applied sciences

MDPI

Article

Combining SABSA and Vis4Sec to the Process Framework IdMSecMan to Continuously Improve Identity Management Security in Heterogeneous ICT Infrastructures

Daniela Pöhn *, Sebastian Seeber and Wolfgang Hommel

Universität der Bundeswehr München, Research Institute CODE, 85579 Neubiberg, Germany
* Correspondence: daniela.poehn@unibw.de; Tel.: +49-(0)89-6004-7356

Abstract: Identity management ensures that users have appropriate access to resources, such as ICT services and data. Thereby, identity management does not only identify, authenticate, and authorize individuals, but also the hardware devices and software applications which the users need for access. In consequence, identity management is an important element of information security management (ISM) and data governance. As ICT infrastructures are constantly changing, and new threats emerge, identity management has to be continuously improved, just like any other business process. In order to align the identity management process with business requirements, and provide a systematic approach supported by reporting and supporting visualizations, we apply Sherwood Applied Business Security Architecture (SABSA) and Visualization for Security (Vis4Sec) together in our approach, IdMSecMan (identity management security management). We first introduce IdMSecMan, before applying it to the central technical process activities of identification, authentication, and authorization. Our approach is underlined by a case study. Thereby, we, for example, see that enabling multi-factor authentication in organizations impacts other areas that may be overlooked without a structured approach. With IdMSecMan, we provide a process framework to align all decisions and to constantly improve identity management within organizations and inter-organizational collaborations.

Keywords: identity management; enterprise architectures; SABSA; continuous improvement; information security

Citation: Pöhn, D.; Seeber, S.; Hommel, W. Combining SABSA and Vis4Sec to the Process Framework IdMSecMan to Continuously Improve Identity Management Security in Heterogeneous ICT Infrastructures. *Appl. Sci.* **2023**, *13*, 2349. https://doi.org/10.3390/app13042349

Academic Editors: Gianluca Lax and Antonia Russo

Received: 29 December 2022
Revised: 8 February 2023
Accepted: 10 February 2023
Published: 11 February 2023

1. Introduction

Authentication is a critical technical verification process to confirm that the pretended user is the actual user. Classical simple methods, like usernames and passwords, are still often used, where service backends or identity management systems store passwords in a salted, hashed format. However, from the usability perspective, passwords come with the problem that users tend to reuse them across several services [1]. In the case of password leaks, this may result in credential stuffing attacks, where attackers try the same credentials at different services. Without enforcing password policies, passwords may also be guessable; for example, through wordlists or information gathered via social engineering attacks. Social engineering may be utilized to collect credentials via, for example, phishing emails and websites. Several popular web service providers, such as Google and Amazon, employ multi-factor authentication (MFA) as an optional security feature. Security practitioners in organizations also face serious challenges securing their systems, where MFA is one possible additional security method [2].

In order to enroll MFA, several processes and concepts have to first be in place. Not all applications used within an organization or inter-organizational collaboration may support MFA at all, or may, at least, be limited to selected MFA solutions. Users require more time for the login process, which may lead to them trying to bypass MFA. Even when using widely available technology for MFA, such as smartphone-based authenticator apps

applying Time-based One-Time Passwords (TOTPs), enabling MFA for a single service which may require only a simple click for a system administrator, there are several more aspects to consider. The complexity of this task makes it difficult for security practitioners to enroll and improve MFA. Security standards and frameworks are either too broad or too narrow for this topic, while enterprise architecture frameworks have the drawback of often not sufficiently covering security aspects. This is also true for several research approaches. In addition, MFA is only one of many aspects of identity management (IdM) related to the central technical processes of identification, authentication, and authorization used in every organization.

As a structured solution, we propose IdMSecMan, a security management process tailored for IdM. The process cycles are based on Visualization for Security (Vis4Sec) [3] and the Sherwood Applied Business Security Architecture (SABSA) [4,5], which, in combination, help to measure and continuously improve the maturity of the identity management activities aligned to business requirements. Thereby, IdMSecMan brings together business management and security, enabling the controlled introduction and improvement of authentication methods, as one example.

This article enhances our previous work [6] in several ways. Whereas the first version of IdMSecMan concentrated on identities in servers, our latest results widen the area to identity management with the central technical process activities of identification, authentication, and authorization in general. We especially focus on important examples, such as MFA. In addition, SABSA was integrated to align the security improvements with the business processes and requirements. In consequence, every aspect from top to bottom is considered.

Thereby, we provide the following *contributions*: (1) a framework for improving the security of identity management and its aspects, in alignment with business management, with a visual overview; (2) adaption for the introduction of national electronic identities (eIDs), MFA, and risk-based authentication (RBA) in respect to zero trust architecture (ZTA); (3) an evaluation based on a case study. The case study features the computer science (CS) department at a university with different user groups, projects, and resources (central and decentral).

The remainder of this article is organized as follows. We start with a motivating scenario in Section 2. In Section 3, we briefly describe the background and related work. Based on the concept of IdMSecMan, in Section 4, we apply the framework to the areas of eID, MFA, and RBA in Section 5. IdMSecMan is then evaluated based on a case study in Section 6. We discuss our approach and application in Section 7. Section 8 concludes the article with a brief discussion and outlook to further research.

2. Motivating Scenario

The supply chain attack on SolarWinds' Orion software in 2019 and 2020 was one of the most impactful for many organizations [7]. The attack was noticed by the cyber-security company FireEye. FireEye, like many other organizations, monitored its own network with the Orion platform. The attack went unnoticed for months. The attackers then proceeded to connect to the FireEye Virtual Private Network (VPN) by adding a cell phone as an approved device for two-factor authentication on an employee's account. When a new device is added to an employee's account at FireEye, it triggers an alert to the system administration, which was followed up, and, thereby, it was discovered that a second phone was registered and the newly added phone was not the employee's phone. In order to register another factor, the employee's username and password had to be already known to the attackers.

In further investigation, the hack became visible. The attackers were able to access and modify the source code for Orion on SolarWind's internal repositories. SolarWinds used the weak password "solarwinds123" for File Transfer Protocol (FTP), which was additionally checked into a public repository at GitHub. After the malware was inserted in Orion's source code, a backdoor was planted onto FireEye's network. The backdoor was

then used to access domain credentials, such as user accounts and passphrases. In stage three, token-signing certificates were used to access Office 365; for example, specific email accounts. This was the first occurrence of a Golden Security Assertion Markup Language (SAML) attack in the wild. At this stage, trusted domains were also modified or added and credentials were compromised. Last, but not least, the red team tools were stolen from FireEye. As a consequence, FireEye had to publish its internal tools and signatures for them to be recognized to avoid their misuse [8].

Crawlers can search for sensitive information in public repositories and use the information after its discovery. Consequently, such information should never be published. Even without publishing, a weak password could, similarly to default passwords, easily be brute-forced; for example, by wordlists and dictionary-based attacks. If passwords are reused, attackers, who know one of them, can try to guess further credentials based on their knowledge. This shows that passwords with a low entropy pose a threat to organizations and should be avoided by, for example, enforcing quality-ensuring password policies. Depending on the criticality and the possible methods, further factors might be required for using a specific service. Even though a self-service portal for users improves usability and reduces the hassle in contacting the service desk, further checks during the authentication lifecycle, for example, when enrolling additional factors, are required.

3. Background and Related Work

This section gives a brief overview of identity management with the central technical process activities of identification, authentication, and authorization, before explaining the process frameworks Vis4Sec, SABSA, and related approaches.

3.1. Identity Management

Within an effective identity security framework, the three activities of identification, authentication, and authorization work together to keep the resources secure. The identification mainly takes place during the provisioning, i.e., the second phase of the identity lifecycle. The identity lifecycle [9] can be adapted from the Deming Cycle [10]. Authentication and authorization, short AuthNZ, provide the user with access to the requested services if the permissions are good enough. The relevant element of the user account lifecycle is the user resp., the digital identity, as shown in Figure 1. The lifecycle includes the following phases:

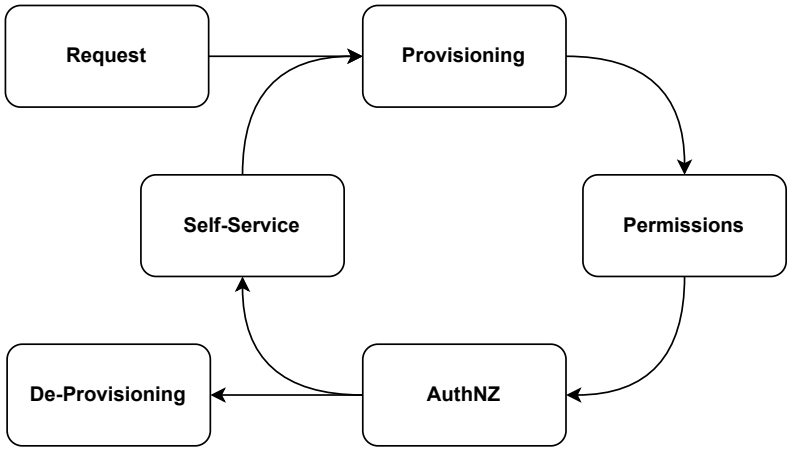

Figure 1. User account lifecycle based on [9].

Request: The user requests an account at an organization.

Provisioning: The account is provisioned (attributes, roles, and permissions) and assigned to an entity after identification.

Permissions: The permissions are set for the account.

Authentication and Authorization: For accessing resources, such as services or data, the user must first be authenticated, using their identifier and the pre-defined authentication method(s). Then, the service checks the authorization of the user.

Self-Service and Core Account Management: The user can access a self-service to change information, such as MFA methods. At the same time, the user makes use of identity management.

De-Provisioning: In the end, the user account is de-provisioned.

In the following, we describe the main processes during the usage of an identity, i.e., identification, authentication, and authorization.

3.1.1. Identification

Identification is the starting point for digital identities, as the user presents proof of his or her real-world identity. Users are typically assigned unique identifiers during enrolment by organizations. These identifiers are then utilized as logins or usernames for services. According to L'Amrani et al. [11], an identity represents an entity, such as a person, an organization, or resources. It is defined for a specific context and has certain characteristics, either artificially defined or natural.

While the process of assigning a digital identifier to a person is a standard process in many organizations, the certainty that the person is actually the person they pretend to be differs. In order to characterize these and other differences, levels of assurances (LoAs) are applied for cross-organizational contexts. One example of a LoA is the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, where enrolment and identity proofing are described in document A [12]. The lowest level, i.e., identity assurance level (IAL) 1, has no requirements to link the applicant to a specific real-life identity. IAL 2 supports the real-world existence of the claimed identity and verifies that the applicant is associated with this real-world identity. The highest level of IAL 3 requires physical presence for identity proofing. Although identification is important in practice, it is almost not regarded in research [13]. Exceptions are the identification of users on mobile devices [14,15], in virtual reality (VR) settings [16,17], and across social networks [18,19].

3.1.2. Authentication

Authentication is the stage where the user proves their claimed identity by providing at least one authentication method assigned to the identifier. Often, the provided credential is a password, i.e., something-you-know, even though many users make a poor choice on passwords [20]. Other method categories are something-you-have, like an access card or token, or something-you-are, for example, a fingerprint or other biometric data. Bachmann [21] provides an overview of different methods, which are roughly compared by Miessler [22]. Credentials, usually the three different categories, can be combined for MFA to increase overall security. A common form of MFA is Two-Factor-Authentication (2FA). However, this, at the same time, poses the risk of getting locked out of one's account when losing one of the factors. The security and further aspects of authentication is categorized in NIST SP 800-63 B [23].

Several approaches compare and improve MFA for web applications and specific settings like cyber-physical systems [24] or mobile scenarios [25]. Realpe et al. [26] proposed a set of heuristics to evaluate the security, usability, and other characteristics of user authentication, whereas Timón López et al. [27] evaluated legal aspects of user-device authentication in the Internet of Things (IoT) settings. In order to continuously improve the current state, a structured process is required. Security frameworks and standards provide either a narrow, or a broad, overview, but do not go into technical details. Damon and Coetzee [28] proposed an identity and access assurance model based on SABSA, covering generic identity management. No specific approaches for authentication and MFA were known to the others. Das et al. [29] analyzed the participants' perception of MFA.

The authentication lifecycle, according to NIST [23], comprises the following phases, as visualized in Figure 2. In addition, a backup strategy needs to be established.

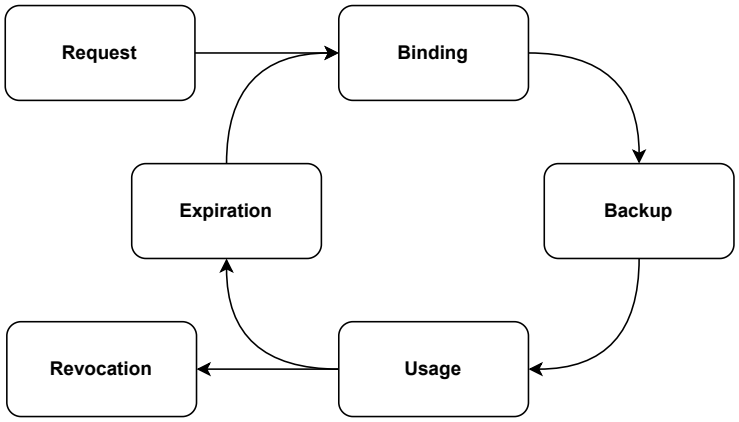

Figure 2. Authentication Lifecycle according to NIST [23].

Authenticator Binding: In the beginning, an association between a specific authenticator and a subscriber's account is established. This enables the authenticator to be used to authenticate that account. The binding includes binding at enrolment, post-enrolment binding, and binding to a subscriber-provided authenticator.

Renewal, Loss, Theft, Damage, and Unauthorized Duplication: Potentially compromised and malfunctioning authenticators need to be guarded against any possibility of extraction of the authenticator secret. For the following processes, the incident should be reported and a backup or an alternate authenticator should be used instead.

Expiration: Authenticators may expire and should not be used for authentications. In consequence, a renewed authenticator should be issued if required.

Revocation and Termination: At the end of the lifecycle, an authenticator is revoked, i.e., the binding between an authenticator and a credential is removed.

During all stages of the lifecycle, different threats are possible, such as theft, duplication, and eavesdropping. In consequence, all potential threats have to be known and, depending on the risk management, adequately mitigated.

3.1.3. Authorization

After the user has been authenticated, authorization provides the answer to the final question during resource access: "Is the user allowed to access the resources?". Authorization describes the following: (1) the organizational process of granting access permissions to identities, and (2) the technical process performed by the ICT services whenever a user attempts to access protected resources. Organization-wide identity management controls which ICT services a user is allowed to access. The more fine-grained access permissions are specific to each ICT service and managed locally; for example, by using access control lists for file servers, the eXtensible Access Control Markup Language (XACML), or other proprietary management interfaces for services [30]. This step is also called policy specification.

Access control policies are mostly logical statements, which result from an identity's attributes, roles, and the structure of the organization. According to the *principle of least privilege* or *need-to-know*, each identity should only receive those permissions that are needed to fulfil its tasks. Modern access control policy languages support a higher degree of dynamics; for example, with risk-based authentication. As an example, sensitive data may only be accessed during office hours from a known device within the office. Other attempts are blocked, based on the current time, device certificate, and Internet protocol (IP) address. Misbahuddin et al. [31] provided an overview of different factors. Though this gives more flexibility and might reduce the total amount of authentication factors,

it also increases the complexity and can lead to user frustration [32–34]. RBA can be applied in different scenarios, such as border control [35], online accounts [36], and mobile devices [37]. Leiba described [38] Open Authorization (OAuth), a protocol focusing on web authorization. This could be used for identity federations, i.e., a circle of trust of several cooperating organizations sharing web-based services with their users. Nevertheless, in such an identity federation, the home organization typically sends more attributes to the service provider than required, as pointed out by Nishioka and Okabe [39].

As mentioned by Fujun and Junshan [40], trust is an important aspect during authorization. Access control can prevent illegal operations of users and protect security. In consequence, the system needs to estimate the trust in the applicant resp. the authentication and apply different roles and permissions (policy evaluation and enforcement). Zero trust architectures [41] continuously monitor the trust during regular authorizations and re-evaluate the trust related to the action. Depending on the evaluation and the requested resources, either one or up to multiple factors are required for authentication, or access is not granted at all. The UK's National Cyber Security Centre (NCSC) released a guideline on zero trust architecture design principles in 2021 [42]. Similarly, Wylde [43] provided an overview of ZTA. Dimitrakos et al. [44] proposed such an approach for consumer IoT. In the context of identity federations, ZTA could be used [45]. Bobbert and Scheerder [46] evaluated the implementation of ZTA. The authors formulated four critical success factors: (1) alignment with risk management and existing frameworks; (2) board and business involvement and explicit sign-off; (3) ownership for asset risks and measures; (4) focus on the change and on the run. This shows alignment with business management is important.

3.2. Continuous Improvement Process Framework Vis4Sec

Continuous improvement is applied in several standards, such as the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001 [47], and, hence, is an established topic with fewer current publications having a focus on security. Bilbao and Bilbao [48] summarized how to measure security, whereas Sun et al. [49] measured the effectiveness of information security controls. Yang et al. [50] emphasized the involvement of employees. Zeb et al. [51] assessed security during the migration of virtual machines. In contrast, Brunner et al. [52] proposed tool support to continuously improve security. Sacher [53] described how to better integrate continuous improvement into security monitoring by utilizing post-incident activities.

The process framework Vis4Sec for security visualization. introduced in [3,54] and adapted for Linux server authentication in [6], enhances the Deming cycle [10] by visualization. It supports the generation of an overview and the manageability of an organization's ICT, its processes, selected security-specific tasks, and the data they rely on. Vis4Sec thereby generates knowledge for various stakeholders and the organization through transfer and transformation. In consequence, it consists of the following states and phases (see Figure 3):

Initiation: Information about the environment, requirements, stakeholders, and planned actions are gathered.

Question Phase: The question is driven by the goal of the current iteration; for example, the result of a security incident or the goal to improve security.

Data Management Phase: Required data and its sources are identified, and a data model is utilized. The data is then collected and analyzed. This step consists of the phases: (1) define data; (2) acquire data; (3) analyze data; (4) ensure data quality; and (5) dispose or reuse data (see Figure 3).

Visualization Phase: The data is visualized to provide actionable information in an overview. This might be stakeholder-dependent.

Interaction Phase: The data source quality and stakeholder-specific visualizations are presented, leading to communication between the stakeholders.

During iterations, postponed issues are reviewed and related questions, data sources, visualizations, and interactions are refined, based on feedback.

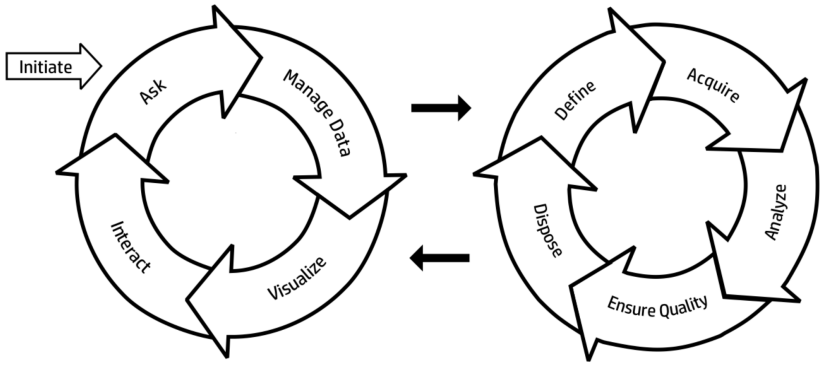

Figure 3. Process Framework Vis4Sec [54].

3.3. Enterprise Security Architecture SABSA

Enterprise Architecture (EA) is a business function focusing on the structures and behaviors of business roles and processes that create and use business data. Thereby, EA is at the highest level of the architect hierarchy. Various EA frameworks exist, including SABSA. SABSA [4,5] is a methodology and standard for developing business-driven, risk and opportunity-focused enterprise security and information assurance architectures. The goal is to deliver security infrastructure solutions that, in a traceable manner, support critical business initiatives. The framework consists of several integrated frameworks, models, methods, and processes. It follows Zachmann's methodology [55] of distinct and controlled layers, which try to answer the questions "What is done on this layer?" and "How are the requirements fulfilled on this layer?". The layers, ranging from contextual to management, are described in Table 1. According to Pleinevaux [56], the meta-model of SABSA consists of the architectural levels (what, why, how, who, where, and when), and common entity attributes (ID, name, description, category, source, and owner), as well as the domain model, business attribute profiles, risk and opportunity framework, roles and responsibilities, trust framework, architectural strategies, and through-life risk management.

Table 1. SABSA Matrix based on [57].

SABSA Layer	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	Business goals and decisions	Business risks	Business meta-processes	Business governance	Business geography	Business time dependence
Conceptual	Business value and knowledge strategy	Risk management strategy and objectives	Strategies for process assurance	Security and risk governance; trust framework	Domain framework	Time management framework
Logical	Information assets	Risk management policies	Process maps and services	Trust relationships	Domain maps	Calendar and timetable
Physical	Data assets	Risk management practices	Process mechanisms	Human interface	Infrastructure	Processing schedule
Component	Component assets	Risk management components and standards	Process components and standards	Human entities: components and standards	Locator components and standards	Step timing and sequencing components and standards
Management	Delivery and continuity management	Operational risk management	Process delivery management	Governance, relationship and personal management	Environment management	Time and performance management

Al-Turkistani et al. [58] compared several EA frameworks, like SABSA, The Open Group Architecture Framework (TOGAF), and Control Objectives for Information and Related Technology (COBIT) 19, concluding that these EA frameworks were generally missing cyber-security. SABSA complied with existing security standards and, thereby, these should be used in addition. Bulusu et al. [59] applied SABSA to choose suitable security requirements. Similarly, Rajba [60] utilized SABSA to receive more secure applications. Other authors customized SABSA for their areas. Najib et al. [61] adapted SABSA and ISO/IEC 27000 for oil and gas business activities. Martynov and Shiryaev [62] outlinef their EA for the energy sector. Rubio et al. [63] proposed an architecture based on the Open Security Architecture (OSA) concepts and SABSA methodology for SMEs. Mayer et al. [64] used an integrated conceptual model for information system security risk management by utilizing SABSA. However, this approach was rather generic and tailored to the area of home care. Sialm and Knittl [65] gathered their requirements for eIDs from SABSA but did not otherwise use SABSA.

3.4. Summary

Although several approaches targeted identity management and their central technical process activities of identification, authentication, and authorization, no approach found by the authors tried to improve security by an integrated method. Hence, no approach focused on improving identity management in alignment with business management, although this is important in business environments. In consequence, we proposed IdMSecMan to fill this gap. IdMSecMan's approach is outlined in Figure 4. Vis4Sec mainly concentrates on server security. Nonetheless, this approach can be used as a basis. Continuous improvement processes are relevant to improve, in our case, the security of any organization. This is the case as identity management is used for humans, legal persons, devices, and applications in every organization, ranging from universities and eGovernment to health care and industry. According to Guimarães et al. [66], visualization for business management is underrepresented. This state seems not to have changed since their publication. To align with business management, SABSA can be applied. Few approaches adapt SABSA for security risk management or the gathering of requirements for their use case. In consequence, we used [6] as a basis and developed an integrated framework to improve security related to identity management.

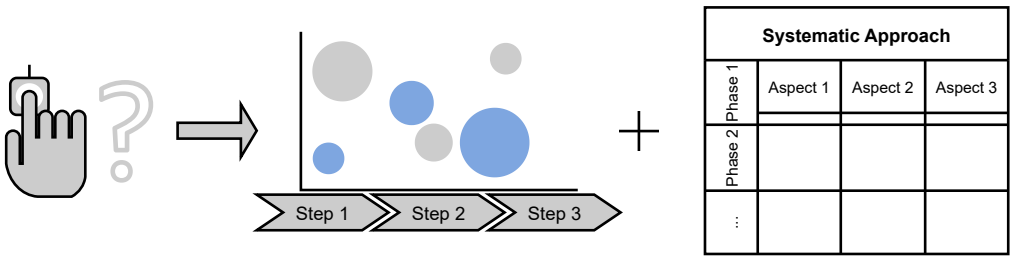

Figure 4. Approach of IdMSecMan.

4. Process Framework IdMSecMan

The process framework IdMSecMan collects and aggregates relevant data, such as log files, inventory, user groups, and permissions, taking existing organizational and security-relevant information into account. It combines Vis4Sec and SABSA. The process, based on the Vis4Sec approach by Hanauer et al. [3], provides a framework to acquire, aggregate, visualize, and distribute the gathered information, as visualization provides a useful extension for improvements, to identity management [6] and consists of the following:

Initiation: Information about the environment, requirements, stakeholders, and planned actions are collected. One possible input for the process run are selected security controls.

Question Phase: This phase is driven by the goal of the iteration; for example, a security incident or an asset. In order to improve the results in a managed and structured way, only one question per iteration is asked.

Data Management Phase: Required data and relevant data sources are identified and the data model is utilized. If data is not needed anymore, it is disposed of, while the data sources are refined during the iteration runs.

Visualization Phase: Overview representing the data, along with the quality of each source, for the process, entries, and metrics. The visualization provides a quick overview, helping to improve security by providing actionable information for the stakeholders.

Interaction Phase: Postponed issues are reviewed and the questions, data sources visualizations, and interactions are refined. After the feedback from the stakeholders is received, a new iteration of the process can start.

SABSA applies a layered approach to answer the questions of what, why, how, who, where, and when at different business levels. The development process of SABSA follows the lifecycle of a security architecture and, hence, can be mapped to the lifecycle of processes, like authentication. By integrating SABSA into Vis4Sec, we derived a method to develop security aspects related to identification, authentication, and authorization (IAA), as well as the governance and management of identities in an integral way, which could be continuously improved, helping to prevent situations like the motivating scenario. IdMSecMan answers the organization's internal questions "Who when why needs identification, authentication, and authorization for what applications, how, and with which policies?". We describe each phase of IdMSecMan in the following.

4.1. Initiation

We utilized the layers of SABSA to identify the relevant information about the following: (1) environment, (2) stakeholders, (3) controls, and (4) requirements. Generally, environment (1) consists of several applications and some sort of identity management system. The stakeholders (2) include users (humans, organizations, devices, etc.), system administrators, security practitioners, (ICT) management staff, and maybe other staff members. Most likely, the users do not receive reports. Nevertheless, they are important for the usability of the result. Controls (3) depend on the actual application, but might be derived from standards, such as NIST SP 800-63 and 800-53. There are several standards with security controls for different use cases. NIST SP 800-63 focuses on identity management. Nonetheless, the security controls need to be adapted for the organization-specific environment and further standards may be incorporated. The SABSA framework proposes a list of high-level business security concerns, which are refined for the specific business attributes (4). The list can be extended with new criteria, similar to [59]. In this section, we describe the outline of IdMSecMan before applying the approach to three selected areas.

4.2. Question Phase

We utilized the different contextual layers of SABSA in our controlled cycles. By doing so, the following questions and layers were targeted. After answering these questions, an extensive overview was gained, which was the basis to improve the current state.

Contextual: What is the business risk without proper IAA, governance, and management? What are the requirements for improved identity management? How should improved identity management be implemented and for which areas? What are the legal and regulatory restrictions?

Conceptual: What goals and design does an improved identity management follow? What exactly does improved identity management look like and what is it supposed to achieve? How should it be integrated into the current infrastructure?

Logical: Which logical components does an improved identity management (software, hardware, backup, ...) have? What should improved identity management protect and how to protect identity management? How to make identity management with the central technical process activities of identification, authentication, and authorization usable for the users?

Physical: What are the specifications and processes for improved identity management? What are the physical components? What is the content of the monitoring (identity management with its central technical process activities identification, authentication, and authorization with underlying management, governance, and policies, including their lifecycles) and how is it carried out? What are the necessary standards, procedures, baselines, interfaces, and process steps for improved identity management?

Component: Which products, applications, tools, and people are being used to improve identity management? Are components required to provide the lifecycle?

Management: How is improved identity management maintained, updated, and upgraded? What can be automated? What operational aspects, like the service desk and self-service portal, do we have to consider? How to ensure the security of improved identity management?

4.3. Data Management Phase

When a question (for example, "What is the business risk without proper IAA, governance, and management?") is selected, the indicators and measures need to be acquired. For the first question, the data may include the risks of incidents with resp. without improved identity management, as well as the related business damage caused by an incident and the costs to improve and extend identity management. This might be broken down into different areas, as described in the application. For the calculation of the risks of an incident, the risks first need to be identified. The risk assessments include the assets, potential consequences, threats, and levels, as well as the likelihood of their exploitation. Then, they can be analyzed and measured. If, within the organization, no proper ICT risk management is yet in place, at least the consequences of an incident should be evaluated.

4.4. Visualization Phase

The visualization phase provides actionable information, for example, business risk per application and user group with and without improved identity management, by offering a quick overview. As improved identity management is rather generic, specific aspects should be regarded in more detail by corresponding visualizations.

4.5. Interaction Phase

During the interaction phase, the visualizations are presented and discussed within the stakeholder groups. Reactions are embedded into the feedback system, while actions taken and the process run are summarized.

4.6. Next Iterations

Either the question is further refined and improved or, if no additional actions are required, the next iteration starts with a new question. Here, the following question in the contextual layer was picked: "What are the requirements for improved identity management?". Especially in the beginning, asking all questions of IdMSecMan requires time.

5. Application of IdMSecMan

In this section, we applied IdMSecMan in the areas of identification (see Section 5.1), authentication (see Section 5.2), and authorization (see Section 5.3). The applications explain the contribution of IdMSecMan practically. Table 2 provides an overview of which action of identity management is relevant on which SABSA layer. The table indicates that identification, authentication, and authorization need to work hand in hand. While

authentication is progressing in research and practice, identification and authorization are less regarded. The context of these applications is summarized in Table 3. Here, the assets (what), motivation (why), process (how), people (who), location (where), and time (when) are specified for identity management and identification, authentication, and authorization, according to SABSA's scheme. This ensured the architectural traceability and justification for the elements of the architecture. All aspects of identity management are relevant anytime. Based on the table, we see that policies are important besides technology. Hence, security controls are needed for both sides. The individual actions are detailed in the following by applying the use case.

The descriptions were partly based on the computer science department of a university used for the case study in Section 6. The production environment mainly consisted of various physical, and especially virtual, Linux-based machines for different purposes, including operations and infrastructure. In addition, several heterogeneous laboratory infrastructures operated. The infrastructure, hence, consisted of different user groups, projects, and resources (central and decentral) with various requirements of trust, data protection, and security. While central services (such as project management software and GitLab), and servers for projects, were administrated centrally, professors and researchers might also run their own infrastructures. The projects again had different requirements, ranging from public to restricted projects. Even though the risks and benefits of changes typically did not result in a higher budget, security incidents might have consequences for upcoming projects and collaborations. As a consequence, their risks were estimated based on that.

Table 2. Integration of SABSA with IdMSecMan.

SABSA Layer	Identity Management	Identification	Authentication	Authorization
Contextual	Organizational structure and regulations	GDPR	Costs of, e.g., incidents	
Conceptual	Stakeholders, policies, processes	Concepts for identity proofing and verification	Authentication concept	Role concept
Logical	Assets, logical components	Trust	Trust	Privileges, trust
Physical	User interface, security	Identification methods	Authentication methods, physical components	Access control system
Component	Functions, components for security	Identification	Authentication components	Access, roles
Management	User support	Identification management	Authentication lifecycle	Control lists

Table 3. Context of IdMSecMan.

SABSA	What	Why	How	Who	Where	When
Identity Management	Management of identities	Security	Processes, policies, best practice	Stakeholders	Anywhere	Anytime
Identification	Digital identity	Management of identity	Processes related to identities	Stakeholders	Anywhere	Anytime, business hours
Authentication	Authentication of user	Verifying identities	Authentication lifecycle	Stakeholders	Anywhere	Anytime, business hours
Authorization	Access to resources	Access protection	Access policies	Stakeholders	Anywhere	Anytime, business hours

5.1. Process for Identification

According to NIST SP 800-63A, identity proofing has the following expected outcomes: (1) resolving a claimed identity to a single, unique identity of a user; (2) validating that the supplied evidence is correct and genuine; (3) validating that the claimed identity exists; and (4) verifying that the claimed identity is associated with the real person claiming the identity. Depending on the assurance, different LoAs resp. IALs are provided. In consequence, attributes, such as full name, date of birth, and home address, might be provided with the identification for resolution. This evidence is then validated and verified.

Traditionally, ID cards were used as the primary source of identity proofing in many countries. For example, future employees had to show their ID cards in a face-to-face setting to be physically verified. Similarly, students presented their IDs card during enrolment. This process has partly changed over the last few years. Students may present their ID cards for the first time during their first exams. However, other physical and digital methods might also be possible, including eID, driver's licenses, and social accounts. These may make identity proofing more flexible but can have other dependencies and consequences, such as a higher resp. a lower level of trust and requirements for data collection. By integrating SABSA, we derived a method to decide on the following question in an integral way: "Who when why needs which identity proofing (such as eID) for what application and how?". We outline each phase in the following.

5.1.1. Initiation

We first identified the relevant information about the environment, stakeholders, controls, and requirements. In order to prove the identity before, during, or after enrolment, we needed some sort of identity proofing. Hence, the stakeholders comprised users, system administrators, security practitioners, and ICT and HR management staff. If the eID integration of the university could be used by the different departments, then CS might apply it; for example, for the registration of Network Access Control (NAC) access with acceptance of the terms of use. Controls were taken from NIST SP 800-63A, which describes identification. The threats of identity proofing include falsified identity proofing evidence, fraudulent use of an identity, and enrolment repudiation. With artificial intelligence, a context in which identity theft may become more difficult to identify. The requirements partly resulted from that standard as well. The issuing source of the evidence confirmed the claimed identity through some sort of identity-proofing process with a reasonable assumption about the result delivered. Depending on the requirements of the organization, stronger evidence might be necessary. The organization of the user case wanted strong evidence requirements. As a result, facial portraits, physical security, expiration dates, and further elements had to be part of the evidence. In consequence, eID might be a suitable type of digital evidence.

5.1.2. Question Phase

Vis4Sec requires controlled process cycles. In order to enable them, we used SABSA with its layers. We started with the first question of the contextual layer and gathered related information. We then proceeded either by refining and improving the question or moving on to the next question. Thereby, we proceeded from the top down until we answered the last question of the management layer.

Contextual: What is the business risk without the usage of a proper and usable identification proof, such as eID? What are the requirements for eID? How should eID be integrated and for which areas? What are the legal and regulatory restrictions? What are the consequences of eID in relation to the General Data Protection Regulation (GDPR) or other data protection regulations?

Conceptual: Which concepts for identity proofing and verification are possible? What goals and design does the usage of eID follow? How should they be integrated into the current infrastructure?

Logical: What level of trust in the identification is required? For which areas is a higher level of trust needed? Which identification methods provide which level of trust? Which logical components are necessary for the eID integration (software, hardware, backup, ...)? What should eID protect and how to protect eID and its information? What are the threats?

Physical: Which identification methods can and should be used? What are the specifications and processes for integrating eID? What are the physical components? What is the content of the monitoring and how is it carried out?

Component: Which products, applications, tools, and people will be using eID? Are additional components required?

Management: How is the eID integration maintained, updated, and upgraded? What operational aspects do we have to consider due to the integration of eID (service desk, cross-organizational processes, etc.)? How to ensure the security of the integration?

5.1.3. Data Management Phase

In this phase, we first identified the required data for the question "What is the business risk without the usage of a proper and usable identification proof, such as eID?". As we already had identity proofing, we collected the related data of the process, problems, and possible improvements. Next, we estimated the costs for integrating eID for either specific or for all users and compared the pros and cons. By implementing and operating an eID integration, the ID could be verified online without the hassle of traveling to the HR department before actually starting employment. This would reduce the number of appointments for the HR department, but required proper maintenance and data handling. In addition, further use cases which might apply the eID integration were summarized.

5.1.4. Visualization Phase

The visualization phase makes two ways of identity proofing, i.e., ID card and eID, visually comparable. Thereby, costs, time reduction, etc. can be used for management meetings and decisions.

5.1.5. Interaction Phase

The visualizations are presented and discussed with the stakeholders. In our example, management visualizations were used to debate and decide about the next steps.

5.1.6. Next Iterations

Either the question is refined or the next question is selected. With the first version of the electronic Identification, Authentication and trust Services (eIDAS) regulation, the integration of eID largely depended on the actual country. For example, in Germany, high requirements must be met. In addition, financial constraints may reduce the likelihood of integration. Due to the upcoming eIDAS version 2.0, this may change. As a certain time frame was blocked for the evaluation, the management decided to continue. In this case, the management noticed that the integration of eID might be beneficial and now looked into the requirements for eID. These were more complex than with ID cards, as shown in Table 4. The following summarizes IdMSecMan for eID:

What: Security and usability related to identity proofing by deciding on the integration of eID.

Why: Improve security and usability related to identification in a controlled way according to business needs.

How: Controlled cycles with data based on business processes and identity proofing.

Who: Stakeholders.

Where: Anywhere.

When: Business hours.

Table 4. Integration of SABSA with eID.

SABSA Layer	eID
Contextual Conceptual Logical	Processes, procedures, policies, GDPR, local regulations and law, trust, threats, contracts and liabilities
Physical Component	Internal (Portal for identity proofing, which might be combined with the self-service portal, proxies, applications, etc.) and external (eID wallet/app/reader) technology with related security
Management	Internal and cross-organizational governance, monitoring, and service management

5.2. Process for MFA

The development process of SABSA follows the lifecycle of a security architecture and, hence, can be mapped to the lifecycle of the authentication process. By integrating SABSA into Vis4Sec, we derived a method to develop security aspects related to MFA in an integral way, which could be continuously improved, helping to prevent situations like that in the motivating scenario (see Section 2). MFASecMan, the application of IdMSecMan on MFA, answered the organization's internal question "Who when why needs MFA for what applications and how?". We describe each phase of MFASecMan in the following.

5.2.1. Initiation

We used the layers of SABSA to identify the relevant information. Generally, the environment consisted of several applications and some sort of identity management system. The stakeholders included users, system administrators, security practitioners, but also management staff. Even though the users did receive reports, their opinion about usability was crucial for success, as MFA introduced additional complexity. Generic controls could be taken from standards, such as NIST 800-53 [67], though they needed to be adapted for the environment. Similar to identification, NIST SP 800-63 B differentiates three authenticator assurance levels. Depending on the level, various authenticator types are allowed. In addition, validation, reauthentication, security controls, and several resistance types are described. The threats for authentication comprise assertion manufacture or modification, theft, duplication, eavesdropping, offline cracking, side channel attack, phishing and other types of social engineering, online guessing, endpoint compromise, and unauthorized binding. Mitigation strategies incline the usage of MFA with high entropy, ensure the security of all elements, reduce the risk of social engineering by choosing the factors, such that no third-party hotlines are required, and lock the device or account after a certain number of attempts. The SABSA framework handles the elicitation issue by proposing a list of generic high-level business security concerns, so-called business attributes, which are refined for specific business requirements. The list can be extended with new criteria, similar to [59].

5.2.2. Question Phase

In order to have controlled cycles, we first picked one question of the contextual layer and gathered related information. Then, the following questions and layers were targeted.

Contextual: What is the business risk without MFA? What are the requirements for MFA? How should MFA be implemented and for which areas? What are the legal and regulatory restrictions?

Conceptual: What goals and design does MFA follow? What exactly does MFA look like and what is it supposed to achieve? How should it be integrated into the current infrastructure?

Logical: Which logical components has MFA (software, hardware, backup, ...)? What should MFA protect and how to protect MFA? How to make MFA usable for users?

Physical: What are the specifications and processes for MFA? What are the physical components? What is the content of the monitoring (MFA and normal authentication during the authentication lifecycle) and how is it carried out? What are the necessary standards, procedures, baselines, interfaces, and process steps for MFA including the lifecycle phases of authenticator binding; renewal, loss, theft, damage, and unauthorized duplication; expiration; and revocation and termination?

Component: Which products, applications, tools, and people will be using MFA? Are components required to provide the lifecycle?

Management: How is MFA maintained, updated, and upgraded? What can be automated? What operational aspects like the service desk and self-service portal do we have to consider? How to ensure the security of MFA?

5.2.3. Data Management Phase

After selecting the first question, for example, "What is the business risk without MFA?", indicators and measures were acquired. Required data and its source needed to be identified. The data for this first question might include the risk of an incident with and without MFA. In addition, the related business damage caused by an incident and the costs, which might be required for MFA, could be generated. Depending on the type of MFA, further costs could arise. For example, if TOTP apps are preferred, then smartphones and their management might be regarded. The data is best split up into the various applications, their trust requirements, and user groups (especially roles and permissions).

5.2.4. Visualization Phase

The visualization phase provides actionable information, for example, business risk per application and user group with and without MFA. The visualization offers a quick overview. In the first layers of SABSA, the visualization is targeted at management personnel. This process helps to acquire the support and the resources of the management to achieve improvements.

5.2.5. Interaction Phase

The visualizations are presented and discussed within the stakeholder groups. Here, the management, especially, received an overview of the business risks and related costs with and without MFA. In later cycles, the visualizations were more relevant for technical personnel, who could then evaluate the requirements per application and usage. For example, not all applications may be suitable for MFA without further implementations or MFA only works for the web part, but not other ways to use it. These are additional factors to consider, which need to be mirrored to the management.

5.2.6. Next Iterations

Here, the following question in the contextual layer was picked: "What are the requirements for applying MFA?". Especially in the beginning, asking all questions of MFASecMan required time. Later, the iterations could concentrate on improvements like the integration of further applications, additional sources for monitoring, such as IP geo-locations, and Open Web Application Security Project (OWASP) Cheat Sheets related to authentication.

Table 5 provides an overview of the mapping of SABSA with MFASecMan. This mapping was used within the application of MFASecMan. The following shows the context of MFASecMan:

Table 5. Integration of SABSA with MFASecMan.

SABSA Layer	MFASecMan
Contextual Conceptual Logical	Processes, procedures, policies, regulations, law
Physical Component	Technology (self-service portal, devices, proxies, applications, etc.) and related security
Management	Governance, monitoring, service management

What: Security related to authentication by deciding on and improving MFA.

Why: Improve security related to authentication in a controlled way according to business needs.

How: Controlled cycles with data based on identity management with a focus on authentication and risks.

Who: Stakeholders.

Where: Anywhere.

When: Business hours (decision, authentication might be outside of business hours as well).

MFASecMan focuses on the lifecycle of authentication as well as the background processes (*what*). In the beginning, processes, procedures, policies, regulations, and laws are important. Then the focus is shifted to technology and related security. Last but not least, the operation is managed. When we regard people (*who*), we notice that organizational structure is a prerequisite. Then the stakeholders are taken into account. The users are represented with trust models and privileges. The user interface and the authentication methods interact with the user. Within components, the digital representation of the identity is relevant, while the authentication lifecycle is in accordance with the management. *Why* is providing secure authentication and protecting business assets and improving the current state in controlled cycles. *How* relates to processes and policies. *Where* is basically everywhere, depending on the organization. Time is either during business hours (user support) or at any time (authentication).

5.3. Process for Authorization

While the identity management system of an organization gives users rather generic roles, such as student or teacher, the service may detail the permissions, depending on roles and attributes, among others. This concept was introduced at a time when the boundaries of internal and external IT were clear. With cloud computing, outsourcing, and working remotely, there are no clear boundaries anymore. In consequence, the question arises if the authentication decision is trustworthy. As MFA often cannot be implemented for all users or reduces usability and, in consequence, security, risk-based authentication and zero trust are discussed. Although RBA adds additional factors to the authentication process, it also estimates the trust depending on the user's situation before authorizing the user to access a service, which requires a certain trust level determined by its criticality. ZTA, in contrast, never trusts anything but always requires verification. This verification varies on the situation and criticality. For example, a user makes a connection to the policy enforcement point, which queries the policy engine for an access decision or any other component enforcing the policy. The policy engine evaluates the request against an access policy. This access decision is continually evaluated in real-time by monitoring signals from users, devices, and applications. A change in security posture results in, for example, the termination of the connection or re-authentication.

5.3.1. Initiation

Similarly to the applications before, the environment has several applications resp. services, devices, identities, and an identity management system. The stakeholders are users, system administrators, security practitioners, (ICT) management staff, and data protection officers. The controls range from standards like NIST SP 800-53 and 800-63 to the NCSC guideline (for ZTA). NIST SP 800-63 C [68] relates to federation and assertions, and, hence, does not fit completely for authorization within an organization. Although the stakeholders make use of federated identity management by accessing specific services within the corresponding federations DFN-AAI [69] and eduGAIN [70], the services of CS are only provided for local usage. Nevertheless, due to the ZTA, the central components need to be protected. One way is to use multiple signals.

5.3.2. Question Phase

Again, we used the SABSA layers for the question phase and, thereby, aligned business requirements with technical possibilities. In this case, we tried to compare the current role-based access control with risk-based authentication due to the required trust per application, and with zero trust. For zero trust, an inventory of applications, services, devices, and identities was required, which were then evaluated towards their trust requirements and risks. This was aided by the already established risk management.

Contextual: What is the business risk without improving authorization? What are the requirements for RBA/ZTA? What are the consequences of integrating RBA or ZTA? What are the regulatory restrictions (e.g., GDPR and works council)?

Conceptual: Which concepts for RBA and ZTA are possible and what are their pros and cons? What goals and design do the usage of RBA and ZTA follow? How should it be integrated into the current infrastructure?

Logical: What are the trust requirements for each item? When is which trust requirement met? Which logical components are required for RBA or ZTA (software, algorithms, hardware, MFA, backup, ...)? What should RBA resp. ZTA protect and how to protect RBA/ZTA and its information as more information is required?

Physical: Which access control decisions based on trust requirements are necessary? What are the technical consequences due to the introduction of RBA or ZTA (such as further factors)? What are the specifications, processes, and required physical components for integrating either of them? What is the content of the monitoring, how is it carried out, and how are the regulations applied?

Component: Which additional components are needed and which consequences do they have?

Management: How is the integration maintained, updated, and upgraded? What operational aspects do we have to consider due to the integration (service desk, cross-organizational dependencies, processes, etc.)? How to ensure the security of the integration?

5.3.3. Data Management Phase

The first question was selected and the corresponding data was collected. In a university, the business risk os hard to calculate but the consequences, in terms of future projects, can be derived. The costs for RBA and ZTA included indirect costs for the integration of several authentication factors and more. The costs were split up into different applications and their requirements. Although ZTA was seen as a central concept, it could theoretically be adapted for a certain use case.

5.3.4. Visualization Phase

The data was next visualized to provide actionable items. In this case, the data for the current status and two alternatives are displayed and suggestions for a partial integration laid out.

5.3.5. Interaction Phase

The visualizations were presented and discussed with the stakeholder groups. Here, the visualizations provided a quick overview of the costs and risks for each variant and further suggestions. This made it easier for the management to reduce the number of options.

5.3.6. Next Iterations

The management noticee that RBA resp. ZTA might cost more than they wanted to spend. This is also indicated in Table 6, where dependencies and the related components were noted among other things. As a result, suggestions for specific areas were further discussed in the next iteration. In the following, the integration of a better way for authorization is summarized.

Table 6. Integration of SABSA with RBA/ZTA.

SABSA Layer	RBA/ZTO
Contextual Conceptual Logical	Processes, procedures, policies, GDPR, local regulations and law, trust, role concept, threats, vendors, dependencies, and liabilities
Physical Component	Portal for RBA/ZTA based on a central application with the decision engine and interfaces to monitoring, policies, etc. with related security
Management	Interface for RBA/ZTA, monitoring, management of RBA/ZTA, and service management

What: Security, data protection, and usability related to the RBA resp. ZTA. This includes the trust required by applications, the persons needing access to them (role concept), and the trust provided by users with different means (authentication, user setting).

Why: Improve security and trust in the access decisions in a controlled way according to business needs.

How: Controlled cycles with data based on business processes, role concepts, resources (such as projects with their requirements), and authorization policies.

Who: Stakeholders.

Where: Anywhere.

When: Business hours (decision) and anytime (access).

6. Case Study

In this section, we provide the case study for IdMSecMan, based on the applications on eID, MFA, and RBA/ZTA, from the previous section. In addition, we use the scenario already introduced in the last section of a CS department with several services in a heterogeneous ICT infrastructure. Similar results may be received by other universities. In industry, there should be a more centralized setting and a higher awareness of security. This does not indicate that this is always the case. There might be areas, which work independently. Even with a good setting, maturity can always be improved. Last but not least, we provide a short summary.

6.1. Case eID

As eID integration would be beneficial but is not realistic before eIDAS 2.0, we focused on MFA and related access management. Nevertheless, some processes and evaluations were taking place. First of all, suitable applications were evaluated. The university and the computer science department operate various applications, from project and study-related ones to administrative tools. Besides the proof of identity of new employees and students,

as shown in Figure 5, eID could be used to register a thesis, renew accounts and cards, or request official documents. Although these were in the minority, they occupied time due to several manual steps, including verifying the ID card or contract.

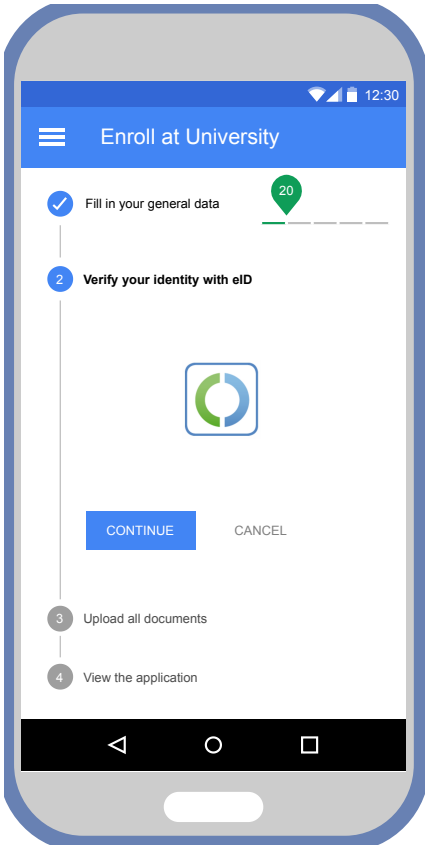

Figure 5. Mockup of one exemplary application for eID.

The eID integration itself had several requirements on the web application resp. server regarding security, data security, and privacy. In contrast to other countries, no official implementation was offered. In consequence, different commercial solutions and the option to host it on its own were compared. For comparison, several inquiries were sent to commercial companies. Either way, as the university already used Shibboleth, the integration was at least, from the protocol level, feasible. The corresponding office also offered an environment to test for conformity. Although three eID login solutions [71] were open-source, the integration and hosting might be difficult to maintain. In consequence, buying such integration, including a service contract, was preferred. The favorites were noted. The process, based on IdMSecMan, is summarized in the following. All questions and answers were archived until eIDAS 2.0 is released.

Contextual Layer: Stakeholders, policies, and further regulations, such as GDPR, processes, and security controls, were identified. In addition, costs with, and without, eID were gathered.

Conceptual Layer: Different options of identity proofing and verification were compared, especially the current status with eID. Then, a way to integrate eID was searched for.

Logical Layer: The assets for proper identity proofing relatec to the user data, internal data, and services resp. the access to it. In consequence, applications and areas with higher levels of trust were identified. In addition, logical components for the integration of eID were outlined.

Physical Layer: Based on the research about the logical components, the specifications, processes, and physical components were analyzed. In addition, monitoring and actual requirements on the server and application were specified.

Component Layer: Due to the evaluation steps beforehand, applications and people applying the eID integration were already known. Additional components were evaluated, but not found. Though the possibility of terminals was discussed.

Management Layer: Maintenance, updates, upgrades, and the integration into current infrastructure (service desk, processes) was regarded. Whereas buying such a solution reduced the questions related to the logical, physical, and component layer in some ways, the management layer became more relevant as it was cross-organizational. In consequence, interfaces to the company had to be established and the service desk needed to be instructed.

6.2. Case MFA

The projects in the CS department ranged from individual research and collaborations for papers to third-party-funded research and classified projects with industry partners. The department operated some kind of project management software, such as Jira, and a versioning system, for example, GitLab. Even though only rudimentary risk management was enabled (risks were known and partly mitigated, but not monetary quantified), the risk of incidents with, and without, MFA was regarded. As a result, the questions were "Should we improve the security with MFA?" and "If so, how should we introduce MFA?".

The business goals and decisions are based on business risks. These depend on, for example, the organizational structure of projects, regulations for classified projects, and, consequently, costs of incidents. As a result, different groups (professors, project managers, system administrators, and project members among others) exist, as shown in Figure 6. Green corresponds to OK, orange represents a lower threat, orange to red is a medium threat, red shows a higher threat, and blue indicates that it is not used. The security controls were adapted from NIST SP 800-53 and 800-63. Regarding the layers of SABSA, we see the following.

	Professors and project manager	System administrators and Lab Supervisors	Project members	Other personell
Generic services	uses	administrates	uses	uses
Project-related infrastructure	manages	administrates	uses	-
Background infrastructure	indirectly uses	administrates resp. uses	indirectly uses	indirectly uses

Figure 6. User groups per infrastructure group.

Contextual Layer: First, stakeholders, policies, and processes for authentication and MFA were identified. In addition, the role concept and required trust were outlined.

The CS department had a role concept but it frequently changed with the different assignments to projects. As the role concept was not up-to-date, a hierarchical concept for updating and verifying it was introduced.

Conceptual Layer: MFA exists in different variants (architectures, factors, vendors, etc.). Either way, additional factors should increase security, which is possible with appropriate monitoring and independency of factors. In order to decide on the actual implementation, the different variants were outlined and discussed.

Logical Layer: The assets relate to the data, identities, and the relation between them. Privileges should be only granted if necessary for work. In consequence, trust in the users must be as high as required by the data. While most projects, courses, and theses only need a normal level, classified projects and specific servers are much more restricted with a high level of trust and a limited user group.

Physical Layer: So far, a self-service portal exists, where users can edit their profiles, request certificates, and more. This self-service portal could be adapted to manage further devices required for MFA. In addition, a user interface, either per application or as a central element, is required. Here, usability is an important issue, as people try to bypass security measures if they feel these are a burden. Consequently, increasing security might even result in the opposite. Last, but not least, the security of each variant with its components was analyzed. TOTP seemed like a good variant of MFA as the users can decide between smartphone apps and password managers with the functionality, among others. On the other hand, the employees might request employer-provided smartphones, which, in consequence, need to be managed as well.

Component Layer: Here, the functions and components were evaluated. Jira, for example, integrated with GitLab used for versioning. Both web applications can require MFA in form of TOTP. In contrast, using *git* on the command line does not enable it. In addition, with TOTP, smartphones for the corresponding employees and their management were discussed. The stakeholders came to the conclusion that only professors, project managers, and members of classified projects (see red color in Figure 6), as well as administrators, required MFA. The consequences of rolling it out on all employees would be higher costs and effort (service desk and device management among others). As all applications with classified projects were suitable for TOTP, this method was chosen due to low costs and maintenance. In addition, the usability was regarded as acceptable by the employees, which was in accordance with Das et al. [29]. For administration purposes, a security key, such as Yubikey [72], was a more suited method. In addition, it provided a higher level of assurance, according to NIST SP 800-63 B. As the number of persons administrating servers was limited, this option was chosen for them.

Management Layer: Although the introduction of MFA was restricted to a limited amount of users, user support, backup, and rollback were outlined. Due to the limited amount of users, user support in its current form did not have to change. Nevertheless, MFA had to be regarding during the whole authentication lifecycle, from enrolment to de-provisioning. As a result of Section 2, proper monitoring was established.

Regarding the authentication lifecycle, MFA was taken care of in every stage.

Authenticator Binding: In the beginning, the authenticator and the account are associated with each other. With TOTP and security key, this is (mostly) done on the application level. Hence, the self-service portal cannot be used to enrol MFA. Nevertheless, the loss of TOTP can be reported and processes in accordance with this are started. In addition, the handling of backup codes is described in the self-service portal and before the binding of new authenticators.

Renewal, Loss, Theft, Damage, and Unauthorized Duplication: As explained above, the loss/theft/damage could be reported in the self-service portal, displayed in Figure 7.

Depending on the problem, different actions were taken. Renewal was possible within the respective applications, while monitoring should notice the unauthorized duplication. In addition, duplication was forbidden by policy.

Expiration: In the current setting, expiration was not enabled. This decision was made to reduce the overheads. The expiration might be introduced in future MFASecMan runs.

Revocation and Termination: With the termination of the user account, the TOTP token was revoked. Thereby, the association between the authenticator and the account was deleted and the token removed.

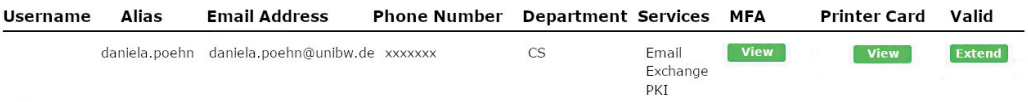

Figure 7. Proof-of-Concept of the Self-Service Portal.

6.3. Case ZTA

As a consequence of limiting the application of MFA, ZTA was not further regarded. RBA could be used instead of MFA, but as only certain applications were selected, RBA would not change anything in that respect. Nevertheless, in order to provide access only to the relevant users, the role concept was renewed. Due to the partly decentralized setting of the university, all professors and project managers updated the roles of their employees resp. members, as well as projects, with their applications once a month. Thereby, the role concept stayed up-to-date. In the future, devices could be associated with their users. Only if users, devices, and applications are trustworthy enough, would access be granted. To document the process run, the following summary is generated.

Contextual: The business risks without ZTA and the requirements for ZTA were summarized. For ZTA, the employees had to accept the usage. In consequence, the documents before the employment started had to be adapted.

Conceptual: Different concepts for ZTA were compared and their integration into the current infrastructure discussed. As the infrastructure was only partly centralized within CS and the central servers were better secured due to their purposes, the central part was chosen. Here, a logging and monitoring solution already operated, which could be extended to ZTA. In theory, a centralized architecture could be a consequence. In practice, due to the freedom of research and teaching, this was not likely.

Logical: To establish ZTA, an inventory of applications, services, devices, and identities was taken for the central part. These items were evaluated towards their trust requirements, typical usage, and permissions. Next, the components for ZTA were identified and analyzed for their security. The core components needed to be properly secured, as they analyzed and enforced the policies. In addition, the policies were discussed for their elements. Since this was not entirely clear, a test bed would be set up beforehand. Last, but not least, emergency procedures were discussed.

Physical: In order to introduce ZTA, further factors needed to be enrolled. Due to the case of MFA, experiences with TOTP and security keys were gained. Next, specifications, physical components (resp. extensions to the current solution), processes, and monitoring were outlined.

Component: In relation to case MFA, mobile device management was brought up but declined, due to the research character of the university and the limited budget. This could be included in future iterations.

Management: Last, but not least, the operational aspects of the integration were documented. As the service desk application was part of the central infrastructure, an email interface was favored if access to the application was restricted.

6.4. Summary

In the case study, we analyzed the application of IdMSecMan for eID, MFA, and ZTA. For eID, we noticed that an introduction was currently not suitable, but all required information was gathered. Thereby, the introduction should be faster and more organized. Regarding MFA, test users resp. groups were identified with corresponding requirements. Based on them, MFA methods were chosen. The methods and the corresponding processes were aligned with business requirements. Thereby, first experiences could be gained to either roll out MFA for all employees or establish RBA resp. ZTA for specific use cases. Here, the required information was also gathered. Some aspects, such as mobile device management, are more common in commercial companies than at universities. To apply the bringing of own devices, those devices would receive a lower level of trust. Although these results might seem logical, with IdMSecMan an approach could be used to systematically evaluate all business requirements. With the related work outlined in Section 3, this would not be possible.

7. Discussion

By applying IdMSecMan, business requirements, needs, and decisions go hand in hand with those of the technical setting. Every aspect is systematically evaluated before a decision is made and changes are implemented. Vis4Sec is an advanced Deming approach with visualization for all stakeholder groups. Thereby, Vis4Sec aids interaction by providing a quick and easy-to-access overview. SABSA, in contrast, helps to develop business-driven, risk, and opportunity-focused enterprise security and information assurance architectures. It is suited for evaluating every aspect, from context to management, by means of its layered approach. By integrating both in a decision framework, a clear distinction of business layers utilized in a systematic process framework for security visualizations was possible, and we derived a method to develop security aspects related to identity management in a systematic way. In consequence, simple actions were aligned with strategies and all aspects were regarded. We showed how to adapt IdMSecMan for identification, authentication, and authorization. Further aspects of identity management, such as governance, could be improved by IdMSecMan as well.

Although we provided a case study based on the CS department, and discussed the approach for the related applications with different organizations known to us, a broader application to several organizations would help to further improve IdMSecMan. Here, also, a tool guiding the involved stakeholders by means of an integrated questions template and suitable visualizations could lead to better results. One issue with a larger evaluation is that several organizations have complicated processes before releasing data for publication. Due to this, we limited the evaluation to the case study as it is. We noticed during the application, that suitable security controls and, respectively, a systematic way to identify suitable security controls in the field of identity management, is missing. Some generic ones are provided by NIST SP 800-53 but these need to be adapted and might not be enough, especially in the case of authorization. This is also noted by NIST in its SP 800-63 version 4 all for comments [73].

8. Conclusions and Outlook

Authentication is a critical method to verify that a user is actually the user they pretend to be. To enrol MFA for a higher level of security, several information and concepts have to be in place first. To align the decision for, or against, the exact type of MFA with business management, we proposed IdMSecMan, a security management process tailored for identity management with the integration of visualization and SABSA. We first described a motivating scenario related to the supply chain attack on SolarWinds' Orion software, which used the enrolment of another smartphone to gain control over an account among other things. Next, we gave a brief overview of the background and related work. In the following section, we introduced IdMSecMan with initiation, the phases question, data management, visualization, and interaction, as well as iterations. IdMSecMan was

then applied to selected areas of the central technical process activities identification (identification with eID), authentication (multi-factor authentication), and authorization (the trust evaluation of risk-based authentication or zero trust architecture). In order to explain MFA in more detail and verify that IdMSecMan was actually usable, we conducted a case study of a university deciding upon increasing security by introducing multi-factor authentication. Last, but not least, we discussed our approach. With IdMSecMan, we gained a flexible process framework for identity management to align decisions with business requirements and the technical setting. Although this approach might seem logical, we noticed that a simple decision might have more consequences than first concluded. IdMSecMan helped to systematically evaluate all aspects of such a decision before actually implementing it.

In future work, we plan to gain feedback on the implementation of IdMSecMan in different organizations. This will help us to generalize the transferability and usage of IdMSecMan. The input generated by IdMSecMan will be enhanced by a recursive cyber incident handling support approach, such as PoCyMa [74] or [75], and could lead to situation awareness [76]. Incident handling is a fundamental activity of a security incident response team. In order to improve this task, procedural or decision support systems, which process relevant data, are proposed. This integration could help to sustainably improve aspects which are the cause of security incidents. Last, but not least, we plan to investigate identifying suitable security controls.

Author Contributions: Conceptualization, D.P. and S.S.; methodology, D.P. and S.S.; validation, D.P., S.S. and W.H.; writing—original draft preparation, D.P.; writing—review and editing, D.P. and W.H.; visualization, D.P.; supervision, W.H.; funding acquisition, W.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was inline with the Ethics Board of the university.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data presented in this study are not publicly available due to privacy reasons.

Acknowledgments: We thank Tanja Hanauer, Jule A. Ziegler, and David Schmitz for the useful input and discussion.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

2FA	Two-Factor Authentication
AuthNZ	Authentication and Authorization
CS	Computer Science
COBIT	Control Objectives for Information and Related Technology
EA	Enterprise Architecture
eID	electronic Identity
eIDAS	electronic IDentification, Authentication and trust Services
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
IAA	Identification, Authentication, and Authorization
IAL	Identity Assurance Level
ICT	Information and Communication Technology
ID	Identity
IdM	Identity Management
IdMSecMan	Identity Management Security Management
IEC	International Electrotechnical Commission
IoT	Internet of Things

IP	Internet Protocol
ISM	Information Security Management
ISO	International Organization for Standarization
LoA	Level of Assurance
MFA	Multi-Factor Authentication
MFASecMan	MFA Security Management
NAC	Network Access Control
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
OAuth	Open Authorization
OSA	Open Security Architecture
OWASP	Open Web Application Security Project
PoCyMa	PotatoCyb0rMap
RBA	Risk-Based Authentication
SABSA	Sherwood Applied Business Security Architecture
SAML	Security Assertion Markup Language
SP	Special Publication
TOGAF	The Open Group Architecture Framework
TOTP	Time-based One-Time-Password
Vis4Sec	Visualization for Security
VPN	Virtual Private Network
VR	Virtual Reality
XACML	eXtensible Access Control Markup Language
ZTA	Zero Trust Architecture

References

1. Wang, C.; Jan, S.T.; Hu, H.; Bossart, D.; Wang, G. The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services. In Proceedings of the 8th ACM Conference on Data and Application Security and Privacy (CODASPY), Tempe, AZ, USA, 19–21 March 2018; pp. 196–203. [CrossRef]
2. Henricks, A.; Kettani, H. On Data Protection Using Multi-Factor Authentication. In Proceedings of the 1st ACM International Conference on Information System and System Management (ISSM), Rabat, Morocco, 14–16 October 2019; pp. 1–4. [CrossRef]
3. Hanauer, T.; Hommel, W.; Metzger, S.; Pöhn, D. A Process Framework for Stakeholder-Specific Visualization of Security Metrics. In Proceedings of the 13th ACM International Conference on Availability, Reliability and Security (ARES), Hamburg, Germany, 27–30 August 2018. [CrossRef]
4. Sherwood, J.; Clark, A.; Lynas, D. *Enterprise Security Architecture*; Whitepaper: Liverpool, UK, 1995.
5. Sherwood, N. *Enterprise Security Architecture: A Business-Driven Approach*; CRC Press: Boca Raton, FL, USA, 2005.
6. Pöhn, D.; Seeber, S.; Hanauer, T.; Ziegler, J.A.; Schmitz, D. Towards Improving Identity and Access Management with the IdMSecMan Process Framework. In Proceedings of the 16th ACM International Conference on Availability, Reliability and Security (ARES), Vienna, Austria, 17–20 August 2021. [CrossRef]
7. MANDIANT. Assembling the Russian Nesting Doll: UNC2452 Merged into APT29, 2022. Available online: https://www.mandiant.com/resources/blog/unc2452-merged-into-apt29 (accessed on 28 December 2022).
8. MANDIANT. FireEye Red Team Tool Countermeasures, 2021. Available online: https://github.com/mandiant/red_team_tool_countermeasures (accessed on 28 December 2022).
9. Pöhn, D.; Hommel, W. IMC: A Classification of Identity Management Approaches. In Proceedings of the Computer Security: ESORICS 2020 International Workshops, DETIPS, DeSECSys, MPS, and SPOSE, Guildford, UK, 17–18 September 2020; Springer: Berlin/Heidelberg, Germany; pp. 3–20. [CrossRef]
10. Milgram, L.; Spector, A.; Treger, M. *Plan, Do, Check, Act: The Deming or Shewhart Cycle*; Gulf Professional Publishing: Boston, MA, USA, 1999; Chapter 21.
11. L'Amrani, H.; Berroukech, B.E.; El Bouzekri El Idrissi, Y.; Ajhoun, R. Identity management systems: Laws of identity for models7 evaluation. In Proceedings of the 4th IEEE International Colloquium on Information Science and Technology (CiSt), Tangier, Morocco, 24–26 October 2016; pp. 736–740. [CrossRef]
12. Grassi, P.A.; Fenton, J.L.; Lefkovitz, N.B.; Danker, J.M.; Choong, Y.Y.C.; Greene, K.K.; Theofanos, M. *Digital Identity Guidelines—Enrollment and Identity Proofing*; Special Publication 800-63a; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2017. [CrossRef]
13. Yang, Y.; Wang, Y.; Chen, Y.; Wang, C. EchoLock: Towards Low-Effort Mobile User Identification Leveraging Structure-Borne Echos. In Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (Asia CCS), Taipei, Taiwan, 5–9 October 2020; pp. 772–783. [CrossRef]

14. Davarci, E.; Anarim, E. User Identification on Smartphones with Motion Sensors and Touching Behaviors. In Proceedings of the 30th IEEE Signal Processing and Communications Applications Conference (SIU), Safranbolu, Turkey, 15–18 May 2022; pp. 1–4. [CrossRef]
15. Lee, H.; Lee, S.H.; Kim, T.; Bahn, H. Secure user identification for consumer electronics devices. *IEEE Trans. Consum. Electron.* **2008**, *54*, 1798–1802. [CrossRef]
16. Irfan, B.; Ortiz, M.G.; Lyubova, N.; Belpaeme, T. Multi-Modal Open World User Identification. *J. Hum.-Robot Interact.* **2021**, *11*, 6. [CrossRef]
17. Shahzad, M.; Zhang, S. Augmenting User Identification with WiFi Based Gesture Recognition. *Interact. Mob. Wearable Ubiquitous Technol.* **2018**, *2*, 134. [CrossRef]
18. He, Z.; Li, W. Research on User Identification across Multiple Social Networks Based on Preference. In Proceedings of the 5th IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS), Nanjing, China, 23–25 November 2018; pp. 122–128. [CrossRef]
19. Solanki, P.; Hui Lim, K.w.; Harwood, A. User Identification across Social Networking Sites using User Profiles and Posting Patterns. In Proceedings of the 31st IEEE International Joint Conference on Neural Networks (IJCNN), Shenzhen, China, 18–22 July 2021; pp. 1–8. [CrossRef]
20. Bonneau, J. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In Proceedings of the 33rd IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 20–23 May 2012; IEEE Computer Society: New York, NY, USA, 2012; pp. 538–552. [CrossRef]
21. Bachmann, M. Passwords are Dead: Alternative Authentication Methods. In Proceedings of the 1st IEEE Joint Intelligence and Security Informatics Conference (JISIC), The Hague, The Netherlands, 24–26 September 2014; p. 322. [CrossRef]
22. Miessler, D. The Consumer Authentication Strength Maturity Model (CASMM) v5, 2022. Available online: https://danielmiessler.com/blog/casmm-consumer-authentication-security-maturity-model/ (accessed on 28 December 2022).
23. Grassi, P.A.; Fenton, J.L.; Newton, E.M.; Perler, R.A.; Regenscheid, A.R.; Burr, W.E.; Richer, J.P.; Lefkovitz, N.B.; Danker, J.M.; Choong, Y.Y.; et al. *Digital Identity Guidelines—Authentication and Lifecycle Management*; Special publication 800-63b; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2017. [CrossRef]
24. Vegh, L. Cyber-physical systems security through multi-factor authentication and data analytics. In Proceedings of the IEEE International Conference on Industrial Technology (ICIT), Lyon, France, 20–22 February 2018; pp. 1369–1374. [CrossRef]
25. Sciarretta, G.; Carbone, R.; Ranise, S.; Viganò, L. Formal Analysis of Mobile Multi-Factor Authentication with Single Sign-On Login. *ACM Trans. Priv. Secur.* **2020**, *23*, 13. [CrossRef]
26. Realpe, P.C.; Collazos, C.A.; Hurtado, J.; Granollers, A. A Set of Heuristics for Usable Security and User Authentication. In Proceedings of the 17th ACM International Conference on Human Computer Interaction (Interacción), Salamanca, Spain, 13–16 September 2016. [CrossRef]
27. Timón López, C.; Alamillo Alamillo Domingo, I.; Valero Valero Torrijos, J. Which Authentication Method to Choose. A Legal Perspective on User-Device Authentication in IoT Ecosystems. In Proceedings of the 16th ACM International Conference on Availability, Reliability and Security (ARES), Vienna, Austria, 17–20 August 2021. [CrossRef]
28. Damon, F.; Coetzee, M. Towards a generic Identity and Access Assurance model by component analysis—A conceptual review. In Proceedings of the 1st IEEE International Conference on Enterprise Systems (ES), Cape Town, South Africa, 7–8 November 2013; pp. 1–11. [CrossRef]
29. Das, S.; Kim, A.; Camp, L.J. Short Paper: Organizational Security: Implementing a Risk-Reduction-Based Incentivization Model for MFA Adoption. In Proceedings of the Financial Cryptography and Data Security, Virtual, 1–5 March 2021; Borisov, N., Diaz, C., Eds.; Springer: Berlin/Heidelberg, Germany, 2021; pp. 406–413. [CrossRef]
30. Demchenko, Y.; Cristea, M.; de Laat, C. XACML Policy Profile for Multidomain Network Resource Provisioning and Supporting Authorisation Infrastructure. In Proceedings of the 10th IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY), London, UK, 20–22 July 2009; pp. 98–101. [CrossRef]
31. Misbahuddin, M.; Bindhumadhava, B.S.; Dheeptha, B. Design of a risk based authentication system using machine learning techniques. In Proceedings of the 14th IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), San Francisco, CA, USA, 4–8 August 2017; pp. 1–6. [CrossRef]
32. Wiefling, S.; Dürmuth, M.; Lo Iacono, L. More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-Based Authentication. In Proceedings of the 36th ACM Annual Computer Security Applications Conference (ACSAC), Austin, TX, USA, 7–11 December 2020; pp. 203–218. [CrossRef]
33. Wiefling, S.; Jørgensen, P.R.; Thunem, S.; Iacono, L.L. Pump Up Password Security! Evaluating and Enhancing Risk-Based Authentication on a Real-World Large-Scale Online Service. *ACM Trans. Priv. Secur.* **2022**, *26*, 6. [CrossRef]
34. Wiefling, S.; Dürmuth, M.; Lo Iacono, L. Verify It's You: How Users Perceive Risk-Based Authentication. *IEEE Secur. Priv.* **2021**, *19*, 47–57. [CrossRef]
35. Papaioannou, M.; Mantas, G.; Essop, A.; Cox, P.; Otung, I.E.; Rodriguez, J. Risk-Based Adaptive User Authentication for Mobile Passenger ID Devices for Land/Sea Border Control. In Proceedings of the 26th IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Porto, Portugal, 25–27 October 2021; pp. 1–6. [CrossRef]

36. Akiyama, T.; Otani, K.; Kakizaki, Y.; Sasaki, R. Evaluation of a Risk-Based Management Method for Online Accounts. In Proceedings of the 4th IEEE International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec), Jakarta, Indonesia, 29–31 October 2015; pp. 52–57. [CrossRef]
37. Ashibani, Y.; Mahmoud, Q.H. An Intelligent Risk-Based Authentication Approach for Smartphone Applications. In Proceedings of the 33rd IEEE International Conference on Systems, Man, and Cybernetics (SMC), Toronto, ON, Canada, 11–14 October 2020; pp. 3807–3812. [CrossRef]
38. Leiba, B. OAuth Web Authorization Protocol. *IEEE Internet Comput.* **2012**, *16*, 74–77. [CrossRef]
39. Nishioka, S.; Okabe, Y. Mutual Secrecy of Attributes and Authorization Policies in Identity Federation. In Proceedings of the 45th IEEE Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 12–16 July 2021; IEEE: New York, NY, USA, 2021; pp. 1202–1209. [CrossRef]
40. Fujun, F.; Junshan, L. Trust Based Authorization and Access Control. In Proceedings of the 3rd IEEE International Forum on Information Technology and Applications (IFITA), Chengdu, China, 15–17 May 2009; pp. 162–165. [CrossRef]
41. Kindervag, J. No More Chewy Centers: The Zero Trust Model Of Information Security. *For Secur. Risk Prof.* **2016**, *23*, 1–16.
42. National Cyber Security Centre, 2021. Available online: https://www.ncsc.gov.uk/collection/zero-trust-architecture (accessed on 28 December 2022).
43. Wylde, A. Zero trust: Never trust, always verify. In Proceedings of the 7th IEEE International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 14–18 June 2021; pp. 1–4. [CrossRef]
44. Dimitrakos, T.; Dilshener, T.; Kravtsov, A.; La Marra, A.; Martinelli, F.; Rizos, A.; Rosetti, A.; Saracino, A. Trust Aware Continuous Authorization for Zero Trust in Consumer Internet of Things. In Proceedings of the 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December 2020–1 January 2021; pp. 1801–1812. [CrossRef]
45. Hatakeyama, K.; Kotani, D.; Okabe, Y. Zero Trust Federation: Sharing Context under User Control towards Zero Trust in Identity Federation. In Proceedings of the 19th IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), Kassel, Germany, 22–26 March 2021; pp. 514–519. [CrossRef]
46. Bobbert, Y.; Scheerder, J. Zero Trust Validation: From Practice to Theory: An empirical research project to improve Zero Trust implementations. In Proceedings of the 29th IEEE Annual Software Technology Conference (STC), Gaithersburg, MD, USA, 3–6 October 2022; pp. 93–104. [CrossRef]
47. *ISO/IEC 27001:2022*; Information Security, Cybersecurity and Privacy Protection. Information Security Management System. Requirements. BSI: London, UK, 2022.
48. Bilbao, A.; Bilbao, E. Measuring security. In Proceedings of the 47th IEEE International Carnahan Conference on Security Technology (ICCST), Medellin, Colombia, 8–11 October 2013; pp. 1–5. [CrossRef]
49. Sun, Z.; Zhang, J.; Yang, H.; Li, J. Research on the Effectiveness Analysis of Information Security Controls. In Proceedings of the 4th IEEE Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, 12–14 June 2020; pp. 894–897. [CrossRef]
50. Yang, Y.; Li, Z.; Shi, L. Continuous improvement actions: Moderating effects of the consciousness of employees. In Proceedings of the 3rd IEEE International Conference on Industrial Economics System and Industrial Security Engineering (IEIS), Sydney, NSW, Australia, 24–27 July 2016; pp. 1–5. [CrossRef]
51. Zeb, T.; Yousaf, M.; Afzal, H.; Mufti, M.R. A quantitative security metric model for security controls: Secure virtual machine migration protocol as target of assessment. *China Comm.* **2018**, *15*, 126–140. [CrossRef]
52. Brunner, M.; Mussmann, A.; Breu, R. Introduction of a Tool-Based Continuous Information Security Management System: An Exploratory Case Study. In Proceedings of the 18th IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, 16–20 July 2018; pp. 483–490. [CrossRef]
53. Sacher, D. Fingerpointing False Positives: How to Better Integrate Continuous Improvement into Security Monitoring. *Digit. Threat.* **2020**, *1*, 7. [CrossRef]
54. Hanauer, T. Visualization-Based Enhancement of IT Security Management and Operations. Ph.D. Thesis, Universität der Bundeswehr München, Neubiberg, Germany, 2021.
55. Zachman, J.A. *The Zachman Framework for Enterprise Architecture: Primer for Enterprise Engineering and Manufactoring*. Zachman International: Monument, CO, USA, 2003.
56. Pleinevaux, P. Towards a Metamodel for SABSA Conceptual Architecture Descriptions. In Proceedings of the 11th IEEE International Conference on Availability, Reliability and Security (ARES), Salzburg, Austria, 31 August–2 September 2016; pp. 187–194. [CrossRef]
57. The SABSA Institute. SABSA Executive Summary, 2022. Available online: https://sabsa.org/sabsa-executive-summary/ (accessed on 28 December 2022).
58. Al-Turkistani, H.F.; Aldobaian, S.; Latif, R. Enterprise Architecture Frameworks Assessment: Capabilities, Cyber Security and Resiliency Review. In Proceedings of the 1st IEEE International Conference on Artificial Intelligence and Data Analytics (CAIDA), Riyadh, Saudi Arabia, 6–7 April 2021; pp. 79–84. [CrossRef]
59. Bulusu, S.T.; Laborde, R.; Wazan, A.S.; Barrère, F.; Benzekri, A. Which Security Requirements Engineering Methodology Should I Choose? Towards a Requirements Engineering-Based Evaluation Approach. In Proceedings of the 12th ACM International Conference on Availability, Reliability and Security (ARES), Reggio Calabria, Italy, 29 August–1 September 2017. [CrossRef]

60. Rajba, P. Challenges and Mitigation Approaches for Getting Secured Applications in an Enterprise Company. In Proceedings of the 13th ACM International Conference on Availability, Reliability and Security (ARES), Hamburg, Germany, 27–30 August 2018. [CrossRef]
61. Najib, W.; Sumaryono, S.; Nugroho, L.E.; Putra, G.D. Development of Enterprise Security Framework in SKK Migas Based on Integration of ISO 27000 and SABSA Model. In Proceedings of the 10th IEEE International Conference on Information Technology and Electrical Engineering (ICITEE), Bali, Indonesia, 24–26 July 2018; pp. 382–387. [CrossRef]
62. Martynov, V.V.; Shiryaev, O.V. Ensuring integrated security as part of building digital architecture for energy companies. In Proceedings of the IEEE International Conference on Electrotechnical Complexes and Systems (ICOECS), Ufa, Russia, 16–18 November 2021; pp. 191–195. [CrossRef]
63. Rubio, N.; Chavarria, L.; Mauricio, D. Security architecture for the protection of digital assets in SMEs. In Proceedings of the IEEE International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Istanbul, Turkey, 12–13 June 2020; pp. 1–6. [CrossRef]
64. Mayer, N.; Aubert, J.; Grandry, E.; Feltus, C.; Goettelmann, E.; Wieringa, R. An integrated conceptual model for information system security risk management supported by enterprise architecture management. *Softw. Syst. Model.* **2019**, *18*, 2285–2312. [CrossRef]
65. Sialm, G.; Knittl, S. Bring Your Own Identity—Case Study from the Swiss Government. In Proceedings of the Privacy Technologies and Policy, Frankfurt/Main, Germany, 7–8 September 2016; Schiffner, S., Serna, J., Ikonomou, D., Rannenberg, K., Eds.; Springer International Publishing: Cham, Switzerland, 2016; pp. 38–47. [CrossRef]
66. Guimarães, V.T.; Freitas, C.M.D.S.; Sadre, R.; Tarouco, L.M.R.; Granville, L.Z. A Survey on Information Visualization for Network and Service Management. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 285–323. [CrossRef]
67. Deasy, D.; Sherman, J.; Hakun, M.; Dulany, K.; Romine, C.H.; Stine, K.; Scholl, M.; Ross, R.; Kozma, M.A.; Waschull, M.E.; et al. *Security and Privacy Controls for Information Systems and Organizations*; Special publication 800-53—Revision 5; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020. [CrossRef]
68. Grassi, P.A.; Richer, J.P.; Squire, S.K.; Fenton, J.L.; Newton, E.M.; Lefkovitz, N.B.; Danker, J.M.; Choong, Y.Y.; Greene, K.K.; Theofanos, M.F. *Digital Identity Guidelines—Federation and Assertions*; Special publication 800-63c; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2017. [CrossRef]
69. DFN. DFN-AAI—Authentication and Authorization Infrastructure for Research and Education Communities in Germany, 2023. Available online: https://www.aai.dfn.de/index.en.html (accessed on 28 December 2022).
70. eduGAIN. eduGAIN—Enabling Worldwide Access, 2023. Available online: https://edugain.org (accessed on 28 December 2022).
71. ecsec. eID-Login, 2022. Available online: https://github.com/eid-login/ (accessed on 28 December 2022).
72. Das, S.; Russo, G.; Dingman, A.C.; Dev, J.; Kenny, O.; Camp, L.J. A Qualitative Study on Usability and Acceptability of Yubico Security Key. In Proceedings of the 7th ACM Workshop on Socio-Technical Aspects in Security and Trust (STAST), Orlando, FL, USA, 5 December 2017; pp. 28–39. [CrossRef]
73. NIST. NIST SP 800-63 Digital Identity Guidelines—Call for Comments on Initial Public Draft of Revision 4, 2022. Available online: https://pages.nist.gov/800-63-4/ (accessed on 28 December 2022).
74. localos. PoCyMa, 2019. Available online: https://github.com/localos/PoCyMa (accessed on 28 December 2022).
75. Husák, M.; Čermák, M. SoK: Applications and Challenges of Using Recommender Systems in Cybersecurity Incident Handling and Response. In Proceedings of the 17th ACM International Conference on Availability, Reliability and Security (ARES), Vienna, Austria, 23–26 August 2022. [CrossRef]
76. Jiang, L.; Jayatilaka, A.; Nasim, M.; Grobler, M.; Zahedi, M.; Babar, M.A. Systematic Literature Review on Cyber Situational Awareness Visualizations. *IEEE Access* **2022**, *10*, 57525–57554. [CrossRef]