Human Factors and Systems Interaction, Vol. 84, 2023, 238–248
https://doi.org/10.54941/ahfe1003609

Security and Privacy for Interoperable Organizations

Anacleto Correia[1], Pedro Água[1], Armindo Frias[1,2], and Mário Simões-Marques[1]

[1]CINAV, Escola Naval, Instituto Universitário Militar, Base Naval de Lisboa, 2810–001 Almada, Portugal
[2]Advance/CSG, ISEG-Universidade de Lisboa, Rua Miguel Lupi n° 20, 1249–078 Lisboa, Portugal

ABSTRACT

There are organizations for whom interoperability is crucial for the accomplishment of their mission, such as in the areas of disaster management, security, and defense. However, those organizations also must comply with the constraints and rules for information security and privacy. The ISO 27001 provides a global standard framework to help organizations to protect their information in a systematic way, through the adoption of an information security management system. Furthermore, the ISO 27701, provides specific data privacy controls, allowing the organization to demonstrate effective privacy data management. A challenge organizations face is how to comply with information security and privacy policies and procedures together with the accomplishment of their mission. In this paper, we argue this can be achieved with an Enterprise Architecture (EA) framework. Particularly, the NATO Architecture Framework (NAF) provides a methodology to develop EA artifacts, however it lacks the tools amenable to enforce information security and privacy. We also propose the integration of ISO 27001 and ISO 27701 in NAF, in order that the EA artifacts delivered by NAF framework, could have embedded the information security and privacy principles by design.

Keywords: Enterprise architecture, Information security, Information privacy, NATO architecture framework, Digital transformation

INTRODUCTION

In response to the need for greater adaptability, resilience, and flexibility in changing environments, organizations have placed greater emphasis on information management. This is especially true for organizations for whom interoperability with different partners is crucial for the accomplishment of their mission, such as in the areas of disaster management, security, and defense. For instance, in a particular context of disaster management, the interoperability of different systems, from disaster response teams from different origins (countries, languages, and cultures), is crucial for effective information sharing in a catastrophe scenario. Ideally, these different response organizations should be able to share their data, safeguarding information security and privacy (Correia et al., 2021).

Regardless of the kind of organization, the advancement of technology has made information assets management more challenging. Digital transformation disrupted traditional processes, altering the value of critical business information, changing where it is stored, how it is shared, and the business processes it influences. The convergence of technologies has brought about many benefits for innovative organizations, such as reduced operational costs and improved operational efficiency. However, they also introduce new risks, threats, and vulnerabilities. Organizations that do not adequately address information security and privacy, in the face of technologies with potential to transform business processes and functions, may be exposed to significant risks. This is because the traditional organizational perimeter has changed and became more volatile - encompassing customers, suppliers, partners, and the mobile workforce – and increased the corporate risk. Consequently, the new blurred organizational perimeter should be conveniently managed to avoid: (i) the decrease in the quality of service of the shared infrastructure; (ii) the distribution and increase in complexity of authentication and authorization mechanisms; (iii) the increase in potential attack points; (iv) greater confusion over staff responsibility and accountability; and (v) greater difficulty detecting and responding to incidents in interconnected environments with multiple external parties (TISN, 2007).

Balancing conflicting priorities of operational needs and information protection is a challenge that can only be met if the entire organization takes part on it, making protection of corporate information assets becoming the responsibility of all stakeholders. It is along this line that organizations are also facing demands to meet the regulatory requirements on information assets protection, making compliance with international standards, such as ISO 2700x (ISO/IEC, 2022a, 2022b) and 27701 (ISO/IEC, 2019), a requirement for the development of their information security and privacy strategy.

To accomplish their mission, organizations in general, and particularly those required to be highly interoperable with their partners, have being adopting Enterprise Architecture (EA) frameworks. The main objective of EA is to align with the business strategy by providing a high-level definition of the technology and process structure of an organization. EA not only helps the organization visualize current and future business and technology needs, but it also plays a crucial role in the development and management of the organization’s information assets.

The aim of this work is to propose the inclusion of information security and privacy principles in an EA framework suited for interoperable organizations, in order that attained EA outcomes fulfill information security and privacy requirements by design. Hence, the EA framework would function as a security and privacy governance framework to address the management of the security perimeter. The method followed for deriving the enhanced EA framework will include three steps: (i) elicit the best current EA framework used by organizations with the paramount requirement of interoperability; (ii) elicit the current standard principles of information security and privacy; (iii) embed the principles of information security and privacy protection into the chosen EA framework, deriving an extended version of the framework considering now those principles.

The article is organized as follows: the next section surveys the literature for interoperable EA frameworks; Section "NATO Architecture Framework" presents the EA framework chosen given its relevant characteristics; Section "Information Security and Privacy" overviews the main information security and privacy principles and recommendations by international standards' organizations; Section "Extending NAF for Information Security and Privacy" describes how the principles of information security and privacy were implemented in the chosen EA framework; The last section offers some conclusions.

BACKGROUND

'Enterprise Architecture' is a formal representation of stakeholders' concerns in the context of the organization. EA brings together both business and technical aspects to emphasize their interdependence. This approach facilitates change by providing understanding of areas that need improvement. EA takes a comprehensive approach to managing problems within a system-of-interest by demonstrating the interaction between technology and business processes. The goal of EA is to streamline legacy processes and systems within the organization into a unified and change-responsive environment that aligns with the business strategy. EA is designed to aid in strategic planning, change, and analysis (such as gap, impact, and risk assessments) and the decision-making that occurs during these processes. Other benefits include determining necessary capabilities, connecting needs to system development and integration, ensuring interoperability and maintainability, and managing investments (NATO, 2018).

The tool used in EA creation, an EA framework, can be viewed as a method to handle complexity. John Zachman was the first to formalize an EA framework (Zachman, 1997). The Zachman EA model is an ontology of a structured set of essential components of a system for which explicit expressions are used for creating, operating, and changing the system. Zachman's original model was the basis to enable development of new frameworks of EA. Since then, many other EA frameworks have been proposed and used by different kinds of organizations (e. g. governmental, corporate, military).

The EA framework of Open Group Architecture (TOGAF) is nowadays the *de facto* standard for governmental and corporate organizations (OG, 2022b). The TOGAF ADM (Architecture Development Method) component of the framework has evolved over practical experience and consists of nine phases. The initial phase sets the vision, objectives, and scope, and prepares the resources for the main cycle of architecture development, which covers phases A through H. Although the phases are depicted as sequential, the activities within each phase often take place concurrently. The ADM is a repetitive process, both throughout the whole process and within each phase. The central aspect of requirements management is to collect, organize, and incorporate architecture requirements into each phase of the cycle. Phase A continues the work started in the preliminary phase by defining the vision, objectives, principles, and scope of the architecture. Phases B, C, and D gather information and populate the architecture model with business, information systems, and technology descriptions respectively. Phases E and F use the architecture to select and govern development projects. Phases G and H handle the long-term governance and change management of the architecture (Jørgensen et al., 2011).

The NATO Architecture Framework (NAF) takes its core structure of views and subviews from the US Department of Defense Architecture Framework (DoDAF) (DoD, 2010). In addition, it incorporates additional views from the UK Ministry of Defense Architecture Framework (MODAF) and is aligned with MODAF's metamodel (Jørgensen et al., 2011; MoD, 2021). NAF also prescribes a comprehensive methodology for EA deployment (NATO, 2018).

The NAF approach to physical systems engineering differs from TOGAF's focus on information systems. On the other hand, TOGAF's puts emphasis on enterprise-wide portfolio management while NAF focuses on acquisition projects and highlights systems' interoperability. These differences reveal the diverse nature of the organizations using each of the frameworks. In most corporate organizations, hardware is considered a utility, with most of the Information Technology (IT) complexity residing in application software, which is the primary focus of TOGAF. In contrast, safety and security organizations frequently utilize custom-made hardware and intricate communication systems, resulting in greater expenses, unpredictability, and complexity within the physical level of the IT architecture. That is why NAF places more emphasis on these latter aspects than TOGAF does (Jørgensen et al., 2011). Since NAF is the most well-suited EA framework for organizations requiring a high degree of interoperability, the next section summarizes the main characteristics of this framework.

NATO ARCHITECTURE FRAMEWORK

The NAF offers a standardized method for creating architecture artifacts. The framework includes: (i) a *methodology* for developing architectures and managing architecture projects; (ii) *viewpoints* to outline conventions for constructing, interpreting, and utilizing architecture views to communicate the EA to different stakeholders, (iii) a *meta-model* that aligns with NATO policy, and (iv) a *glossary*, references, and bibliography (NATO, 2018).

The NAF architectural approach supports various types of analyses, some of them requiring special tools to be performed, including: (i) static analyses - this type of analysis could include capability audit, interoperability analysis, or functional analysis. The analyses are often carried out using simple analysis tools such as database queries and comparisons; (ii) dynamic analyses - also called executable models, this type of analysis focuses on examining the temporal, spatial, or other performance aspects of a system through dynamic simulations. Dynamic analyses are useful in assessing the latency of time-sensitive targeting systems or performing traffic analyses on deployed tactical networks under different loading scenarios; (iii) experimentation analysis involves deploying live and simulated systems to differing degrees, with a high degree of control over the experiment variables. Experimentation can serve various purposes, from analyzing intervention options to validating new capabilities before they are fielded; (iv) trials - these are medium to large-scale exercises that involve fully functional systems and large numbers of personnel, usually conducted in an operational environment as realistically as possible. Trials are typically expensive and are usually only used for formal system acceptance or operational readiness assessment.

The objectives of the NAF framework can be summarized as: (i) arranging and displaying architecture in a way that is easy to understand by stakeholders; (ii) giving direction, rules, and descriptions for creating and showcasing architecture data; (iii) guaranteeing that there is a shared approach to understanding, comparing, and integrating architectures; (iv) acting as a facilitator for acquiring and deploying interoperable and economical capabilities, and; (v) aligning with architecture references created by other international standards organizations.

The NAF framework, however, does not explicitly address holistic organization-wide information security and privacy goals, although considering that organizations should follow a risk management approach to address those concerns. Hence, besides the above-mentioned objectives, NAF needs to include precise information security and privacy practices aligned with the common EA strategy. Thus, organizations should also focus on building a resilient approach, beyond protection, detection and prevention, and be ready to withstand against the cyber threats applying a relevant cyber resiliency approach and improving the way of dealing with impacts of cybersecurity risks. To make this possible NAF framework should consider embedding well proven practices such as the ones prescribed by international standards on information security and privacy, namely those specified in the ISO 27001 standard, to mitigate identified risks, by an information security management, and the ISO 27701 standard for deployment of a privacy information management.

INFORMATION SECURITY AND PRIVACY STANDARDS

Information security (InfoSec) consists of the implementation of a set of measures, methods, and tools designed to safeguard sensitive and confidential information from unauthorized access, damage, disruption, or destruction. This includes physical and environmental security, access control, and cybersecurity. ISO/IEC 27001 (ISO/IEC, 2022a) is the international standard that provides a code of practice for information security management, with a set of criteria covering various aspects of information security management systems, information technology, information security techniques, and information security requirements. ISO/IEC 27001 covers a wide range of areas, including risk management, security policies, access control, cryptography, physical security, and business continuity management. The main goal of ISO/IEC 27001 certification is to help organizations protect sensitive information, mitigate the risks of security breaches, and build stakeholders' trust.

Organizations that are ISO/IEC 27001 compliant reached a mature level of operations security. Compliance with ISO/IEC 27001, although not mandatory, can be required for applying to the certification in other security frameworks. As a result of achieving ISO/IEC 27001 certification organizations become trusted by their customers and partners for the security of their information assets. The ISO framework offers organizations, irrespective of their size, a consolidated guide for necessary security policies and processes to improve their security posture. The Information Security Management System (ISMS) implemented by organizations aims to manage information security risks using a set of cybersecurity controls. The primary objective of the ISMS is not to prevent data breaches but to restrict their impact on sensitive resources.

The ISO 27001 standard consists of two parts: (i) Eleven Clauses (0-10) - Clauses 0–3 serve as an introduction to the ISO/IEC 27001 standard, while Clauses 4–10 outline the minimum compliance expectations for certification; (ii) Annex A - Defines the guidelines for the 114 control objects that support ISO/IEC 27001 compliance. ISO/IEC 27002 (ISO/IEC, 2022b) describes how to implement the security controls mentioned in the Annex A of ISO/IEC 27001.

The field of information privacy deals with the appropriate management of data, encompassing aspects such as consent, notification, and adherence to regulatory requirements. Information privacy is a subset of data security, which aims to ensure that sensitive and Personally Identifiable Information (PII), held in computer systems, is kept protected from unauthorized access or misuse.

The objective of the ISO/IEC 27701 (ISO/IEC, 2019) standard is the protection of information privacy, which basically means that this standard is focused on information security and PII. ISO 27701 seeks the integration between the ISMS of ISO 27001, the best practices in ISO 27002, and the requirements of privacy regulations, to deliver a Privacy Information Management System (PIMS). By combining an ISO 27701-compliant PIMS with an ISMS through an integrated management system, the strict personal data protection expectations can be met. ISO 27701 is the needed tool to integrate privacy regulations (e.g., GDPR (EU, 2016), CCPA (DoJ, 2023), LGPD) with ISO 27001 prescribed information security management. Because ISO/IEC 27701 standard defines a management system, the base of a continual improvement model is necessary, and the best way to do this is to use the structure of ISO/IEC 27001, which has a continual improvement model and, furthermore, is related to information security.

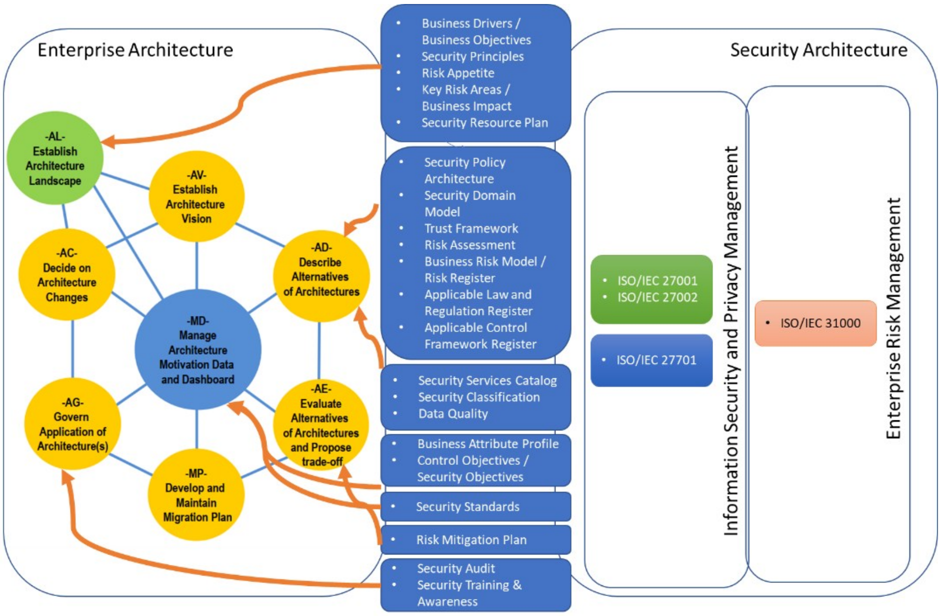
Hence, ISO/IEC 27701 has the 114 security controls of ISO/IEC 27001-Annex A and the guide of ISO/IEC 27002 to implement the security controls. ISO/IEC 27701 includes, additionally, specific security controls, exclusively related to PII, grouped into two categories, depending on the organization's role: (i) controller - the organization determines the means of processing personal data, regardless of whether they directly collect the data from data subjects; (ii) processor - the organization handles personal data on behalf of the controller.

Summarizing, the ISO/IEC 27701 standard provides a framework for managing privacy risks, protecting personal data, and demonstrating compliance with applicable privacy regulations. ISO/IEC 27701 also provides guidance on implementing privacy controls, conducting privacy impact assessments, and managing data breaches. Thus, ISO 27701 is intended to help organizations establish and maintain effective privacy management systems that align with the organization's information security objectives and overall strategic goals.

EXTENDING NAF FOR INFORMATION SECURITY AND PRIVACY

This section describes how security and privacy is integrated into NAF. The section also provides guidance on how to ensure information security and privacy for the EA outcomes. Figure 1 shows the relationship between Enterprise Architecture and a Security Architecture, highlighting the core security and risk concepts that are used in information security and privacy management, as well as in enterprise risk management. The concepts, borrowed from (OG, 2022a), are listed in the center column, and constitute an extension to the NAF framework. The concepts are also linked to the NAF methodology phases by stages to which they most contribute. The rest of the section explains the meaning of each concept, as follows:

- Business Drivers/Business Objectives: the purposes for which an organization exists, often internally generated or externally imposed, such through regulatory compliance. Information security is one of the many factors that affect the achievement of these objectives.



Enterprise Architecture
Security Architecture
-AL- Establish Architecture Landscape
-AV- Establish Architecture Vision
-AC- Decide on Architecture Changes
-AD- Describe Alternatives of Architectures
-MD- Manage Architecture Motivation Data and Dashboard
-AG- Govern Application of Architecture(s)
-AE- Evaluate Alternatives of Architectures and Propose trade-off
-MP- Develop and Maintain Migration Plan
Business Drivers / Business Objectives
Security Principles
Risk Appetite
Key Risk Areas / Business Impact
Security Resource Plan
Security Policy Architecture
Security Domain Model
Trust Framework
Risk Assessment
Business Risk Model / Risk Register
Applicable Law and Regulation Register
Applicable Control Framework Register
Security Services Catalog
Security Classification
Data Quality
Business Attribute Profile
Control Objectives / Security Objectives
Security Standards
Risk Mitigation Plan
Security Audit
Security Training & Awareness
ISO/IEC 27001
ISO/IEC 27002
ISO/IEC 27701
Information Security and Privacy Management
ISO/IEC 31000
Enterprise Risk Management

Figure 1: Information security and privacy in the NAF framework (based on: (OG, 2022a)).

- Security principles: provide valuable guidance for making business decisions in accordance with an organization's risk appetite. Their usage is similar to the usage of other architecture principles.
- Risk appetite: describes the organization's attitude towards risk and provides decision-making guidance on how much risk should be taken to achieve an expected outcome. It sets both the acceptable level of risk and the strategy for defining it. The strategy for mitigating risks above this level, such as transference or avoidance, is also defined.
- Key Risk Areas/Business Impact Analysis: tools that can be applied to all domains and architecture roadmaps to determine their fitness. A business impact analysis identifies potential damage that could result from inappropriate or insufficient information security in the business process. It identifies the impact relevant to the business process that should be avoided, rather than the likelihood of its occurrence, and produces a list of key risk areas within the architecture scope. This information is used in the risk assessment.
- Security Resource Plan: identifies the necessary security resources to deliver the security elements of the architecture, based on the scope of the Enterprise Architecture team's responsibility and the scope of any architecture project.
- Security Policy Architecture: is made up of a collection of security policies that define the organization's approach to security. It designates individuals who are responsible for security and risk management, and also outlines how different security aspects such as business continuity, information security, system security, and physical security are connected and prioritized.
- Security Domain Model: a way to group assets with similar security levels that fall under the authority of a single security policy. It helps to define areas of responsibility and establish relationships with external parties, and can be used to differentiate areas of different security or trust levels. The security policy authority is responsible for setting and enforcing the security policy within the domain. If the organization collaborates with other entities, the extent of security cooperation should be established at this stage, taking into account shared data objects or activities. The security implications and agreements of contractual federation arrangements should be evaluated, and joint architecture meetings may be necessary for members of the same security domain.
- Trust Framework: specifies the trust relationships between different entities in the architecture domain and the basis on which this trust is established. Trust relationships can be one-way, two-way, or non-existent. The responsibility for assessing trust rests with those who choose to enter into contracts and their legal advisors.
- Risk Assessment: refers to the process of identifying the risks relevant to an asset or objective. A qualitative risk assessment produces a list of significant risk scenarios with high-level prioritization (high-medium-low), while a quantitative approach aims to determine the numerical value of the risk. This is generally based on the likelihood of identified threats materializing and the potential impact of an incident.

- Business Risk Model/Risk Register: a product of a Risk Assessment, which determines the cost (both qualitative and quantitative) of asset loss/impact in failure cases. The business impact should align with the definitions in the Business Attribute Profile, which act as pseudo-assets. Security classification should be carried out at this stage based on the identified risks. The business risk model outlines the risk strategy of an organization, including the maximum risk the business is willing to accept, and the information owner decides what level of mitigation is appropriate for their information.
- Applicable Law and Regulation Register: stores the list of laws and regulations that apply to the Enterprise Architecture engagement according to the business function inventory. It is constantly updated in line with legal and regulatory changes, and it is essential to comply with the regulations.
- Applicable Control Framework Register: lists the appropriate control frameworks that meet the needs and handle the risks associated with the scope and context of the engagement. Control frameworks include specific security measures and requirements, such as ISO/IEC 2700x, ISO/IEC 27701, and others.
- Security Services Catalog: refers to a list of security-specific functionalities that are part of the entire architecture. Unlike control frameworks that only contain requirements, the Security Services Catalog provides security building blocks that help in achieving security goals. It is a reference framework for the security management domain, providing conceptual definitions of the services, and operational information on their implementation and usage.
- Security Classification: attach a label to an asset based on a classification scheme, which is usually defined and described in the corporate information security policy. The asset classification is based on one or more characteristics of the asset.
- Data Quality: plays a vital role in operational risk management. Several attributes contribute to data quality, such as accuracy, relevance, timeliness, currency, completeness, consistency, availability, and accessibility. To ensure data quality, an overview of datasets needs to be maintained, and ownership and responsibility assigned for data quality. The data owner authorizes people or processes trusted for certain activities on the data under specific circumstances. Sometimes, information systems may require changes to handle the data properly. Finally, each of the key attributes should be measured based on log and performance data.
- Business Attribute Profile: a method that uses a risk-based approach to convert business goals and drivers into requirements.
- Control Objectives/Security Objectives: desired levels of security for specific processes, individuals, activities, systems, or datasets. They are distinct from security requirements since they represent goals to achieve. The control objective may not precisely match the security requirement and is associated with business attributes.
- Security Standards: provide guidance on which security standards are suitable for a given situation. It is the responsibility of the business owner or analyst to decide if a particular security standard applies. If so,

it is incorporated into the architecture work through the Management of Architecture Motivation Data. These standards can specify security controls for different architecture domains such as Business, Data, Application, or Technology Architecture.

- Risk Mitigation Plan: outlines the actions that need to be taken to reduce or eliminate risks. The plan is developed based on the risk mitigation strategy, which could involve various measures such as increasing control, transferring risk to another party, changing the business activity to avoid the risk, postponing the risk, compensating for the risk, and so on. The risk mitigation plan provides a roadmap for managing the risks that have been identified.
- Security Audit: a review of the security of implemented processes, technical designs, developed code, and configurations. This review is done to ensure that they comply with the relevant policies and requirements. Security testing is also conducted, including functional security testing, performance testing, and penetration testing.
- Security Training and Awareness: Adequate training is necessary to ensure that security-relevant subsystems and components are deployed, configured, and operated correctly. All users and non-privileged operators of the system and/or its components must receive awareness training. This is essential for proper, continuous, and secure system performance.

CONCLUSION

In this work, we proposed to attain Enterprise Architecture outcomes for interoperable organizations that could fulfill, by design, information security and privacy requirements, which are relevant attributes in the interaction among and with systems, namely those in the areas of crises management, security, and defense, considering multiple perspectives, including the Human Factors. The first step of the process was the selection of an Enterprise Architecture framework for organizations with interoperability requirement. The chosen EA framework was the NAF. The next step of the process was collecting the principles of information security and privacy from ISO 27001 and ISO 27701 respectively. Finally, we embed those principles of information security and privacy protection into the NAF, deriving an extended version of the framework that considers those principles.

ACKNOWLEDGMENT

The authors would like to acknowledge the EU MEDEA Project and the Portuguese Navy for their support.

REFERENCES

Correia, A., Água, P. B. & Simões-Marques, M. (2021). Linked Open Data Supporting Semantic Integration and Collaboration in Disaster Management Cycle. *International Conference on Applied Human Factors and Ergonomics*, 19–27.

DoD. (2010). *DODAF - DOD Architecture Framework Version 2.02* (DOD Deputy Chief Information Officer (ed.)). US Department of Defense. https://tinyurl.com/yc7jauy5.

DoJ. (2023). *California Consumer Privacy Act (CCPA)*. State of California - Department of Justice - Office of the Attorney General. https://oag.ca.gov/privacy/ccpa.

EU. (2016). *General Data Protection Regulation*. Regulation (EU) 2016/679. https://bit.ly/3wNbcVr.

ISO/IEC. (2019). *27701:2019 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*. https://www.iso.org/standard/71670.html.

ISO/IEC. (2022a). *27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/82875.html.

ISO/IEC. (2022b). *27002:2022 - Information security, cybersecurity and privacy protection — Information security controls*. https://www.iso.org/standard/75652.html.

Jørgensen, H. D., Liland, T. & Skogvold, S. (2011). Aligning TOGAF and NAF - Experiences from the Norwegian armed forces. *Lecture Notes in Business Information Processing*, *92 LNBIP*, 131–146. https://doi.org/10.1007/978-3-642-24849-8_11.

MoD. (2021). *MOD Architecture Framework*. https://tinyurl.com/229upmuk.

NATO. (2018). *NAFv4 - NATO Architecture Framework, Version 4*. Architecture Capability Team. https://tinyurl.com/3322c5bs.

OG. (2022a). *Integrating Risk and Security within a TOGAF® Enterprise Architecture*. The Open Group. https://tinyurl.com/54cvppyf.

OG. (2022b). *The TOGAF® Standard, 10th Edition*. Open Group. https://publications.opengroup.org/standards/togaf/specifications/c220.

TISN. (2007). *Secure Your Information: Information Security Principles for Enterprise Architecture* (p. 13). Trusted Information Sharing Network for Critical Infrastructure Protection. https://tinyurl.com/v4m3vfw7.

Zachman, J. A. (1997). Enterprise Architecture: The Issue of the Century (unedited version 1996). *Database Programming and Design*, *10*(3), 44–53. https://www.aeablogs.org/eakd/files/EA_The_Issue_of_the_Century.pdf.