Complex Systems Informatics and Modeling Quarterly (CSIMQ)
eISSN: 2255-9922
Published online by RTU Press, https://csimq-journals.rtu.lv
Article 140, Issue 24, September/October 2020, Pages 31–48
https://doi.org/10.7250/csimq.2020-24.03

Enterprise Architecture Frameworks as Support for Implementation of Regulations: Approach and Experiences from GDPR

Johannes Wichmann[*1,4], Kurt Sandkuhl[1,2], Nikolay Shilov[3], Alexander Smirnov[3], Felix Timm[1], and Matthias Wißotzki[4]

[1]Rostock University, 18051 Rostock, Germany
[2]Jönköping University, 553 18 Jönköping, Sweden
[3]SPC RAS, 199178 St. Petersburg, Russia
[4]Wismar University of Applied Sciences, 23966 Wismar, Germany

{felix.timm, kurt.sandkuhl}@uni-rostock.de, {smir, nick}@iias.spb.su,
{johannes.wichmann, matthias.wissotzki}@hs-wismar.de

Abstract. Enterprise Architecture (EA) management has been discussed as being supportive for implementation of regulations in enterprises and organizations, but the role of EA frameworks in this context has not been addressed intensely. The EU General Data Protection Regulation (GDPR) is one of the most frequently discussed regulation in industry and research, and expected to cause a shift in viewpoint of enterprises from a technological perspective dominated by information security issues to an organizational perspective governed by GDPR-compliant organizational structures and processes. A well-documented Enterprise Architecture (EA) and a working Enterprise Architecture Management (EAM) are expected to significantly ease the roadmap planning for GDPR implementation. Therefore, this article focuses on the practice of EA use for GDPR implementation. The main contributions of this article are (a) an analysis and comparison of existing architecture frameworks and how they address security-related issues, and (b) a case study from financial industries illustrating the use of EA for implementing GDPR compliance.
Keywords: GDPR, Enterprise Architecture, Enterprise Architecture Framework, Security, Security Architecture Frameworks.

1 Introduction

Many industrial sectors are affected by an increasing number of regulations that are mandatory for enterprises and organizations in these sectors. Implementation of such regulations in an

* Corresponding author

Reference: J. Wichmann, K. Sandkuhl, N. Shilov, A. Smirnov, F. Timm, and M. Wißotzki, "Enterprise Architecture Frameworks as Support for Implementation of Regulations: Approach and Experiences from GDPR," Complex Systems Informatics and Modeling Quarterly, CSIMQ, no. 24, pp. 31–48, 2020. Available: https://doi.org/10.7250/csimq.2020-24.03

Additional information. Author ORCID iD: J. Wichmann – https://orcid.org/0000-0002-9877-1422, K. Sandkuhl – https://orcid.org/0000-0002-7431-8412, and N. Shilov – https://orcid.org/0000-0002-9264-9127. PII S225599222000140X. Received: 26 September 2019. Accepted: 8 October 2020. Available online: 31 October 2020.

organizational context usually causes modifications in business processes, organizational structures, role distribution and supporting IT-infrastructures. Enterprise Architecture (EA) management as a means to capture and systematically analyze dependencies in an enterprise has been discussed as being supportive for implementation of regulations. However, the role of EA frameworks (EAFs) has not been addressed intensely in this context.

One of the regulations frequently discussed in media, society and research is the EU General Data Protection Regulation (GDPR), valid from May 2018. The GDPR is considered as one of the most severe changes in data privacy regulations in 20 years [1] and expected to cause significant efforts in industry and public authorities. Thus, we argue that GDPR could be a suitable example for investigating to what extent EAFs support enterprises in implementing regulations. One of the most important changes for enterprises is the shift of the viewpoint from a technological perspective dominated by information security issues to an organizational perspective governed by GDPR-compliant organizational structures and processes, i.e. a kind of management system [2]. In the process of implementing GDPR, the introduction of new roles, such as the data protection officer, in an enterprise and the determination of explicitly defined processes as well as a procedure for reacting on data privacy breaches requires an awareness about the existing data and how they have to be protected [3], [4]. Furthermore, it has to be clear, in which business processes they are used, and what kind of IT-systems store and process them. A well-documented EA and a working Enterprise Architecture Management (EAM) are expected to significantly ease the roadmap planning for GDPR implementation.

This article focuses on the practicability of EAF use for GDPR implementation, i.e. how can EAFs support the implementation of GDPR compliance in organizations. Organizations seeking advice on how to become GDPR compliant might turn to EAFs and the instruments presented in these frameworks. Thus, part of the research is to analyze prominent EAFs in order to identify their security-related structures and, consequently, to consider if they could be appropriate for GDPR implementation. Furthermore, a general process for GDPR implementation is devised and a case study from the financial industry is conducted to demonstrate the different process steps applied.

The main contributions of this article are (a) an analysis and comparison of existing architecture frameworks and how they address security-related issues relevant for the GDPR implementation and (b) a case study from the financial industry illustrating the use of EA for implementing GDPR compliance. The article is structured as follows: Section 2 briefly describes the research method used. In Section 3, important terms and definitions are clarified. Section 4 contains the analysis of selected EAF concerning their security features, an approach (process) for GDPR implementation and, respectively, an analysis of EAF suitability for the GDPR implementation process. In Section 5, the designed process is used in a case study. Section 6 summarizes the work and discusses conclusions.

2 Research Method

In the context of the motivation presented in Section 1, the research is guided by the research question:

RQ: How could Enterprise Architecture Frameworks support the implementation of EU General Data Protection Regulation compliance in enterprises from a structural stance?

The research method used for conducting this research is a combination of literature analysis and descriptive case study. Based on the research question defined, we identified research areas containing relevant publications for this question and analyzed them. The purpose of the analysis was to find existing theories, approaches or technologies, which help explaining or investigating how EA can support GDPR implementation. Due to the existence and wide use of EAFs in industries, the literature analysis explicitly included work on EAFs.

Since the literature study yielded only general EAF-based structures, processes and recommendations for implementing information security structures, processes and policies but

not specific GDPR-focused recommendations (see Section 4), a case study was performed in order to gather additional information pertinent for the research question. The approach is a qualitative case study that facilitates an exploration of a phenomenon within its context using a variety of data sources. This ensures that the subject under consideration is not explored from only one perspective, but rather from a variety of perspectives that allow for multiple facets of the phenomenon to be revealed and understood. Within the case study, two different perspectives were used, which, at the same time, represent sources of data: the established EA was examined and experts in the subject domain interviewed.

Yin distinguishes various kinds of case studies [5] explanatory, exploratory and descriptive. The case study presented in Section 5 has to be considered as descriptive, as it is used to describe the phenomenon of process outsourcing and the real-life context in which it occurs.

3 Relevant Terms and Definitions

In order to investigate the role of EAF in the implementation of GDPR, it is important to define the relevant terms. Therefore, EAM in Section 3.1, the conjunction to security in Section 3.2 as well as the GDPR in Section 3.3 are introduced.

3.1 Enterprise Architecture Management

The concept of EA has been introduced in 1987 when John Zachman published his suggested information systems architecture framework in IBM Systems Journal [6]. However, in 1970 Dewey Walker, as the team leader of Zachman in IBM, defined the information architecture concept in a Business System Planning (BSP) method [7]. By now, there is no universally accepted definition for EA in research communities and industry. However, most of the definitions generally agree, that "architecture is about the structure of important things (systems or enterprises), their components, and how the components fit and work together to fulfill some purpose" [8]. The ISO 15704 defines enterprise as [9] "one or more organizations sharing a definite mission, goals and objectives to offer an output such as a product or a service." Also, according to this standard, "an architecture is a description of the basic arrangement and connectivity of parts of a system (either a physical or a conceptual object or entity)." IEEE has defined the architecture concept and developed ANSI/IEEE Std 1471-2000 [10] as a standard for architecture, which has been referred by most of the later frameworks such as DoDAF and MoDAF. According to ISO/IEC architecture is defined as the "fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution" [11].

Consequently, we understand an EA as the overall structure of an organization that connects several entities important for an enterprise's success, such as business and IT processes and services, applications, technologies, strategies, domains, functions, visions and interests of the stakeholders. These structures and their interrelations are represented by an enterprise architecture model. In addition, EAM represents a discipline that is dedicated to optimizing the mutual alignment of the aforementioned entities by taking a comprehensive perspective of the entire EA [12]. Traditionally, companies have introduced EAM to better understand, plan, develop and control their IT assets, such as enterprise IT [13], [14].

By using EAM and respectively by analyzing it, positive business value and business impacts in terms of costs, scalability, portability and security can be generated [15].

3.2 Information Security and Security Architecture Development

The concept of "security" as a component of every organization was described in different ways in the literature. Bayle defines security as "the act of minimizing the risk of exposure of assets and resources to vulnerabilities and threats of various kinds" [16]. The word "security" is always

tied to two words, control and risk. According to Kim and Leem risk and control are cause and effects since "controls are implemented to mitigate risk and to reduce the potential for loss which may be caused by the risk" [17]. Information security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical). ISO/IEC 27000:2018 defines the information, security as a "preservation of confidentiality, integrity and availability of information. In addition, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved" [18].

ISACA defines the information security as an approach, which "ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)" [19]. It is important to acknowledge that there is no single definition for a security architecture (SA) that works across the thousands enterprises and organizations in existence today. Open security architecture (OSA) defines the security architecture as "the design artifacts that describe how the security controls (or security countermeasures) are positioned, and how they relate to the overall IT Architecture. These controls serve the purpose to maintain the system's quality attributes, among them confidentiality, integrity, availability, accountability and assurance" [20]. Initially, information security has been considered as a separate discipline isolated from the EA and business processes. Nowadays, the different EAFs coexist with a specific SA [21]. According to the Federal Deposit Insurance Corporation in connection with the National Institute of Standards and Technology, "[…] an enterprise security architecture describes the structure and behavior of an organization's security process, information security systems, personal and organizational subunits, and shows their alignment with the organization's mission and strategic plans. The enterprise security architecture links the components of an organization's security infrastructure as one cohesive unit, with the ultimate goal of protecting corporate information" [22].

According to the definition of an enterprise SA by the Open Group, it is a structure, that:

- contains "[…] organizational, conceptual, logical, and physical components that interact in a coherent fashion in order to achieve and maintain a state of managed risk;"
- enables / drives secure, safe, resilient and reliable behavior and upholds the privacy at risk areas throughout the whole enterprise.

Therefore, the elements within the SA are always related to components in the EA. Thus, although it might be possible to acknowledge the SA as a standalone one, it can never be an isolated architecture [21].

3.3 GDPR

The General Data Protection Regulation, or GDPR EU (Regulation EU 2016/679 of the European Parliament and of Council of 27 April 2016) is a regulation of the European Union introduced to improve and unify personal data protection of individuals within the European Union [1]. It entered into application in May 2018. The GDPR applies to processes carried out by organizations operating within the EU. It also applies to organizations outside the EU that offer goods or services to individuals in the EU.

The GDPR defines the instrument of data protection impact assessment (DPIA) to ensure regulation compliance [1]. According to the DPIA, companies are always responsible, even if they have outsourced data processing. They have to use data protection by design and default to ensure confidentiality, integrity, availability and resilience and have to have a process for regularly testing, assessing and evaluating technical and organizational measures. For automated decision-making and profiling, companies have to provide "meaningful information about the logic involved". They also have to keep track of all the personal data stored and of all activities processed, including the purpose of doing so, the location of data and third parties receiving it. No processing or profiling without the explicit permission from the subject should be done

(unless specific conditions apply). The removing of the personal data at the request of the subject is necessary and companies have to demonstrate compliance.

The requirements mentioned above lead to the need of the introduction of new roles (such as the data protection officer) in an enterprise and of explicitly defined processes (such as a procedure for reacting on data privacy breaches).

4 Selected EA Frameworks and their Suitability for GDPR Implementation

To investigate the GDPR suitability of enterprise architectures, specific frameworks are described shortly in Section 4.1. Afterwards, an implementation process for GDPR into EA is introduced in Section 4.2 and the respective architectures are tested concerning the implementation process in Section 4.3.

4.1 Selected Frameworks

Due to the substantial number of existing EAFs, not all of them were analyzed in the study. Furthermore, representatives in terms of selected frameworks were used that are dedicated to different business domains. First, we chose TOGAF as it is a widely accepted standard for the private sector and is frequently revised [23]. Second, we chose FEAF as a representative for the public sector (FEAF) [24]. Third, we chose two frameworks from the military domain (DoDAF and NAF) as the military is prone to treat security aspects with particular care [25].

Federal Enterprise Architecture Framework (FEAF)

FEAF presents an overall approach to developing and using EA in the US federal government [26]. FEAF consists of a suite of tools to help government planners implement a consolidated EA. At its core is the Consolidated Reference Model (CRM). It consists of a set of interrelated "reference models" that describe the six sub-architecture domains of the framework:

- The *Performance Reference Model* (PRM) that connects the strategy of the agency under consideration with internal business elements and investments, providing an opportunity to measure the impact of investments on strategic outcomes.
- The *Business Reference Model* (BRM) describes mission and support service areas of an organization through a taxonomy and promotes intra- and inter-agency collaboration.
- The *Data Reference Model* (DRM) facilitates integration of earlier separated information. It is the basis for understanding the meaning of the data, how to access it and how to leverage it to support the organization.
- The *Application Reference Model* (ARM) categorizes the system- and application-related technologies and prepares the delivery of service capabilities.
- The *Infrastructure Reference Model* (IRM) categorizes the network and technology related standards and their use in connection with technologies.
- The *Security Reference Model* (SRM) provides a common language and methodology for designing security and privacy in the context of public authorities.

Security is integral to all architectural domains and at all levels of an organization. As a result, the Security Reference Model (SRM) must be woven into all of the sub-architectures of the overarching EA across all the other reference models and it must be considered on different levels of the enterprise. At the highest levels, the SRM is used to transform federal laws, regulations, and publications into specific policies. At the segment level, the SRM is used to transform department specific policies into security controls and measurements. At the system level, it is used to transform segment controls into system specific designs or requirements. Each level of the SRM is critical to the overall security posture and health of an organization and/or system [27].

The SRM has three areas: Purpose, Risk, and Controls, they are divided into six total subareas:

- Purpose – Regulatory conditions, Risk profile.
- Risk – Risk assessment processes, Impact mitigation.
- Controls – Compliance, Control categories.

For GDPR implementation the following instruments of the SRM framework are relevant:

- The *Security Controls Catalog* (core), which determines the complete collection of security controls. The developer is then able to choose those controls that are applicable for the effort.
- The *Security and Privacy Plan* as an overview concerning the enterprise security and privacy programs, procedures and privacy relevant for the agency.
- The *Security Authorization Documentation* as a collocation of security documents which are relevant to each system.
- The *Continuous Monitoring Plan* that represents the enterprises' actions concerning monitoring and analyzing of security controls.

However, FEAF, in general, does not provide any specific elements in the above plan or documentations for achieving GDPR compliance.

Department of Defense Architecture Framework (DoDAF)

DoDAF has been developed as a mean of representing EA. It helps stakeholders focus on their specific concerns while they retain oversight of the big picture of the enterprise. The current version of DoDAF (Version 2.0) focuses on understandable representation of complex EA descriptions and models to facilitate decision-making. In DoDAF, architectural descriptions are divided into eight main viewpoints, with each viewpoint being described by architectural descriptions and models as well as graphical and tabular data [28]:

1. The *All Viewpoint* describes the overarching aspects of architecture context that relate to all viewpoints.
2. The *Capability Viewpoint* articulates the capability requirements, the delivery timing and the deployed capability.
3. The *Data and Information Viewpoint* articulates the data relationships and alignment structures in the architecture content for the capability and operational requirements, system engineering processes and systems and services.
4. The *Operational Viewpoint* includes the operational scenarios, activities, and requirements that support capabilities.
5. The *Project Viewpoint* describes the relationships between operational and capability requirements and the various projects being implemented. The Project Viewpoint also details dependencies among capability and operational requirements, system engineering processes, systems design and services design within the Defense Acquisition System process.
6. The *Services Viewpoint* is the design for solutions articulating the performers, activities, services and their exchanges, providing for or supporting operational and capability functions.
7. The *Standards Viewpoint* articulates the applicable operational, business, technical, and industry policies, standards, guidance, constraints and forecasts that apply to capability and operational requirements, system engineering processes and systems and services.
8. The *Systems Viewpoint* for legacy support is the design for solutions articulating the systems, their composition, interconnectivity, and context providing for, or supporting, operational and capability functions.

In connection to many other enterprise architecture frameworks, DoDAF does not approach security matters severally. Within the DoDAF framework, the following possibilities with regard

to the requirements exist: as a nonfunctional or performance system, as a functional system or as an operational mission [28].

To encounter potential threats and to reduce vulnerabilities, DoDAF identifies the following measures: Physical, Procedural, Communication Security, Transient Electromagnetic Pulse Emanation Standard and Information Security. In order to assess the risks and apply minimum but necessary security measures, DoDAF also analyzes the following four characteristics:

- *Environment*, and the respective hostility of it, in which the asset is located.
- *Asset Value* in terms of the cost of the asset spent for protection. They are described by the loss, disclosure and replacement of the asset.
- *Criticality* as a measure for the criticality of the asset concerning the government's ability to conduct their activities.
- *Personnel Clearance* as a measure for the degree of trustworthiness of staff that the government considers appropriate to access the asset.

Though DoDAF does not have a separate viewpoint for security, it treats security like any other requirement. Security characteristics are mapped to each of those building blocks to enable the assessment of the security risks and appropriate measures of protection [28].

The Open Group Architecture Framework (TOGAF)

TOGAF is defined as a "tool for developing information system architectures." Its main purpose is to facilitate the process of developing the architecture of a particular organization, while ensuring the possibility of future development [29].

The TOGAF model consists of two main components – the ADM (Architecture Development Method) methodology, which defines the architecture development process, and the Foundation Architecture. It is supplemented by a corresponding database of resources, including descriptions of architectural principles, implementation examples, and the specialized language ADML. TOGAF divides enterprise architecture into four categories as follows:

1. The *Business architecture* that describes the processes the business uses to meet its goals.
2. The *Application architecture*, which describes how specific applications are designed and how they interact with each other.
3. The *Data architecture* that describes how the enterprise data stores are organized and accessed.
4. The *Technical architecture*, which describes the hardware and software infrastructure that support applications and their interactions.

According to the Open Group, the SA is considered separately and contains its own frameworks and methods that are introduced to its own non-typical scenarios. Examples for these situations are the IT architects who define normative information flow and use IT services and respectively the security architects that define the scenario for which the IT service might fail. Furthermore, it is recommended that the security architects interact with the other architects in the early modeling phase. Therefore, the inputs and outputs of EA and SA in the particular phases of EA development are explained by ADM. Consequently, the security is considered to interact in the background of other EA aspects such as the information exchange matrix.

To avoid missing critical security concerns, a guidance intended to help the enterprise architects and the security practitioners is included in TOGAF. Considering the SAs, they contain five key elements.

1. They have an own discrete security methodology.
2. The security methodology is composed to own discrete views and viewpoints.
3. The methodology addresses non-normative processes through systems and among applications and introduces own, non-normative ones.
4. The methodology introduces single-purpose and unique components within the design.
5. The methodology requires an own and unique skills- and competencies-set concerning the enterprise and IT architects.

The necessary steps and the artefacts that should be created to model security-specific information are offered as a guidance throughout the phases of the ADM within TOGAF. The areas of concern that are generally accepted in terms of the security architects are:

- *Authentication* as evidence for the identity of a person or entity that is related to the system or enterprise in some way.
- *Authorization* as an enforcement and definition of permitted capabilities for an established identity like an entity or person.
- *Audit* as an ability to test the system in terms of accordance with the stated security policies. Therefore, forensic data is provided.
- *Assurance* as the progression of the audit concerning ability and prove of the enterprise architecture, if the system contains the security attributes required to maintain the stated security roles.
- *Availability* as a function-ability of the enterprise concerning depletion despite malicious or abnormal events as well as the system's flow without service interruption.
- *Asset Protection* for information assets that are protected from unintended disclosure or loss and for resources from unintended and unauthorized use.
- *Administration* as the ability to change and add security policies, relations between entities, people and systems as well as implementation of policies in the enterprise.
- *Risk Management* as the organization's tolerance and attitude concerning risks.

Open Group also published the Open Information Security Management Maturity Model (ISM3), which helps organizations to ensure that security management processes are implemented appropriately and aligned with business requirements. It includes operational metrics to evaluate the maturity of security management processes. To put it simple, enterprises can use ISM3 metrics to evaluate their current information security management. At the next step, they can define organization targets for each process and control process improvement annually, so that ISM3 can be categorized as a reference model for information security management [30], [31].

NATO Architecture Framework (NAF)

The NATO Architecture Framework has been derived from MoDAF and DoDAF [32]. As opposed to other, system-oriented approaches, the framework is service-oriented and uses a views approach in terms of model categories or in other words: determines what the stakeholder wants to see. As a standard for developing EA it answers the following main questions:

- What is the required functionality of the enterprise?
- How can this functionality be achieved?
- What approaches can be used or how can solutions be implemented?

The framework defines three main properties, which are:

1. *Methodology* in terms of how to run an architecture project and respectively how to develop an architecture.
2. *Viewpoints* as conventions for the designing, interpretation and value of architecture views for presenting the enterprise architecture to different stakeholders.
3. *Meta-models* as standard ontologies for determining the key architectural elements and their interdependencies.

The framework includes seven views and associated products that align with the DoDAF viewpoints and views: NATO All View (NAV), NATO Capability View (NCV), NATO Operation View (NOV), NATO Service-Oriented View (NSOV), NATO Systems View (NSV), NATO Technical View (NTV) and NATO Programme View (NPV). The usual types of views that exist at each level are:

- *Classification/ontology* that are structures of concepts such as capabilities, services, etc...
- *Structure* as how elements are assembled, e.g. enterprises, nodes, resources, etc...
- *Connectivity* as a summary of everything from high-level capability dependencies to detailed system connectivity.
- *Behavior* as a description of how things work.
- *Information* concerning a collaboration about what information/data is used, and how it is structured.
- *Constraints* as rules that govern the enterprise, nodes and resources etc...
- *Programme* as project timelines and respective milestones affecting the elements in the architecture.

Concerning this research's interest, the NAF does not provide a special security view. In general, it provides a mature common meta-model to describe the contents of the corresponding views. Every view contains a section of the overall meta-model in order to describe view-specific contents and their relations. In addition to the concepts and relationships, the meta-model also defines the semantics of each of these elements. Concerning the security, the existing views could be used for domain based security and entity trust models.

4.2 GDPR Implementation Process

For the implementation of GDPR compliant structures and processes, a multitude of processes and approaches are being proposed in literature. However, there is no established opinion yet, which would be the best way to proceed. Because of that, this research uses a simplified approach consisting of five steps that were devised from security information within the EU GDPR portal [1], the respective application from the German information security agency BSI concerning their privacy policy [33] and information from ISACA regarding information security [19]. The steps (sX) to take in the approach (the proposed GDPR implementation process) are described in the following in a "cookbook"-like style:

S1 Develop a 'privacy inventory' (for identification and classification of data):

Classify all data and assess whether it counts as personal; describe the purpose for which it was collected; and is there the subject's consent for using it? Pay extra attention to special categories of personal data (e.g. related to health, biometrics, politics, religion, and ethnicity). The use is only allowed in very specific circumstances!

S2 Analyze the use of personal data (for identification of applications, processes and parties that use the data):

Which applications, processes, people and parties use this data, at which locations, for which purpose? Which data is used where and by whom (location, users)? How is secure data transferred (start with high-risk areas and most sensitive data; model data flows)? Data subjects' rights – Consider if individuals are likely to exercise their new rights against your company and what this could mean for your business in practice. Based on that analysis, set up processes to capture, record and act on those requests and privacy notices.

S3 Identify and assess risks to sensitive data (for identification and risk assessment to sensitive data):

Where is your company vulnerable in terms of sensitive data? What could go wrong? Does the company share data with suppliers? Do they adhere to data security regulations?

S4 Define controls & mitigating measures:

Is there a person employed, which is responsible for the processing of personal data in the company? Prioritize risks, allocate budgets and plan changes. Evaluate cost of measures vs. risk (expected loss). Integrate with the company's project/change portfolio and roadmaps.

S5 Implement controls:

Does the company have an impact analysis / data protection impact assessment? It is necessary to create and maintain a record of the personal data processing carried out (unless exempt). Consider setting up a central breach management unit to collate, review and notify breaches, where appropriate review and update the security measures in regarding the increased security obligations in the regulation processors.

Figure 1 graphically illustrates the approach (process) for GDPR implementation with the aforementioned steps.

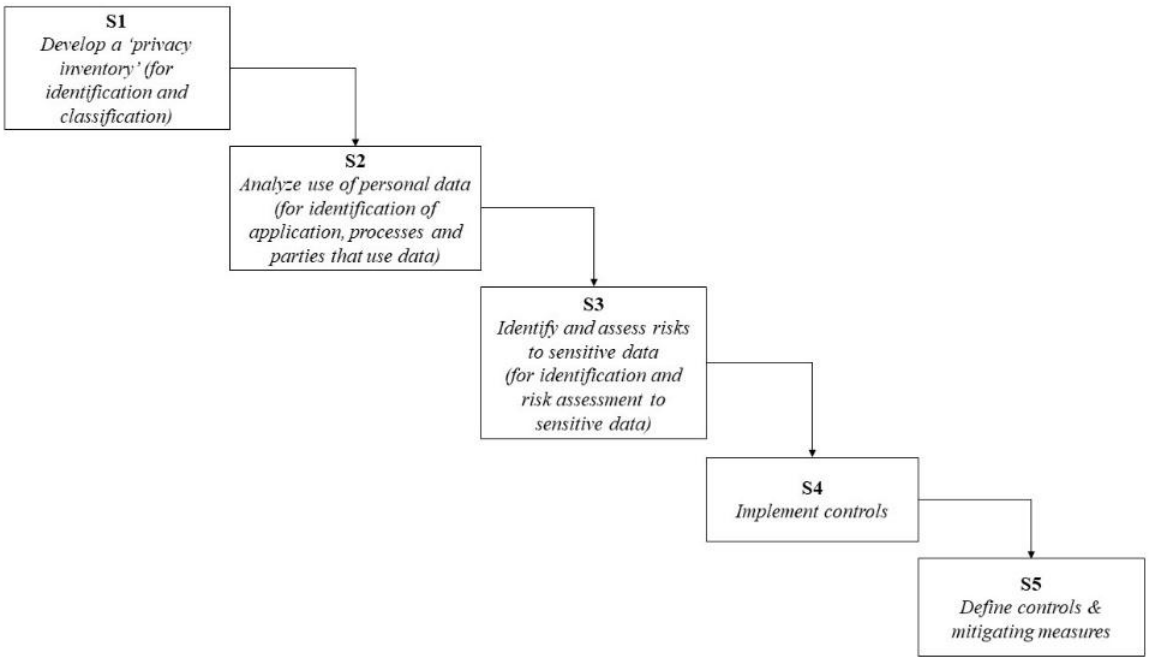

Figure 1. Proposed GDPR implementation process

4.3 EAF Suitability for the GDPR Implementation Process

Based on the GDPR implementation process presented in Section 4.2, the selected frameworks from Section 4.1 are compared concerning the fulfillment of the steps from Section 4.2. Table 1 presents the results of the analysis of possibility to execute the steps of GDPR implementation process ("+" means that the step is possible, "-" means that the step is not supported).

The analysis of the EAF possibilities for the GDPR implementation showed that the frameworks, to a large extent, implement the five steps.

With regard to the identification and risk assessment to sensitive data, it was identified that DoDAF takes the characteristics of *environment, asset value, criticality* and *personal clearance* into account, but in contrast to the FEAF, does not contain an explicit model for security (see Section 4.1 – DoDAF). Derived from this comparison, this action is considered as "not fulfilled" ("-"). The same applies to the NAF, as the framework does not contain an explicit security model, but the characteristics *classification/ontology, structure, connectivity, behavior, information, constraints* and *program*, which are intended to describe the corresponding views. The *constrains* characteristic is suitable for security related issues; however, the previously defined action, in relation to the TOGAF security model, is considered as "not fulfilled."

Table 1. Comparison of the EAF based on the GDPR requirements

Action \ Notation	FEAF	DoDAF	TOGAF	NAF
Identification and classification of data	+ Data Model	+ Data and Information Viewpoint	+ Data Architecture	+ NATO Capability View
Identification of application, processes and parties that use data	+ Components Model	+ Operational and Project Viewpoints	+ Technical and Application Architecture	+ NATO Operational View
Identification and risk assessment to sensitive data	+ Security Model	- Four characteristics to assess the risk	-	- Constraints
Define controls & mitigating measures	+ Security Controls Catalogue	+ The Standards Viewpoint	+ Business Architecture	+ All Views
Implement controls	+ Continuous Monitoring Plan	+ The Standards Viewpoint	+ ISM3	+ All Views

5 Case Study on GDPR Implementation

The case study originates from financial industries and the field of IT-based compliance management. The GDPR implementation process is applied to a reference enterprise architecture, which holistically captures all relevant aspects of the financial organization affected by regulation. The reference enterprise architecture (REA) is supposed to help financial institutes to effectively and efficiently implement a compliance organization. The REA includes business architecture, data and application architecture and technology architecture layers, uses TOGAF, and is represented in ArchiMate[†] as modeling language. One part of the REA addresses the prevention of "other criminal acts" (abbr. ssH for German "sonstige strafbare Handlungen"), which is regulated in §25h Abs. 1 KWG and applies for every financial institution [34]. Such crimes may be fraud, corruption or treason. Other parts address anti-money laundry and Know-Your-Customer (KYC). KYC is in focus for the case study with the customer onboarding part.

When building the REA, 64 structured interviews with responsible people from distinct financial institutes were conducted and described in total. The structure of the interviews was developed by using deductive techniques. Compliance experts were consulted in order to gain a first structure of a compliance implementation system and to study the laws as well as guidelines provided by the Federal Financial Supervisory Authority [35]. Afterwards, all interviews were transferred to EA models using the same modeling structure and guidelines, which was done according to Lankhorst [8]. Each individual EA model was structured by eight different ArchiMate viewpoints, which displayed different aspects of the EA models. Each viewpoint relates to a certain purpose. From the individual models, the REA was derived. The process and method behind this REA development is documented in more detail in [36].

Based on this REA, the application of the GDPR shows how a much elaborated compliance organizations are affected by GDPR and how a defined EA affects the process of GDPR implementation. Concerning the application of GDPR into the case study, the process followed the steps defined in Section 4.2. For each step, it is demonstrated how this step was performed,

[†] https://www.opengroup.org/archimate-forum/archimate-overview

including excerpts from the REA. Each step was conducted in consultation with compliance experts.

S1 Develop a 'privacy inventory': In this step, data was identified, which can contain personal data. In this case, it is all data, which links to a natural person. The corresponding model elements are colored red in Figure 2. The overall purpose of collecting the presented data is to enable a sophisticated risk portfolio analysis of the financial institution's customer base as it is required by the Federal Financial Supervisory Authority.

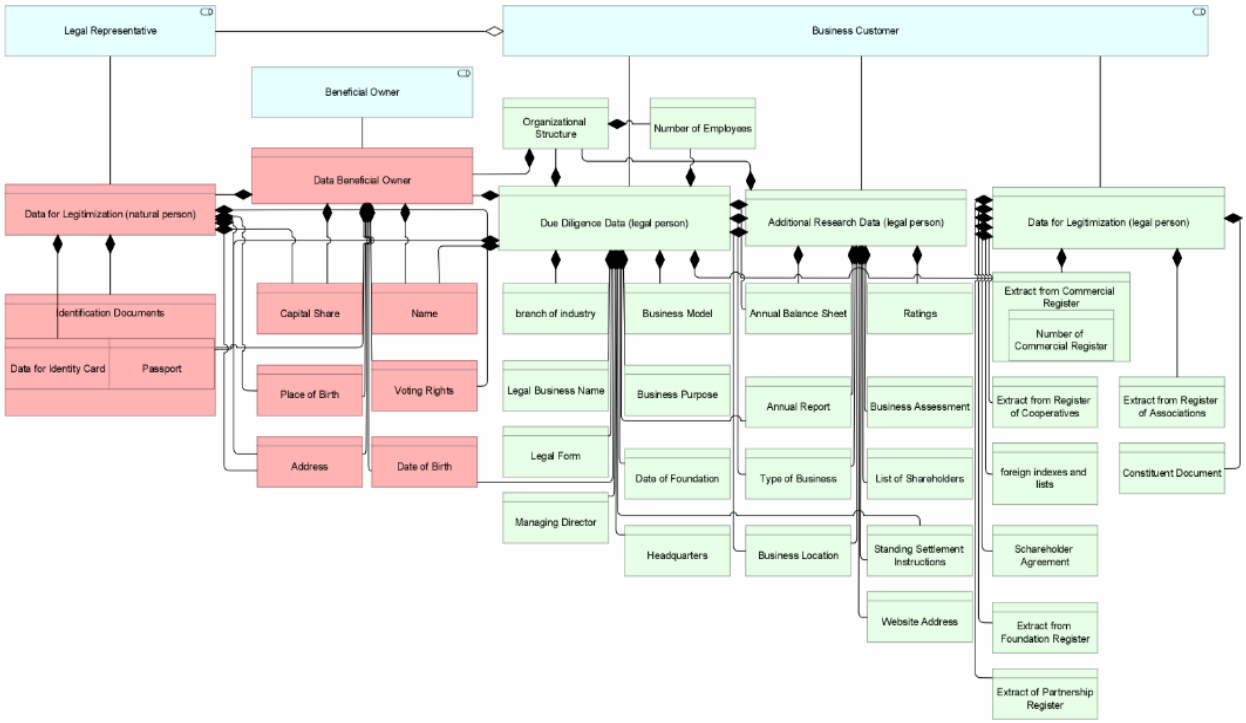

Figure 2. Identification of personal data

S2 Analyze the use of personal data: This step consists of three activities as described in the following.

S2.1 Which business functions use personal data? Based on extracted data, it is comprehensible which business functions are using this data (again, they are marked red). Figure 3 shows an excerpt from KYC for the part of the customer identification program. It should be noted, that the identification of the affected business functions is done using the information captured in the ArchiMate model, i.e. there is no manual processes required.

S2.2 Which procedures use personal data? The process steps were identified and are shown in Figure 4. The figure also visualizes all business functions in the scope and how they are linked. It can be useful for understanding the scale of the functions, which have to be considered. Furthermore, one can derive what parties can access the respective data (see blue elements in Figure 4, which represent the business role in ArchiMate).

S2.3 Which applications use personal data? Based on marked business functions, the content of the REA model can link them with the applications of the company (see Figure 5).

S3 Identify and assess risks to sensitive data: In this step, the sets of risks were identified (e.g. weak encryption of data, insecurity transmission channel) and assessed. The risk level is indicated in Figure 6 using traffic light symbols from low risks (green traffic light) to high risks (red traffic light).

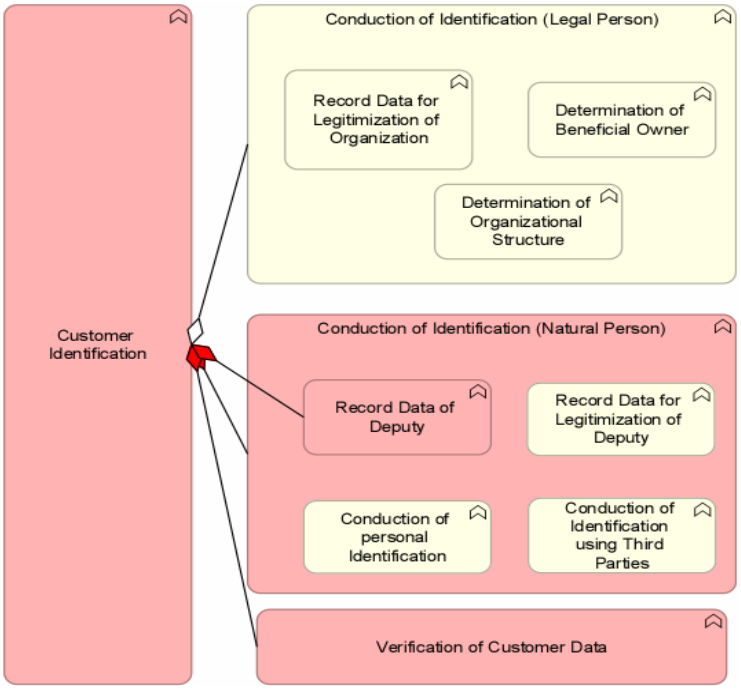

Figure 3. Customer Identification Program (CIP)

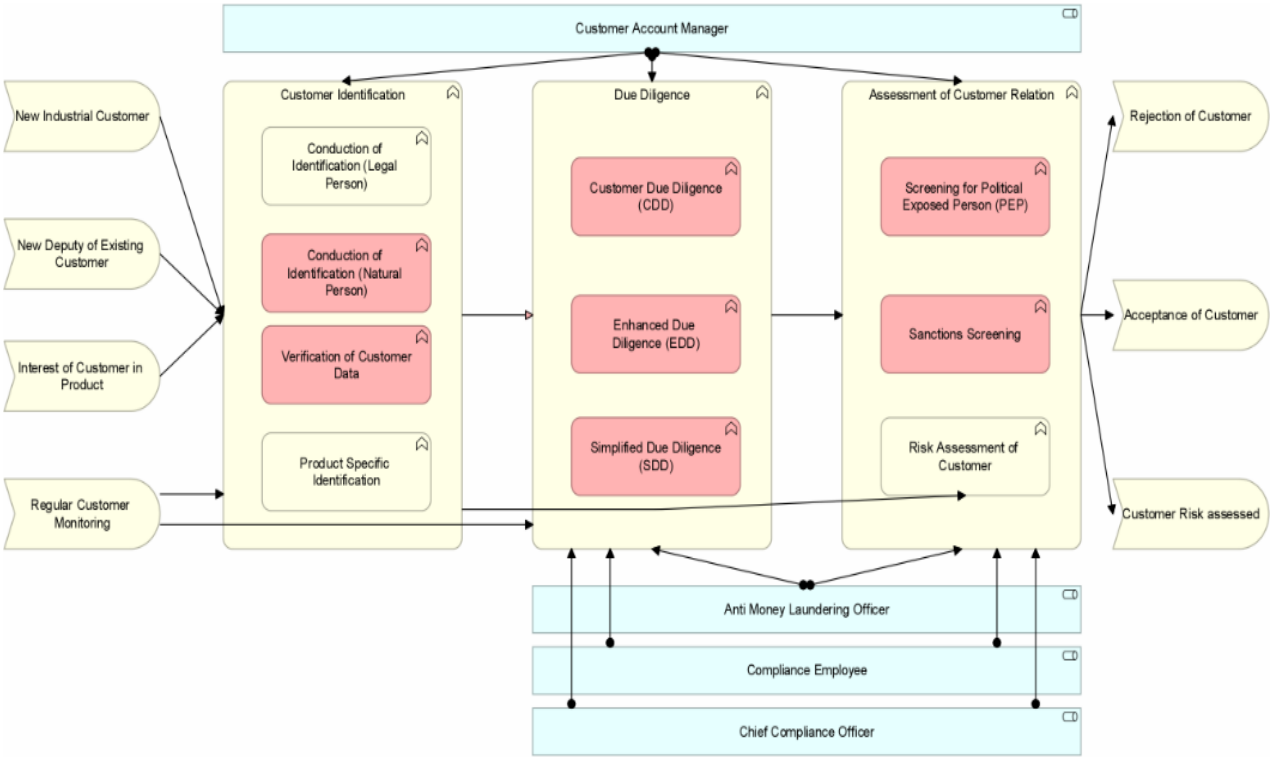

Figure 4. Complete model of the business process

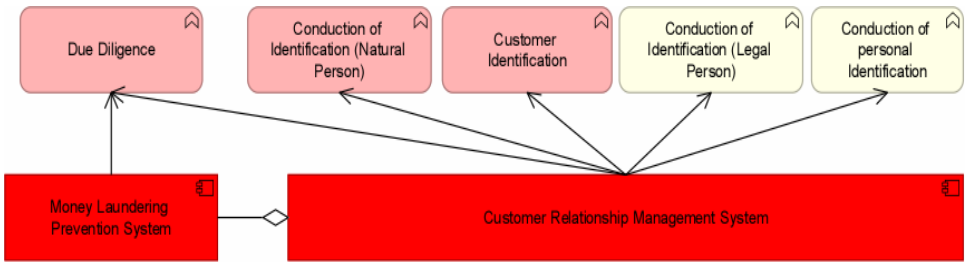

Figure 5. Application model

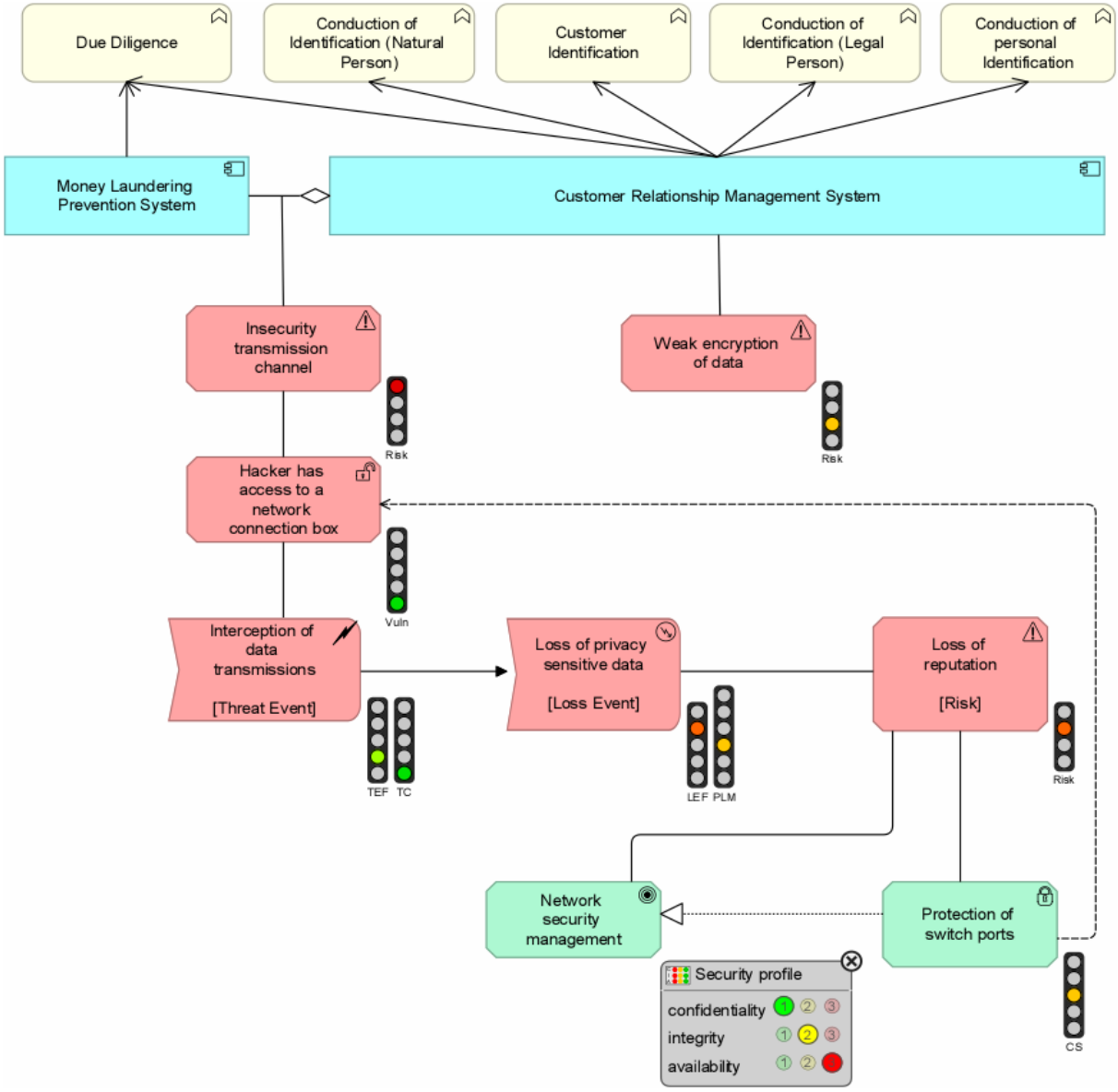

Figure 6. Identifications and assessing of risks

S4 Define controls & mitigating measures and S5 Implement Controls: The final step is the implementation of controls & mitigating measures. Based on identified risks in the previous step, improvements were proposed by creating GDPR-compliant structures, which can help the company manage risks (e.g. and additional encryption service, see Figure 7).

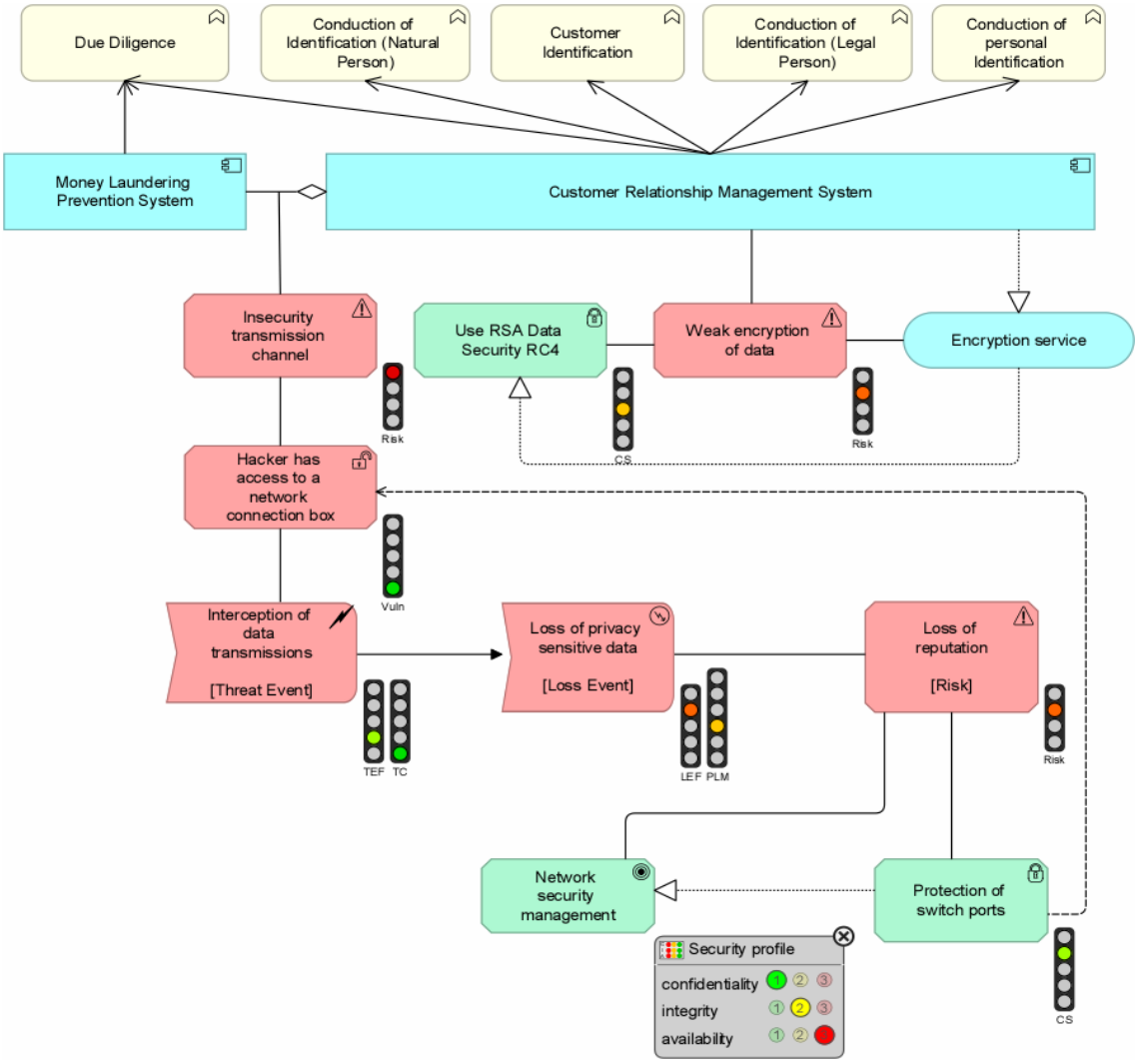

Figure 7. Implementation of controls & mitigating measures

6 Conclusion

Research presented in this article aimed to achieve two primary goals: (a) to gain an overview about existing EAFs and their approaches to handle security-related issues, and (b) to introduce a possible approach for GDPR implementation into EAs. The first goal was addressed in an analysis of established EAFs. The conclusion from the analysis is that all architecture frameworks provide approaches to tackle security-related issues, but the underlying philosophy is different and can be roughly grouped into EAFs, which favor a separate and defined SA and those that treat security aspects as attributes of the objects in individual architectures. For the practice of GDPR implementation, this means that organizations practicing EAM in accordance to one of the existing frameworks (a) have all information available in the EA model required to support the GDPR implementation and (b) should follow the individual EAF's philosophy. However, GDPR as a necessity in terms of regulations still has to be integrated.

The second goal of the research, an approach for GDPR implementation, is tackled in Section 4.2 by proposing a GDPR implementation process. The example of applying this process in a use case from the financial services domain shows that EA models are a helpful tool to make GDPR related issues not only transparent, but also enable identifying current usage of sensible data within an organization. However, such an endeavor stands or falls with the validity of elicited information (i.e. how to gather the necessary data for such an EA model?) and the existence of EA models within the organization in the first place. Overall, this article provides a theoretical lens on using EAM to establish a compliant GDPR process. Although the results show that EAM

provides appropriate means, it is open how practical such an approach is for organizations. Such a question may be at the core of future research in this domain.

Furthermore, the research also resulted in observations regarding advantages and drawbacks of SA development strategies presented in Section 3.2:

- *Effectiveness*: the effectiveness of SA development strategies is evaluated considering general goals of developing SA such as holistic approach, security and business alignment, integration, change management, security requirements analysis, security cost reduction and compliance. According to the results of this study, by using EA knowledge and developing SA as a part of EA, security and business alignment could be inherited from EA to SA. In addition, integration of SA with other IT architectures would be more effective when EA artifacts could be used to develop SA. Since independent strategies are not related to a particular EA framework, the independent methods could be used to develop SA in enterprises that have to comply with special security regulations; however, in this case integration of SA with EA will not be achieved completely.
- *Efficiency*: the most important difference exists between the efficiency of SA development strategies deep rooted in reusing EA knowledge and artifacts and reusability of SA building blocks. Therefore, the most efficient strategy is to develop SA as a part of EA because knowledge, artifacts and governance processes of EA could be reused in the development of SA. An independent approach could be the most expensive strategy since business requirements have to be captured and analyzed as part of SA development. The efficiency of other strategies (using EA knowledge and using EA artifacts) would be at the efficiency interval of these two extreme approaches.
- *Impact*: the practicality of SA outputs could be increased when SA is developing as a sub-architecture of EA because supportive transitional processes of EA help SA in terms of implementation. Moreover, some of the security requirements can be implemented just through other architectures such as software development, database and network. Therefore, an important question for enterprises that want to develop SA is how they should select or customize their EA frameworks to support SA development effectively and efficiently.

Further research concerning the aforementioned GDPR implementation process is necessary to validate the approach presented and illustrated in this article.

Acknowledgements

The analysis of EAFs (Section 4.1) is due to the grant from RFBR (project number 19-07-00928), the GDPR implementation process (Section 4.2) is partially due to the grant from RFBR (project number 20-07-00455).

References

[1] European Commission: GDPR.eu – Data Protection Impact Assessment. Available: https://gdpr.eu/data-protection-impact-assessment-template/. Accessed on Aug.14, 2019.

[2] C. Bartolini, A. Calabró, and E. Marchetti, "GDPR and business processes: An effective solution," *Proceedings of the 2nd International Conference on Applications of Intelligent Systems (APPIS), ACM International Conference Proceedings Series*, no. 7, 2019. Available: https://doi.org/10.1145/3309772.3309779

[3] S. Agostinelli, F. M. Maggi, A. Marraella, and F.Sapio, "Achieving GDPR Compliance of BPMN Process Models," *Proceedings of the International Conference on Advanced Information Systems Engineering (CAiSE), LNBIP*, vol. 350, pp. 10–22, 2019. Available: https://doi.org/10.1007/978-3-030-21297-1_2

[4] D. Gouveia, and D. Aveiro, "Modeling the system described by the EU general data protection regulation with DEMO," *Proceedings of the 8th Enterprise Engineering Working Conference (EEWC), LNBIP*, vol. 334, pp. 144–158, 2019. Available: https://doi.org/10.1007/978-3-030-06097-8_9

[5] R. K. Yin, *Case Study Research: Design and Methods*, 3rd Edition, Applied Social Research Methods Series, Sage Publications, 2002.

[6] J. A. Zachman, "A framework for information systems architecture," *IBM Systems Journal*, vol. 26, no. 3, pp. 276–292, 1987. Available: https://doi.org/10.1147/sj.263.0276

[7] S. Kotusev, "The history of enterprise architecture: An evidence-based review," *Journal of Enterprise Architecture*, vol. 12, no. 1, pp. 29–37, 2016.

[8] M. Lankhorst, *Enterprise Architecture at Work – Modelling, Communication and Analysis*. Springer, 2017. Available: https://doi.org/10.1007/978-3-662-53933-0

[9] International Organization for Standardization: ISO 15704:2000, Industrial Automation Systems – Requirements for Enterprise-Reference Architectures and Methodologies. Available: https://www.iso.org/standard/28777.html. Accessed on Aug. 14, 2019.

[10] IEEE Standards Association: IEEE 1471-2000, IEEE Recommended Practice for Architectural Description for Software-Intensive Systems. Available: https://standards.ieee.org/standard/1471-2000.html. Accessed on Aug. 15, 2019.

[11] International Organization for Standardization: ISO/IEC/IEEE 42010:2011, Systems and Software Engineering – Architecture Description. Available: https://www.iso.org/standard/50508.html. Accessed on Aug. 15, 2019.

[12] K. Winter, S. Buckl, F. Matthes, and C. M. Schweda, "Investigating the State-of-the-Art in Enterprise Architecture Management Methods in Literature and Practice," *The 5th Mediterranean Conference on Information Systems, MCIS 2010 Proceedings*, p. 90, 2010.

[13] D. Simon, K. Fischbach, and D. Schoder, "Enterprise architecture management and its role in corporate strategic management," *Information Systems and e-Business Management*, vol. 12, pp. 5–42, 2014. Available: https://doi.org/10.1007/s10257-013-0213-4

[14] M. Wißotzki, H. Koc, and T. Weichert, "Development of an Enterprise Architecture Management Capability Catalog," *Perspectives in Business Informatics Research, LNBIP*, vol. 158, pp. 112–126, 2013. Available: https://doi.org/10.1007/978-3-642-40823-6_10

[15] R. Schmidt, M. Wißotzki, D. Jugel, M. Möhring, K. Sandkuhl, and A. Zimmermann, "Towards a framework for enterprise architecture analytics," *2014 IEEE 18th International Enterprise Distributed Object Computing Conference Workshops and Demonstrations*, pp. 266–275, 2014. Available: https://doi.org/10.1109/EDOCW.2014.47

[16] A. J. Bayle, "Security in open system networks: a tutorial survey," *Computer & Security*, vol. 7, no. 5, p. 523, 1988. Available: https://doi.org/10.1016/0167-4048(88)90291-X

[17] S. Kim, and C. S. Leem, "Enterprise security architecture in business convergence environments," *Industrial Management & Data Systems*, vol. 105, no. 7, pp. 919–936, 2005. Available: https://doi.org/10.1108/02635570510616111

[18] International Organization for Standardization: ISO/IEC 27000:2018, Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary. Available: https://www.iso.org/standard/73906.html. Accessed on Jan. 9, 2020.

[19] ISACA: Information Security. Available: https://www.isaca.org/Pages/Glossary.aspx?tid=1486&char=I. Accessed on Aug. 14, 2019.

[20] Open Security Architecture: Definition Security Architecture. Available: https://www.opensecurityarchitecture.org/cms/definitions/it-security-architecture. Accessed on Aug. 15, 2019.

[21] The Open Group: Integrating Risk and Security within a TOGAF® Enterprise Architecture. Available: https://publications.opengroup.org/g152. Accessed on Aug. 15, 2019.

[22] Federal Deposit Insurance Corporation: The FDIC's Governance of Information Technology Initiatives. Audit Report. Information Technology Audits and Cyber, 2018. Available: https://www.fdicoig.gov/sites/default/files/report-release/18-004AUD.pdf. Accessed on Aug. 15, 2019.

[23] The Open Group: The TOGAF® Standard, Version 9.2 Overview. Available: https://www.opengroup.org/togaf, Accessed on Aug. 22, 2019.

[24] Office of Management and Budget: The Common Approach to Federal Enterprise Architecture, 2012. Available: https://www.immagic.com/eLibrary/ARCHIVES/GENERAL/WHITEHSE/W120502C.pdf. Accessed on Aug. 22, 2019.

[25] W. Wang, H. Luo, and H. Deng, "Research on data and workflow security of electronic military systems," *Proceedings of the 4th International Conference on Intelligent Control and Information Processing (ICICP)*, IEEE, pp. 705–709, 2013. Available: https://doi.org/10.1109/ICICIP.2013.6568164

[26] United States of America: Federal Enterprise Architecture Framework (FEAF). Version 2, 2013. Available: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/fea_v2.pdf. Accessed on Aug. 14, 2019.

[27] B. Yoon, P. D. Lam, P. H. Son, P. T. Dat, D. V. Thien, V. V. Vu, D. H. Quan, and D. N. Toan, "A Study on EA based IT Governance," *Proceedings of the International Conference on Advanced Communications Technology (ICACT)*, IEEE, pp. 686–691, 2019. Available: https://doi.org/10.23919/ICACT.2019.8701962

[28] L. Ertaul and J. Hao, "Enterprise Security Planning with Department of Defense Architecture Framework (DODAF)," Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.217.8179&rep=rep1&type=pdf. Accessed on Aug. 14, 2019.

[29] The Open Group: TOGAF. Available: http://pubs.opengroup.org/architecture/togaf9-doc/arch/. Accessed on Aug. 14, 2019.

[30] SABSA: Introduction. Available: https://sabsa.org/. Accessed on Aug. 14, 2019.

[31] The Open Group: Open Information Security Management Maturity Model (O-ISM3), Version 2.0. Available: https://publications.opengroup.org/c17b. Accessed on Aug. 9, 2019.

[32] North Atlantic Treaty Organization: NATO Architecture Framework, Version 4. Available: https://www.nato.int/cps/en/natohq/topics_157575.htm. Accessed on Aug. 15, 2019.

[33] German Federal Office for Information Security: Privacy Policy. Available: https://www.bsi.bund.de/EN/Service/Imprint/DataProtectionStatement/dataprotect.html. Accessed on Aug. 8, 2019.

[34] German Federal Ministry of Justice and Consumer Protection. Federal Office of Justice: §25h KWG – Interne Sicherungsmaßnahmen (internal preservation measures). Available: https://www.gesetze-im-internet.de/kredwg/__25h.html. Accessed on Aug. 14, 2019.

[35] German Federal Financial Supervisory Autority: Auslegungs- und Anwendungshinweise zu §25c KWG – Sonstige strafbare Handlungen (other criminal acts). Available: https://www.bafin.de/SharedDocs/Downloads/DE/Auslegungsentscheidung/dl_ae_rs_1107_gw_anlage1.html. Accessed on Aug. 14, 2019.

[36] F. Timm and K. Sandkuhl, "A Reference Enterprise Architecture for Holistic Compliance Management in the Financial Sector" *ICIS 2018 Proceedings*, 2018.