AI Governance: A Security and Privacy Organizational Standard Architecture (SPOSA)

Sergio Barezzani[1]

[1]Università degli Studi di Milano, Via Celoria 18, Milan, 20133, Italy

Abstract

Artificial Intelligence (AI) capabilities and ubiquitousness allow us to embrace unprecedented opportunities but also magnifie risks for organizations and individuals alike. Machine Learning plays a relevant role stressing out the importance of cybersecurity and data protection in a context where also the regulatory framework is evolving rapidly (e.g., the European Union AI Act, NIS2, CRA). To cope with such scenario, governance frameworks are fundamental. However, the actual value that such frameworks may deliver is tightly related not only to the governance framework per se, but also to the ability to bridge the gap between a theoretical AI Governance model, and day-by-day activities. Moreover, standardisation and simplification are relevant considerations to support smaller organizations in their AI journey. This paper puts forward the idea of a conceptual model that if properly developed might aim at helping organizations to navigate the complex and evolving scenario generated by the widespread adoption of AI, with a specific focus on cybersecurity and privacy as main concerns: the Security and Privacy Organizational Standard Architecture (SPOSA).

Keywords

Artificial Intelligence, AI Governance, ICT Governance, Cybersecurity, Data Protection

1. Introduction

Artificial Intelligence (AI) came a long way to become what it is today. Its name goes back to the 50s but it moved its first steps even earlier. However, the AI adoption went through a series of acceleration and slowdown cycles, with Machine Learning (ML) playing a fundamental role in AI ultimate take off. Learning from data provides an unprecedented flexibility in crafting models capable to solve, with super-human accuracy, problems whose solution may be elusive even for the most-skilled domain experts. Therefore, even if data have always played an important role in Information and Communication Technologies (ICTs), the advent of ML has turned the spotlight even more definitely. Indeed, data drive a learning algorithm in drawing the final model from a function class, it is therefore of paramount importance to ensure that appropriate quality standards are in place, that data are protected from unauthorized manipulations, and confidentiality is ensured. Indeed, data governance, data protection, and cybersecurity are essential prerequisites for the development of a trustworthy AI.

The impacts that AI may have on the daily life of individuals, business organizations, and countries are so profound and vast that the governance of such technology represents a priority for our society at large. The geopolitical and economic context is evolving as well, with cybersecurity front and center. As a result, the regulatory context is changing with initiatives taken to design strategies, processes, and to shape legal frameworks regarding AI, digital transformation, cybersecurity, and data protection. An example is provided by the European Union (EU) evolving regulatory framework that includes, among others, the AI Act [1, 2], NIS2 Directive [3], CRA [4], and GDPR [5, 6]. In such complex scenario, simplification becomes increasingly important. Recently, an effort to simplify the steps that an organization shall take to be compliant with the EU legal framework is being carried out, including a proposal amending the AI Act. The proposal considers several factors that could become challenges in applying in practice the provisions of the regulation including complexity and lack of tools especially for smaller organizations [7].

Joint National Conference on Cybersecurity (ITASEC & SERICS 2026), February 09-13, 2026, Cagliari, IT

sergio.barezzani@unimi.it (S. Barezzani)

https://orcid.org/0009-0008-6782-1627 (S. Barezzani)

0009-0008-6782-1627 (S. Barezzani)

Grouping frameworks, models, organizations, processes and tools that aim at this goal under the umbrella-term AI Governance [8] allows us to identify a strategic subject matter regarding the quest for trustworthy AI. Similarly to ICT Governance, AI Governance is a vast multidisciplinary field with technical roots (e.g., the management of the technology complexity, its integration in existing IT enterprise landscapes, and the IT processes and organization involved), a legal perspective (e.g., with respect to the compliance to applicable regulations such as the EU AI Act), a business process view (e.g., to craft an AI solution considering the specific business context), a focus on the alignment to ethical values, and much more. Moreover, considering the primary role that Machine Learning plays nowadays, AI Governance is tightly related to data governance, protection, and cybersecurity. The complexity of the topic, the heterogeneity of contributions, and the increasing impact that AI has on our society make AI Governance an interesting research area where several efforts have been carried out in the development of frameworks [9, 10, 11].

However, the complexity entailed by AI Governance is such that, the availability of a governance framework by itself might not ensure a seamless transition to a trustworthy AI. A significant gap might form among a unifying overall governance framework and the myriad of factors that support its implementation. It is therefore important to leverage tools that allow us to possibly prevent, detect and manage the divergence between an AI governance model and the underlying ICT processes.

This paper outlines the Security and Privacy Organizational Standard Architecture (SPOSA), a model that has the goal to help organizations that are reviewing their ICT Governance practices to cope with the challenges that AI poses.

After introducing the model, rather than an exhaustive description of SPOSA, the focus of this paper is highlighting the role that such model could play in the current context where the resiliency of the cyberspace is a major concern (e.g., EU NIS2 directive). The paper focus is on the idea that releasing information implies a risk, and that such risk shall be approached with an holistic view. The approach adopted should be coherent to the risk management procedures that an organization has shaped, accordingly to the applicable regulations and standards. Therefore, SPOSA proposed approach is to leverage information from risk management and ICT asset management to analyze information requests and outline a possible course of action. In doing so, SPOSA strives to provide a contribution in bridging the gap between what an organization risk management framework establishes in terms of acceptable risks built upon the outcomes of AI Governance, and the day-by-day disclosing of information that an organization decides to perform. The rest of the paper is the following:

- Section 2 provides background and related work information.
- Section 3 describes the design criteria adopted for SPOSA.
- Section 4 provides a description of SPOSA model organization.
- Section 5 is focused on SPOSA Information and Risk Management.
- Section 6 reports the conclusions and future work opportunities.

2. Background and Related Work

The advancements in AI have driven to its broad adoption in countless scenarios and also to a review of governance frameworks and standards in order to cope with unprecedented challenges. AI Governance is a broad and evolving field where several initiatives have been carried out globally that brought to the definition of the OECD AI principles [12], the Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment [13], the NIST Artificial Intelligence Risk Management Framework [14], the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems [15], and more [10].

However, it is worth noticing that AI is causing a disruption from different points of view that might further increase the gap between on the one hand requirements that become more complex and on the other hand the day-to-day operations (Figure 1). An interesting consideration that is emerging [8] is the importance of a tight integration of AI Governance with ICT Governance and data governance in order to move from theoretical frameworks to practice. Indeed, SPOSA focuses on such aspect, paying attention to the relationship of AI Governance and ICT governance, data governance, data protection,

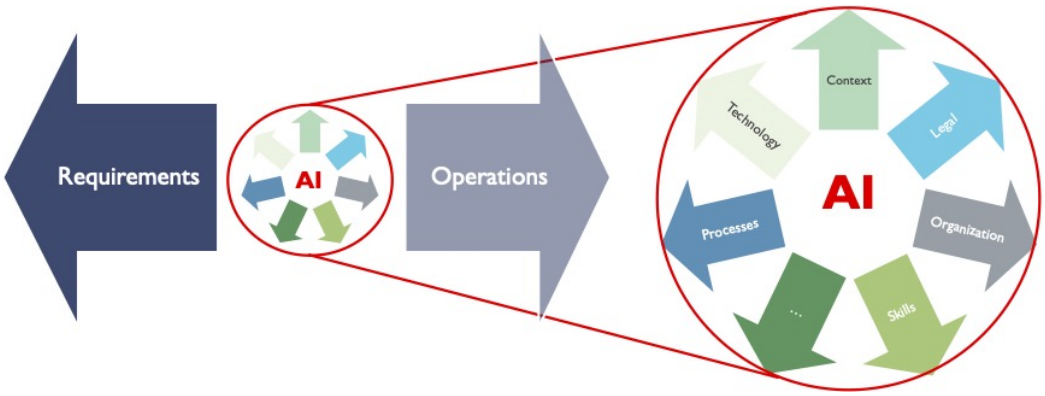

Figure 1: The Risk of a Widening Gap

and cybersecurity. Another crucial topic to be considered in positioning SPOSA is Risk Management. The literature regarding Risk Management applied to information systems is vast with several works focusing on the methodology to be adopted or reporting the results of case studies (e.g., [16, 17]), with international bodies shaping global standards [18]) only to mention a few topics. Other research works focus on information retrieval and the impact of AI (e.g., [19]). SPOSA has a different focus, it tries to facilitate the control of the gap between ICT governance and day-to-day operations relying on existing AI Governance and Risk Management frameworks and linking the assessed risks to information request handling. Therefore, SPOSA is more tightly related to the scope identified by the publication from the National Institute of Standards and Technology (NIST) about the integration of Cybersecurity and Enterprise Risk Management [14]. It is also worth mentioning that the design criteria proposed for SPOSA are coherent to the approach and guidelines defined by the author in a previous work that presented the PII Trusted Exchange (PTE) framework [20]. PTE has been designed with the primary target to protect personal data in AI contexts with the underlying idea that cybersecurity and data protection would contribute to make AI sustainable in the long run. Even if SPOSA and PTE have different perspectives and structures, they both aim at improving security, privacy and the resilience of the cyberspace and share similar criteria, guidelines and a layered model layout.

3. SPOSA Design Criteria

Our modern societies may benefit in the long from the opportunities offered by innovative technologies if the risks entailed by managing information are properly identified, assessed and managed. The number of stakeholders involved in the processes that support our daily activities can be so high that an issue experienced by a single organization may have broad impacts. An important example of the growing attention to such aspects is represented by NIS2, an EU directive that is extending the number of organization considered important or even essential for the EU ecosystem that shall adopt adequate procedures to manage properly their cyber resilience. Moreover, AI is bringing a change of paradigm in the way several problems are addressed, offering unprecedented opportunities but also emphasizing the risks to be managed. Such context has driven the definition of SPOSA design criteria. SPOSA puts forward the idea of a model combining different views, complementary to the mentioned AI Governance and Risk Management frameworks. SPOSA goal is to support the integration of AI Governance processes with the overall organizational governance, according to a non-invasive and straightforward approach, according to the following design criteria:

- the model shall be unique but capable of combining different point of views such as the stakeholders, their processes, and the underlying technology,
- the design of the model shall minimize the amount of changes required to keep it up to date,
- the target organization is at the center, with specific reference to its digital information assets,

- the model shall strive to create a level playing field among the stakeholders,
- trust among the stakeholders shall be favoured,
- minimize risks but at the same time maximize stakeholder's outcome,
- compliance shall be a by-product of daily operations and shall favour innovation,
- simplification,
- complementarity,
- congruity,
- exercisability.

While most of the design criteria outlined above are self-explanatory, it might be worth providing a few more insights about a few of them.

About simplification e complementarity: SPOSA shall attempt to provide a simple and straightforward approach to link the outputs of AI Governance and Risk Management to daily operations (e.g., information request handling). Such approach should be enforced considering the needs of a growing number of small organizations that are trying to unleash the benefits of AI. Besides, it is resonates with the relevance given to risk management by the existing regulations and standards. Another consideration regards factoring in an information request handling also the risks related to the threats that the underlying ICT assets might be exposed to. This consideration aligns with the growing importance given to the cybersecurity resilience of ICT systems as further stressed out in the EU by Directive 2022/2555 (NIS2) and Cyber Resilience Act (CRA).

About exercisability: a model that aims at supporting information exchange shall foresee proper protection features but shall not prevent or excessively slowdown data circulation. Moreover, the pace of technology innovation accelerates requiring a model that is capable to adapt to an evolving ecosystem. Therefore, such model shall be designed with availability as a main constraint and also taking into account the extensibility to new scenarios while preserving the overall model structure.

About congruity: the information inferred from data might have a value, might have an owner. Exchanging data, process and analyze them might extract value from such information but may also imply a risk. It is safe to assume that the sustainability of a model where stakeholders exchange valuable assets shall include considerations related to the congruity of the transactions taking place. Such assumption leads to several consequences in the model design summarized as follows. The model shall foresee a quantitative approach to measure the value exchanged/risk while sharing information, and this might in turn lead to view data as digital assets relying on scarcity. Moreover, it is also important to ensure that the exchange of information takes place as intended by the parties, therefore to have means to track such exchanges. Besides, information exchange is not necessarily a simple one-to-one atomic interaction, it might rather be broken in multiple steps not even synchronous, involving multiple stakeholders.

To comply to such design criteria, and to support organizations in managing the risks related to information management, the following guidelines have been adopted:

- the organization shall have control of the risks entailed by managing data,
- requests to access data shall be evaluated to ensure they are legit and comply with a holistic evaluation of the risks implied,
- data exchange shall not only be allowed, it should be favoured, provided it complies to the applicable regulation, the organization policies, and risk posture,
- the resulting model shall be scalable and open.

To cope with the identified design criteria and guidelines, SPOSA has been organized in layers as shown in Figure 2. Moving from top to bottom, each deeper layer does not only provide a more detailed view of the layer on top, but it also provides a different perspective: the top most layer focuses on mapping the stakeholders of the information exchange, moving down, the second layer focuses on the capabilities each stakeholder has to master in order to interact properly with the rest of the ecosystem, the third layer outlines the processes required by each capability, and the fourth layer identifies the

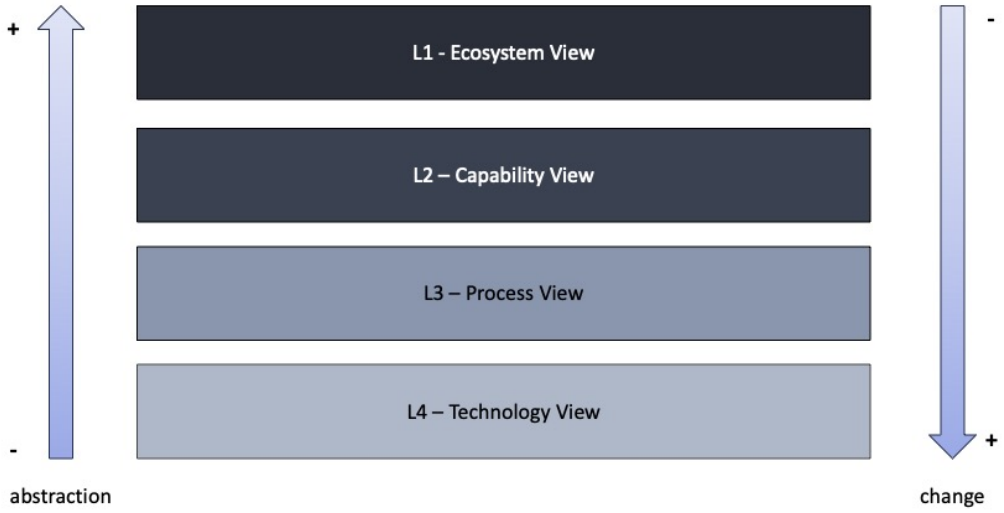

Figure 2: SPOSA Layered Model

technological solutions that might support each process area. Such layered structure has several advantages. It allows us to accommodate different point of views (horizontal stratification) focusing first on concepts such as key stakeholders identification with respect to their roles, relationships and capabilities they should rely on. The lower layers become more specific regarding the processes that shall be managed, and the underlying technology. The proposed structure also allows us to connect such different perspectives maintaining the coherence of a unique model (vertical view) trying as applicable to map each element on a layer to the elements supporting it in the lower layers. Moreover, SPOSA model organization also strives to offer an innovation-proof design that limits the changes required to the model when an innovative solution enters the ecosystem. Indeed, the layers are organized so that the top layers shall be relatively more stable (e.g., the stakeholders), while moving down to the lower layers the probability of significant changes might increase. The lower layer (technology) is the most likely to be updated: in case a technical tool adopted today to support a given process is replaced by an innovative solution, all other elements being equal, the impact on the model would be probably confined to layer 4. This consideration does not imply that more impactful model revisions might not be necessary but it means that such broader revisions might be less frequent.

4. SPOSA Model Description

An introduction to each layer of SPOSA is provided in this section moving from the top level down. The focus of this paper is on the interplay between risk management and information request management, that is an important aspect of the model considering the current focus on the resiliency of the cyberspace (e.g., NIS2, CRA). Therefore, although a description of SPOSA as a whole is provided, it is not exhaustive. In this section and the following, specific SPOSA components are presented, coherently with the identified scope.

4.1. SPOSA Layer 1

SPOSA topmost layer focuses on mapping the key stakeholders that interact in the context analyzed. According to the design criteria, the organization occupies the center of the model. The stakeholders

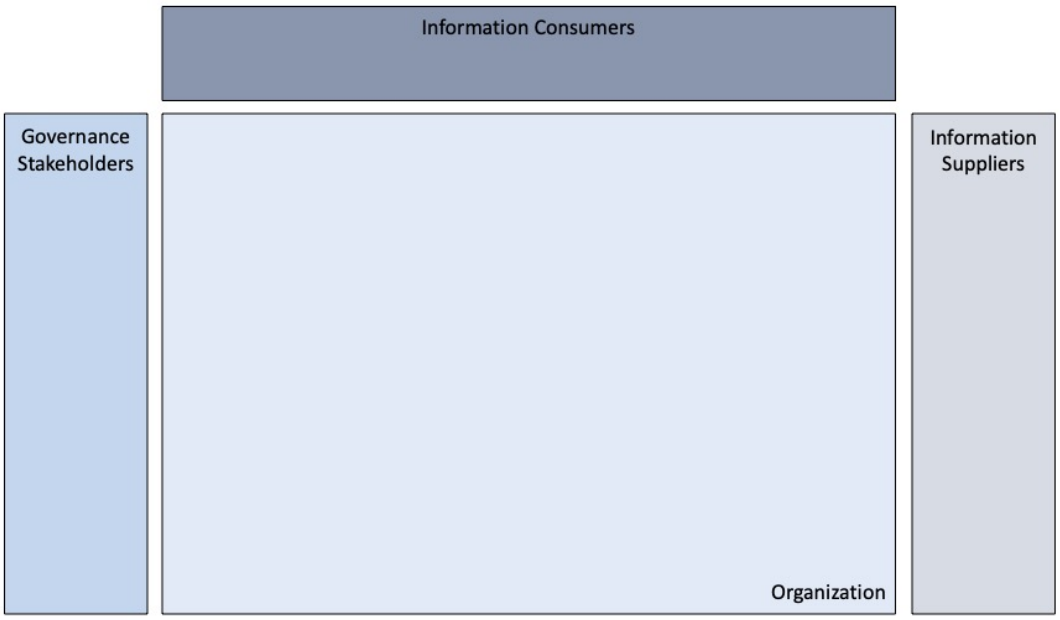

Figure 3: SPOSA layer 1 - Ecosystem View

willing to access the organization's information assets (requestors) are mapped at the top. Requestors might be organized according to different criteria, as an example in internal and external, and then further split them as needed into more specific groups that are homogeneous in terms of information requests. On the left of layer 1 the stakeholders that focus on governance and compliance to applicable regulations or standards are grouped together. The regulations and standards applicable may vary based on the organization (e.g., a private vs. a public organization, the industry it operates in), in this paper the focus is on the EU NIS2, AI Act and GDPR. On the right of the layer is mapped the ecosystem of actors that an organization might rely on to manage information. With a growing complexity of the IT system landscapes, the number of actors that contribute to information management increases including as an example, cloud service providers, cybersecurity service providers, software vendors, and others. The advent of AI further extends such network and the complexity of the relationships. As an example, in the the case of a Machine Learning system, the stakeholders should include also data providers on top of others. The potentially high number of operators involved, the impact that they could have on information management, and the complexity of their relationships suggest to consider such actors as part of an information management supply chain with a clearly identified role in the layer 1 of SPOSA. Figure 3 shows SPOSA layer 1 that maps the main stakeholders considered.

4.2. SPOSA Layer 2

SPOSA layer 2 is focused on the capabilities that stakeholders shall master to manage information requests according to the model. The main focus of layer 2 is on the organization considered. Information requestors at the top submit an authentication request to the service provided by the organization. Information requestors prepare and submit a specific request for information. The request shall then be handled to determine if it is properly shaped, if it is authorized, if fulfilling the request is consistent with the risks the organization has decided to accept. Indeed, this is the main aspect of SPOSA considered in this paper: linking the management of an information request to an evaluation of the entailed risk, that is in turn connected to the risk management framework an organization has established and to AI Governance if AI systems are involved. Risk evaluation shall include different aspects, as an example, if fulfilling the information request matches the risk posture that the organization has defined with respect to the information to be retrieved (e.g., personal data, organization information), possibly adjusted by a

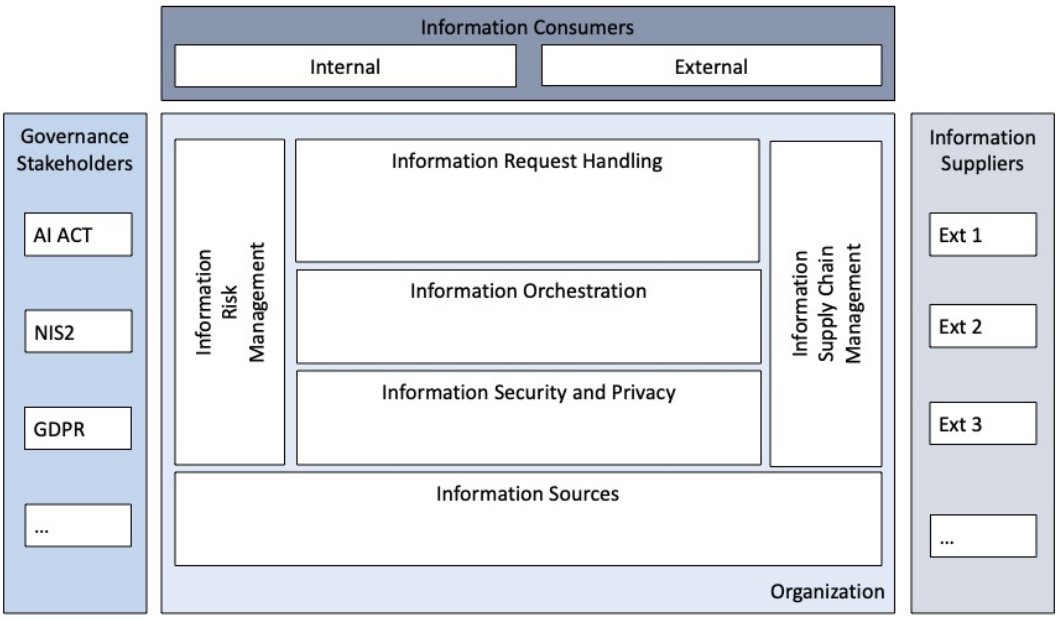

Figure 4: SPOSA layer 2 - Capability View

factor considering the risk represented by the specific information requestor (e.g., in an aggregated form such as internal vs. external user, or an internal user of an HR department accessing personnel information with respect to an employee of another department, or related to the specific requestor). Moreover, organizations should also consider the cybersecurity threats related to each information request (e.g., NIS2) that become another aspect to factor in. These considerations should then be adjusted with respect to the overall risk profile of the organization. The output of the request handling step could be to drop the request altogether or else to enrich the request with metadata reporting the output of the risk assessment and pass it to the following step. Information requests may be specific to a record in a table or rather might require to orchestrate contributions from several sources that are internal or external to the organization. Therefore, information orchestration is identified to implement the required service composition. The orchestration layer may rely on internal information sources as well as on the supply chain of external partners highlighted in layer 1. Figure 4 shows SPOSA layer 2 that maps the main capabilities considered.

4.3. SPOSA Layer 3

Moving down one more layer, the focus switches to processes. The Information Request Handling capability is managed by means of an authorization evaluation process that focuses on preventing any unauthorized request to be fulfilled but also to enrich the request metadata. Requests that are not authorized are logged with the purpose of contributing to event monitoring and threat analysis. The authorized requests are further processed to evaluate the request with respect to several considerations including:

- the risk posture the organization has defined,
- the potential threats that might be associated to the requests,
- any policy applied to requests submitted by a given requestor.

The outcome of the process is an execution plan associated to the query that is passed to the orchestrator. The orchestrator interprets and executes the request plan components that are split mainly in:

- the actual information fetching step,

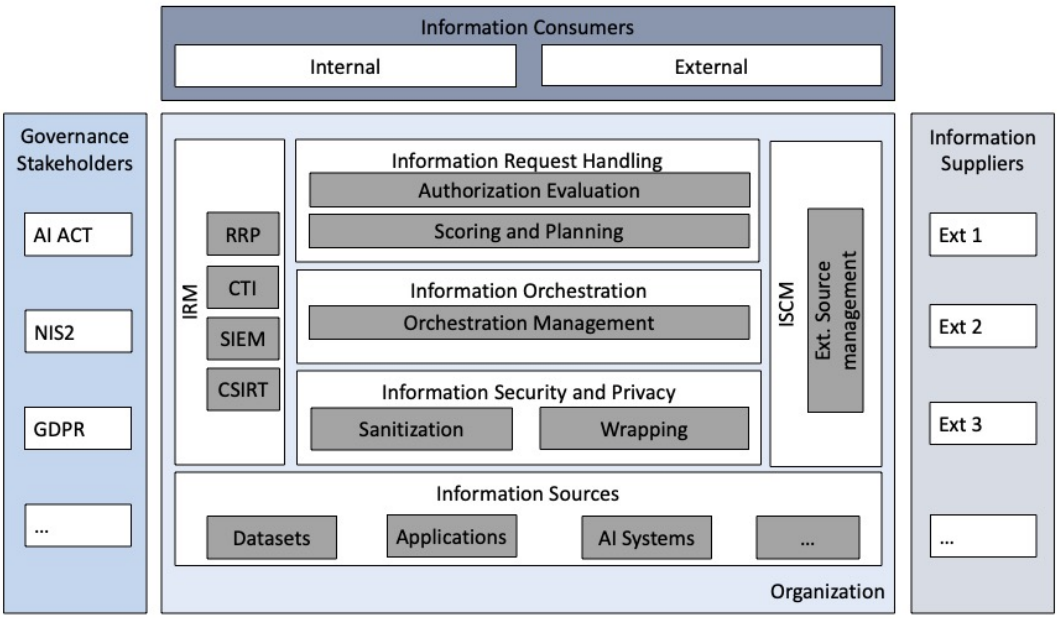

Figure 5: SPOSA layer 3 - Process View

- the enforcement of any data protection technique defined in the execution plan.

Information security and privacy includes the processes (e.g., sanitization or wrapping) aimed at protecting the information retrieved from the underlying information sources that could span from AI systems, to datasets storing raw data or aggregated information as well a other sources. Such information sources could be managed internally by the organization, or could be provided by third-parties. Figure 5 shows SPOSA layer 3 that maps the main processes relevant for the identified scenario.

4.4. SPOSA Layer 4

SPOSA fourth layer maps the technical tools leveraged by an organization to implement the processes identified in layer 3. As an example, in the context of Information security and privacy the organization should be able to access a library of techniques (e.g., sanitization or wrapping) that are selected according to the metadata associated to the information request. Such techniques may include Name Entity Recognition, k-anonymity, l-diversity, t-closeness, differential privacy or other techniques [21]. Metadata would also be used to select the adequate technique parameter values (e.g., proper value k for k-anonymity or l for l-diversity). The choice of the proper technique to be applied shall also take into account the data sources considered and the processing task. As an example, an organization may choose k-anonymity to protect personal data stored in a dataset while fulfilling a request of releasing such information. If the request is to train an ML model over such dataset, the organization might choose an anonymization technique that limits the impacts on the data utility for training [22].

4.5. The Cross-Layer View

The elements to be mapped in SPOSA should be identified leveraging the outcomes of the implementation of the relevant governance frameworks (including AI Governance and Risk Management, as applicable). Moreover, the relevant information regarding each element should be recorded as element attributes. Once the elements belonging to each layer have been mapped, the relationships among each element of the topmost layer (ecosystem view) and the elements representing the capabilities of the corresponding stakeholder are identified and linked together. The same process is repeated for the elements of layers

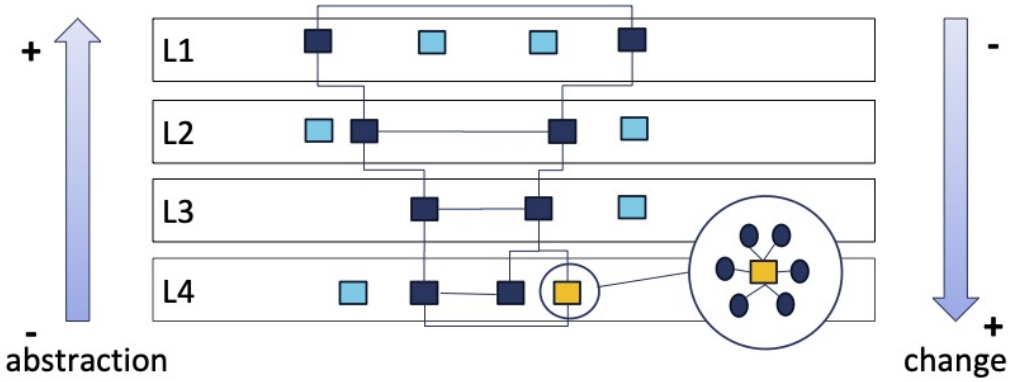

Figure 6: SPOSA - Cross-Layer View

2 and 3. Once the mapping of such information is completed, an interesting perspective that SPOSA offers is to view the interaction among two elements of the same layer as the interaction of the linked elements of the layers below. Therefore, a chain of elements that contribute to the use case considered is established. Since each element of such chain has its own attributes, the identified chain establishes a relationship among the information mapped in the element attributes and the considered use case (Figure 6). As an example, consider the use case of an organization managing an AI system among its information sources. The AI system is mapped on layer 4. The result of the risk assessment on the AI system is mapped as an element attribute. Any information request that relies on data gathered from such AI system is mapped by means of SPOSA to a chain of elements that establishes a relationship among the request and the attributes of the AI system, including the result of the risk assessment.

5. SPOSA Information and Risk Management

Information Risk Management (IRM) represents a core component of SPOSA and thus deserves a specific focus. IRM is introduced in the model to stress the importance of handling requests coherently to the Risk Management procedures enforced by the organization. The scoring of an information request takes place considering the evaluation of the risk associated to it. The organization shall define its risk posture coherently to its governance policies. Such posture may have a high level definition and then more specific details regarding progressively more detailed scopes, as an example down to the policy level about categories of data (e.g., personal data). The details concerning the risk posture are managed in the Risk Resource Planning (RRP). Any organization might have different criteria, therefore the following illustrates one of many possible approaches to the evaluation of the risk related to an information request:

- the organization posture on risk shall be factored in and it might be derived from the global organization posture with respect to risk management defining a bias in the administration of information requests in a range from restrictive to open,
- the requestor risk profile should be considered, possibly as a score assigned to each requestor representing an assessment of the risks entailed in disclosing information to such specific party,
- each specific request has its own risk entailed that is bound to the request semantics,
- the presence of vulnerabilities that might be exploited by the request is a potential source of risk affecting the organization resilience,
- if an AI system is involved, then the the risk related to such system (assessed according to the applicable framework) shall be considered.

A request should be evaluated in the perspective of the potential cybersecurity threats. There could be multiple sources to lookup for vulnerabilities. In 2025, ENISA has established the European Union

Vulnerability Database (EUVD) according to Directive (EU) 2022/2555 (NIS2) [23]. The EUVD plays an important role in aggregating, enriching and distributing vulnerabilities information. EUVD collects information from public sources (e.g., CVE), but also from the network of CSIRTs (Computer Security Incident Report Teams). The use of machine-readable formats such as the OASIS Common Security Advisory Framework (CSAF) allows us to further simplify the automated distribution of vulnerability advisories. The organization shall also rely on the internal sources of information such as its own CSIRT, CTI, and SIEM as applicable.

Request scoring is part of the broader request handling that shall take into account several topics including:

- identify the applicable policies,
- check if the access request matches the criteria stated in the procedure,
- actual scoring,
- check the security and privacy measures to be applied and the related parameters.

According to the analysis performed, the request execution plan is composed and submitted to orchestration. The actual scoring plays a crucial role and therefore a specific focus is dedicated to it.

5.1. SPOSA Scoring Function

The request scoring is evaluated by means of a function f of the applicable risks:

$$req\_score = f(r_0, r_1, r_2, r_3, r_4),$$

where a possible breakdown of risk factors (to be tailored to an organization needs) is:

- $r0$: represents the risk bias associated to the organization risk posture,
- $r1$: represents the requestor risk profile,
- $r2$: represents the specific request semantics,
- $r3$: represents the risk implied by the presence of vulnerabilities that might be exploited by the request,
- $r4$: represents any other applicable risk.

The risk factors r_i summarize the evaluation of the risks associated to each specific risk that might be relevant in fulfilling an information request. To estimate the risk factors an organization shall rely on the risk management process it already has in place, integrating the information that might be missing. The risk factor values shall be normalized.

The choice of the scoring function shall be tuned to the organization needs. An organization that is looking for a simplified approach to start its journey towards more sophisticated models, might choose a simple version of f such as the weighted sum of the risk factors plus an overall adjustment.

$$req\_score = r_0 + \sum_{i=1}^{4} w_i * r_i,$$

with the organization posture acting as a bias, and the other risk factors multiplied by a vector of weights. Choosing a linear function such as the one above might help an organization to focus on steps that are critical in an initial phase such as:

- identify a catalog of the most relevant risk factors r_i,
- choose an approach to the definition of the risk factors (e.g., direct assessment, by means of a proxy),
- formalize a quantitative definition of the risk factors,
- verify the feasibility of measuring the risk factors for the scope considered,
- focus on the organization specific weight vector.

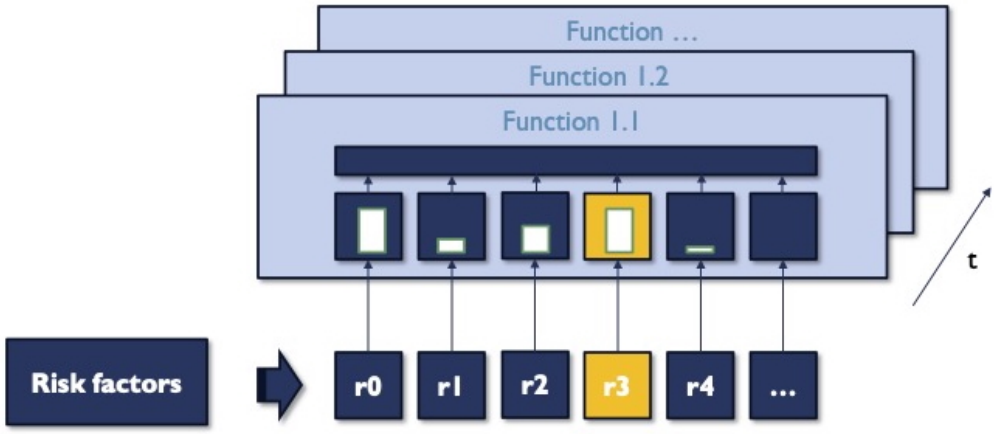

Figure 7: Risk Scoring

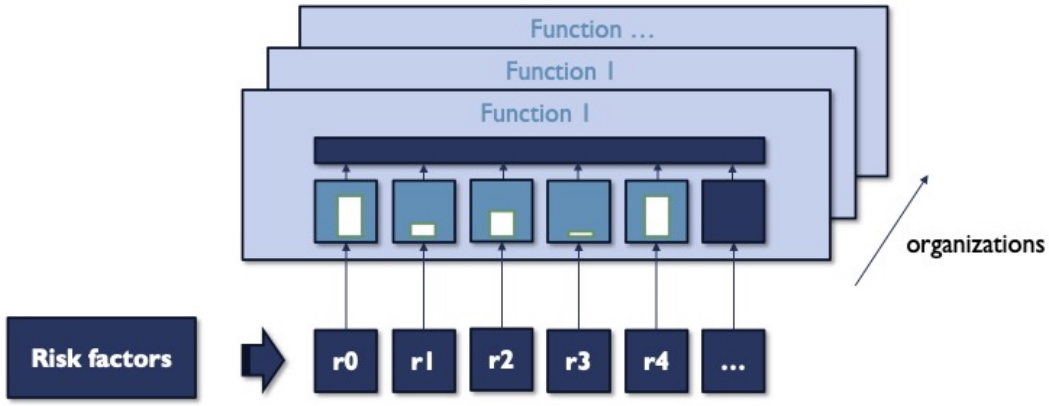

Figure 8: Risk Factors Analysis

On the other hand, an organization that has a more consolidated experience may choose a more complicated function in order to model more properly the relationship among the identified risk factors and the desired information request handling outcome. Organizations have also the opportunity to choose different approaches to the definition of the scoring function f: one approach could be to define a scoring function and then test the False Positives and False Negatives obtained, tuning the weights accordingly. Another approach could be to organize a dataset reporting risk factors and information requests handling outcomes and then learn the scoring function f by means of an ML model. Such approach might not only allow to draw the scoring function from a more complex class of functions, but also to gain an higher flexibility in adapting it over time.

5.2. Risk Factors and Weight Vector

As represented in Figure 7 the risk factor $r3$ play an important role in the overall request scoring. It could be viewed as a composition of the risk factors that are specific to the systems contributing to the fulfilment of an information request. If any of such systems is an AI model, the evaluating the risk factor $r3$ should be evaluated leveraging the organization Risk Management and AI Governance frameworks.

Assuming an organization has defined a proper set of risk factors, the weight vector represents the relevance of each risk, thus providing an interesting summary of the organization risk attitude that could be compared with the organization global risk profile. Such information may be monitored to control how it evolves with respect to external events (e.g., the identification of a new vulnerability) or internal events (e.g., the release of a new AI system). Indeed, the weight vector shall evolve over time to reflect changes in the relevance of the risk factors, as well as the evaluation of the risk factors. As an example, the identification of a vulnerability published on the EUVD that impacts a system that is present in the layer 4 of the SPOSA model of a given organization should suggest to update the risk factor and possibly the corresponding weight. Another comment regards $r4$ that could be viewed as a way to consider the level of uncertainty in evaluating risk factors. Its value, compared to the other risk factors, represents an assessment of the level of uncertainty in the risk evaluation. Therefore, an organization should carefully monitor $r4$ and perform risk assessment activities trying to reduce its value over time. Besides, similar organizations (e.g., organization operating in the same industry and/or same geographical area) might find useful to contribute to the definition of a catalog of risk factors tuned to the specific needs of organizations with similar characteristics (Figure 8). The catalog might then lead to the definition of a standard that similar organizations might be willing to compare to.

5.3. SPOSA Planner and Orchestrator

The request scoring contributes to the evaluation of the risk related to a specific instance of a request. Once it is completed, the planning phase has the goal to consider the specific request in the broader perspective of the overall risk assessed in delivering the information. Such assessment should be compared with the budget that the organization has defined for a given requestor. The underlying idea is to consider a budget of acceptable risk. An organization might decide that a group of users (e.g., internal employees) are not bound to any limitation in terms of information they receive from the organization, while other users might be subject to a limitation. The planner takes into account the assessed request information and compare it with the limits the organization has set, possibly considering a given observation period. Such limit might be set during a trial period or learned. The orchestrator takes care of composing the services required to fulfil the request.

6. Conclusion and Future Work

The evolving scenario where public and private organizations operate nowadays suggests to carefully review ICT Governance frameworks with a specific focus on the cybersecurity and privacy challenges emphasized by the widespread adoption of AI and by cyberspace resilience concerns. Moreover, when emerging and disruptive technologies go mainstream, the governance frameworks are reviewed, but a gap among governance models and day-to-day ICT operations may increase and thus shall be assessed and controlled as necessary. Besides, standardisation and simplification are relevant considerations to support smaller organizations in their AI journey. This paper puts forward the idea of the Security and Privacy Organizational Standard Architecture (SPOSA), a conceptual model that if properly developed might aim at helping organizations to manage such gap. SPOSA is a model combining different views, complementary to governance frameworks, designed to support organizations building upon the information provided by the enforcement of AI governance and Risk Management frameworks. Future work on SPOSA should focus on the one hand in detailing SPOSA elements on the different layers, their interactions, and drill-down on the scoring function, on the other to choose a case study to refine the model, balancing between specificity and generality.

Acknowledgments

This work was supported in part by project SERICS (PE00000014) under the NRRP MUR program funded by the EU - NGEU. Views and opinions expressed are however those of the author only and do not

necessarily reflect those of the European Union or the Italian MUR. Neither the European Union nor the Italian MUR can be held responsible for them.

Declaration on Generative AI

The author has not employed any Generative AI tools.

References

[1] European Parliament and Council, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 june 2024 laying down harmonised rules on artificial intelligence and amending regulations (EC) no 300/2008, (EU) no 167/2013, (EU) no 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (text with EEA relevance), [online], 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689.

[2] S. Barezzani, Artificial Intelligence Act (AI Act) and the GDPR, in: S. Jajodia, P. Samarati, M. Yung (Eds.), Encyclopedia of Cryptography, Security and Privacy, Springer Nature Switzerland, Cham, 2025, pp. 102–107. doi:10.1007/978-3-030-71522-9_1820.

[3] European Parliament and Council, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 december 2022 on measures for a high common level of cybersecurity across the union, amending regulation (EU) no 910/2014 and directive (EU) 2018/1972, and repealing directive (EU) 2016/1148 (NIS 2 Directive) (text with EEA relevance), [online], 2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555.

[4] European Parliament and Council, Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 october 2024 on horizontal cybersecurity requirements for products with digital elements and amending regulations (EU) no 168/2013 and (EU) no 2019/1020 and directive (EU) 2020/1828 (Cyber Resilience Act) (text with EEA relevance), [online], 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847.

[5] European Parliament and Council, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation) (text with EEA relevance), [online], 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679.

[6] S. Barezzani, General Data Protection Regulation (GDPR), in: S. Jajodia, P. Samarati, M. Yung (Eds.), Encyclopedia of Cryptography, Security and Privacy, Springer Nature Switzerland, Cham, 2025, pp. 997–1002. doi:10.1007/978-3-030-71522-9_1811.

[7] European Parliament and Council, Proposal for a regulation of the European Parliament and of the Council amending regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), [online], 2025. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0836.

[8] N. Malter, EU Commission Futurium Apply AI Alliance Forum: Implementing AI governance: from framework to practice, [online], 2023. URL: https://futurium.ec.europa.eu/en/european-ai-alliance/community-content/implementing-ai-governance-framework-practice.

[9] M. Mäntymäki, M. Minkkinen, T. Birkstedt, M. Viljanen, Defining organizational AI governance, AI and Ethics 2 (2022) 603–609. doi:10.1007/s43681-022-00143-x.

[10] A. Batool, D. Zowghi, M. Bano, AI governance: a systematic literature review, AI and Ethics 5 (2025) 3265–3279. doi:10.1007/s43681-024-00653-w.

[11] L. Floridi, J. Cowls, M. Beltrametti, R. Chatila, P. Chazerand, V. Dignum, C. Luetge, R. Madelin, U. Pagallo, F. Rossi, B. Schafer, P. Valcke, E. Vayena, AI4People—an ethical framework for a good AI society: Opportunities, risks, principles, and recommendations, Minds and Machines 28 (2018) 689–707. doi:10.1007/s11023-018-9482-5.

[12] Organization for Economic Co-operation and Development (OECD), OECD AI principles, [online], 2019. URL: https://www.oecd.org/en/topics/ai-principles.html.

[13] European Commission, Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment, [online], 2020. URL: https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment.

[14] National Institute of Standards and Technology (NIST), Integrating cybersecurity and enterprise risk management (ERM), [online], 2025. URL: https://csrc.nist.gov/pubs/ir/8286/r1/final.

[15] IEEE, IEEE GET program for AI ethics and governance standards, [online], 2025. URL: https://ieeexplore.ieee.org/browse/standards/get-program/page/series?id=93.

[16] J. Oliveira, M. d. C. Ribeiro, Risk Management, Springer International Publishing, Cham, 2023, pp. 2818–2822. doi:10.1007/978-3-031-25984-5_574.

[17] H. I. Kure, S. Islam, H. Mouratidis, An integrated cyber security risk management framework and risk predication for the critical infrastructure protection, Neural Computing and Applications (2022). doi:10.1007/s00521-022-06959-2.

[18] ISO, ISO 31000:2018. Risk Management, [online], 2018. URL: https://www.iso.org/standard/65694.html.

[19] K. A. Hambarde, H. Proença, Information retrieval: Recent advances and beyond, IEEE Access 11 (2023) 76581–76604. doi:10.1109/ACCESS.2023.3295776.

[20] S. Barezzani, Dalle certificazioni verdi COVID-19 all'Intelligenza Artificiale: la protezione dei dati personali tra resilienza e innovazione sostenibile, Diritto Politecnico 1 (2021). URL: https://www.dirittopolitecnico.it/condividiArticolo/19/.

[21] S. De Capitani di Vimercati, S. Foresti, G. Livraga, P. Samarati, Data privacy: Definitions and techniques, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 20 (2012) 793–817. doi:10.1142/S0218488512400247.

[22] S. Barezzani, S. De Capitani di Vimercati, S. Foresti, V. Ghirimoldi, P. Samarati, TA_DA: Target-Aware Data Anonymization, IEEE Transactions on Privacy 2 (2025) 15–26. doi:10.1109/TP.2025.3527461.

[23] ENISA, European Union Vulnerability Database (EUVD), [online], 2025. URL: https://euvd.enisa.europa.eu/homepage.