated scientific understanding of IAM metrics and their alignment with IAM goals, like security, compliance, and operational efficiency. This systematic review aims to identify and classify IAM metrics from the literature to support evidence-based IAM. It links collected metrics to IAM goals and audiences. The literature review followed the guidelines of Levy and Ellis. It includes publications from databases SpringerLink, AIS eLibrary, IEEE Explore, ScienceDirect, ACM Digital Library, and relevant cross-referenced publications. The search strategy used keyword combinations, like “Identity and Access Management” and “Metrics,” since 2000. We screened and included publications based on eligibility criteria for relevance, quality, and the explicit presentation of IAM metrics, resulting in sixty publications. The review identified 43 IAM metrics, categorized by seven perspectives derived from IAM goals and processes. Each metric was analyzed by its target, impact on IAM goals, and relevant audiences. The synthesis shows that the literature lacks unified terminology and frameworks for IAM metrics. Future research includes standardizing terminology, linking metrics and targets to maturity levels, and establishing IAM process metrics. The DEVISE project funded this work. It was not registered in PROSPERO.

CCS Concepts: • **General and reference** → **Surveys and overviews**; **Metrics**; • **Security and privacy** → **Security services**; • **Information systems** → **Enterprise information systems**; • **Applied computing** → **Business-IT alignment**; **IT governance**;

Additional Key Words and Phrases: Identity and access management, metrics, measures, governance, data quality

ACM Reference Format:

Thomas Baumer, Sascha Kern, Ludwig Fuchs, and Günther Pernul. 2026. Identity and Access Management Metrics: A Systematic Review. *ACM Comput. Surv.* 58, 8, Article 213 (February 2026), 37 pages. <https://doi.org/10.1145/3788858>

This work was supported by the German Federal Ministry of Education and Research with the project DEVISE. We also want to thank our students: Marco Rauchecker, Johanna Kopp, Nikola Strobel, and Mathis Müller.

Authors' Contact Information: Thomas Baumer (corresponding author), University of Regensburg, Regensburg, Germany and Nexis GmbH, Regensburg, Germany; e-mail: thomas.baumer@ur.de; Sascha Kern, Nexis GmbH, Regensburg, Germany; e-mail: sascha.kern@nexis-secure.com; Ludwig Fuchs, Nexis GmbH, Regensburg, Germany; e-mail: ludwig.fuchs@nexis-secure.com; Günther Pernul, University of Regensburg, Regensburg, Germany; e-mail: Guenther.Pernul@informatik.uni-regensburg.de.



This work is licensed under a Creative Commons Attribution 4.0 International License.

© 2026 Copyright held by the owner/author(s).

ACM 0360-0300/2026/02-ART213

<https://doi.org/10.1145/3788858>

1 Introduction

Despite the availability of mature technologies for enforcing authentication and authorization, organizations encounter challenges in securing and efficiently managing users' access to digital resources [83]. Numerous reports list this as one of the most frequent and critical cybersecurity vulnerabilities, citing insufficient or broken access control [4, 20]. Such vulnerabilities can open the door for both internal and external attackers, allowing them to bypass security mechanisms to conduct malicious actions. Organizations worldwide counter this threat by investing significant shares of their Information Technology (IT) security budgets into Identity and Access Management (IAM) [49]. IAM metrics aid in the management by helping to identify the need for action and assess their effectiveness. While IAM and related problems such as *identity chaos* [48] and the *policy explosion problem* [39] have received broad research attention, to the best of the authors' knowledge, no scientific study exists that holistically examines IAM metrics and their impact on IAM goals. Thus, our research objective is to present an understandable collection of IAM metrics and link them to strategic IAM goals, audiences, and target values. This work presents a literature survey identifying 43 strategic IAM metrics based on seven perspectives derived from strategic IAM goals. We summarize the metrics for each perspective and categorize them by their target, goal interdependence, and audience. We also discuss open challenges for the perspectives, the relevance of IAM goals, understandability, and limitations.

We structure the remainder as follows. Section 2 introduces the background for IAM, metrics, goals, and audiences, while Section 3 presents related work. Using the method outlined in Section 4, we conduct a structured literature review and extract IAM metrics, examining their impact on IAM goals and relevance to IAM audiences in Section 5. Section 6 discusses open challenges for research on IAM metrics and limitations of this study. Lastly, Section 7 concludes.

2 Background

2.1 IAM

IAM deals with the administration of (digital) identities and the secure access of users to digital resources within an organizational context. It manages a range of processes, policies, and technologies designed to ensure that the cybersecurity objectives of authentication and authorization are met without disproportionately limiting operations. The tasks required for this include creating and managing user accounts, verifying user credentials, defining and enforcing adequate authorizations, ensuring regulatory compliance (mandated by a magnitude of regulations, such as Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), Basel III, etc.), and several ancillary activities. IAM also has to interact with business processes that do not originate from IAM: Prominent examples are a person joining the organization, changing department affiliation, or leaving the organization (i.e., joiner, mover, and leaver processes); or infrastructure changes, like onboarding an application, that require an adjustment of the access structures. The scale of these activities quickly requires specialized technologies, such as directories or IAM systems, to process IAM-specific data and processes [45, 51, 140].

2.2 Metrics and Measures

This work focuses on metrics and measures based on NIST guidelines [22, 27, 141] and enriches them with literature about metrics [64, 168]. We introduce their precise meaning in this section, as literature inconsistently uses the terms metrics, measures, measurements, Key Performance Indicators (KPIs), assessments, scores, indicators, and so on.

Most confusion about metrics and measures arises because of their similarity. Both concepts manage numeric values, leading to similar behavior in collecting data, their measurement, addressing

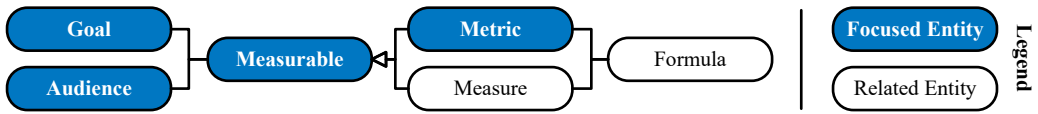


Fig. 1. Metrics and related entities (own depiction, derived from Black et al. [22], Chew et al. [27], and Schroeder et al. [141]).

the audience, visualization, or reporting. However, both concepts differ in their abstraction levels [22]. While a measure objectively measures evidence, a metric interprets a set of measures towards goals on a higher abstraction level. An example of a measure is the password length by counting password characters. While this measure is a standalone property, its actual expressiveness is limited since it could not distinguish a password like “1111111” from a stronger one. In an intuitive process, one might combine the password length with additional measures like the used charsets or its monotonicity to raise expressiveness. Measures are converted into a more expressive (password strength) metric using a formula that determines the selection and weighting of considered measures. These formulas can adapt to a specific context, while the metric concept *password strength* remains objective. While this aggregation raises expressiveness, the standalone measures preserve as drill-down functionalities, allowing decomposing metrics for deeper insights. Furthermore, some fine-tuning of a metric to fit the subjective context is required to maximize its expressiveness. E.g., a dedicated, standalone study [33] compares different formulas for password strength metrics of popular web services. It shows the depth of analyzing even one metric in detail. In contrast, our study focuses on an overview of IAM metrics. It does not detail specific measures and formulas that might support a metric. Figure 1 visualizes measures, metrics, and their relationships. We let measures and metrics inherit from an abstract *measurable* entity for shared properties. The following paragraphs detail these.

Measurables hold shared properties [27] of measures and metrics. A measurable requires a unique *identifier* to enable structured processing. Another property is *goals*. A metric can affect goals positively or negatively. For example, a good evaluation of a password strength metric might support a security goal while hampering operations [70]. The *target* property defines the measurable’s desired value (like min or max). The *audience* property specifies interest groups for measurables. A measurable has a *description* property for readability purposes. Another property is *frequency*, distinguishing between collection and reporting frequency. The frequency property indicates *history*, storing historic values scheduled by the collection frequency. The *automation* property documents the procedure for automatically retrieving the measurable, for example, via a database query. For certain data collection methods, such as interviews or user studies, automation may not be feasible. Finally, the *reporting format* property indicates the desired visualization.

Measures inherit properties described for the measurable entity. Additional properties are evidence, unit, and data source. The *evidence* exactly describes the data collection. It can refer to a database query, a manual user study, and so on. The *unit* property indicates the measure unit. Possible values are percentage, number, and so on. Finally, the *data source* property defines the location from which data is retrieved. It includes databases, tools, organizations, roles, or users.

Formula is a relationship between metrics and measures. It thus contains a set of relationships to *measures* with their *weighting* and *combination rule* for the metric (e.g., by [19]).

Metrics inherit measurables’ properties and are this study’s primary focus. Metrics are calculated using their relationship property *formula*. Additional requirements are defined for IT security [168] and data quality [64]. A metric thus needs to be *bounded*. One metric bound represents the perfectly good (IT security, data quality, etc.), while the other represents the perfectly poor [64]. The *scale* of

a metric is metrical, which includes ratio and interval scaling. That allows for the comparison of metric values. Furthermore, metrics satisfy *quality* based on objectivity, reliability, and validity. (i) Objectivity describes the independence of external influences. E.g., the objectivity of a password strength metric is limited if relevant measures, such as password length or monotonicity, are not accounted for. (ii) Reliability ensures the reproducibility of determining a metric value. E.g., the value of a password strength metric should not change when applied *ceteris paribus*. (iii) Validity means that a metric actually measures the theoretical construct it tries to. For example, if a password strength metric also considers unrelated user satisfaction, its validity decreases. Another requirement is *sound aggregation* so that a metric is consistently applicable for single and multiple data values (e.g., for a single user or a whole department). Finally, a metric must be *economically efficient*, meaning that the costs of defining and (automatically [168]) measuring the metric cannot outweigh the expected payoff.

2.3 Goals and Audiences for IAM Metrics

The performance of an organization is generally determined by the alignment of cost reduction, revenue growth, and quality improvement [111]. We use these three dimensions to structure strategic IAM goals. Cutting unnecessary operational costs, like expenses, efforts, or resources, achieves cost reduction. Delivering value-added products and services that satisfy actual needs leads to revenue growth. Quality improvement helps reduce costs and drive revenue growth by fostering refined, less error-prone processes. IAM aligns with these strategic dimensions by improving quality and reducing costs. However, value addition usually remains unaffected, as IAM supports an organization internally without improving the delivered products or services.

Cost reduction by IAM distinguishes security, compliance, and operations. (i) Security focuses on preventing unauthorized access to valuable resources like trade secrets or customer data. These leaks might jeopardize an organization's trade secrets or damage its reputation. IAM provides basic mechanisms like password management, authentication, authorization, and access logging. (ii) Compliance requirements are imposed by (inter-) national authorities and regulate access management and audit essentials. Penalties apply for violations. For large organizations, avoiding compliance violations and their penalties is a primary driver of IAM capabilities [83]. (iii) Operations aim for smooth processes. Easy and fast access to required resources enables efficient task processing. Missing permissions disrupt important user tasks, wasting the time of individual users or putting entire organizations on hold. For example, Single Sign On (SSO) technology improves operations by easing organization-wide user authentication.

Quality-based goals support cost-based and value-based goals. For this work, we break down IAM quality into further subgoals: IAM processes, identities, IAM policies, and IAM software. These align closely with the domains described by [45] and add identity quality as a further goal. (i) IAM utilizes processes that require high quality in their definition and execution to ensure the desired outcome. These IAM processes span from governance to modeling processes, like identity and policy lifecycles, access reviews, or operational processes (e.g., authentication, self-service, or help desk processes). (ii) The quality of both identities and IAM policies closely ties to the quality of IAM data: Since digital identities are commonly defined as a set of attributes, their quality reduces to the quality of the comprised attributes [117]. (iii) The quality of IAM policies is more complex, as the underlying access control models require consideration [85]. While many authors conceptualize IAM policy quality as data quality with dimensions such as accuracy, complexity, and redundancy, other authors (especially in the eXtensible Access Control Markup Language (XACML) domain) conceptualize it as software quality and focus on features such as evaluation runtime or testing of policy configurations [84, 86]. (iv) Ultimately, IAM software quality is the foundation for its effectiveness, as other quality considerations depend on high-quality software.

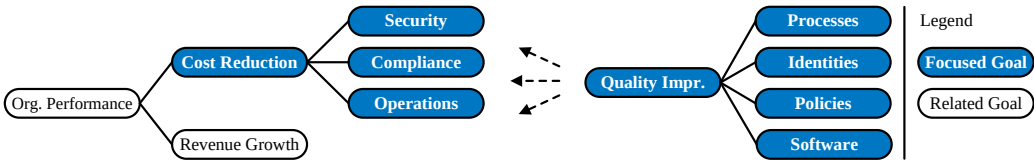


Fig. 2. Strategic IAM goals (own depiction, derived from Oh and Pinsonneault [111], Hummer et al. [70], and Fuchs et al. [45]).

Table 1. IAM Audiences Considered for Our Study

Audience	Description
Governance	A governance audience contains management, compliance, and audit responsibilities.
Identity Admins	Identity admins, such as HR or supervisors, maintain identities throughout the lifecycle.
Policy Admins	Policy admins design and maintain policies, working with policy engineers or owners.
Operations	Operations keep IAM systems running, spanning help desks, DevOps, and provisioning engineers.
Users	IAM users that need access to fulfill their daily duties.

Additionally, the quality of these components is mutually connected to the quality of other elements that are not directly related to IAM, such as data quality, process quality, or information system quality.

Figure 2 lists cost-based (left) and quality-based (right) IAM goals. These goals are drivers that shape IAM strategy [45]. IAM metrics assess the degree of achievement of these IAM goals. They are relevant tools for identifying problems (e.g., outdated identity attributes), selecting and prioritizing investments, and determining the success of IAM efforts.

The audience determines for whom an IAM metric is relevant. In real-world organizations, many actors are involved in or affected by IAM processes. However, neither the job description (e.g., recruiter) nor the organizational affiliation (e.g., department head) is well-suited to describing a role in an IAM context, since these are organization-specific. Instead, we focus on prototypical stakeholder roles to determine the audience of an IAM metric. Depending on their tasks and responsibilities, a person holds one, several, or none of these stakeholder roles. Despite some efforts [27, 45, 69], IAM stakeholders differ in scope and detail across research. This work derives five audience roles: (i) governance, (ii) identity admins, (iii) policy admins, (iv) operations, and (v) IAM users. Table 1 lists these audiences with a short description.

3 Related Work

IAM metrics complement related work covering aligning and integrating metrics in an organizational context, including their goals and strategy. The consequences of misaligned metrics, goals, and strategies include projects that have no impact on organizational strategy or even harm the organization, even though they look good on paper. [15, 65]. Therefore, it is paramount to avoid misalignments for effective decision-making.

Several approaches for integrating metrics in an organizational context have been published. E.g., the renowned Goal Question Metric (GQM) approach [10] uses a cascade to derive expressive metrics based on goals. It starts with conceptual goals, later formulated in greater detail with questions. These questions then allow for a quantitative measurement of the goal by using metrics. This approach can also be extended with the GQM+Strategies approach [11], which underlines the need to align metrics with goals and derive goals from organizational strategies. Similar approaches are the Balanced Scorecard (BSC) [81] and the Model, Measure, Manage Paradigm (M3P) [109]. The BSC compactly presents complex information at a glance for management audiences. The

perspectives of customer, financial, internal business, and innovation and learning connect goals to actions. This approach allows for a strategic perspective on metrics. The M3P framework also puts the metrics in a more holistic context of an organization. It highlights the importance of identifying and understanding strategies and organizational goals to yield effective metrics and measures.

From an IT governance perspective, Control Objectives for Information and Related Technologies (COBIT) [74] and Information Technology Infrastructure Library (ITIL) [150] are well-known complementary frameworks. These frameworks comprehensively align organizational strategies and goals with controls and measurements. Both are widely adopted in the industry, still improved with their versions COBIT 2019 and ITIL 4, and cascade strategies and goals towards metrics. However, these frameworks lack the simplicity of the GQM or the BSC.

These frameworks for integrating metrics thus benefit from (IAM) metric collections, like the IAM metric collection of our survey. Similar yet less comprehensive IAM metric collections are discussed in the literature. Hummer et al. [70] derive performance indicators from IAM goals using the GQM method and evaluate the results by an expert survey. A limitation of this contribution is its lack of comprehensiveness, suggested as future work. Elimity [38] derives eight IAM metrics with measurements from International Organization for Standardization (ISO)27001 and connects them to IAM goals, similar to the ones argued by Hummer et al. [70]. Additionally, the authors suggest a feedback loop based on the metrics. A limitation of this contribution is a missing peer review, and its sole focus is on the ISO27001. Hu et al. [68, 69] contribute via National Institute of Standards and Technology (NIST) publications with access control metrics. An XACML-based architecture, ontology, and responsible principals classify measurements to metrics. While this contribution is more comprehensive than the other contributions covered by this related work section, it lacks the coverage of quality factors. The authors also consider composing the metrics for custom use cases.

With this related work, system architects can implement IAM metrics in organizations. As suggested by Kern et al. [83], governance stakeholders define and prioritize IAM goals aligned with organizational strategy. With this scope, implementers set their objectives and allocate suitable IAM metrics for relevant audiences. Additionally, implementers must align the IAM metrics with their organization by adjusting the weighting and use of context-specific measures. IAM metrics monitor the effects of the tools used and the actions taken. Stakeholders, such as implementers and governance, receive IAM metric reports regularly, e.g., via a dedicated IAM governance dashboard [121].

4 Method

The literature research followed the process proposed by Levy and Ellis [88]. It consists of three phases: (i) The input phase serves to gather a literature body. It includes searching for literature and filtering it for relevant works. (ii) The review step aims to develop an understanding of the obtained literature. It includes the analysis, structuring, comparison, and critical assessment of identified publications. (iii) In the output phase, the obtained knowledge is transformed into a comprehensible presentation that helps answer the original research question. Note that these three phases serve as a structural framework for the research process and are not necessarily carried out in a strictly sequential manner. In our case, the literature review helped to develop a better understanding of the presented concepts, leading to further iterations of the literature search and filtering steps as described in the first phase. To improve transparency and reproducibility, we also report the research criteria using the PRISMA checklist.¹

¹<https://anonymous.4open.science/r/prismachecklist-184B/PRISMA%20Checklist.pdf>

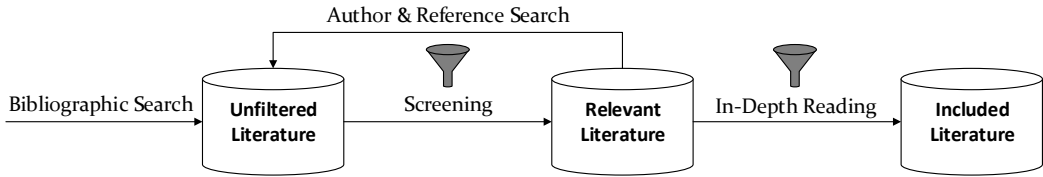


Fig. 3. Applied literature search and filtering process.

Starting with the input phase, we define the scope of included publications as *scientific publications that propose metrics for at least one of the seven identified cost- or quality-based IAM goals*. In a few cases, we also included gray literature if we considered it high-quality and relevant, e.g., standards such as [69]. The literature search began with a bibliographic search. We used permutations of keywords related to IAM (Identity Management, Identity and Access Management, and Identity Governance and Administration) and metrics (Metric, Measurement, Assessment, KPI, and Score). The keywords were mutated to improve result coverage (singular/plural, abbreviated and elongated writing, literal “and” or &). We queried high-quality online databases such as Springer Link,² AIS eLibrary,³ IEEE Xplore,⁴ ScienceDirect,⁵ and ACM Digital Library.⁶ The search filter included the year range 2000-2025. The last access date for all online databases was 07.11.2025.

All publications that were not obviously related to another topic were added to an initial collection of **unfiltered literature**. Each publication in this list was screened, that is, read superficially to determine whether it is relevant to the survey topic. The screening included reading the title, abstract, introduction, and conclusion, and conducting a document search to determine how the identified bibliographic keywords were used. The screening process narrowed the literature body to a list of **relevant literature** by the following criteria: (i) The publication is written in English. (ii) The publication is a paper in a scientific journal or conference, or selected gray literature. (iii) The paper quality is sufficient for general consideration. (iv) The title indicates that the paper measures IAM or characteristics of it. All publications that passed the process were then reviewed in depth to determine whether they should be included in the final list of **included literature**. The final inclusion criteria were: (v) The publication must present metrics relevant to IAM. (vi) Metrics are introduced or presented exclusively in a separate section or subsection. (vii) The paper cites relevant literature itself. Furthermore, we excluded papers that do not add novel insights or that also collect cybersecurity metrics but measure only whether an organization uses IAM, e.g., [147]. In an interactive search and filtering process, we used the collection of *relevant literature* that had passed the initial screening for author and reference search. The resulting publications were added to the list of *unfiltered literature* and processed by the same criteria. We used Google Scholar⁷ for the author and reference search. The literature review was conducted by two people working in parallel, using a shared document collection and standard office tools. During the research process, we found that IAM metrics are not a well-established scientific field. This made the bibliographic search difficult due to insufficient standardization of terminology. Instead, we found author and reference searches more rewarding, yielding high-quality publications that fit the scope of this survey. In total, we collected 60 publications. The literature search and filtering process is summarized in Figure 3.

²<https://link.springer.com/advanced-search>

³<https://aisel.aisnet.org/do/search/advanced/>

⁴<https://ieeexplore.ieee.org/search/advanced>

⁵<https://www.sciencedirect.com/search/entry>

⁶<https://dl.acm.org/search/advanced>

⁷<https://scholar.google.de/>

Table 2. The Seven Perspectives Giving Structure for IAM Metrics Synthesized in the Review

Perspective	Contains metrics for...
Identity Lifecycle	Managing digital identities during their lifecycle, incl. authentication.
Policy Lifecycle	Managing Access Control Policies (ACPs) during their lifecycle.
Management and Governance	Operational and strategic steering of IAM to realize regulations.
Identity Quality	Assessing the quality of digital identities, such as accounts or identities.
IAM Process Quality	Assessing general process quality for any process in IAM.
IAM Policy Quality	Assessing the quality of ACPs, such as roles or attribute-based policies.
IAM Software Quality	Assessing software quality operated for IAM systems.

In the review phase, we structured the list of included publications and analyzed them to gain a deeper understanding. We collected metrics defined in the *included publications* and ordered them according to the addressed IAM goals (compare Section 2.3). We developed a mind map to group metrics and reference measures that implement them. Building on this knowledge base, we synthesized a compilation of IAM metrics in the output phase. It was designed to provide an understandable overview of relevant IAM metrics. For this purpose, we organized them into seven perspectives based on common IAM processes and goals: On the one hand, perspectives derived from the cost-reduction goal comprise the primary IAM process frameworks: the identity lifecycle, policy lifecycle, and a management and governance perspective. On the other hand, we map a perspective for each quality goal, namely identity quality, process quality, policy quality, and software quality. To address the varying levels of abstraction and detail of metrics, measures, and formulae (see Section 2.2), we chose to limit each perspective to a set of relevant, well-understandable metrics. Renowned psychological research shows that a collection of 7 ± 2 concepts remains understandable [96]. Following this scale, we aimed to collect approximately 7 relevant metrics for each perspective and, if applicable, summarize them into a higher-level abstraction. In total, we synthesized 43 metrics that cover 7 IAM perspectives. Table 2 summarizes the seven perspectives for IAM metrics.

We then developed a presentation on the IAM metrics. For this purpose, we developed categorizations to ease understanding and applicability: We traced for each metric its target (minimization, maximization, or neither), its impact on IAM goals (positive, negative, or none), and the addressed audience in the IAM context (compare Section 2.3). We then summarized the metrics textually. Section 5 presents the results for each of the seven perspectives. Each subsection covers a single perspective, with a textual summary of the metrics and a table visualization of their categorization results. Both the affected goals⁸ and audiences⁹ are abbreviated for compact presentation.

5 IAM Metrics

5.1 Identity Lifecycle Perspective

The identity lifecycle defines creating, managing, and deleting digital identities and links to joiner, mover, leaver, or support processes [77, 113]. The lifecycle accompanies an identity in all phases and ensures granting the required but not excessive access. The lifecycle includes a timely (de-)provisioning of identities [13], education for members of an organization, and revoking excessive access. Identities also need operational support, like when requesting missing authorizations or changing credentials. Since authentication schemes use knowledge-based, biometric-based,

⁸Goal abbreviations: cost reduction (COST), security (SEC), compliance (COM), operations (OPS), process quality (PRC), identity quality (ID), policy quality (POL), and software quality (SW).

⁹Audience abbreviations: management and governance (GOV), identity admins (ID), policy admins (POL), operations (OPS), and the end users (USR).

Table 3. Identity and Access Management Metrics: Identity Lifecycle Perspective

Metric	Target	Cost Goal				Quality Goal				IAM Audience				
		COST	SEC	COM	OPS	PRC	ID	POL	SW	GOV	ID	POL	OPS	USR
Readiness	max	–		+	+		+		+	✓	✓		✓	✓
Education	target	–	+		+				+	✓	✓	✓	✓	✓
Orphans	min	+	–	–	+	+	–			✓	✓			
Excess	target		–	–		–	–			✓	✓			
Password Strength	max	–	+	+	–		+		+	✓			✓	✓
Biometric Strength	max	–	+	+	–		+		+	✓			✓	✓
Ownership Strength	max	–	+	+	–		+		+	✓			✓	✓
Multi-factor Strength	max	–	+	+	–		+		+	✓			✓	✓

ownership-based, and multi-factor-based authentication factors, these strengths are measurable [110]. Table 3 summarizes the metrics for this perspective [45, 127].

Readiness describes the degree to which identities are ready and prepared to operate. It includes creating identities and accounts with valid, appropriate authorizations and avoiding unnecessary downtimes for users. Joiner and mover processes of the identity lifecycle or provisioning tasks are thus especially relevant. Suitable measures are the duration upon readiness achievement, error rates for identity, and account creation or costs [19, 70, 137]. Despite the technical dimension, readiness might also encompass the IAM education of the organization’s members, considered in a separate metric. Readiness eases operations and supports compliance by indicating controls for timely authorization grants. However, achieving readiness either requires cost-intensive manual administration or, preferably, providing appropriate automation. As quality side-effects, readiness mainly affects identities and software. Timely propagated identities and accounts benefit the identity quality across multiple applications. Accessible and high-quality IAM software also encompasses means for external administration of their identities. Relevant IAM audiences cover governance, identity admins, operations, and users. Identity admins and users are directly affected by this metric. For operations, lower readiness evaluations signal more prospective support. E.g., expecting more requests for missing access. Finally, a governance audience concerns readiness as an indicator for good IAM controls.

Education expresses IAM awareness and knowledge. Even the best IAM systems render useless for arbitrary authorization grants or authorized yet inappropriate user behavior. All users who require sensible authorizations need at least a basic IAM and IT security training. General user guidance and awareness on *Dos and Don’ts* should be accessible and taught. This guidance includes appropriate password handling [154], recognizing and withdrawing from suspicious situations (e.g., say no), or awareness of sharing protected information on different media (internal communication, personal talks, e-mail, etc.) [163]. More vulnerable groups also require more intensive training. Vulnerable groups include front-liners like help-desk or telephone operators and privileged users. These groups should not hesitate to escalate or report incidents on recognition boldly [163]. The *dual knowledge gap* [43] points out a lack of security specialists with a combined understanding of technologies and security policies, highlighting a need for IAM education. Measures for these aspects include (but are not limited to) user screening, training certificates, expected or blind field tests, training hours, budget on training, or reported incidents attributed to missing training [36, 163]. Timeliness is also a factor, as training needs to start immediately after joining an organization. Ongoing educational efforts counter its decay and keep the gained education up-to-date. In summary, education imposes initial and ongoing educational costs but eases security and operations. Education also affects the IAM software, as usability demands learnability. The target for an education metric is not the maximum. Users should be appropriately aware and trained for IAM to operate safely and securely within their responsibilities. Education is relevant for the full IAM audience spectrum.

Orphans are accounts without a valid owner. In a narrow sense, it applies to accounts without any owner. In a broader sense, however, it also applies to accounts with invalid owners, including inactive, expired, or never used ones. Orphan accounts represent violations of Principle of Least Privilege (PoLP) and compliance. Unused accounts are de facto unnecessary, and missing owners negatively affect the traceability of audit logs. Besides the number of accounts without an owner, measures for orphan accounts may include those never logged on, inactive (after 60 or 90 days, etc.), locked, or expired accounts [19, 38]. Orphan accounts are rooted in a mismatch of the identity lifecycle and deprovisioning. E.g., authentication-based protocols, like Security Assertion Markup Language (SAML) [123], OAuth 2.0 [62], or OpenID Connect [131], may provision accounts on demand and authentication, but do not consider deprovisioning. More recent approaches, like System for Cross-domain Identity Management (SCIM) [90], separate authentication and provisioning contexts, enabling centralized real-time automatism [140], thus eliminating a technical reason for orphan accounts. However, orphans can still originate from improper identity lifecycle processes. E.g., former organization members' access is a common anti-pattern [20]. In summary, orphan accounts indicate security risks, compliance issues, and poor identity and process quality. However, a missing or ineffective deprovisioning process indicates cut implementation costs at the expense of security. Because of their avoidable issues, the target value for an orphans metric should be minimal. The relevant IAM audiences for an orphans metric are foremost governance and identity admins.

Excess refers to users with an intended or unintended high number of authorizations [32]. Sources for excess are granting much access during joiner and mover processes or missing revokes on mover or leaver ones. Following PoLP, intended excess occurs for users with administrative duties or responsibilities for sensitive data. Means for reducing the resulting security risks are Privileged Access Management (PAM), education, or reorganizations. Measures for intended excess target necessary yet excessive user authorizations. Examples include the number of superusers or privileged accounts and users with access to sensitive data or privileged authorizations [36, 38, 151]. Unintended excess occurs on a violation of the PoLP. Due to its unintended nature, this excess negatively impacts the security goal. Measures include outliers with significantly more access than their peers [38]. Orphans or the number or ratio of received approvals for privileged accounts [19] also raise an unintended excess metric. Further measures for excess are the support for specifying and enforcing the PoLP [69], the duration for an (emergency) deactivation of authorizations [70], or the usage for constraints avoiding excess [69]. Despite its positive effect on the security goal, the target value for an excess metric is not minimal, as some excess is intentional. In this sense, careless reduction of authorizations might lead to a shortage, hampering operations. However, unrestricted excess on a non-PoLP-compliant level harms security and compliance while staying neutral to cost reduction and operations goals. From a quality perspective, a higher value for an excess metric indicates a broken identity lifecycle and low-quality authorizations for identities. Finally, the relevant audiences for excess are especially governance and identity admins.

Password Strength is one of the most famous and well-studied IAM metrics. Most users notice this metric during support processes like registration or password change. Approaches for password strength vary in their scaling but assign similar labels like low, medium, and high, used for visualizing in password strength meters [33, 167]. The discussion of password strength effects points back to the seventies [102] and maps it to operations and security goals. From a theoretical perspective, a robust password strength metric indicates security because passwords become harder to crack. Various measures have been proposed [3, 33, 154]. However, humans find strong passwords more difficult to remember, which hampers operations [107]. E.g., users forget their passwords and require costly help-desk or self-service processes afterward [70, 163] or utilize anti-patterns like writing passwords down and leaving the notes nearby their devices. This clash of security and

operations goals is leading to the most recent recommendation of the NIST to lower password strength calculations by enforcing requirements like special characters [54]. Since passwords are a vital cornerstone of modern IT security, a dedicated community of the usable security realm actively studies password-strength aspects, improving security and operations. For example, these studies include serious games to educate about password strength [80], user perception on password expiration [56], or further strengthening passwords [93, 144]. From a compliance perspective, the GDPR [40] demands “*appropriate technical and organizational measures to ensure a level of security appropriate to the risk*” requiring state-of-the-art authentication. A securely stored password is part of identity and software quality. The relevant IAM audience for password strength includes especially the users themselves when they choose their password. However, the overall strength of utilized passwords is also interesting for governance and operations. For governance, robust authentication methods support compliant protection against unauthorized access. For operations, a strong password strength metric hints at raised support expenses.

Biometric Strength describes the security biometric authentication approaches achieve. E.g., Ryu et al. [130] collected 54 performance measures for biometric authentication schemes spanning various categories: functionality, security, usability, operation time, operation cost, satisfaction/acceptance, and stability. Most approaches evaluate their accuracy measured with False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER) which depict effects both on security and operations. The EER levels out both FAR and FRR to achieve an acceptable degree of both security and operations. Ryu et al. [128] point out that other categories like efficiency, usability, security, and privacy need consideration when evaluating biometrics despite the widely applied accuracy. Biometric factors can be a non-intrusive control like keystroke dynamics which would not interrupt a user’s task. Other biometric factors, like fingerprints, interrupt a user’s workflow, which hampers operations. Therefore, users perceive biometric authentication schemes as more usable, supporting operations. However, security suffers from the probabilistic behavior of the error rates and robustness, like for varying input device quality [112]. As for the password strength, the GDPR applies, requiring a state-of-the-art authentication scheme for which biometric factors enhance as an added factor. From a quality perspective, a biometric strength metric aligns with the password strength metric indicating properties for high-quality identities and software. Finally, relevant IAM audiences for the biometric strength are governance for compliance reasons, operations, and the users themselves.

Ownership Strength refers to authentication schemes which are based on *What You Have*. These authentication approaches rely less on the chance of extracting features correctly, like biometrics. Its strength lies in the fact that only an authorized identity controls the transponder for authentication. This assumption is valid for devices such as an Radio-Frequency IDentification (RFID) transponder securely attached to a keychain, in a wallet, a smartphone, or wearables that are always near their owner. Some approaches have attempted to reach perfection in this regard and implanted RFID transponders in living creatures, as done for livestock [76]. However, privacy and security concerns make implants only feasible for identification, rather than authentication, due to cloning, destruction, or unauthorized tag reading issues, which limit their usage [60, 126]. Measures thus include, for example, lost transponders or their resistance to cloning. While requiring the user to authenticate hampers operations and cost reduction, organizations raise security and compliance. Compared to other authentication factors, ownership does not rely on biometric probabilities or remembering passwords, while introducing the risk of losing a transponder. Relevant IAM audiences are the users and operations responsible for managing transponders and governance to ensure compliant authentication.

Multi-factor Strength describes the IT security of combined authentication factors [112]. This approach assumes that a combination of stand-alone authentication factors creates a more effective

Table 4. Identity and Access Management Metrics: Policy Lifecycle Perspective

Metric	Target	Cost Goal				Quality Goal				IAM Audience				
		COST	SEC	COM	OPS	PRC	ID	POL	SW	GOV	ID	POL	OPS	USR
Bypass	min	–	–	–	+	–	–	–	–	✓	✓	✓	✓	✓
Adaptability	max	+	+	+	+			+	+			✓		
Constraints	target		+	+	–		+	+	+	✓	✓	✓		

authentication scheme. Examples include passwords additionally requiring a fingerprint, or passkeys requiring their unlocking on a user device with a secondary factor. Rating and benchmarking factors help identify the relevant ones. Ometov et al. [112] compare factors based on universality, uniqueness, collectability, performance, acceptability, and spoofing. In detail, universality and uniqueness indicate whether all identities can be applied to and be distinguished by the factor. Collectability denotes the ease of data collection. Performance aggregates the property’s accuracy, speed, and robustness. Acceptability relates to usability and gives information about the practical usage of the factor. Finally, spoofing indicates the security of a factor. A multi-factor strength metric aggregates these measures. An emerging research field is adaptive authentication [6], which responds to the given authentication context, enhancing both operations and security goals. It works by either parametric adaptation or structural adaptation. A parametric adaptation fine-tunes the parameters of the authenticator, such as reducing the allowed password attempts when logging in off-site. A structural adaptation changes the system’s structure, like requiring an additional factor for the off-site login example. These adoptions require added measures for security, usability, and user context. These measures include time, location, activity, data sensitivity, hardware measures, and user preferences, among others. For compliance, multi-factor authentication is currently the best practice for state-of-the-art authentication, recommended by the NIST for most applications [54]. Like other authentication factors, interrupting a user’s tasks hampers operations and raises costs. Compared to other authentication schemes, combined factors raise security. Relevant IAM audiences are users, operations, and governance.

5.2 Policy Lifecycle Perspective

Policy lifecycle models are present for Role-Based Access Control (RBAC) [44, 47] and Attribute-Based Access Control (ABAC) [67]. These models include suggestions for introducing policy systems, the derivation and implementation of policies for an organization, the operational maintenance or optimization of policies and systems [83], and final disposal. Table 4 summarizes the IAM metrics *bypass*, *adaptability*, and *constraints* for the policy lifecycle.

Bypass describes any failure in translating a security policy to an authorization or ACP up to an effectively granted access. Any bypass thus undermines the desired IAM state and is detectable from various perspectives. E.g., for a preventive perspective, measures include risk-based assessments of applications, cases for ignoring the actual Policy Decision Point (PDP) or Policy Enforcement Point (PEP), and the IAM system’s verification capabilities as policies might grow into complex constructs leaking authorizations [69]. Additionally, Beres et al. [19] suggest including bypassed approval processes for provisioning. From a detective perspective, Security Information and Event Management (SIEM) systems provide relevant measures, including the number of security incidents due to authorization management [70], unauthorized access to confidential or sensitive data, shared credentials, multiple and quick location changes, off-hour access, and so on [97]. From a corrective perspective, quality is a relevant factor. Measures for this corrective perspective may utilize insights from periodic Access Reviews, as these indicate timeliness and accuracy of ACPs [55]. While bypasses boost short-term operations, they hamper security and compliance. A bypass also indicates poor quality across all traced goals: Policies should appropriately authorize users. Operational

support processes, such as self-service, help users obtain missing authorizations without bypasses, and IAM software should prevent bypasses. Despite its positive effect on operations, the target value for a bypass metric is minimal. Relevant IAM audiences encompass governance, identity and policy admins, and operations.

Adaptability is the capability of an IAM environment to reconfigure its security policies, authorizations or ACPs. Since policies reflect the status quo of an organization, changes in the environment or the organization lead to a policy decay, demanding timely adaptation capabilities. Adaptability is thus a prerequisite for (periodic) improvements [46, 84]. Measures include the system's flexibility and the ease of adapting or distributing updated policies. (i) Flexibility measures hence encompass assessments for the system's ability to cover various use cases [72, 87], features to handle policy changes, situational awareness, or capabilities to combine policies [69]. (ii) Measures for an eased adaptation may include discovery features, steps required to assign authorizations, the degree of syntactic or semantic ACPs specification support, capability and usage of delegation features, or the duration for taking adjustments [32, 69, 70]. (iii) Finally, the updated policies must also be accessible to other system components [13]. Measures for this evaluate the distribution, source management, repositories, and retrieval of the policies [69] or the level of interoperability to communicate with other IAM systems. Connectivity to other systems via standardized protocols, like Lightweight Directory Access Protocol (LDAP) [169], SAML [123], Service Provisioning Markup Language (SPML) [31], SCIM [90], or XACML [125], indicates policy adaptability. Since adaptability enables staying up-to-date with organizational needs, it benefits security, compliance, and operations goals, ultimately leading to cost reductions. From a quality perspective, high-quality IAM software provides adaptability, while policy quality benefits from eased adaptations when required. The target value for an adaptability metric is thus its maximum. Policy admins are the primary audience.

Constraints describe the capability of an IAM system to effectively realize restrictions for the utilized policies, enabling a safer and more secure IAM. E.g., for RBAC models, constraints restrict the number of permissions assigned to a role (cardinality) or enforce Segregation of Dutys (SoDs) [41, 135]. E.g., software engineers might be excluded from testing their written code because they may become professionally blinkered. A static SoD disallows the software engineer from testing any code. A dynamic SoD prevents activating a software engineering and testing role for a given feature simultaneously. A constraints metric can thus encompass measures regarding the number of violations or the modeling capabilities of the IAM system. Various perspectives show the number of violations. E.g., the plain total number of violations found among users [19], security incidents of SoD violations [70], and discrimination for SoD violation types [38]. Furthermore, measures for constraint modeling include the system's support for cardinalities like the PoLP [69], and SoDs like supporting policy admins to decide toxic authorization combinations [38] or providing features to specify dynamic or static SoD rules [69]. The target value for a constraint metric is ambiguous. While violation measures should be minimized, modeling capabilities should meet the organization's needs. From the goals' perspective, a *good* value of the constraints metric benefits security and compliance. For the operations goal, however, an adverse effect originates from slowed down processes when SoDs require multiple parties for participation. From a quality goal perspective, modeling constraints raise the accuracy of identities and policies. The enforcement of these constraints indicates high-quality IAM software. Relevant IAM audiences are governance or identity and policy admins.

5.3 Management and Governance Perspective

While IT governance refers to looking forward and steering an organization's goals and the resulting IT resource assignments, IT management organizes and plans IT resources in the present.

Table 5. Identity and Access Management Metrics: Governance Perspective

Metric	Target	Cost Goal				Quality Goal				IAM Audience				
		COST	SEC	COM	OPS	PRC	ID	POL	SW	GOV	ID	POL	OPS	USR
Completeness	target	–		+		+			+	✓				
Control	max	–	+	+	+	+	+	+		✓			✓	
Traceability	max	–	+	+					+	✓				
Size	target	–	–		–	+			+	✓	✓	✓		✓
Hygiene	max	–	+		+	+	+	+			✓	✓	✓	

IT governance covers effective objectives, while IT management focuses on efficient execution. Therefore, IT governance and management are semantically close to compliance requirements [132]. Metrics to evaluate both concepts are available for IAM systems. These encompass especially *completeness*, *control*, *traceability*, *size*, and *hygiene*, and are summarized in Table 5.

Completeness describes the degree of actually having all requirements imposed on governance applied to an organization. This metric thus indicates the effectiveness of the IAM implementation and is also of interest to an organization’s environment [12]. Measures supporting completeness include the number of successful audits, audit findings [70, 151], updates, and security policies [75]. Furthermore, decision-makers can use capability maturity models [140] or metric collections (as in this work) to assess the current state. The target for completeness is to maximize it while accounting for economic constraints. Completeness benefits compliance goals by ensuring their implementation across processes and software, thereby providing complete support for all organizational needs and technical features. However, it also harms cost reduction as completing all requirements is an ongoing investment for organizations [70]. The relevant IAM audience is primarily governance.

Control evaluates the overall capability to operate an IAM system within an organization. It is closely linked to the completeness metric and compliance regulations. An IAM audience can interpret control as actually controlling an IAM or just its capability. Actual control is traceable by risk and criticality assessments [71], while compliance violations or education show the control capability. Measures for actual control thus include open audit or SoD findings and violations [58, 70, 85, 151], or time-spans to resolve IAM- related incidents, such as an (emergency) ACP deactivation [70, 75]. From the control capability perspective, measures include the amount of IAM entities in compliance [36, 87], the amount and frequency of taken audits, updates, backups, or logs [75, 151], assessments for proper security mechanisms supporting security policies [75], or evaluations of risks and criticality for IAM entities [70, 71, 116, 151]. The target for a control metric is maximum. Controlling IAM can negatively affect cost reduction, while security, compliance, operations, and quality benefit. The relevant IAM audiences for a control metric are governance and operations.

Traceability captures the capability for tamper-proof tracking of authorization and authentication decisions. This capability is rooted in compliance regulations, like SOX [152]. However, understanding the status quo is also a relevant capability, such as during the debugging of ACPs or during security incidents. Attackers might cover their tracks when causing a security incident, raising the need for tamper-proof tracking [108] for a variety of IAM events [124]. Measures include the presence, content, frequency, and accessibility of audit logging or backups [2, 59, 69, 75]. Additionally, the ratio of monitored logs, the number of documented unauthorized access attempts, or the ratio of administrative logs [59]. From a trust perspective [103], missing traceability hints at a loss of control, which regulations mandate to make otherwise undetected threats noticeable [58]. Thus, traceability drives the compliance, security, and software quality goals. However, the metric negatively impacts the cost reduction goal, as software for managing logs must be developed,

purchased, and operated. Therefore, the target value for a traceability metric is its maximum, while maintaining cost efficiency. Relevant IAM audiences are governance and operations.

Size is a relevant metric for the management realm. It indicates the magnitude, feasibility, or requirements of the challenges faced while operating an IAM system. E.g., an organization with hundreds of members requires different approaches for IAM as one with tens of thousands. Thus, size measures include managed entities and their type. E.g., the size of the (IAM) repository is a basis for risk calculations [116]. Elimity [38] cover a broad range of size measures for different RBAC entities and their types, like users (newly created, disabled, or IT users) [151], permissions (total amount or relative to users and roles), roles (organizational, IT, business, technical, etc.), or connected applications. From a quality perspective, a broad consensus on avoiding a role explosion during role mining is present [85], thus limiting the number of roles. Furthermore, role coverage indicates the number of relationships between IAM entities as a measure for a size metric [38, 86]. A bigger size metric indicates raised costs, more risk, and hampered operations, negatively affecting their respective IAM goals. Size, however, also forces processes and software towards more efficiency and quality to work on higher scales. The target value for a size metric is hence ambiguous. It just indicates the magnitude of challenges ahead, but this does not mean it should primarily grow or shrink. The relevant IAM audiences are governance, identity or policy admins, and operations.

Hygiene depicts the amount of futile entities within an IAM system. These entities make operating an IAM system more cumbersome while adding no value. Measures for hygiene thus encompass inactive, empty, or unnecessary IAM entities [19, 38, 151], error rates for processes producing unnecessary data artifacts [70], or undecided changes to IAM entities [38]. Inactive or empty IAM entities thus include orphans like described by the orphans metric before, users without access to any application, roles with no permissions or users, users with permissions assignable by roles, test entities not deleted after the test, and so on. For misaligned processes, error rates on creating IAM entities measure the production of unnecessary entities. Finally, measures for undecided changes also give insights into outdated and unclear IAM data, as hanging reviews for entities impose decay of data quality and raise risks. Hygiene especially benefits identity and policy quality goals for avoiding unnecessary IAM entities. Hygiene also benefits security since decision-makers and admins get a clearer picture of the data managed by the IAM system. Operations and process goals are also positively affected as fewer unnecessary IAM entities improve the efficiency of technology-supported business processes. However, the cost reduction goal is affected negatively as cleanup processes or software for IAM systems require an appropriate setup and ongoing efforts. The target value for a hygiene metric is cost-efficient maximization. Relevant IAM audiences are (identity and policy) admins and operations.

5.4 Identity Quality Perspective

The quality of identities is crucial because it affects not only the results of IAM-related processes and data consumers (such as policy admins or department heads) but also the daily work routines of humans or machines, represented by digital identities in information systems. Pfitzmann and Hansen [117] define identities as a subset of attributes of an individual that at least identifies this individual among any set of individuals. This well-established definition carries two important implications: First, a person has many identities and can choose to use one or another for identification in a particular context. Second, a digital identity is only a set of entity attributes in an information system. The quality of digital identities is hence an instance of the data quality concept. Existing IAM standards and technologies commonly consider two kinds of semantic entities that fit the definition of digital identities: (i) Identity (or user, subject, employee, etc. [86]) datasets are a digital representation of a person. (ii) Accounts represent a digital identity in an application context with an optional association to an identity. Following these definitions and with established data

Table 6. Identity and Access Management Metrics: Identity Quality Perspective (Derived from Cichy and Rass [28])

Metric	Target	Cost Goal				Quality Goal				IAM Audience				
		COST	SEC	COM	OPS	PRC	ID	POL	SW	GOV	ID	POL	OPS	USR
Accuracy	max	+	+	+	+	+	+	+	+		✓	✓	✓	
Timeliness	max	-	+		+		+	+			✓	✓		✓
Accessibility	target		-	-	+				+	✓	✓	✓		
Understandability	max				+		+	+			✓			
Privacy	target		+	+	-					✓				✓

quality theory, we define the quality of digital identities as the *fitness for use* of an identity or account dataset in an IAM context. Table 6 summarizes the identity quality metrics presented in the following.

Accuracy means that identity data accurately represents a real-world state [157]. Common examples of inaccurate identity attributes are misspelled names or outdated addresses. Accuracy is an *intrinsic* quality dimension, so it applies to stored data, not requiring a representation to data consumers or an application context to be valid. Established data quality research considers accuracy one of the most significant data quality dimensions. Maintaining accuracy is a particular challenge [149] since organizations usually utilize a heterogeneous identity management infrastructure (e.g., HR systems, directories, application systems, or staging databases [45]). Accuracy affects the quality of work results for all data consumers, leading to far-reaching repercussions of poor identity accuracy: Deficiencies in identity data can cause incorrect authentication or authorization decisions, inoperable accounts, or process interruptions (e.g., when an approver needs to double-check implausible data before proceeding). As a result, we define the target function of this metric as maximization and consider all IAM goals as positively affected by high accuracy.

Timeliness determines whether data is up-to-date, either in terms of accuracy or being able to serve a task at hand [158]. While timeliness for accuracy is primarily relevant for preventing identity data errors [137, 148], timeliness for serving a task at hand is essential if data loses validity after some time (e.g., real-time status data). For example, outdated identity data is a problem for engineering roles or attribute-based policies, as it also affects correct authorization decisions in real-time [86]. In these cases, the timeliness of identity data greatly benefits policy quality, security, and operations goals. However, keeping identities up-to-date over a longer period requires regular effort, which contrasts with the cost reduction goal. The primary audience for this metric is identity admins and users, as their source. Also, policy engineers rely on identity data, making them a relevant audience.

Accessibility issues can prevent data consumers from working with data for several reasons [149]: IAM infrastructures typically comprise a variety of (identity) data sources with varying data schemas and integration levels [45]. Although this data may be technically accessible, its distribution and lack of standardization are common reasons for data consumers to perceive it as inaccessible or unprocessable. Poor data understandability and inconsistent data representation can have the same effect. Another typical availability issue is incomplete data: Supplementary identity information, such as access logs, can often only be collected to a limited extent or only for parts of the IAM infrastructure [84]. Similarly, large data volumes (e.g., user activity logs) can easily lead to timeliness problems (e.g., when collected in batches over longer intervals). As a result, the computed data is unavailable when needed. At last, authorization constraints are intentionally designed to impair accessibility: both confidentiality and privacy are essential security goals that necessitate restricting access to identity data. The goal is thus not to maximize data accessibility but to manage it accurately based on an organization’s security policy [136]. High accessibility can

positively impact operations but may harm security and compliance goals. Inaccessible identity data can prevent software from functioning correctly (e.g., when relevant steering attributes are unavailable to authentication or authorization mechanisms). The primary audiences for this metric are identity admins and governance teams.

Understandability determines whether data consumers can understand and use identity data [120, 149]. This quality property is crucial when human data consumers need to process unfamiliar digital identities (e.g., policy administrators or decision-makers in a self-service process). Sufficient understandability is a common requirement when IAM processes integrate users throughout an organization (e.g., when applying domain knowledge in approval processes). Examples of improving identity understandability include using display names rather than cryptic identifiers, pseudonyms, or proper descriptions in languages that data consumers understand. Understandability is closely related to data accessibility and can conflict with privacy (e.g., for anonymized or pseudonymized identity processing requirements). Altogether, identity understandability benefits operations and policy quality. The primary audience includes identity admins, ensuring that humans unfamiliar with the identity data can comprehend it.

Privacy refers to the restriction of personal identity data regarding the extent, processing, and moment [161]. In the context of IAM, privacy is relevant for data management and software (see Section 5.7). When working with digital identities, data privacy requirements of users or regulators require consideration [2, 57, 58, 72, 75, 87, 137, 148]. Additionally, numerous regulations and frameworks outline corresponding principles. E.g., the GDPR requires user consent and minimal processing of personal data. Furthermore, personal data requires special security measures that prevent unauthorized reading or leaks. Wagner and Eckhoff [156] present 79 privacy-related metrics regarding uncertainty, data similarity, indistinguishability, time, error, accuracy, adversary's success probability, and information gain or loss. Arsah and Asghar [8] present another compilation covering 16 privacy metrics. Further typical privacy metrics are anonymity and linkability [29, 30]. Identity privacy is vital for compliance, and identity data minimization also benefits security, as only accessible data can be compromised during a security incident. At the same time, missing or inaccessible data hampers processing for productive tasks and negatively affects operations [149]. The goal of IAM is thus not privacy maximization but ensuring *sufficient* privacy under productive operation. Privacy metrics are crucial for governance and user audiences.

5.5 IAM Process Quality Perspective

Processes are crucial for IAM, reflected by the broad range of process frameworks in literature: (i) Identity lifecycle models focus on joining, moving, and leaving identities or (de-)provisioning in distributed application landscapes [77, 113, 127, 162]. (ii) Policy lifecycle models focus on creating, enforcing, maintaining, and deleting policies, their provisioning in a decentralized application landscape, managing and enforcing responsibilities, and requesting missing authorizations [47, 67, 83, 91]. (iii) Finally, IAM capability maturity models include processes such as help desks, approvals, access reviews, and logging and tracking of activities within an IAM infrastructure [113, 140, 162]. Process quality is well-studied by business and information systems research. We thus apply the widely acknowledged Quality Evaluation Framework (QEF) [63] for IAM process quality. QEF defines a quantitative assessment of process quality based on six essential quality dimensions: Performance, efficiency, reliability, recoverability, permissibility, and availability. Table 7 summarizes the metric for this perspective. For simplicity, we use the joiner process as a running example.

Performance determines the efficacy of a process. An example is the process of an identity joining an organization. The new identity should be ready to work as soon as possible. A manager thus needs to request the required authorizations for the identity, involving a manual review of this

Table 7. Identity and Access Management Metrics: Process Quality Perspective (Derived from Heidari and Loucopoulos [63])

Metric	Target	Cost Goal				Quality Goal				IAM Audience				
		COST	SEC	COM	OPS	PRC	ID	POL	SW	GOV	ID	POL	OPS	USR
Performance	max	+			+	+			+	✓			✓	
Efficiency	max	+			+	+			+	✓			✓	
Reliability	max	+	+	+	+	+	+	+	+	✓				
Recoverability	max	+			+	+			+	✓				
Permissibility	max		+	+		+		+	+	✓		✓		
Availability	max	+			+	+			+	✓			✓	

request by the IAM team. (i) The first performance criterion is *throughput* as the number of processed elements in a given period. The example applies throughput to the number of authorization requests the IAM team can review daily. (ii) *Cycle time* refers to the idle time during the preparation and execution of a process. Since cycle time results from process delays, a minimum is desirable. For example, the IAM team may take time to start the authorization check. Added cycle time might occur during the request review. For example, when the IAM team needs to wait for an appointment with an application admin to determine the criticality of a requested permission. Beres et al. [19] provide further meaningful IAM examples for process throughput and lag. (iii) *Timeliness* refers to the time between initiating and terminating a process. While a process starts with perfect timeliness, any delay will reduce it. In the example, the review due time might be specified as two days, meaning that it is sufficient for a manager to order authorizations two days before the join. (iv) Finally, *cost* determines the amount of money required for the process execution. The example includes the hourly personnel costs required for the IAM team to review authorization requests. Operations and cost reduction are positively affected by maximizing process performance. Relevant audiences for process performance are operations and governance, ensuring smooth and cost-efficient processes.

Efficiency relates process performance to its economic viability. (i) *Time efficiency* indicates the ratio of the lead time of a process to the expected execution time. It is thus related to timeliness, but timeliness is an absolute value designed to meet a hard time limit. In contrast, time efficiency looks at the relationship between planned and actual time. For the running example, the expected duration of an activity review is two days. However, the review takes three days to complete. According to the QEF, the time efficiency of the review activity is $2/3 = 66\%$. While timeliness tries to prevent negative outliers altogether, this relative depiction is more helpful for minimizing process runtime. (ii) Similarly, *cost efficiency* is defined as the ratio of planned costs to required costs for an activity execution. Like process performance, maximizing process efficiency is desirable as it positively impacts operations and reduces costs. For the same reasons, the audiences for process efficiency are governance and operations, ensuring smooth and cost-efficient processes.

Reliability concerns the number of failures occurring during process execution in a given period. For example, a created but not activated account of a joining identity may prevent subsequent logins. (i) *Reliableness* describes the probability of failure in a given period. For example, this probability may describe the likelihood of all joining identities having their accounts properly provisioned last month. (ii) *Failure frequency*, in contrast, describes the number of failures in a given period: e.g., the number of joining identities that could not log in last month. High process reliability enables operations to run smoothly and prevents avoidable rectification costs, security risks, and compliance issues. Since failures in lifecycle processes are likely to cause errors for entities, their reliability has a positive impact on identity and policy quality. The key audiences for process reliability metrics are governance and process owners.

Recoverability considers spent failure recovery time. E.g., an admin might spend an hour analyzing reasons for the failed logins and activating an inactive account. The QEF recoverability definition includes two intervals: First, *time to failure* is defined as the time between two failure recoveries (e.g., time since the last failure). Second, *time to recovery* is the time for failure rectification. Building on these variables, *maturity* defines the relative time spent without a failure: E.g., the time for process execution without rectifying errors. Thus, a high maturity leads to recoverability, meaning that processes execute with minimal expenses on failure recovery. High recoverability has a positive impact on operations and cost reduction. Like reliability, the audiences for recoverability are governance and process owners.

Permissibility determines whether the execution of a process conforms to defined authorizations. QEF differentiates between two kinds of authority: (i) *Input authority* determines whether an activity of a process that accesses a process input (e.g., a physical resource or data) is authorized to do so. For example, reviewing authorization orders for a joining identity might require the decider to investigate the joiner's responsibilities. The decider might have authorizations to inspect the joiner's department and job title, but not the authorizations of the colleagues, which is helpful context information [79]. (ii) *Activity authority* determines if an actor that executes an activity is authorized. For example, a responsible decider might not have the security clearance to make authorization decisions for other identities. From the perspective of an individual process, process permissibility should be at 100%, meaning that the process accesses all required resources by responsible actors without violating authorizations. Permissibility has a positive impact on security and compliance goals [19]. The audience for permissibility includes governance and policy admins.

Availability describes the time a process executes as intended. Unlike recoverability, which considers outages caused by failures in process execution, availability is concerned with outages resulting from the unavailability of required inputs. Such input can be physical resources or information required for the process. The *time to shortage* of a process is the time that passes from one shortage to another. The *time to access* refers to the time required until the shortage is remediated. Consequently, QEF defines *availableness* as the ratio of time to a shortage with the total process execution time (time to shortage + time to access): E.g., the ratio of time for a process without a shortage. For example, consider that an IAM self-service is unavailable 10% of the time when a manager orders authorizations. The availability is thus 90%. High availability is crucial for operations, while low availability is a cost driver. Availability is especially relevant for governance and operations, as it contributes to uninterrupted execution.

5.6 IAM Policy Quality Perspective

In IAM, policies commonly refer to Access Control Policies (ACPs). ACPs are machine-processable rules, determining allowed user access [133]. Access Control Models (ACMs), such as RBAC [115, 135] or ABAC [67, 146] define the ACP structure. Consequently, ACP correctness is a prerequisite for correct authorization decisions: While excessive policies pose security risks, overly restrictive ones impede users from doing their work. ACP quality can be considered a quality concept in its own right. Nevertheless, approaches in scientific research place it within a broader framework as an instance of data [84] or software quality [164, 165]. Table 8 summarizes metric alignments of this Section.

Authorization Accuracy describes the precision of authorizations defined by security policies [16]. Two types of errors cause deviations from correct authorizations: excessive and missing authorizations. Excessive authorizations are granted permissions beyond what is necessary, leading to security risks. Missing authorizations refer to a shortage of required authorizations that harms operations. A classical binary confusion matrix can measure authorization accuracy [14]. Still, its measurement is challenging because it requires expert knowledge about which authorizations

Table 8. Identity and Access Management Metrics: Policy Quality Perspective (Derived from Kern et al. [84])

Metric	Target	Cost Goal				Quality Goal				IAM Audience				
		COST	SEC	COM	OPS	PRC	ID	POL	SW	GOV	ID	POL	OPS	USR
Authorization Accuracy	max		+	+	+	+		+		✓		✓		
Evaluation Runtime	min				-	-						✓		
Maintainability	max	+						+		✓		✓	✓	✓
Understandability	max	+		+		+		+		✓		✓		
Complexity	min	-						-				✓		
Redundancy	min	-	-		-	-		-				✓		
Automation	max	+						+				✓		
Policy Attribute Quality	max					+		+				✓		

should have been granted. This requires a profound understanding of a user’s tasks, the implications of each authorization, and the requirements of internal security policies. The permissibility of processes also reflects policy accuracy (e.g., approval accuracy [19]). As authorization accuracy avoids missing authorizations, operations and process quality goals are positively affected. Vice versa, avoiding excessive authorizations benefits security and compliance goals by minimizing risk. Authorization accuracy also influences future policy quality, because policy maintenance often needs to align with existing policies [84]. The audience includes governance and policy admins.

Evaluation Runtime determines the evaluation speed for making an authorization decision [84] and correlates to the response time of an access control system [69]. This quality dimension is essential for XACML [125], a reference architecture with real-time policy evaluation. A high evaluation runtime impedes operations and process quality. The audience for this metric includes policy admins and operations staff.

Maintainability determines the ease of keeping policies up-to-date. It indicates the ability to maintain a high policy quality in the long term and the administrative ease for an access control system [69, 83]. Maintainability, hence, affects the adaptability of an IAM system positively (see the Adaptability metric of Section 5.2). While IAM policy literature often uses the terms maintainability and understandability interchangeably, many sub-metrics aggregate to policy maintainability: understandability, complexity, redundancy, automation, and their attribute quality. Proper maintainability is a prerequisite for cost-efficient and effective policy maintenance, and it correlates positively with cost reduction and policy quality. The audience includes governance and policy admins.

Understandability of ACPs is crucial for their management and maintenance. Humans need to understand the meaning and implications of policies to determine which policies should affect certain subjects or objects. Examples include decisions on self-service requests [66] and the correctness of an existing policy during access reviews [55]. Access control systems often offer verification and compliance support functions [69] or visualization techniques [94] to improve ACP understandability. A commonly named requirement for well-understandable policies is their semantic meaningfulness [32]. RBAC directly addresses semantic meaningfulness, treating roles as semantic constructs that represent real-world concepts, such as department affiliations or security clearances. However, the semantic meaningfulness of policies does not depend on the underlying ACM, since both RBAC and ABAC allow modeling policies with significant or little semantic meaning. While the semantic meaning is difficult to grasp algorithmically, Xu [166] proposes measuring the degree of semantic meaningfulness by assessing their relation with semantically meaningful attributes. Other factors that support coherent policies include low complexity, understandable attributes (such as meaningful names or descriptions), and the absence of errors in existing policies. Policy understandability is vital for policy maintainability and for its impact on IAM processes, such as authorization self-services or access reviews. It hence contributes to cost reduction and

future policy quality. Furthermore, human-understandable policies are crucial for compliance, as auditors will verify samples of them regarding correctness and proper management. The primary audience for this metric includes governance and policy admins.

Complexity determines the number of data elements a policy includes. For example, numerous role mining approaches measure complexity with Weighted Structural Complexity (WSC) [99, 166], a prominent approach in IAM literature. Low complexity helps humans understand policies and makes them easier to process algorithmically. Complexity is a popular metric for maintainability because it is straightforward to evaluate [32]. Thus, role mining algorithms leverage complexity to create *good* policies [85]. Due to its maintenance-related function, low policy complexity is mainly relevant for reducing costs and enabling high policy quality. Its audience includes policy admins.

Redundancy occurs if policies define an authorization more than once. E.g., a user receives authorizations via two roles. Redundancy is problematic because it is a common source of error: If a policy set is updated, redundant definitions can prevent a single change from becoming effective unless the update accounts for redundancy. In the worst case, redundant authorizations prevent revocation in emergencies. Policy redundancies contradict security and IAM process quality goals. Suppose a policy update error occurs because of redundant negative authorizations. In that case, an affected user will not receive the required authorizations, harming the operations goal. Besides their potential for error, redundant definitions introduce unnecessary complexity and confusion during policy maintenance, negatively affecting cost-reduction and policy-quality goals. The audience includes policy admins.

Automation describes the grade a policy adapts to a changing environment without manual updates. While RBAC defines static roles, usually many automation mechanisms update roles when changes occur [84]. Since ABAC policies use attributes, environment changes do not affect them if those changes propagate to the attributes. Thus, policy automation is crucial for operational efficiency and for keeping policies up to date longer. However, automation cannot make maintenance obsolete, as every automation mechanism operates within a limited scope and cannot cope with unexpected environmental changes. Moreover, automation mechanisms are subject to quality considerations, because a policy can be faulty to begin with or completely out of date. Policy automation thus benefits cost reduction and policy quality due to its maintenance support. The audience includes policy admins.

Policy Attribute Quality is vital for maintainability: First, human-understandable attributes (like a descriptive display name or an extended description) are decisive for the human understandability of policies [38, 83]. Second, attributes that define responsibilities (e.g., a policy owner) enable humans to identify a point of contact for questions, such as whether the policy is correct. Third, sufficient policy attribute quality is a prerequisite for policy-related processes (like access reviews), requiring a responsible human decider [86]. As a result, it impacts the quality of IAM processes and the future policy quality. A policy attribute quality metric is primarily relevant for policy admins.

5.7 IAM Software Quality Perspective

IAM technologies offer services supporting IAM activities or processes. They comprise standards and specifications (e.g., SSO standards like Kerberos [106], SAML [123], and OIDC [131] or data exchange standards like SCIM [13, 90], SPML [31], or XACML [125]), software solutions (e.g., directory services), and cyber-physical systems (e.g., biometrics). Mladenova [98] shows that software quality is well-studied, with consensus on metrics [23, 37, 53], reflected by ISO 25010 [78]. We connect the ISO 25010 metrics with IAM. Table 9 summarizes the metric alignments for this section.

Functionality describes whether an IAM system comprehensively, correctly, and appropriately provides its functionalities. For IAM systems, these functionalities need to back governance, identity

Table 9. Identity and Access Management Metrics: Software Quality Perspective (Derived from ISO 25010 [78])

Metric	Target	Cost Goal				Quality Goal				IAM Audience				
		COST	SEC	COM	OPS	PRC	ID	POL	SW	GOV	ID	POL	OPS	USR
Functionality	target	—	+	+	+	+	+	+	+	✓			✓	
Performance	max	—			+	+			+	✓				
Compatibility	target	—	+		+		+	+	+	✓			✓	
Usability	max	—	+	+	+	+	+	+	+	✓			✓	
Reliability	max	—	+		+	+			+	✓			✓	
Security	max	—	+	+	—		+	+	+	✓			✓	
Maintainability	max	—	+		+	+		+	+	✓	✓			
Portability	max	—			+	+			+	✓			✓	

and policy lifecycles, as well as support processes. E.g., Hu and Scarfone [69] dedicate a study to 27 comprehensive and appropriate Access Control (AC) system functionalities, along with the corresponding measures. Examples include auditing, eased ACPs discovery and assignment, integration flexibility, connecting and adapting policies of the IAM software into present systems, granularity and scopes of control, avoidance of bypasses or SoDs violations, or ancillary parts like connectivity (imports and exports), compatibility, verification functionalities, user interfaces, and Application Programming Interfaces (APIs), and so on. For the identity lifecycle, the presence of functionalities for the joiner, mover, and leaver processes alongside support processes like authentication (knowledge-, biometric-, ownership, or multi-factor-based [110]), help desks, or self-services are a basis for measuring the functionality of an IAM system [45, 113]. Furthermore, incorrectly implemented IAM functionalities might lead to trust issues [103]. Following this concept, bug trackers or the Common Vulnerability Scoring System (CVSS) [42] also estimate the functional correctness of IAM software. An additional consideration for a functionality metric is organization-specific comprehensiveness. E.g., an organization that does not (need to) utilize SoD policies does not require their functionality or a measure for it. For the goals, a comprehensive, correct, and appropriate set of IAM functionalities acts as a cost factor. However, a functional and powerful IAM improves security, enhances operations, and enables high-quality controls for processes, identities, policies, and other software. Thus, the target value for a functionality metric should be at the maximum (for a comprehensive functionality set) or a cost-efficient target (for the required functionalities of an organization). The relevant IAM audiences for a functionality metric are governance and operations for providing IAM functionalities both on a management and operational level.

Performance represents an efficient usage of system resources. The performance metric distinguishes between time behavior, resource utilization, and capacity. (i) Time behavior considers response and processing times or throughput rates. (ii) Resource utilization measures the amount and types of resources used. (iii) Capacity assesses whether software limits meet the organizational requirements [78]. IAM literature discusses performance of IAM architectures, policy maintenance, and runtime (see the Evaluation Runtime in Section 5.6). Examples include response times [69, 73, 137, 170], resource usage [2, 73, 137], amounts of requests [73, 116], available bandwidth [148], connected systems [151], scalability [72, 87, 137], or time consumption for maintenance [73, 101]. A high value for a performance metric negatively affects the short-term cost-reduction goal because maintaining proper performance requires ongoing assessments and adjustments to the software in use. However, other goals benefit from high-performance software, such as operations, processes, and software quality. A performance metric thus targets a maximization strategy. The relevant IAM audience for performance includes governance and operations officers, as they are responsible for selecting and running software.

Compatibility as a metric assesses the capability of a system or software component to exchange information and perform functions in a shared environment. Compatibility thus encompasses co-existence and interoperability. Co-existence describes the ability to execute required functions efficiently without harming other components in a shared environment. Interoperability describes the capability to provide, exchange, and use information from other components [78]. For IAM approaches, trust metrics include co-existence, by assessing the trustworthiness of a user's identity across a Federated Identity Management (FIM) covering a wide range of aspects [5, 35, 52, 103, 104, 119, 134]. Measures for a healthy co-existence may include ex post assessments, such as unauthorized access to confidential data, including Personally Identifiable Information (PII) or financial details [97]. IAM interoperability relies on standardized protocols and also covers organizational factors such as seamless software integration (e.g., SSO) [72]. Interoperability measures thus encompass the number of connected systems [151] or the exchange protocol support [2, 69, 87, 145], like LDAP [169], SAML [123], SPML [31], SCIM [90], or XACML [125]. For the goals, compatibility undermines the cost-reduction goal in the short term due to its higher development costs. Other IAM goals benefit from compatibility as co-existence considers security, while interoperability supports operations and identity or policy quality. Overall compatibility positively affects IAM software. A compatibility metric has an ambiguous target value, as improving compatibility beyond required organizational use cases is inefficient. The relevant IAM audiences for a compatibility metric are governance and operations, since these select and operate compatible software.

Usability of IAM systems is being an appropriate tool for IAM tasks. Users thus process their tasks efficiently and effectively while staying satisfied working with the system [2, 25]. Moreover, the ISO25010 [78] details other properties, like appropriateness, recognizability, learnability, operability, user error protection, user interface aesthetics, and accessibility. The literature addresses these properties, especially in the context of authentication. Authentication measures include task efficiency (e.g., time to authenticate), task effectiveness (e.g., login attempts), and user preferences [82, 112]. For example, task efficiency is reflected in the processing duration of user requests, and task effectiveness is reflected in the number of failed authentication requests [70]. In that sense, Staite and Bahsoon [148] point out the importance of usability through an understandable, common authentication interface (e.g., SSO [69]). Additionally, influences based on age [107], cognitive abilities [17, 18], or device characteristics [139, 155] should be considered as measures for a usability metric [95]. In this context, the Fail To Enrol (FTE) rate highlights that a one-size-fits-all authentication factor does not exist. E.g., a person with deformed eyes might have trouble using an iris scan, while manual labor might wear down a fingerprint [7, 100], rendering particular authentication schemes unusable [92]. Despite these specific authentication usability measures, more general usability metrics such as System Usability Scale (SUS) [25, 26] and Quality in Use Integrated Measurement (QUIM) [142, 143] have been shown to be effective for expressing IAM usability [24, 129]. SUS includes ten well-studied statements with a Likert scale and is quick to set up [9, 89]. Alternatively, QUIM proposes a system of 10 usability factors: efficiency, effectiveness, productivity, satisfaction, learnability, safety, trustfulness, accessibility, universality, and usefulness, supported by 26 potential measures. Usability for IAM systems is also discussed for administrative purposes. While general usability metrics, such as SUS and QUIM, also apply, the literature discusses specific measures spanning effectiveness, efficiency, and satisfaction. For example, measures include the effectiveness of the modeled policies and associated verification functionalities [69], efficiency assessments of consistent user interfaces and experience [69, 87], and satisfaction or reductions in administrative effort in general [14, 70, 101]. While introducing usability entails initial costs, it benefits all other goals because IAM tasks are executed with higher user satisfaction. Since the GDPR [40] also demands appropriate state-of-the-art security tools, a baseline for usability is required. The metric thus targets its maximum. The relevant IAM audience of

a usability metric includes especially governance and operations for selecting and operating (usable) tools.

Reliability describes whether software components perform specified functions in specified conditions. Furthermore, a reliability metric includes maturity, availability, fault tolerance, and recoverability. (i) Maturity denotes whether a software component fulfills requirements under usual operation. (ii) Availability describes whether a software component is accessible and operational for its required usage. (iii) Fault tolerance assesses the degree to which a software component operates as intended, although hardware and software faults are present. (iv) Finally, recoverability measures whether a system returns to its desired state after an interrupting event [78]. For IAM, maturity measures encompass maturity models allowing a comprehensive overview of a system's maturity [140]. For FIM, maturity assessments also include connected applications [151] or the support of standardized exchange protocols [69, 145]. Examples of availability measures are the amount of time (or its percentage) a system is available for regular operation [75], its scaling capability, or potential points of failure [87]. In addition, IAM availability also covers exchanging (authentication) data, as measures for authentication and of the identity (profile) point out [148]. For fault tolerance, wrong access control decisions due to insufficient data or the service's access control independence assess the system's behavior in tense situations [72, 137]. Besides, an assessment for potential weaknesses leading to these failures is also relevant [75]. Another aspect of fault tolerance is trust [137]. Rigorous research on trust metric in the context of FIM proposes a wide range of aspects [5, 35, 52, 103, 104, 119, 134]. Finally, recoverability measures include the time a software component takes to recover from an interruption or the speed at which a backup can be rolled out [75]. In this sense, measuring the frequency of backups for specific data types, such as critical or audit trail data, is also reasonable [75]. Reliability positively affects IAM goals by reducing the risk of blackouts and enabling reliable operations. Users also expect reliability for processes and software. The target for a reliability metric is its maximum. The IAM audience includes governance and operations for choosing and operating reliable software.

Security includes confidentiality, integrity, non-repudiation, accountability, and authenticity in the ISO25010 [78]. Please note that the Confidentiality, Integrity, Availability (CIA)-Triad, another common security model, also includes availability, which is already covered by reliability. (i) Confidentiality describes that data is accessible only to authorized identities. (ii) Integrity assesses the prevention of unauthorized modification of data or programs. (iii) Non-repudiation describes the execution of an action or event so that it is indisputable afterward. (iv) Accountability measures the degree of uniquely traceable actions of its responsible identity. (v) Authenticity denotes whether an identity is proven to be the one claimed [78]. For IAM, confidentiality measures cover privacy [1, 156, 160] affecting identity attribute disclosure [57, 58, 72, 75, 87, 137, 148]. A comprehensive survey [156] highlights the depth of this research area by categorizing 79 privacy metrics into uncertainty, data similarity, indistinguishability, time, error, accuracy, the adversary's success probability, and information gain or loss. Privacy-enhancing IAM internalizes these metrics [43, 61], like linkability or anonymity [29, 30]. Beside that, privacy also affects (biometric) authentication schemes, as additional (biological) information might leak [95]. Despite its low acceptance, an illustrative example is the use of body odor as a biometric factor, revealing further personal information, such as recent activities or possible diseases [21, 50]. Additional IAM confidentiality measures include the number of identity data attacks, such as eavesdropping, skimming, or snooping [58]. For integrity, wrong access or authorization decisions based on insufficient or altered data or software indicate integrity [137]. Additionally, the number of integrity-related attacks, such as data tampering, privilege escalation, spoofing, identity theft, or lure attacks, is a valid measure [58]. For non-repudiation and accountability, the previously mentioned traceability applies. Additionally, access reviews [55, 79] or (blockchain-based) audit trails [108] document non-reputable and accountable

authorization decisions, making their frequency and scope relevant to measure. Authenticity utilizes the password, biometric, ownership, and multi-factor strength metrics (see Section 5.1) and the authentication strength of services [87]. Attacks affecting authenticity include identity theft, replay, or spoofing attacks [58], whose occurrences are relevant measures. Finally, general security metrics, such as CVSS [42], influence IAM. High security often negatively affects operations and cost reduction by interrupting security checks, such as authentication. However, security benefits other IAM goals, such as reduced security risks from unauthorized actions or fulfilled compliance requirements [43]. From a quality perspective, identities and policies need to be protected against unauthorized access. The security metric target is thus its maximum. The relevant IAM audiences for a security metric are governance and operations for selecting and operating secure software.

Maintainability represents the ability of a system to modify, correct, or adapt to changes in the environment or requirements. Other features are modularity, reusability, analysability, modifiability, and testability. (i) Modularity denotes whether a system comprises discrete and easily exchangeable components. (ii) Reusability describes whether a component can or could be used more than once in a system. (iii) Analysability measures a software component's features for diagnosing its impact, deficiencies, causes of failure, or parts requiring modification. (iv) Modifiability denotes the capability of a software component for modifications without causing defects or degradation. (v) Testability describes whether operators can set up, perform, and evaluate test criteria for the software component [78]. In IAM software, modularity is evident, as multiple components must fulfill interdependent tasks [122]. XACML [125], the reference architecture for ABAC, highlights modularity by distinguishing between crucial and replaceable software components, such as the PEP, PDP, Policy Information Point (PIP), and Policy Administration Point (PAP). The horizontal scope of IAM software (e.g., single- or multi-host deployment), the presence of APIs, the ability to import and export policies, and the risk of vendor lock-in are measures of modularity [69, 72]. Moreover, reusability builds upon modularity. For IAM, measures should include standardized APIs, like LDAP [169], SAML [123], SPML [31], SCIM [90], or XACML [125]. Modularity and reusability intersect with compatibility and portability metrics. Analysability measures include the ability to trace modifications, as described by the traceability metric. Effective Graphical User Interfaces (GUIs) and verification functionalities also foster analysability [69]. Modifiability measures include the ability to configure policies within existing systems and to adapt them during their lifecycle [69]. This characteristic thus intersects with the adaptability metric. Additionally, modification or integration costs for software measure its modifiability [72, 137]. Finally, testability measures include verification features for policy engineers [69]. Maintainability is a driver for short-term costs. However, security, operations, and process quality goals benefit, especially through continuous adaptation of software components to current needs. Policy quality also profits from the testability aspect of maintainability. The target for maintainability is thus maximum. The IAM audiences are governance and operations for selecting and operating the software. For policy administrators, the testability characteristic is relevant.

Portability describes an operator's ease of installing, adapting, and replacing software components on hardware or organization-specific environments [78]. For installing (and uninstalling), measures include Operation System (OS) compatibility [69, 87, 105]. Ease of adaptation includes metrics such as the maintenance and adaptability metrics described earlier [69, 87]. Measures for replacing IAM software include the capability to provide a consistent experience across multiple software components [57, 58, 87, 105], avoidance of vendor lock-in, or the use of standardized protocols [57, 105]. Furthermore, a portability metric is especially relevant for recent approaches for cloud-based IAM. Criteria thus include using standards to ensure a consistent user experience, as well as lightweight and scalable communication between software components [105]. Portability negatively affects short-term cost reduction due to higher vendor expenses for specific

OSes or environments. However, operations, process quality, and software quality goals benefit from the eased introduction of IAM software. The target value for portability is its maximum. The relevant IAM audiences are governance and operations for selecting and operating portable software.

6 Discussion

Based on our collection of IAM metrics, we discuss open challenges for research on IAM metrics and limitations of our study. The challenges and limitations cover aspects of the taken IAM perspectives, goals, metrics, understandability, and economic factors.

6.1 Open Challenges

► **Different levels of maturity across perspectives:** We developed the perspectives based on metrics and measures in literature and existing ways to structure them. On the one hand, structuring perspectives for quality goals already has a certain maturity, as we could rely on established metrics for data quality [28], policy quality [84], process quality [63], and software quality [78]. We thus could structure the metrics and measures found in the literature and connect them to these frameworks. On the other hand, we noticed lower maturity for the cost-related goals as we structured the metrics and measures during the metric synthesis. As a general structure, we thus drew from common IAM processes, such as the identity lifecycle, policy lifecycle, and governance and management processes. While yielding better results, we still note a lack of maturity in structuring IAM metrics by IAM processes or cost-related goals, compared to the quality-related goal perspectives.

► **Economic feasibility of measures:** Taking measures needs consideration of economic feasibility. While SQL queries might cost-effectively provide measures (assuming data availability), other measures might require costly questionnaires or interviews. Also, databases containing the required data need implementation and maintenance. While this economic feasibility is discussed in greater detail in the context of data quality than in IT security, it is a relevant aspect for both [64]. The costs of IAM metrics cannot exceed the expected savings from their use. For example, an organization-wide daily user satisfaction questionnaire might give insights, but it also violates this economic feasibility. However, not running the questionnaire at all may lead to false decisions down the line.

► **Interwoven requirements:** IAM goals originate from interwoven requirements that compete with each other. Access Reviews are an example of this [14, 79]: While necessary for compliance, domain experts who are involved in them face a time-consuming task (harming the cost-reduction goal), which interrupts their usual responsibilities (hurting the operational efficiency goal). Under this pressure, a domain expert might seek immediate treatment of the Access Review, leading to relatively quick but unqualified decision-making. Thus, at the expense of security, a domain expert might *just accept* the presented authorizations, since revoking them might harm the operations goal due to missing authorizations. At least this Access Review meets the compliance requirement, since the domain expert conducted the periodic check. Thus, optimizing only some of the interwoven IAM goals and metrics could lead to unintended outcomes, asking for a more balanced approach that considers all IAM goals. Compliance is a special factor for the interwovenness of IAM goals. The need for compliance originates from internal and external regulations. This dependency has three implications: First, multiple regulations might apply simultaneously, e.g., like SOX for US public boards and HIPAA for the healthcare sector. Second, regulations are subject to change. A new regulation might come into effect (such as the EU AI Act), or an existing one might be updated (such as ISO 27001 in 2022). Third, unlike other goals, compliance does not necessarily require a timeless or valid argumentation but somewhat situational or political reasoning. An

example is SOX [152], which came into effect after major accounting scandals (Enron, WorldCom, etc.), highlighting the role of situational and political reasoning. Thus, the existence, update, or nature of regulation can effectively steer IAM goals and their metrics in a different direction at any time.

► **IAM metrics need an IAM goal:** IAM metrics must support an IAM goal, otherwise its motivation is dubious. For example, a standalone measure, such as the number of roles, is easily obtainable and visualizable but lacks clear grounding in IAM goals. Without further background, such as the organization's size or role coverage [85], a high number of roles could indicate either a well-designed or a distorted role model. While the number of roles can serve as a measure for other IAM metrics, its relationship to IAM goals is unclear, making it unsuitable as a metric. For this reason, the IAM metric collection in this work is based on IAM goals. The metrics decouple from the measures to depict more abstract concepts. This decoupling and link to IAM goals have two implications: First, IAM metrics require a relationship to IAM goals derived from organizational strategy. An IAM metric thus needs to show its impact and alignment to that strategy. Otherwise, the justification for the IAM metric is dubious. Second, an IAM metric requires decoupling from the actual measures or underlying data. For example, IAM systems include organization-specific data and interpretation. However, the IAM metric remains the same, regardless of the organization or system. Thus, the formula for a metric might need to be tailored to an organizational context to use the available measures.

► **Tradeoffs for IAM metrics and goals:** A challenging aspect of IAM metrics and goals are their tradeoffs. On the one hand, improving one IAM metric can interfere with other goals and metrics. On the other hand, a single metric can have goal equilibria, preventing it from reaching its optimum. Consider improving the value of the password strength metric. To make it more secure, one might alter the password policy by increasing the required password length. First, the security goal might benefit, but other metrics, such as process efficiency, might suffer negative side effects from failed authentications due to forgotten or hard-to-remember passwords. Thus, we recommend focusing on the big picture and improving IAM goals holistically rather than relying on single metrics. Second, the password strength example also illustrates a well-known tradeoff between security and operational efficiency goals [24, 56, 80, 102]. An unbalanced increase in password security parameters improves security but harms operations, and vice versa. Thus, a password strength metric cannot simultaneously maximize both the security and operational efficiency goals, due to their mutual interference. These tradeoffs are also present in other metrics that have both negative and positive impacts on IAM goals, as presented in the Tables of Section 5. These tradeoffs can prevent IAM metrics from achieving certain properties, but they also indicate opportunities for detailed, scientific discussion of the tradeoffs.

► **Choosing a suitable abstraction level:** Due to the large amounts of metrics and measures, they need aggregation and provide drill-down functionalities [22]. Aggregation allows for reducing the presented metrics. This reduction is necessary to achieve a comprehensible number of metrics. A drawback of this approach is that specific metrics merge. These metrics are no longer available as standalone metrics but as components of more abstract metrics. This can lead to describing the IAM of an organization using a single [12] or a few [140] metrics, similar to a maturity model. Opposite to aggregation is a drill-down functionality. The drill-down allows a metric to be decomposed into its sub-metrics or measures. This decomposition enables analysts to identify causes of failing target values for IAM goals.

► **Considering the audience:** The audience for IAM metrics needs to be considered. Since organizations require flexibility, the presented IAM metrics are not a fixed set but a suggestion of valid concepts. This suggestion allows for configurations of measures and formulas (e.g., for ranking and weighting [138]) or even the exclusion of specific metrics for the organization. This

customization ensures the necessary fine-tuning for specific organizations, fostering a tailored, comprehensive, and aligned IAM metric collection. Furthermore, various audiences require specific considerations. For example, policy administrators are likely more interested in policy lifecycle and quality metrics. Compared with that, a staff with a non-technical skill set might be less interested in software quality metrics. Careful consideration of the specific IAM audiences is thus required to facilitate further comprehension.

6.2 Limitations

► **Options for organizing perspectives:** While we end up with the presented organization of perspectives based on common IAM processes and IAM quality considerations, other options are feasible. Perspectives might split into more detail or combine to a higher level of aggregation, allowing for other levels of abstraction. Following the abstraction to its extreme, this allows us to summarize IAM quality into a single metric for assessing and comparing organizations' IAM [12]. Another example is the metrics for password, biometric, ownership, and multi-factor strength. We added them to the identity lifecycle, but they might as well stand on their own from an "authentication strength" perspective, or they might be abstracted into a single authentication strength metric.

► **Options for organizing metrics:** For our chosen perspectives, there are options for structuring quality-related metrics. This includes data quality frameworks for identity quality [28, 118, 159], as identities and accounts can be interpreted as entities with attributes; process quality frameworks for process quality [63, 114, 153] to support general IAM processes; and software quality frameworks for technology quality [23, 37, 53, 78, 98], as IAM systems heavily rely on their software quality. In general, these alternative frameworks are also suitable to organize IAM metrics. We selected our frameworks [28, 63, 78] for their maturity, their alignment with IAM, and their alignment with the metrics and measures we identified in our survey.

► **Only one not the only valid solution:** We want to emphasize that the proposed collection of IAM metrics is not *the single optimal* solution but rather *one valid* solution among many. This solution space implies that other solutions for a comprehensive IAM collection are also feasible and valid. As in this study, the chosen combination of IAM metrics might be based on objective criteria: a solid literature review, grounding in IAM goals, limiting their number for the sake of understandability, or using existing collections of related metrics (as done for software quality). Furthermore, instantiating these metrics in organizations, some metrics and measures might not be applicable. For example, a biometric strength metric is unnecessary if an organization does not use biometric authentication. Additionally, organizations might need to address specific needs, leading them to use only metrics and measures tailored to their context and personal needs, leading to another set of metrics when instantiated [22]. In this sense, this collection of IAM metrics can serve as a guide to appropriate and grounded IAM metrics, but they need to be tailored to the applying organization (compare Related Work in Section 3).

7 Conclusion

Our work identifies 43 IAM metrics spanning seven perspectives while limiting itself to understandable dimensions, metrics with an impact on IAM goals, and metrics with relevance in the literature. These IAM metrics enable organizations to maintain a holistic overview of essential IAM topics and to trace the effective utilization of their IAM security budget. To the best of our knowledge, this work is the most comprehensive scientific study of IAM metrics and their alignment with strategic IAM goals. These IAM metrics, based on IAM goals, provide an accessible, broad overview of IAM while remaining understandable. This work also includes guidance on implementing these IAM metrics into organizational strategy and hints at practical features such as drill-down and

aggregation. Based on our work, we recommend the following future research direction regarding IAM metrics:

- Use standard terminology for metrics and measures. We recommend aligning with the NIST guidelines of Schroeder et al. [141]. Current research on quantifying IAM is scattered across the literature due to inconsistent and imprecise terminology and keyword usage. Establishing a common terminology will ease future discussions of IAM quality and its characteristics.
- Develop metric sets for common IAM processes. For example, a general understanding of common IAM processes is partly available (see expert interviews for access review [14, 79] or leaver [34] processes). However, a detailed discussion about holistically quantifying these processes is missing in the literature.
- Build and test an IAM maturity model based on these metrics. A combination of present maturity models [140] and systems for comparing organizations [12] can yield an insightful comparison of IAM across organizations using a quantifiable benchmark.

References

- [1] Aymen Akremi and Mohsen Rouached. 2021. A comprehensive and holistic knowledge model for cloud privacy protection. *The Journal of Supercomputing* 77, 8 (2021), 7956–7988. DOI : <https://doi.org/10.1007/s11227-020-03594-3>
- [2] Bandar Alamri, Ita Richardson, and Katie Crowley. 2024. Cybersecurity risk management and evaluation framework of blockchain identity management systems in HIoT: Experts evaluation. *IEEE Access* 12 (2024), 144652–144683. DOI : <https://doi.org/10.1109/ACCESS.2024.3468379>
- [3] Suood Alrooomi and Frank Li. 2023. Measuring website password creation policies at scale. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS'23)*. Association for Computing Machinery, New York, NY, USA, 3108–3122. DOI : <https://doi.org/10.1145/3576915.3623156>
- [4] Andrew van der Stock, Brian Glas, Neil Smithline, Tanya Janca, Torsten Gigler. 2025. OWASP Top 10:2025 (Release Candidate). Technical Report. Open Web Application Security Project (OWASP). Retrieved from <https://owasp.org/Top10/>
- [5] Patricia Arias-Cabarcos, Florina Almenárez-Mendoza, Andrés Marín-López, Daniel Díaz-Sánchez, and Rosa Sánchez-Guerrero. 2012. A metric-based approach to assess risk for “On cloud” federated identity management. *Journal of Network and Systems Management* 20, 4 (2012), 513–533. DOI : <https://doi.org/10.1007/s10922-012-9244-2>
- [6] Patricia Arias-Cabarcos, Christian Krupitzer, and Christian Becker. 2019. A survey on adaptive authentication. *ACM Computing Surveys* 52, 4, Article 80 (2019), 30 pages. DOI : <https://doi.org/10.1145/3336117>
- [7] Rashid Arsalaan, Lateef Mehreen, Kaur Balbir, O. P. Aggarwal, Hamid Sajad, and Gupta Neeraj. 2013. Biometric finger print identification is it a reliable tool or not? *Journal of Indian Academy of Forensic Medicine* 35, 2 (2013), 109–112.
- [8] Razi Arshad and Muhammad Rizwan Asghar. 2025. Characterization and quantification of user privacy: Key challenges, regulations, and future directions. *IEEE Communications Surveys and Tutorials* 27, 5 (2025), 3266–3307. DOI : <https://doi.org/10.1109/COMST.2024.3519861>
- [9] Aaron Bangor, Philip T. Kortum, and James T. Miller. 2008. An empirical evaluation of the system usability scale. *International Journal of Human–Computer Interaction* 24, 6 (2008), 574–594.
- [10] Victor Basili, Gianluigi Caliera, and H. Dieter Rombach. 1994. The goal question metric approach. *Encyclopedia of Software Engineering* 1, 1 (1994), 528–532.
- [11] Victor Basili, Jens Heidrich, Mikael Lindvall, Jurgen Munch, Myrna Regardie, and Adam Trendowicz. 2007. GQM+ strategies—aligning business strategies with software measurement. In *Proceedings of the 1st International Symposium on Empirical Software Engineering and Measurement (ESEM 2007)*. IEEE, Madrid, Spain, 488–490. DOI : <https://doi.org/10.1109/ESEM.2007.66>
- [12] Thomas Baumer, Johannes Grill, Jacob Adan, and Günther Pernul. 2024. A trust and reputation system for examining compliance with access control. In *Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES'24)*. Association for Computing Machinery, New York, NY, USA, Article 181, 10 pages. DOI : <https://doi.org/10.1145/3664476.3670883>
- [13] Thomas Baumer, Mathis Müller, and Günther Pernul. 2023. System for cross-domain identity management (SCIM): Survey and enhancement with RBAC. *IEEE Access* 11 (2023), 86872–86894. DOI : <https://doi.org/10.1109/ACCESS.2023.3304270>
- [14] Thomas Baumer, Tobias Reitinger, Sascha Kern, and Günther Pernul. 2024. Digital nudges for access reviews: Guiding deciders to revoke excessive authorizations. In *Proceedings of the 20th USENIX Conference on Usable Privacy and Security (SOUPS'24)*. USENIX Association, USA, Article 13, 20 pages.

- [15] Shirley A. Becker and Mitchell L. Bostelman. 1999. Aligning strategic and project measurement systems. *IEEE Software* 16, 3 (1999), 46–51. DOI : <https://doi.org/10.1109/52.765786>
- [16] Matthias Beckerle and Leonardo A. Martucci. 2013. Formal definitions for usable access control rule sets from goals to metrics. In *Proceedings of the 9th Symposium on Usable Privacy and Security (SOUPS'13)*. Association for Computing Machinery, New York, NY, USA, Article 2, 11 pages. DOI : <https://doi.org/10.1145/2501604.2501606>
- [17] Marios Belk, Christos Fidas, Panagiotis Germanakos, and George Samaras. 2015. Do human cognitive differences in information processing affect preference and performance of CAPTCHA? *International Journal of Human-Computer Studies* 84, 84 (2015), 1–18. DOI : <https://doi.org/10.1016/j.ijhcs.2015.07.002>
- [18] Marios Belk, Panagiotis Germanakos, Christos Fidas, and George Samaras. 2013. Studying the effect of human cognition on user authentication tasks. In *Proceedings of the User Modeling, Adaptation, and Personalization*, Sandra Carberry, Stephan Weibelzahl, Alessandro Micarelli, and Giovanni Semeraro (Eds.). Springer, Berlin, 102–113. DOI : https://doi.org/10.1007/978-3-642-38844-6_9
- [19] Yolanta Beres, Marco Casassa Mont, Jonathan Griffin, and Simon Shiu. 2009. Using security metrics coupled with predictive modeling and simulation to assess security processes. In *Proceedings of the 2009 3rd International Symposium on Empirical Software Engineering and Measurement (ESEM'09)*. IEEE Computer Society, USA, 564–573. DOI : <https://doi.org/10.1109/ESEM.2009.5314213>
- [20] Beyond Identity. 2022. Former employees admit to using continued account access to harm previous employers. Retrieved January 20, 2025 from <https://www.beyondidentity.com/blog/great-resignation-impact-on-company-security>
- [21] Debnath Bhattacharyya, Rahul Ranjan, Farkhod Alisherov, Minkyu Choi, et al. 2009. Biometric authentication: A review. *International Journal of u-and e-Service, Science, and Technology* 2, 3 (2009), 13–28.
- [22] Paul Black, Karen Scarfone, and Murugiah Souppaya. 2009. *Cyber Security Metrics and Measures*. John Wiley and Sons, Inc., Hoboken, NJ, Nebraska. Retrieved from https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=51292
- [23] B. W. Boehm, J. R. Brown, and M. Lipow. 1976. Quantitative evaluation of software quality. In *Proceedings of the 2nd International Conference on Software Engineering (ICSE'76)*. IEEE Computer Society Press, Washington, DC, USA, 592–605. DOI : <https://dl.acm.org/doi/abs/10.5555/800253.807736>
- [24] Christina Braz, Ahmed Seffah, and David M'Raihi. 2007. Designing a tradeoff between usability and security: A metrics based-model. In *Proceedings of the Human-Computer Interaction—INTERACT 2007*, Cécilia Baranauskas, Philippe Palanque, Julio Abascal, and Simone Diniz Junqueira Barbosa (Eds.). Springer, Berlin, 114–126. DOI : https://doi.org/10.1007/978-3-540-74800-7_9
- [25] John Brooke. 1996. SUS: A quick and dirty usability scale. In *Proceedings of the Usability Evaluation In Industry*. Taylor and Francis, London, United Kingdom, 207–212. DOI : <https://doi.org/10.1201/9781498710411-35>
- [26] John Brooke. 2013. SUS: A retrospective. *Journal of Usability Studies* 8, 2 (2013), 29–40.
- [27] Elizabeth Chew, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, and Will Robinson. 2008. *Performance Measurement Guide for Information Security*. Technical Report. National Institute of Standards and Technology, Gaithersburg, MD.
- [28] Corinna Cichy and Stefan Rass. 2019. An Overview of Data Quality Frameworks. *IEEE Access* 7 (2019), 24634–24648. DOI : <https://doi.org/10.1109/ACCESS.2019.2899751>
- [29] Sebastian Clauß. 2006. A framework for quantification of linkability within a privacy-enhancing identity management system. In *Proceedings of the Emerging Trends in Information and Communication Security*, Günter Müller (Ed.). Springer, Berlin, 191–205. DOI : https://doi.org/10.1007/11766155_14
- [30] Sebastian Clauß and Stefan Schiffner. 2006. Structuring anonymity metrics. In *Proceedings of the 2nd ACM Workshop on Digital Identity Management (DIM'06)*. Association for Computing Machinery, New York, NY, USA, 55–62. DOI : <https://doi.org/10.1145/1179529.1179539>
- [31] Gary Cole. 2005. *OASIS Service Provisioning Markup Language (SPML) Version 2*. Committee Draft 1.0 pstc-spml2-cd-01. OASIS. Retrieved from <https://docs.oasis-open.org/provision/spml-2.0-cd-01/pstc-spml2-cd-01.pdf>
- [32] Jon Currey, Robbie McKinstry, Armon Dadgar, and Mark Gritter. 2020. Informed privilege-complexity tradeoffs in RBAC configuration. In *Proceedings of the 25th ACM Symposium on Access Control Models and Technologies (SACMAT'20)*. Association for Computing Machinery, New York, NY, USA, 119–130. DOI : <https://doi.org/10.1145/3381991.3395597>
- [33] Xavier de Carné de Carnavalet and Mohammad Mannan. 2014. From very weak to very strong: Analyzing password-strength meters. In *Proceedings of the Network and Distributed System Security Symposium NDSS 2014*. Internet Society, San Diego, California, 1–16. DOI : <https://doi.org/10.14722/ndss.2014.23268>
- [34] Christina Detsika, Timo Jagusch, Nora Weidner, Larissa Weir, Florin Martius, and Christian Tiefenau. 2025. “You go now! no trouble!”: Understanding the offboarding process in companies from an IT security perspective. In *Proceedings of the 21st USENIX Conference on Usable Privacy and Security (SOUPS'25)*. USENIX Association, USA, Article 5, 20 pages. DOI : <https://dl.acm.org/doi/10.5555/3767870.3767875>
- [35] V. Neelaya Dhatchayani and V. S. Shankar Sriram. 2014. Trust aware identity management for cloud computing. *International Journal of Information and Communication Technology* 6, 3/4 (2014), 369. DOI : <https://doi.org/10.1504/ijict.2014.063220>

- [36] Rainer Diesch and Helmut Krcmar. 2020. SoK: Linking information security metrics to management success factors. In *Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES'20)*. Association for Computing Machinery, New York, NY, USA, Article 98, 10 pages. DOI : <https://doi.org/10.1145/3407023.3407059>
- [37] R. Geoff Dromey. 1996. Cornering the chimera [software quality]. *IEEE Software* 13, 1 (1996), 33–43. DOI : <https://doi.org/10.1109/52.476284>
- [38] Elimity. 2020. KPI-driven approach to Identity and Access Management—A guide to maximize the value of IAM. Retrieved January 20, 2025 from <https://elimity.com/kpi-driven-approach-to-iam-guide>
- [39] Aaron Elliott and Scott Knight. 2010. Role explosion: Acknowledging the problem. In *Proceedings of the Software Engineering Research and Practice*. CSREA Press, Las Vegas, Nevada, 349–355.
- [40] European Commission. 2016. General Data Protection Regulation. Retrieved from <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [41] David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn, and Ramaswamy Chandramouli. 2001. Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security* 4, 3 (2001), 224–274. DOI : <https://doi.org/10.1145/501978.501980>
- [42] FIRST. 2019. CVSS v3.1 Specification Document. Retrieved January 20, 2025 from <https://www.first.org/cvss/specification-document>
- [43] Simone Fischer-Hübner, Cristina Alcaraz, Afonso Ferreira, Carmen Fernandez-Gago, Javier Lopez, Evangelos Markatos, Lejla Islami, and Mahdi Akil. 2021. Stakeholder perspectives and requirements on cybersecurity in Europe. *Journal of Information Security and Applications* 61, 61 (2021), 102916. DOI : <https://doi.org/10.1016/j.jisa.2021.102916>
- [44] Ludwig Fuchs, Michael Kunz, and Günther Pernul. 2014. Role model optimization for secure role-based identity management. In *Proceedings of the European Conference on Information Systems (ECIS)*. AIS, Tel Aviv, Israel, 1–15. Retrieved from <https://epub.uni-regensburg.de/30394/>
- [45] Ludwig Fuchs and Gunther Pernul. 2007. Supporting compliant and secure user handling—A structured approach for in-house identity management. In *Proceedings of the 2nd International Conference on Availability, Reliability and Security (ARES'07)*. IEEE, Vienna, Austria, 374–384. DOI : <https://doi.org/10.1109/ARES.2007.145>
- [46] Ludwig Fuchs and Günther Pernul. 2008. HyDRo—hybrid development of roles. In *Proceedings of the Information Systems Security*, R. Sekar and Arun K. Pujari (Eds.). Springer, Berlin, 287–302.
- [47] Ludwig Fuchs and Günther Pernul. 2008. proROLE: A process-oriented lifecycle model for role systems. In *Proceedings of the 16th European Conference on Information Systems (ECIS 2008)*, Galway, Ireland, June 9–11, 2008. Springer, Berlin, 1322–1333. Retrieved from <https://aisel.aisnet.org/ecis2008/111>
- [48] Ludwig Fuchs and Günther Pernul. 2010. Reducing the risk of insider misuse by revising identity management and useraccount data. *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications* 1, 1 (2010), 14–28. DOI : <https://doi.org/10.22667/JOWUA.2010.06.31.014>
- [49] Inc. Gartner. 17.05.2021. Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed \$150 Billion in 2021. Retrieved January 20, 2025 from <https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-management>
- [50] Martin D. Gibbs. 2010. Biometrics: Body odor authentication perception and acceptance. *ACM SIGCAS Computers and Society* 40, 4 (2010), 16–24. DOI : <https://doi.org/10.1145/1929609.1929612>
- [51] Jana Glöckler, Johannes Sedlmeir, Muriel Frank, and Gilbert Fridgen. 2024. A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. *Business and Information Systems Engineering* 66, 4 (2024), 421–440. DOI : <https://doi.org/10.1007/s12599-023-00830-x>
- [52] Hidehito Gomi. 2011. An authentication trust metric for federated identity management systems. In *Proceedings of the Security and Trust Management*, Jorge Cuellar, Javier Lopez, Gilles Barthe, and Alexander Pretschner (Eds.). Springer, Berlin, 116–131. DOI : https://doi.org/10.1007/978-3-642-22444-7_8
- [53] Robert B. Grady. 1992. *Practical Software Metrics for Project Management and Process Improvement*. Prentice-Hall, Inc., USA. DOI : <https://dl.acm.org/doi/10.5555/140207>
- [54] Paul A. Grassi, James L. Fenton, Elaine M. Newton, Ray A. Perlner, Andrew R. Regenscheid, William E. Burr, Justin P. Richer, Naomi B. Lefkowitz, Jamie M. Danker, Yee-Yin Choong, et al. 2017. *Digital Identity Guidelines: Authentication and Lifecycle Management*. Technical Report. National Institute of Standards and Technology. DOI : <https://doi.org/10.6028/nist.sp.800-63b>
- [55] Sebastian Groll, Sascha Kern, Ludwig Fuchs, and Günther Pernul. 2021. Monitoring access reviews by crowd labelling. In *Proceedings of the Trust, Privacy and Security in Digital Business*, Simone Fischer-Hübner, Costas Lambrinoudakis, Gabriele Kotsis, A. Min Tjoa, and Ismail Khalil (Eds.). Springer International Publishing, Cham, 3–17.
- [56] Hana Habib, Pardis Emami Naeini, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2018. User behaviors and attitudes under password expiration policies. In *Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, 13–30. Retrieved from <https://www.usenix.org/conference/soups2018/presentation/habib-password>

- [57] Umme Habiba, Abdul Ghafoor Abassi, Rahat Masood, and Muhammad Awais Shibli. 2013. Assessment criteria for cloud identity management systems. In *Proceedings of the 2013 IEEE 19th Pacific Rim International Symposium on Dependable Computing*. IEEE, Vancouver, BC, Canada, 188–195. DOI : <https://doi.org/10.1109/PRDC.2013.39>
- [58] Umme Habiba, Rahat Masood, Muhammad Awais Shibli, and Muaz A. Niazi. 2014. Cloud identity management security issues and solutions: A taxonomy. *Complex Adaptive Systems Modeling* 2, 1 (2014), 5. DOI : <https://doi.org/10.1186/s40294-014-0005-9>
- [59] Kemal Hajdarevic and Pat Allen. 2013. A new method for the identification of proactive information security management system metrics. In *Proceedings of the 2013 36th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. IEEE, Opatija, Croatia, 1121–1126.
- [60] John Halamka, Ari Juels, Adam Stubblefield, and Jonathan Westhues. 2006. The security implications of verichip cloning. *Journal of the American Medical Informatics Association* 13, 6 (2006), 601–607. DOI : <https://doi.org/10.1197/jamia.M2143>
- [61] Marit Hansen, Peter Berlich, Jan Camenisch, Sebastian Clauß, Andreas Pfitzmann, and Michael Waidner. 2004. Privacy-enhancing identity management. *Information Security Technical Report* 9, 1 (2004), 35–44. DOI : [https://doi.org/10.1016/S1363-4127\(04\)00014-7](https://doi.org/10.1016/S1363-4127(04)00014-7)
- [62] Dick Hardt. 2012. The OAuth 2.0 Authorization Framework. DOI : <https://doi.org/10.17487/RFC6749>
- [63] Farideh Heidari and Pericles Loucopoulos. 2014. Quality evaluation framework (QEF): Modeling and evaluating quality of business processes. *International Journal of Accounting Information Systems* 15, 3 (2014), 193–223. DOI : <https://doi.org/10.1016/j.accinf.2013.09.002>
- [64] Bernd Heinrich, Diana Hristova, Mathias Klier, Alexander Schiller, and Michael Szubartowicz. 2018. Requirements for data quality metrics. *Journal of Data and Information Quality* 9, 2, Article 12 (2018), 32 pages. DOI : <https://doi.org/10.1145/3148238>
- [65] J. C. Henderson and H. Venkatraman. 1993. Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal* 32, 1 (1993), 472–484. DOI : <https://doi.org/10.1147/sj.382.0472>
- [66] Markus Hornsteiner, Sebastian Groll, and Alexander Puchta. 2021. Towards a user-centric IAM entitlement shop - learnings from the e-Commerce. In *Proceedings of the 13th International Conference on Security of Information and Networks (SIN 2020)*. Association for Computing Machinery, New York, NY, USA, Article 15, 4 pages. DOI : <https://doi.org/10.1145/3433174.3433585>
- [67] Vincent C. Hu, David Ferraiolo, Rick Kuhn, Arthur R. Friedman, Alan J. Lang, Margaret M. Cogdell, Adam Schnitzer, Kenneth Sandlin, Robert Miller, Karen Scarfone, et al. 2014. *Guide to Attribute Based Access Control (abac) Definition and Considerations (draft)*. Technical Report. National Institute of Standards and Technology. 1–54 pages. DOI : <https://doi.org/10.6028/nist.sp.800-162>
- [68] Vincent C. Hu, David F. Ferraiolo, and D. Rick Kuhn. 2006. *Assessment of Access Control Systems*. Technical Report. National Institute of Standards and Technology. DOI : <https://doi.org/10.6028/nist.ir.7316>
- [69] Vincent C. Hu and Karen Scarfone. 2012. *Guidelines for Access Control System Evaluation Metrics*. Technical Report. National Institute of Standards and Technology.
- [70] Matthias Hummer, Sebastian Groll, Michael Kunz, Ludwig Fuchs, and Günther Pernul. 2018. Measuring identity and access management performance—an expert survey on possible performance indicators. In *Proceedings of the 4th International Conference on Information Systems Security and Privacy*. SCITEPRESS - Science and Technology Publications, Funchal, Madeira, Portugal, 233–240. DOI : <https://doi.org/10.5220/0006557702330240>
- [71] Matthias Hummer, Michael Kunz, Michael Netter, Ludwig Fuchs, and Günther Pernul. 2016. Adaptive identity and access management—contextual data based policies. *EURASIP Journal on Information Security* 2016, 1 (2016), 19. DOI : <https://doi.org/10.1186/s13635-016-0043-2>
- [72] Thorsten Höllrigl, Frank Schell, Sebastian Suelmann, and Hannes Hartenstein. 2008. Towards systematic engineering of service-oriented access control in federated environments. In *Proceedings of the 2008 IEEE Congress on Services Part II (Services-2 2008)*. IEEE, Beijing, China, 104–111. DOI : <https://doi.org/10.1109/SERVICES-2.2008.24>
- [73] Zeinab M. Iqal, Ali Selamat, and Ondrej Krejcar. 2024. A comprehensive systematic review of access control in IoT: Requirements, technologies, and evaluation metrics. *IEEE Access* 12 (2024), 12636–12654. DOI : <https://doi.org/10.1109/ACCESS.2023.3347495>
- [74] ISACA. 2018. Introducing COBIT 2019 Overview. Retrieved January 20, 2025 from <https://www.isaca.org/resources/cobit>
- [75] Shareeful Islam and Paolo Falcarin. 2011. Measuring security requirements for software security. In *Proceedings of the 2011 IEEE 10th International Conference on Cybernetic Intelligent Systems (CIS)*. IEEE, London, UK, 70–75. DOI : <https://doi.org/10.1109/CIS.2011.6169137>
- [76] ISO 14223. 2018. *Radiofrequency Identification of Animals*. International Organization for Standardization.
- [77] ISO 24760. 2019. *IT Security and Privacy—A Framework for Identity Management*. International Organization for Standardization.

- [78] ISO 25010. 2011. *Systems and Software Engineering—Systems and software Quality Requirements and Evaluation (SQuaRE)—System and Software Quality Models*. International Organization for Standardization.
- [79] Pooya Jaferian, Hootan Rashtian, and Konstantin Beznosov. 2014. To authorize or not authorize: Helping users review access policies in organizations. In *Proceedings of the 10th USENIX Conference on Usable Privacy and Security (SOUPS'14)*. USENIX Association, USA, 301–320. DOI: <https://dl.acm.org/doi/10.5555/3235838.3235865>
- [80] Gokul Chettoor Jayakrishnan, Gangadhara Reddy Sirigireddy, Sukanya Vaddepalli, Vijayanand Banahatti, Sachin Prem-sukh Lodha, and Sankalp Suneel Pandit. 2020. Password: A serious game to promote password awareness and diversity in an enterprise. In *Proceedings of the 16th Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, online, 1–18. Retrieved from <https://www.usenix.org/conference/soups2020/presentation/jayakrishnan>
- [81] Robert S. Kaplan and David P. Norton. 1992. The balanced scorecard—measures that drive performance. *Havard Business Review* 1, 1 (1992), 71–79. Retrieved from <https://hbr.org/1992/01/the-balanced-scorecard-measures-that-drive-performance-2>
- [82] Christina Katsini, Marios Belk, Christos Fidas, Nikolaos Avouris, and George Samaras. 2016. Security and usability in knowledge-based user authentication: A review. In *Proceedings of the 20th Pan-Hellenic Conference on Informatics (PCI'16)*. Association for Computing Machinery, New York, NY, USA, Article 63, 6 pages. DOI: <https://doi.org/10.1145/3003733.3003764>
- [83] Sascha Kern, Thomas Baumer, Ludwig Fuchs, and Günther Pernul. 2023. Maintain high-quality access control policies: An academic and practice-driven approach. In *Proceedings of the Data and Applications Security and Privacy XXXVII*, Vijayalakshmi Atluri and Anna Lisa Ferrara (Eds.). Springer Nature Switzerland, Cham, 223–242. DOI: https://doi.org/10.1007/978-3-031-37586-6_14
- [84] Sascha Kern, Thomas Baumer, Sebastian Groll, Ludwig Fuchs, and Günther Pernul. 2022. Optimization of access control policies. *Journal of Information Security and Applications* 70, 70 (2022), 103301. DOI: <https://doi.org/10.1016/j.jisa.2022.103301>
- [85] Michael Kunz, Ludwig Fuchs, Michael Netter, and Günther Pernul. 2015. How to discover high-quality roles? a survey and dependency analysis of quality criteria in role mining. In *Proceedings of the Information Systems Security and Privacy*, Olivier Camp, Edgar Weippl, Christophe Bidan, and Esma Aïmeur (Eds.). Springer International Publishing, Cham, 49–67.
- [86] Michael Kunz, Alexander Puchta, Sebastian Groll, Ludwig Fuchs, and Günther Pernul. 2019. Attribute quality management for dynamic identity and access management. *Journal of Information Security and Applications* 44, 44 (2019), 64–79. DOI: <https://doi.org/10.1016/j.jisa.2018.11.004>
- [87] Jesse Leskinen. 2012. Evaluation criteria for future identity management. In *Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, Liverpool, UK, 801–806. DOI: <https://doi.org/10.1109/TrustCom.2012.153>
- [88] Yair Levy and Timothy J. Ellis. 2006. A systems approach to conduct an effective literature review in support of information systems research. *Informing Science: the International Journal of an Emerging Transdiscipline* 9, 9 (2006), 181–212.
- [89] James R. Lewis. 2018. The system usability scale: Past, present, and future. *International Journal of Human–Computer Interaction* 34, 7 (2018), 577–590.
- [90] Kepeng Li, Phil Hunt, Bhumip Khasnabish, Anthony Nadalin, and Zachary Zeltsan. 2015. *System for Cross-domain Identity Management: Definitions, Overview, Concepts, and Requirements*. RFC 7642. DOI: <https://doi.org/10.17487/RFC7642>
- [91] Emil Constantin Lupu. 1998. *A Role Based Framework for Distributed Systems Management*. Ph.D. Dissertation. University of London London, England.
- [92] Vashek Matyáš and Zdeněk Řiha. 2010. Security of biometric authentication systems. In *Proceedings of the 2010 International Conference on Computer Information Systems and Industrial Management Applications (CISIM)*. IEEE, Krakow, Poland, 19–28. DOI: <https://doi.org/10.1109/CISIM.2010.5643698>
- [93] Peter Mayer, Jan Kirchner, and Melanie Volkamer. 2017. A second look at password composition policies in the wild: Comparing samples from 2010 and 2016. In *Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 13–28. Retrieved from <https://www.usenix.org/conference/soups2017/technical-sessions/presentation/mayer>
- [94] Stefan Meier, Ludwig Fuchs, and Günther Pernul. 2013. Managing the access grid—A process view to minimize insider misuse risks. In *Proceedings of the 11th Internationale Tagung Wirtschaftsinformatik, Leipzig, Germany, February 27 – March 1, 2013*. AIS, Leipzig, Germany, 66. Retrieved from <http://aisel.aisnet.org/wi2013/66>
- [95] Martin Mihajlov, Borka Jerman Blazic, and Saso Josimovski. 2011. Quantifying usability and security in authentication. In *Proceedings of the 2011 IEEE 35th Annual Computer Software and Applications Conference*. IEEE, Munich, Germany, 626–629. DOI: <https://doi.org/10.1109/COMPSAC.2011.87>

- [96] George Armitage Miller. 1956. The magical number seven plus or minus two: Some limits on our capacity for processing information. *Psychol Rev* 63, 2 (1956), 81–97.
- [97] Natalia Miloslavskaya. 2016. Security operations centers for information security incident management. In *Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*. IEEE, Vienna, Austria, 131–136. DOI : <https://doi.org/10.1109/FiCloud.2016.26>
- [98] Tsvetelina Mladenova. 2020. Software quality metrics—Research, analysis and recommendation. In *Proceedings of the 2020 International Conference Automatics and Informatics (ICAI)*. IEEE, Varna, Bulgaria, 1–5. DOI : <https://doi.org/10.1109/ICAI50593.2020.9311361>
- [99] Ian Molloy, Hong Chen, Tiancheng Li, Qihua Wang, Ninghui Li, Elisa Bertino, Seraphin Calo, and Jorge Lobo. 2008. Mining roles with semantic meanings. In *Proceedings of the 13th ACM Symposium on Access Control Models and Technologies (SACMAT’08)*. Association for Computing Machinery, New York, NY, USA, 21–30. DOI : <https://doi.org/10.1145/1377836.1377840>
- [100] Keith L. Monson, Maria Antonia Roberts, Kathryn B. Knorr, Sherine Ali, Stephen B. Meagher, Kevin Biggs, Patti Blume, Donna Brandelli, Albert Marzioli, Robert Reneau, et al. 2019. The permanence of friction ridge skin and persistence of friction ridge skin and impressions: A comprehensive review and new results. *Forensic Science International* 297, 297 (2019), 111–131. DOI : <https://doi.org/10.1016/j.forsciint.2019.01.046>
- [101] Roberto Moratore, Eduardo Barbaro, and Yury Zhauniarovich. 2025. IAM role diet: A scalable approach to detecting RBAC data inefficiencies. In *Proceedings of the 2025 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks—Supplemental Volume (DSN-S)*. IEEE, Naples, Italy, 126–132. DOI : <https://doi.org/10.1109/DSN-S65789.2025.00052>
- [102] Robert Morris and Ken Thompson. 1979. Password security: A case history. *Communications of the ACM* 22, 11 (1979), 594–597. DOI : <https://doi.org/10.1145/359168.359172>
- [103] Nkosinathi Mpfu and Wynand J. C. van Staden. 2014. A survey of trust issues constraining the growth of Identity Management-as-a-Service (IdMaaS). In *Proceedings of the 2014 Information Security for South Africa*. IEEE, Johannesburg, South Africa, 1–6. DOI : <https://doi.org/10.1109/ISSA.2014.6950490>
- [104] Nkosinathi Mpfu and Wynand J. C. van Staden. 2017. Evaluating the severity of trust to identity- management-as-a-service. In *Proceedings of the 2017 Information Security for South Africa (ISSA)*. IEEE, Johannesburg, South Africa, 83–89. DOI : <https://doi.org/10.1109/ISSA.2017.8251778>
- [105] Nitin Naik and Paul Jenkins. 2016. A secure mobile cloud identity: Criteria for effective identity and access management standards. In *Proceedings of the 2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*. IEEE, Oxford, United Kingdom, 89–90. DOI : <https://doi.org/10.1109/MobileCloud.2016.22>
- [106] Clifford Neuman, Sam Hartman, Kenneth Raeburn, and Taylor Yu. 2005. *The Kerberos Network Authentication Service (V5)*. RFC 4120. DOI : <https://doi.org/10.17487/RFC4120>
- [107] James Nicholson, Lynne Coventry, and Pam Briggs. 2013. Age-related performance issues for PIN and face-based authentication systems. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI’13)*. Association for Computing Machinery, New York, NY, USA, 323–332. DOI : <https://doi.org/10.1145/2470654.2470701>
- [108] Martin Nuss, Alexander Puchta, and Michael Kunz. 2018. Towards blockchain-based identity and access management for internet of things in enterprises. In *Proceedings of the Trust, Privacy and Security in Digital Business*, Steven Furnell, Haralambos Mouratidis, and Günther Pernul (Eds.). Springer International Publishing, Cham, 167–181. DOI : https://doi.org/10.1007/978-3-319-98385-1_12
- [109] Raymond J. Offen and Ross Jeffery. 1997. Establishing software measurement programs. *IEEE Software* 14, 2 (1997), 45–53. DOI : <https://doi.org/10.1109/52.582974>
- [110] Lawrence O’Gorman. 2003. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE* 91, 12 (2003), 2021–2040. DOI : <https://doi.org/10.1109/JPROC.2003.819611>
- [111] Wonseok Oh and Alain Pinsonneault. 2007. On the assessment of the strategic value of information technologies: Conceptual and analytical approaches. *MIS Quarterly* 31, 2 (2007), 239–265. DOI : <https://doi.org/10.2307/25148790>
- [112] Aleksandr Ometov, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen, and Yevgeni Koucheryavy. 2018. Multi-factor authentication: A survey. *Cryptography* 2, 1 (2018), 1–31. DOI : <https://doi.org/10.3390/cryptography2010001>
- [113] Ertem Osmanoglu. 2013. *Identity and Access Management: Business Performance Through Connected Intelligence*. Elsevier, Waltham, MA, USA.
- [114] Sven Overhage, Dominik Q. Birkmeier, and Sebastian Schlauderer. 2012. Quality marks, metrics, and measurement procedures for business process models. *Business and Information Systems Engineering* 4, 5 (2012), 229–246. DOI : <https://doi.org/10.1007/s12599-012-0230-8>
- [115] Simon Parkinson and Saad Khan. 2022. A survey on empirical security analysis of access-control systems: A real-world perspective. *ACM Computing Surveys* 55, 6, Article 123 (2022), 28 pages. DOI : <https://doi.org/10.1145/3533703>

- [116] G. Peterson. 2006. Introduction to identity management risk metrics. *IEEE Security Privacy* 4, 4 (2006), 88–91. DOI : <https://doi.org/10.1109/MSP.2006.94>
- [117] Andreas Pfitzmann and Marit Hansen. 2010. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. Retrieved from https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf
- [118] Leo L. Pipino, Yang W. Lee, and Richard Y. Wang. 2002. Data quality assessment. *Communications of the ACM* 45, 4 (2002), 211–218. DOI : <https://doi.org/10.1145/505248.506010>
- [119] Uthpala Subodhani Premarathne, Ibrahim Khalil, Zahir Tari, and Albert Zomaya. 2017. Cloud-based utility service framework for trust negotiations using federated identity management. *IEEE Transactions on Cloud Computing* 5, 2 (2017), 290–302. DOI : <https://doi.org/10.1109/TCC.2015.2404816>
- [120] Rosanne Price and Graeme Shanks. 2016. A semiotic information quality framework: Development and comparative analysis. In *Proceedings of the Enacting Research Methods in Information Systems: Volume 3*, Leslie P. Willcocks, Chris Sauer, and Mary C. Lacity (Eds.). Springer International Publishing, Cham, 219–250. DOI : https://doi.org/10.1007/978-3-319-29272-4_7
- [121] Alexander Puchta, Fabian Böhm, and Günther Pernul. 2019. Contributing to current challenges in identity and access management with visual analytics. In *Proceedings of the Data and Applications Security and Privacy XXXIII*, Simon N. Foley (Ed.). Springer International Publishing, Cham, 221–239.
- [122] Alexander Puchta, Sebastian Groll, and Günther Pernul. 2021. Leveraging dynamic information for identity and access management: An extension of current enterprise IAM architecture. In *Proceedings of the 7th International Conference on Information Systems Security and Privacy—ICISSP*. INSTICC, SciTePress, Online Streaming, 611–618. DOI : <https://doi.org/10.5220/0010315706110618>
- [123] Nick Ragouzis, John Hughes, Rob Philpott, Eve Maler, Paul Madsen, and Tom Scavo. 2008. *Security Assertion Markup Language (SAML) V2.0 Technical Overview*. Committee Draft 02 sstc-saml-tech-overview-2.0-cd-02. OASIS. Retrieved from <https://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf>
- [124] Pawel Rajba, Natan Orzechowski, Karol Rzepka, Przemyslaw Szary, Dawid Nastaj, and Krzysztof Cabaj. 2024. Identity and access management architecture in the SILVANUS project. In *Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES'24)*. Association for Computing Machinery, New York, NY, USA, Article 92, 9 pages. DOI : <https://doi.org/10.1145/3664476.3670935>
- [125] Erik Rissanen. 2013. *eXtensible Access Control Markup Language (XACML) Version 3.0*. OASIS Standard XACML-V3.0. OASIS. Retrieved from <http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf>
- [126] Pawel Rotter. 2008. A framework for assessing RFID system security and privacy risks. *IEEE Pervasive Computing* 7, 2 (2008), 70–77. DOI : <https://doi.org/10.1109/MPRV.2008.22>
- [127] Denis Royer. 2008. Enterprise identity management. In *The Future of Identity in the Information Society*, Simone Fischer-Hübner, Penny Duquenoy, Albin Zuccato, and Leonardo Martucci (Eds.). Springer US, Boston, MA, 433–446.
- [128] Zhang Rui and Zheng Yan. 2019. A survey on biometric authentication: Toward secure and privacy-preserving identification. *IEEE Access* 7 (2019), 5994–6009. DOI : <https://doi.org/10.1109/ACCESS.2018.2889996>
- [129] Scott Ruoti and Kent Seamons. 2016. Standard metrics and scenarios for usable authentication. In *Proceedings of the 12th Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 1–2. Retrieved from https://www.usenix.org/conference/soups2016/workshop-program/way2016/presentation/ruoti_metrics
- [130] Riseul Ryu, Soonja Yeom, Soo-Hyung Kim, and David Herbert. 2021. Continuous multimodal biometric authentication schemes: A systematic review. *IEEE Access* 9 (2021), 34541–34557. DOI : <https://doi.org/10.1109/ACCESS.2021.3061589>
- [131] Nat Sakimura, John Bradley, Michael B. Jones, Breno de Medeiros, and Chuck Mortimore. 2014. OpenID Connect Core 1.0 incorporating errata set 1. Retrieved from https://openid.net/specs/openid-connect-core-1_0.html
- [132] Mathias Sallé. 2004. IT Service Management and IT Governance: Review, Comparative Analysis and their Impact on Utility Computing. Retrieved from <https://www.hpl.hp.com/techreports/2004/HPL-2004-98.pdf>
- [133] Pierangela Samarati and Sabrina Capitani de Vimercati. 2001. Access control: Policies, models, and mechanisms. In *Proceedings of the Foundations of Security Analysis and Design*, Riccardo Focardi and Roberto Gorrieri (Eds.). Springer Berlin, Heidelberg, 137–196.
- [134] Rajarajan Sampath and Deepak Goel. 2006. RATING: Rigorous assessment of trust in identity management. In *Proceedings of the 1st International Conference on Availability, Reliability and Security (ARES'06)*. IEEE, Vienna, Austria, 10 pp.–23. DOI : <https://doi.org/10.1109/ARES.2006.103>
- [135] Ravi S. Sandhu. 1998. Role-based access control. Portions of this chapter have been published earlier in Sandhu et al. (1996), Sandhu (1996), Sandhu and Bhamidipati (1997), Sandhu et al. (1997) and Sandhu and Feinstein (1994). In *Proceedings of the Advances in Computers*, Marvin V. Zelkowitz (Ed.). Advances in Computers, Vol. 46, Elsevier, online, 237–286. DOI : [https://doi.org/10.1016/S0065-2458\(08\)60206-5](https://doi.org/10.1016/S0065-2458(08)60206-5)

- [136] Ravi S. Sandhu and Pierangela Samarati. 1994. Access control: Principle and practice. *IEEE Communications Magazine* 32, 9 (1994), 40–48.
- [137] Frank Schell, Jochen Dinger, and Hannes Hartenstein. 2009. Performance evaluation of identity and access management systems in federated environments. In *Scalable Information Systems*, Peter Mueller, Jian-Nong Cao, and Cho-Li Wang (Eds.). Springer, Berlin, 90–107.
- [138] Daniel Schlette, Fabian Böhm, Marco Caselli, and Günther Pernul. 2021. Measuring and visualizing cyber threat intelligence quality. *International Journal of Information Security* 20, 1 (2021), 21–38. DOI : <https://doi.org/10.1007/s10207-020-00490-y>
- [139] Roland Schlöglhofer and Johannes Sametinger. 2012. Secure and usable authentication on mobile devices. In *Proceedings of the 10th International Conference on Advances in Mobile Computing and Multimedia (MoMM'12)*. Association for Computing Machinery, New York, NY, USA, 257–262. DOI : <https://doi.org/10.1145/2428955.2429004>
- [140] Andre Schrimpf, Andreas Drechsler, and Konstantinos Dagianis. 2021. Assessing identity and access management process maturity: First insights from the German financial sector. *Information Systems Management* 38, 2 (2021), 94–115.
- [141] Katherine Schroeder, Hung Trinh, and Victoria Pillitteri. 2024. *Measurement Guide for Information Security: Volume 1—Identifying and Selecting Measures*. National Institute of Standards and Technology. DOI : <https://doi.org/10.6028/NIST.SP.800-55v1>
- [142] Ahmed Seffah, Mohammad Donyaee, Rex B. Kline, and Harkirat K. Padda. 2006. Usability measurement and metrics: A consolidated model. *Software Quality Journal* 14, 2 (2006), 159–178. DOI : <https://doi.org/10.1007/s11219-006-7600-8>
- [143] Ahmed Seffah, N. Kececi, and M. Donyaee. 2001. QUIM: A framework for quantifying usability metrics in software quality models. In *Proceedings of the 2nd Asia-Pacific Conference on Quality Software*. IEEE, NW Washington, DC, United States, 311–318. DOI : <https://doi.org/10.1109/APAQS.2001.990036>
- [144] Sean M. Segreti, William Melicher, Saranga Komanduri, Darya Melicher, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Michelle L. Mazurek. 2017. Diversify to survive: Making passwords stronger with adaptive policies. In *Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 1–12. Retrieved from <https://www.usenix.org/conference/soups2017/technical-sessions/presentation/segreti>
- [145] Nirojan Selvanathan, Dileepa Jayakody, and Violeta Damjanovic-Behrendt. 2019. Federated identity management and interoperability for heterogeneous cloud platform ecosystems. In *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES'19)*. Association for Computing Machinery, New York, NY, USA, Article 103, 7 pages. DOI : <https://doi.org/10.1145/3339252.3341492>
- [146] Daniel Servos and Sylvia L. Osborn. 2017. Current research and open problems in attribute-based access control. *ACM Computing Surveys* 49, 4, Article 65 (2017), 45 pages. DOI : <https://doi.org/10.1145/3007204>
- [147] Rishabh Sharma and Abhishek Singla. 2024. Optimizing cloud security: A study of effective cybersecurity measures for organizations. In *Proceedings of the 2024 International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS)*. IEEE, Bengaluru, India, 277–281. DOI : <https://doi.org/10.1109/ICICNIS64247.2024.10823273>
- [148] Christopher Staite and Rami Bahsoon. 2012. Evaluating identity management architectures. In *Proceedings of the 3rd International ACM SIGSOFT Symposium on Architecting Critical Systems (ISARCS'12)*. Association for Computing Machinery, New York, NY, USA, 11–20. DOI : <https://doi.org/10.1145/2304656.2304659>
- [149] Diane M. Strong, Yang W. Lee, and Richard Y. Wang. 1997. Data quality in context. *Communications of the ACM* 40, 5 (1997), 103–110. DOI : <https://doi.org/10.1145/253769.253804>
- [150] Mark Thomas. 2021. Using ITIL 4 and COBIT 2019 to create an integrated I&T Framework. Retrieved from <https://www.axelos.com/resource-hub/white-paper/using-til-cobit-2019-create-integrated-environment>
- [151] Bianca Trinkenreich, Gleison Santos, and Monalessa Perini Barcellos. 2018. SINIS: A QOM+strategies-based approach for identifying goals, strategies and indicators for IT services. *Information and Software Technology* 100, 100 (2018), 147–164. DOI : <https://doi.org/10.1016/j.infsof.2018.04.006>
- [152] United States Congress. 2002. Sarbanes-Oxley Act of 2002. Corporate responsibility. Retrieved from <https://www.congress.gov/107/plaws/publ204>
- [153] Irene Vanderfeesten, Jorge Cardoso, Jan Mendling, Hajo A. Reijers, and Wil Aalst, van der. 2007. *Quality Metrics for Business Process Models*. Future Strategies, Lighthouse Point, Florida, USA, 179–190.
- [154] Carlos Villarrubia, Eduardo Fernández-Medina, and Mario Piattini. 2006. Metrics of password management policy. In *Proceedings of the Computational Science and Its Applications—ICCSA 2006*, Marina Gavrilova, Osvaldo Gervasi, Vipin Kumar, C. J. Kenneth Tan, David Taniar, Antonio Laganá, Youngsong Mun, and Hyunseung Choo (Eds.). Springer, Berlin, 1013–1023. DOI : https://doi.org/10.1007/11751595_106
- [155] Emanuel von Zeszczwitz, Alexander De Luca, and Heinrich Hussmann. 2014. Honey, i shrunk the keys: Influences of mobile devices on password composition and authentication performance. In *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational (NordiCHI'14)*. Association for Computing Machinery, New York, NY, USA, 461–470. DOI : <https://doi.org/10.1145/2639189.2639218>

- [156] Isabel Wagner and David Eckhoff. 2018. Technical privacy metrics: A systematic survey. *ACM Computing Surveys* 51, 3, Article 57 (2018), 38 pages. DOI : <https://doi.org/10.1145/3168389>
- [157] Yair Wand and Richard Y. Wang. 1996. Anchoring data quality dimensions in ontological foundations. *Communications of the ACM* 39, 11 (1996), 86–95. DOI : <https://doi.org/10.1145/240455.240479>
- [158] Richard Y. Wang, Veda C. Storey, and Christopher P. Firth. 1995. A framework for analysis of data quality research. *IEEE Transactions on Knowledge and Data Engineering* 7, 4 (1995), 623–640.
- [159] Richard Y. Wang and Diane M. Strong. 1996. Beyond accuracy: What data quality means to data consumers. *Journal of Management Information Systems* 12, 4 (1996), 5–33. DOI : <https://doi.org/10.1080/07421222.1996.11518099>
- [160] Jorge Werner, Carla Merkle Westphall, and Carlos Becker Westphall. 2017. Cloud identity management: A survey on privacy strategies. *Computer Networks* 122, 122 (2017), 29–42. DOI : <https://doi.org/10.1016/j.comnet.2017.04.030>
- [161] Alan F. Westin. 1968. Privacy and freedom. *Washington and Lee Law Review* 25, 1 (1968), 166.
- [162] Phillip J. Windley. 2005. *Digital Identity: Unmasking Identity Management Architecture (IMA)*. O'Reilly Media, Inc., Sebastopol, CA.
- [163] Peter Wood. 2005. Implementing identity management security - an ethical hacker's view. *Network Security* 2005, 9 (2005), 12–15. DOI : [https://doi.org/10.1016/S1353-4858\(05\)70282-8](https://doi.org/10.1016/S1353-4858(05)70282-8)
- [164] Chengcheng Xiang, Yudong Wu, Bingyu Shen, Mingyao Shen, Haochen Huang, Tianyin Xu, Yuanyuan Zhou, Cindy Moore, Xinxin Jin, and Tianwei Sheng. 2019. Towards continuous access control validation and forensics. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS'19)*. Association for Computing Machinery, New York, NY, USA, 113–129. DOI : <https://doi.org/10.1145/3319535.3363191>
- [165] Dianxiang Xu, Lijo Thomas, Michael Kent, Tejeddine Mouelhi, and Yves Le Traon. 2012. A model-based approach to automated testing of access control policies. In *Proceedings of the 17th ACM Symposium on Access Control Models and Technologies (SACMAT'12)*. Association for Computing Machinery, New York, NY, USA, 209–218. DOI : <https://doi.org/10.1145/2295136.2295173>
- [166] Zhongyuan Xu. 2014. *Mining Meaningful Role-Based and Attribute-Based Access Control Policies*. Ph. D. Dissertation. State University of New York at Stony Brook.
- [167] Yi Yang, Kheng Cher Yeo, Sami Azam, Asif Karim, Ronju Ahammad, and Rakib Mahmud. 2020. Empirical study of password strength meter design. In *Proceedings of the 2020 5th International Conference on Communication and Electronics Systems (ICCES)*. IEEE, Coimbatore, India, 436–442. DOI : <https://doi.org/10.1109/ICCES48766.2020.9137964>
- [168] Emrah Yasasin and Guido Schryen. 2015. Requirements for IT security metrics—An argumentation theory based approach. In *Proceedings of the 23rd European Conference on Information Systems (ECIS 2015)*. AIS, Münster, Germany, 1–16. DOI : <https://doi.org/10.18151/7217537>
- [169] Kurt Zeilenga. 2006. *Lightweight Directory Access Protocol (LDAP): Directory Information Models*. RFC 4512. DOI : <https://doi.org/10.17487/RFC4512>
- [170] Xiaotong Zhou, Debiao He, Jianting Ning, Min Luo, and Xinyi Huang. 2023. AADEC: Anonymous and auditable distributed access control for edge computing services. *IEEE Transactions on Information Forensics and Security* 18, 18 (2023), 290–303. DOI : <https://doi.org/10.1109/TIFS.2022.3220030>

Received 21 August 2023; revised 20 November 2025; accepted 8 January 2026