International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V71I1P210

Volume 71 Issue 1, 109-123, January 2023

Original Article

An Extended Layered Information Security Architecture (ELISA) for e-Government in Developing Countries

Miton Abel Konnon[1,2,*], Nathalie Lodonou[1], Renaud Horacio Gaffan[1], Eugene Ezin[1]

[1]*Research Laboratory in Computer Science and Applications (LRSIA), University of Abomey-Calavi, Republic of Benin*
[2]*Laboratory of Processes and Technological Innovations (LAPIT), UNSTIM, Republic of Benin*

[*]*Corresponding Author : abelkonnon@insti.edu.bj*

Received: 16 December 2021 Revised: 02 August 2022 Accepted: 07 December 2022 Published: 24 January 2023

Abstract *- Information technologies are improving service delivery to citizens and businesses through access to e-information. Securing e-Government Information involves protecting some information quality criteria and effectively managing risks. This research paper aims to design an Extended Layered Information Security Architecture (ELISA) for e-Government that may be efficient in developing countries. Therefore, an Information Security Architecture is introduced using some recommendations of the USA "National Institute of Standards and Technology" (NIST) Special publications, ISO/ICE 27000 series, and good practices of the TOGAF and COBIT Frameworks. The designed Information Security Architecture ELISA represents a set of three vertical layers and two side layers. The ELISA layers take into consideration people, processes, technology and the concepts of Trust and Reputation (concerning users and applications) and compliance with the regulations in the information systems and the operating environment. The proposed ELISA model is a tool bringing together several components intended for Security Management by operational departments and Security Governance by a special Executive Management responsible for the strategic direction and compliance activities. All security mechanisms provided by the components of the different layers should help to guarantee at least six criteria of Information quality: integrity, availability, confidentiality, effectiveness, efficiency and reliability. The model's applicability is demonstrated by a case study for electronic document authentication management.*

The accurate use of the ELISA should help to avoid the cascade development of security solutions with interoperability issues and, on the other hand, to improve e-Government Information Security by aligning security requirements with e-Government and business objectives.

Keywords *- e-Government Information Security, Information Security Architecture, Information Systems Security, Information Security Framework, Information Security Compliance.*

1. Introduction

Information Security is a big challenge in the context of e-Government, where the volume of data and the speed of data diffusion are increasing. Therefore, Information Security Management should support e-Government and business objectives by reducing risks and building trust.

The USA "Federal Information Security Modernization Act of 2014" defines information security as:

Definition 1 (Information Security): "*The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction*" [1].

The definition below is considered for Information Security Architecture in this research work.

Definition 2 (Information Security Architecture): "*The Information Security Architecture represents the portion of the Enterprise Architecture that specifically addresses information system resilience and provides architectural information for the implementation of capabilities to meet security requirements*" [2].

The Information Security Architecture addresses the Information Systems Security Architecture (ISSA) and the Information Security in the operating environment of the information technology. Initially, in many investigations, Information Security Architectures were developed focusing on ISSA models due to the complexity of Information Security Management in the operating environment. The ISSA is one of the Enterprise Security Architecture (ESA) components. The ESA is at the crossroads of the concepts of Information Systems, Enterprise Architecture (EA) and Security practices (fig. 1).

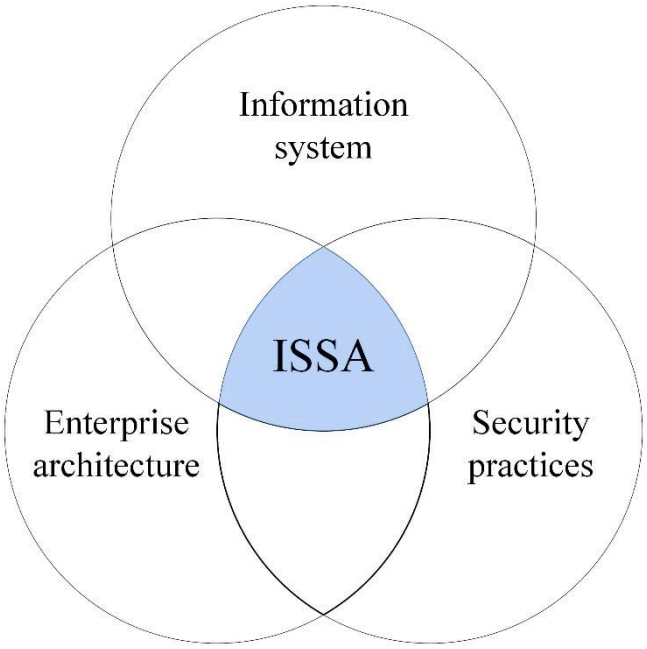

Fig. 1 Connection of the Information System Security Architecture (ISSA) with IT

The Enterprise Architecture is defined in the ISO 42010 standard as:

Definition 3 (Enterprise Architecture): "*The fundamental conception of the organization in its environment, embodied in its elements, their relationships to each other and its environment, and the principles guiding its design and evolution*" [3].

Budget constraints, limitation of resources (technical resources and workforce) and a required level of organizational culture represent key challenges for information security in general [4]. Those challenges are specific to developing countries such as the Republic of Benin (Benin). In Benin (a West African country with a low level of organizational and digital culture), Information Security has been a governmental priority since the intensive deployment of e-Government technologies in the year 2016.

The Government Information Security Directive, adopted on June 6, 2020, specifies that all public offices must ensure the security of the information delivered through their services. All ministerial departments are launching e-service platforms. For instance, the Directorate General of Taxation (DGT) has launched fifteen e-services in three years. The DGT uses a dedicated Data server which is not sufficiently interconnected to others government Information Systems.

Keynote 1: The lack of interconnections between–Government Information Systems represents a big challenge for personal identification control and data assessment when using e-services.

Despite the efforts of the Beninese Government, only a small part of the population has a digital culture enabling them to edit digital documents. In turn, many people make their personal information available to third parties to edit for them documents such as the digital birth certificate and unique tax identification. Also, the tax declaration procedure by companies is digitalized, giving them the right to an online tax certificate. Similarly, digitalization is accelerated in all developing countries to simplify administrative processes to improve service delivery to citizens and support economic growth. However, developing countries' digitalization of economic services makes their economies attractive to cybercriminals [5]. In a global survey published by the Business Software Alliance (BSA) in 2018, the unlicensed software installation rate is alarming in low-income countries, creating serious cyber-attack risks [6]. Several Government offices use unlicensed software due to the malfunctioning of the Security Department or are forced to use them due to budget lack and low level of organizational culture.

Keynote 2: Information Security Compliance is problematic when there is a lack of competence in Information Security Management (ISM) or when existing ISM teams do not report to any Security Governance body.

In [4], a model based on five criteria is proposed to classify security threat, including Security threat agents. Considering internal or external sources, three security agents are addressed: human (authorized users or hackers), environmental factors (natural disasters), and technological threats (caused by physical and chemical processes on material). The human agents are the most critical of all criteria due to attacks by outsiders, errors by authorized users and malicious actions of disgruntled or dismissed employees [7]. Considering the low level of organizational culture and the lack of Information Security competencies, designing an Information Security Architecture that meets the cost requirements remains a big challenge in developing countries.

Keynote 3: A global view of the security arrangements (security policies, audits and controls, compliance etc.) is needed for effective Information Security Management.

A great number of publications have addressed the question of Information Security Architecture [8-13]; specifically, some simplified Layered Information Security Architectures are proposed in [14] and [15]. Nevertheless, in most of those works, detailed and separated structural complements about Security Management and Security Governance are missing in the context of limited resources and low organizational and digital culture levels. Also, those works do not address the question of compliance in the operating environment of the information systems in settings with prevalent document fraud. The above-mentioned

weaknesses of the existing models make their adoption difficult in developing countries for efficient Information Security Management when deploying e-Government systems.

The complexity of Information Security arrangements and the high cost of security management are key reasons for scaling back risk-related activities in settings with limited resources. Nevertheless, document fraud, specifically identity theft, has become one of the main crimes of the information age, requiring the attention of policymakers in developing countries [16]. Also, the digital footprint can lead to society's captivity if adequate security precautions are not provided [17]. Therefore, considering the keynotes mentioned earlier, this paper aims to design an Extended Layered Information Security Architecture focusing on developing countries. To address the research gap, the next methodology is adopted:

- review of related works;
- design of an Extended Layered Information Security Architecture (ELISA) for e-Government Systems Management in developing countries;
- examination of a case study.

Apart from section 1, this paper is organized as follows. Section 2 presents the related works. In Section 3, the proposed ELISA model is introduced. A case study is proposed in Section 4. The results synthesis is discussed in Section 5 with some perspectives. Section 6 concludes this paper.

2. Related Works

2.1. Architecture Frameworks

An Information Security Framework (ISF) describes a prevalent organizational structure for different approaches to secure assets in digitalized systems. Usually, to design an ISF, various security standards, reference documents and best security practices are combined.

A well-known IFS is an American framework NIST SP 800-53. This framework was designed by the USA "National Institute of Standards and Technology" (NIST) to manage critical infrastructure cybersecurity. The framework consists of three important parts:

(i) the "Framework Core" provides outcomes for managing cybersecurity risks through five functions;

(ii) the "Profile" component guides organization in describing their "current cybersecurity posture" and determining the needed controls to achieve the security goals;

(iii) the "Framework Implementation Tiers" are used by an organization to communicate about the degree of NIST SP implementation in it Cybersecurity Strategic Program [18].

The most popular Information Security Framework is ISO 27001. This standard provides requirements and enables organizations, together with others standards of the 27000 series, to implement "Information Security Management Systems" (ISMS) through six domains, including regulatory compliance and a list of security controls [19].

The NIST SP 800-53 considers that Information Security Architecture must be fully integrated into Enterprise Architecture. However, Security Architecture Frameworks with leading authority, such as ISO 27001, have structures that do not align directly with the layers of Enterprise Architecture Frameworks. The concept of the layer in EA Frameworks refers to logical layers (e.g. business layer, data layer and technology layer) when classic Information Security Frameworks are based on structural layers such as application, network or physical layer [2]. From this point of view, the "Sherwood Applied Business Security Architecture" (SABSA) stands out from previous frameworks by providing a business-driven model [20].

The SABSA framework is a six-layers top-down security model based on the Business Attributes profile, enabling the linkage between business requirements and security architecture. Therefore, the SABSA model is closer to EA Frameworks like other IT Governance and/or Management Architecture Frameworks with an Information Security component, such as COBIT, ITIL and COSO.

The most used EA Framework is TOGAF, which was made available to the international community in 1995. TOGAF introduced an architectural construction process that goes beyond simple descriptive modelling. TOGAF is a powerful tool for Enterprise Architecture (particularly for Enterprise Information Security Architecture), which provides an Architecture Development Method (ADM), and deals with the complexity of information systems [21]. The TOGAF Framework uses a model-driven approach based on four domains: business, data, application and technology. A joint project of the TOGAF and SABSA teams started in 2010 to combine the advantages of both frameworks for an effective architecture approach.

According to the "Information Systems Audit and Control Association" (ISACA), the author of the COBIT Framework, the demand for Information Security professionals with a business focus is increasing [22]. This fact justifies the ongoing interest of researchers in mapping Information Security, IT Governance and Management and EA frameworks [23], [24], [25]. The research investigations demonstrated the advantages of the complementary use of different frameworks for security purposes.

Keynote 4: The framework design by mapping different approaches can result in a successful Information Security Architecture aligned with business needs.

Table 1. Management and Governance processes in COBIT 2019 [28]

	Domains
Governance	1) "*Evaluate, Direct and Monitor: EDM*" (5 processes). Goal: to ensure compliance with the main rules of information technologies governance
Management	2) "*Align, Plan and Organize: APO"* (14 processes). Goal: to define the basis of IT management.
	3) "*Build, Acquire, and Implement: BAI*" (11 processes). Goals: to identify solutions, develop them, or acquire and integrate them into business processes.
	4) "*Deliver, Service and Support: DSS"* (6 processes). Goal: to improve the functioning of IT operations.
	5) "*Monitor, Evaluate and Assess: MEA"* (4 processes). Goal: to provide monitoring processes by internal control and internal or external audits.

2.2. Governance Versus Management of Information Security

Several works have been devoted to the comparative study of Information Security standards and frameworks that guide Security Architectures. In [26], the authors described five frameworks' different Information Governance and Information Management tools. They outlined the particularities of ITIL, COBIT and PCIDSS ("Payment Card Industry Data Security Standard") frameworks in terms of Information Governance and Management.

In the literature, the distinction between Information Security Governance and Management has become so essential that the two concepts are used differently.

Definition 4 (Information Security Governance): "*The set of responsibilities and practices exercised by the board and executive management to provide strategic direction, ensures that objectives are achieved, ascertaining that risk is managed appropriately and verifying that the enterprise's resources are used responsibly*" [27].

Definition 5 (Security Management): "*The process of establishing and maintaining security for a computer or network system. The stages of the process of security management include prevention of security problems, detection of intrusions, and investigation of intrusions and resolution*" [27].

According to COBIT, boards and Executive Management are typically accountable for governance processes, while management processes are the domain of Senior and Middle Management. In COBIT 2019, activities are grouped into 40 processes, and processes are subdivided into detailed control objectives. The control processes are grouped into 5 domains. Domains are split between governance and management [28]. This structure helps to define the activities of security management and governance clearly. Table 1 presents the structure of Management and Governance processes in COBIT.

2.3. Trust and Reputation

The concepts of reputation and trust are closely linked, but there is a clear and important difference between them. There exists an important set of definitions of the terms "Trust" and "Reputation" in the literature, among them:

Definition 6 (Trust):

(a) "*The confidence one element has in another, that the second element will behave as expected*" [29];

(b) "*A characteristic of an entity that indicates its ability to perform certain functions or services correctly, fairly and impartially, along with the assurance that the entity and its identifier are genuine*" [49].

Definition 7 (Reputation): "*A collective measure of trustworthiness based on referrals or ratings from members in a community*" [49].

According to Jøsang, Trust is a directional relationship between two parties that can be called "Trustor" and "Trustee". The Trustor may be a "thinking entity" with the ability to make assessments and decisions based on the received information and past experience. One can assume the Trustee to be a person, organization or physical entity, or abstract notions such as information and cryptographic key [31]. In their works on Trust and Reputation, specific authors stated ([32], [33]):

(i) the basic idea of Reputation systems is to let parties rate each other and use the aggregated ratings about a given party to derive its reputation score;

(ii) The basic idea of Trust systems is to analyze and combine paths and networks of Trust relationships to derive measures of trustworthiness (reliability) of specific nodes. Reputation scores and Trust measures can assist Trustors in making transaction decisions with a given party in the future.

In [34], the authors demonstrated that "A reputation value computed by a reputation system is more reliable" for security management. They have concluded their analysis of modelling Trust and Reputation by recommending the approaches which distinguish functional trust (the system knows how to operate safely) from recommendation trust (the system gives reliable recommendations about whether

others can safely operate). These methods are more accurate than conventional trust approaches.

In their survey [35], Gomez Marmol et al. proposed four major classes of Trust models, including the Multi-agent systems models. The REGRET model has addressed reputation by exploring three different dimensions in Multi-agent Systems [36]: the individual dimension (direct interactions with the agent), the social dimension (previous experiences of group members with the agent), and the ontological dimension (rating of the impressions from the interaction of group members with the agent and the ontological structure). Challenges of the application of a four-dimension model ("trust, argumentation, negotiation and semantic alignment") were investigated in [50].

The Group Extension for Trust Model (GTrust) is proposed to support the calculation of Trust values of groups (sets of entities) [38]. The results of an experiment using simulation done for the Layered Trust Information Security Architecture (TISA) model [14] confirm the GTrust model validation.

2.4. Compliance Management

Information Security Compliance measurement and enforcement require many activities, including the management of the security policies levels, procedures and standards. Compliance levels controls must regularly be reported to the Board/ Executive Management for good governance. But there is a problem when the Compliance measurement and enforcement activities are done by the same Information Security Management (Operational Information Security) Department that responds to risk mediation [39]. As a solution, Basie Von Solms proposed to create an objectively independent Department for Information Security Compliance Management that must be affiliated with the board/ Executive Management (Governance body). In his investigation of this Department, the author highlighted an approach based on IT Risk Profile. This Risk Profile is managed by creating real-time IT Risk Compliance Profiles reflecting the level of management of IT risks [40]. In this context, the Operational Information Security Department works based on a Service Level Agreement (SLA) with the Information Security Compliance Department. This SLA can be verified by collecting required data from the IT environment and through interviews with competent external bodies.

The IT Risk Profile helps to automate Compliance management. For instance, S. Sen et al. demonstrated a collection of techniques for automated privacy compliance checking in big data systems [41]. To achieve this goal, authors have designed the LEGALEASE language for stating privacy policies.

Actually, research works are actively devoted to the General Data Protection Regulation (GDPR) Compliance certification in European Union. Some of those works are conducted on assessment tools for the GDPR compliance certification [42], [43].

2.5. Particularities and Limitations of the Existing Simplified Layered Information Security Architectures

One of the particularities of simplified Layered Information Security Architectures (LISA) is the reduced and clear methodology approach that brings in the increased adoption of ISA models. Simplicity is gained by using a logic-layered approach instead of big domains and focusing on the information as an asset.

In the literature, two main LISA models are identified. The Layered Trust Information Security Architecture (TISA) is based on four layers designed "for managing risks at different levels considering information treatment" [14]. The TISA model, proposed by an international group of researchers in 2014, extends the Confidentiality Integrity Authentication (CIA) triad requirement introducing the concept of security extensions at the first layer devoted to the information treatment. The second layer addresses the human resource, processes and technologies they may use. The third layer describes security controls when the vertical layer is based on the group trust model.

George Farah proposed another LISA approach for managing risks with a limited set of security measures in a scalable IT environment in 2004. This architecture represents a "five-phase methodology for security management across data, applications and infrastructure architecture (hardware, systems and networks)" [15].

The analysis of existing architectures has highlighted that layered architectures are easier to implement. However, some extra structural or semantic complements are missing to address Security Management and Governance in limited resource settings.

- They failed to separate Information Security Governance component from the Management component. This issue constitutes a major limitation for adopting those models in developing countries. Suppose the Security Management (Operational Information Security) Department has to measure how well they themselves comply with relevant policies and procedures and how successful their risk mediation efforts are. In that case, the results may not always be objective and true [39]. For example, when using the COBIT framework, the MEA domain must be committed to the Operational Department, while another oversight Department must respond to the EDM governance domain (for compliance).

- The TISA framework introduced the "Information Security extensions" by extrapolating the CIA triad, but, so formulated, the security extensions are optional. However, effectiveness, efficiency and reliability are key Information quality criteria that should state the essence of information security by itself [28], specifically in low- organizational and digital culture settings.

3. The Extended Layered Information Security Architecture (ELISA)

3.1. Design Approach

Considering all the definitions mentioned above and keynotes and the provided analysis in section 2, a security criteria meta-model was developed to meet the specific requirements of settings with low organizational and digital culture levels. The introduced meta-model is inspired by the results presented in [44] that highlighted the concepts of (i) security criteria (describable) and (ii) security aspect and security sub-aspect described by measurable criteria. Then, the reference ELISA model was developed using the meta-model.

To implement the proposed ELISA model, a six-phase methodology was introduced mapping the Information Security Management approach of the ISO/ICE 27000 series [19], [45] with the COBIT best practices in relation to the TOGAF ADM [25], [46]. These are [48]:

- Assets Identification
- Security Vision
- Reference Architecture
- Security Solutions
- Planning of Security Governance and Management
- Implementation

3.2. A meta-model for Information Security

This sub-section aims to state the basis for Information Security improvement.

To describe the management of Information Security, the next concepts are used:

3.2.1. The Security Quality

The security quality of the information addresses the security of the activities associated with capability levels and is described by measurable security criteria.

3.2.2. Criteria and Sub-criteria

Criteria and sub-criteria of Information quality. They refer to security properties in Information Systems and the environment of the IS. In addition to the CIA triad, new criteria define to improve information security when deploying e-Government infrastructures (large-scale distributed networks).

3.2.3. Capability Level

Design factors can influence the choice of quality criteria, breaking their equivalence and making some governance and management objectives more important than others. In practice, this importance is translated by setting various target capability levels for governance and management objectives.

3.2.4. Security Aspect and Sub-Aspect

In [44], the authors present security as a multi-faceted security criterion linked to various information system assets. These facets are called security sub-aspects. For illustration: "Integrity" is a security aspect with several sub-aspects, including application integrity, communications integrity and data integrity.

3.2.5. Security Mechanism

Security mechanism refers to a process or technique designed to detect and prevent threats or recover from a security attack.

3.2.6. Trust and/or Reputation Score

Trust and/or Reputation score is a calculated value of trust and/or reputation that can assist a source in making transaction decisions with a given party.

3.2.7. Security Context

Security context is a situation where sources' Trust and Reputation scores can change.

3.2.8. Threat Scenario

Threat scenario represents a set of actions associated with a source or multiple sources against an asset by exploiting vulnerabilities.

3.2.9. Security Service Level Agreement

Security Service Level Agreement (SLA) refers to a service contract including required capability levels between the Information Security Compliance Management and the Information Security Operational Management.

3.2.10. Security Requirements

Security requirements specify functional and non-functional requirements associated with one or more security objectives.

3.3. Motivating factors for the choice of the Information Quality Criteria

In a developing country, the officer responsible for Information Security is often obliged to perform many other IT tasks. Therefore, he can easily forget to delete the account of a dismissed (transferred) employee. This situation represents a serious vulnerability and demonstrates the importance of the information currency (sufficiently up-to-date). National agencies often develop security solutions

without referring to a national architecture document. Consequently, interoperability problems arise when it is necessary to interconnect the Information Systems of different projects or agencies.

The production of the electronic version of official documents promotes their movement through the Internet. Also, many people refer to document printing centres to print their official electronic documents (OED) delivered by e-Government agencies. Those OED, once copied by a third party, can undergo changes and then be used fraudulently. Therefore, quality criteria such as Concise representation (the information is compactly represented) and Consistent representation (the information is presented in the same format) should help in the rapid detection of editing errors. According to the BSA, the spreading use of unlicensed software by Government offices in developing countries promotes cyber-attacks against their Information Systems [6]. Therefore, securing e-Government systems requires deploying reliability (trust and reputation) based policies.

Considering the facts mentioned above, in addition to the CIA triad, effectiveness (Consistent representation, currency and relevancy), efficiency (Concise representation, ease of manipulation and interoperability) and reliability [46] remain important key criteria to state the basis of any Information Security Architecture in settings with a low level of organizational and digital culture.

3.4. Description of the Proposed ELISA Model

The proposed model is inspired by TISA [14] and based on a layered architecture. An alignment with the COBIT Framework is adopted to define security criteria at layer 1, to reorganize layer 2 of TISA by separating governance from management, and by adding the compliance side layer according to the recommendations of authors in [12], [40], [41] and ISO 27002 standard [45] (fig. 2).

With the top-down and side-layered approach, the different facets of Information Security are well-understood and well-connected in an extended way.

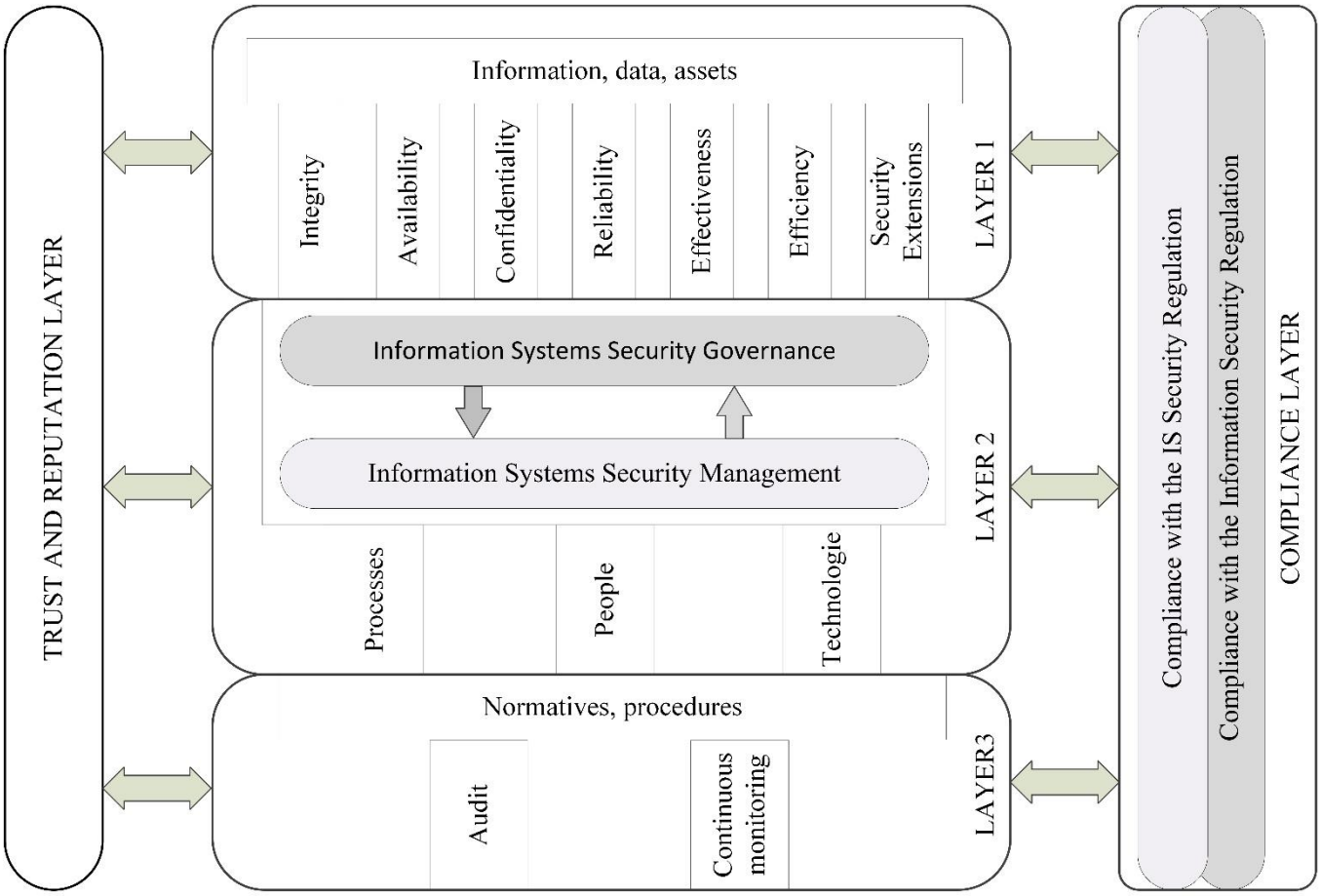

Fig. 2 The Extended Layered Information Security Architecture (ELISA)

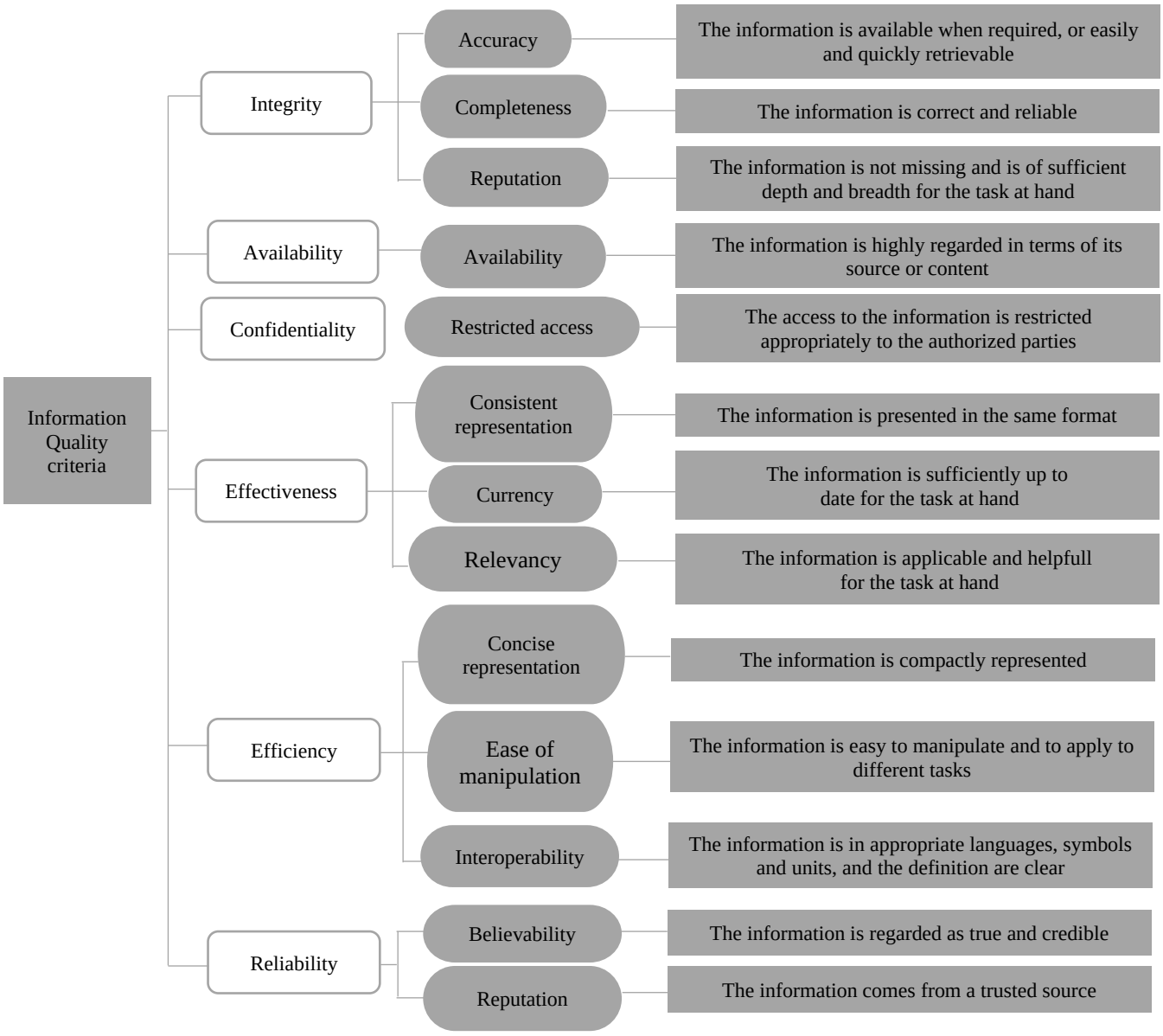

Fig. 3 Linkage between the ELISA information quality criteria and sub-criteria

3.4.1. Layer 1

Version 4 of COBIT mentioned seven basic security criteria (integrity, availability, confidentiality, reliability, effectiveness, efficiency, and compliance) [46]. In order to meet the new security requirements, the number of information quality criteria has increased from seven in COBIT 4 to fifteen (which are now called sub-criteria and grouped into three categories) in COBIT 2019 using a new information model [28].

Considering the analysis of section 2 and sub-section 3.3, six basic Information quality criteria are identified to state the basis of layer 1.

Integrity

Information integrity refers to the accurateness and completeness of the information.

Availability

Property of information, a resource, a service to be available on time and to continue to be so for the accomplishment of a functional process

Confidentiality

Concerns about the protection of sensitive information against disclosure or unauthorized disclosure.

Effectiveness
A piece of information is effective if it meets the needs of the person using it for a given task.

Efficiency
Suppose the information that meets the user's needs is easy to obtain and use (requires few resources - physical or cognitive effort, time, and money). In that case, the use of this information is efficient.

Reliability
Information is reliable if it is fair and credible. Reliability is a more subjective criterion compared to integrity, related to perception and not just facts [28].

According to the new COBIT Information model, each of the six basic information quality criteria adopted in the ELISA model represents a group of sub-criteria [28].

This declination helps to define with precision the security sub-aspects. For instance, application integrity can refer to the application's reputation when data integrity can be evaluated through data accuracy or data completeness. Fig. 3 presents the linkage between the ELISA Information quality criteria and sub-criteria.

Information Security Extensions
Information Security Extensions are properties that can be added to the information security criteria of layer 1. Some extensions are sufficient by themselves, while others depend on a set of factors, such as context, technologies that support them, security objectives etc.

Table 2. Important Information Security Extensions with the related objectives

Extensions	Security objectives
Authentication	To verify the eligibility (identity) of a user to access computerized information
Access control	To control access to information systems and resources
Non-repudiation	To provide verifiable proof of the integrity and origin of the data
Authenticity	To certify the undisputed authorship
Privacy	To ensure that personal data is not processed without the knowledge and consent of the owner
Anonymity	To make a user identity unknown
Authorization	To grant access privileges to a user, program, or process
Identification	To discover the true identity of a user or item from a collection
Accountability	To empower a person to protect and control equipment, keying material and information

Table 2 presents a non-exhaustive list of extensions recommended by popular Information security standards. A security objective is connected to each extension. Sometimes, sub-objectives are required to achieve the main security objective. For example, the NIST Special Publications recommends performing both physical and logical access controls, identity-based authentication or role-based authentication.

3.4.2. Layer 2
At this level, Information Security Governance is separated from Information Security Management. The governance is at the forefront of the reflection and consists of evaluating stakeholders' needs, rules and options to determine balanced objectives that achieve consensus. The management involves planning, building, executing and monitoring activities per the direction set by the governance group to achieve predefined objectives. This distinction helps to situate responsibilities and to guarantee non-repudiation [28], [46].

“People” represent the human resources that create and maintain security processes. “Information Security Processes” refer to the mechanisms to manage and control all information risks. “Technology” is the set of all informatics systems, applications, tools, and infrastructure used to achieve business objectives.

3.4.3. Layer 3
Auditing and continuous monitoring represent the main operations of the Management Department. Auditing is the set of processes to discover risks, technical flaws, policies, principles, procedures and compliance problems. Continuous monitoring can be designed as an active security component which uses a continuous process of sensing and adaptation to discover and defend against threats, including the unforeseeable [47].

3.4.4. Trust and Reputation Layer
The deployment of e-Government infrastructures and services supposes the interconnection of different IS, the growth of online interactions with sensitive machines, and the widespread use of official documents in electronic format. This digital transformation also goes with the increase in various cyberattacks. In settings characterized by a real lack of information security competencies, a low organizational level of IT Security Governance and Management and a low level of digital culture of communities, the implementation of automatized Trust and Reputation measures in the architecture of e-Government infrastructures and services remains an important key to achieve security goals.

One of the discussed Trust and Reputation models in section 2 can be used at this layer depending on the security objectives.

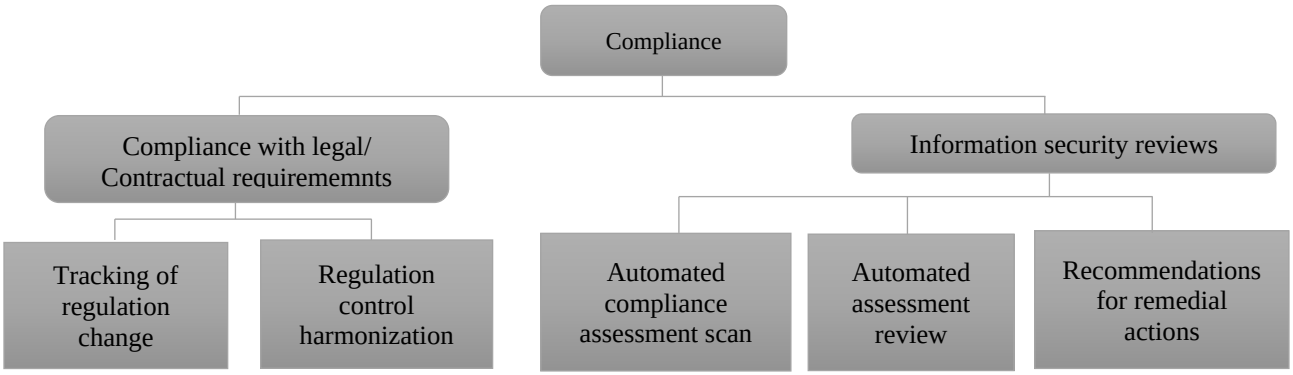

Fig. 4 Possible activities for compliance management in alignment with ISO 27002:2013

3.4.5. The Compliance Layer

The e-Government information (data) is considered a key asset and may be secured in the operating environment. The Information System is a socio-technical system (organizational structure, people, business processes and technology) designed for Information Management and Governance. Therefore, the Compliance layer is a new layer proposed in the ELISA model with two components to address the Information Systems Security Compliance and the Information Security Compliance in the information technology operating environment.

The "Compliance with the Information System Security Regulation" component considers regular compliance controls: organizational, people, physical and technological in the IS.

The "Compliance with the Information Security Regulation" component deals with Information Security Compliance in the operating environment. It is a key layer for the e-Government Information Security strategy due to the dematerialization of official documents for public use in low- organizational and digital culture settings. A compliance control must help check the reliability of the information when used by a third party (non-author). For instance, a customs agency must be able to quickly check an e-document issued by a tax agency using a cost-effective method.

The e-Government Information Security Compliance should be committed to a Department (Agency) for independent review (measurement and enforcement). This Department must support e-Government Information Systems Managers and develop cost-effective Compliance assessment tools that can be used in the operating environment by people with a low level of digital culture. Possible activities of this Department are presented in Fig. 4.

- eDocument Controller (EDC node). EDC nodes are remote systems (users) from the operating environment authorized to communicate with The SEDAM cluster. The eDocument authentication process is initiated only by EDC nodes.

4. A Case Study of the System for Automated Compliance Assessment

This section is devoted to a case study of the proposed ELISA model focusing on the compliance layer. This case study aims to design an automated compliance assessment system for Electronic Official Document (EOD). The System for Electronic Documents Authentication Management (SEDAM) has been developed to achieve this goal. The SEDAM is designed for Security (Compliance) Management; however, it represents by itself an information system that also needs to be secured.

4.1. The SEDAM Objective and Design Requirements

The design objective of the SEDAM is to propose an Information System allowing the automated authentication control of any electronic document delivered by a Government agency. An OED can be issued to a person (e.g. Electronic birth certificate) or a company (e.g. Unique tax identification, Electronic tax certificate). To achieve the SEDAM goal, the next requirements have to be satisfied:

– Any OED delivered by a Government agency is indexed in the SEDAM cluster.

– Only indexing information (metadata) of OED is stored in the SEDAM to limit storage space.

– The secure verification of the authenticity of any OED without going physically to the issuing entity is guaranteed.

– Secure online access to all delivered OED (stored by issuing agencies) by the SEDAM cluster is organized.

– Immediate remote access to metadata of indexed documents by the authorized user (system) is supported.

4.2. The SEDAM Components

The SEDAM architecture is based on three main components.

- eGovernment Service Information Systems (IS nodes). IS nodes are Information Systems of Government agencies delivering official eDocuments.
- SEDAM Cluster (Core component). The core component of the SEDAM is a cluster with two structural levels: control level and storage level. The control level is used to validate the EOD authentication on the interface with the operating environment and to check the security compliance of EOD on the interface with the IS nodes before indexing metadata. Storage nodes store EOD metadata at the second level of the cluster with backup possibilities.
- eDocument Controller (EDC node). EDC nodes are remote systems (users) from the operating environment authorized to communicate with The SEDAM cluster. The eDocument authentication process is initiated only by EDC nodes.

4.3. The SEDAM Security Arrangements in Alignment with the ELISA model

4.3.1. Security Layer 1

To define the security criteria, a model of eDocument is proposed with the next attributes:

(i) IDDocument – the national identification number of the OED;
(ii) IDHolder – the national identification number of the person or company to whom the OED is delivered;
(iii) IDIssuer – the national identification number of the agency that delivered the OED;
(iv) Others useful attributes (security credentials).

All security extensions listed in table 2, apart from the "Anonymity", can be implemented to secure the SEDAM.

All delivered OED have to be secured by a hash value attributed by the issuer agency.

Fig. 5 presents the proposed SEDAM architecture.

Possible measurable security indicators for the SEDAM Information quality sub-criteria in alignment with the ELISA recommendations are summarized in table 3.

4.3.2. Security Layer 2

Since the SEDAM is designed for compliance assessment, it should be managed by a Department for Information Security Compliance. This Department must periodically provide reviews to the Information Security Governance Executive Management. The basic required functions at this layer are:

- Metadata capture and use. The SEDAM is designed to capture and store the metadata of all OED for future use.
- Security control. This function controls access to indexed metadata. Only an authorized group of users (systems) can manage the SEDAM information.
- eDocument Authentication control. The SEDAM is the official mandatory system to validate all OED authentication.

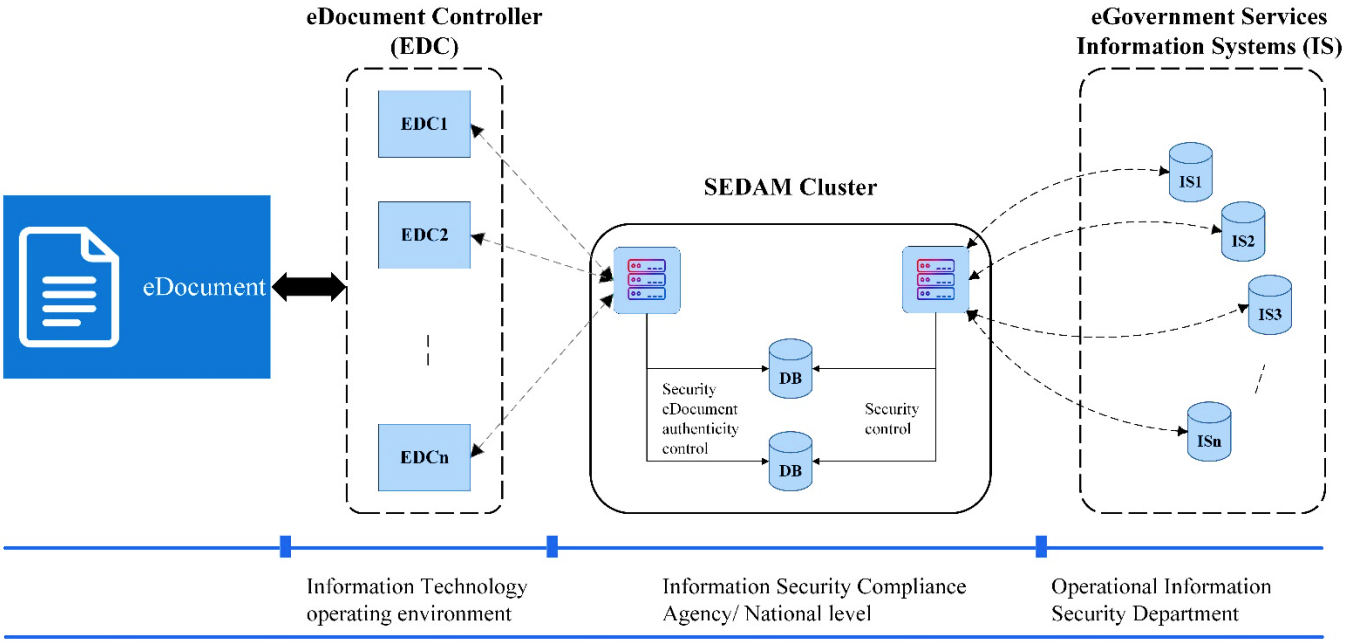

Fig. 5 The SEDAM architecture

4.3.3. Security Layer 3

At this layer, two roles can be dedicated to the SEDAM: the role of a monitoring tool for the IS nodes and the role of a supervised Information System.

- The role of monitoring tool. The SEDAM should be connected to all e-Government IS nodes to index in real time all delivered OED. Therefore, the SEDAM can be used as a monitoring tool to provide a report on the availability of each IS node.
- The role of supervised IS. The SEDAM is an Information System used for compliance assessment. From this point of view, auditing and continuous monitoring operations may be performed to secure the SEDAM.

Table 3. Possible measurable indicators for Information Quality sub-criteria

Quality sub-criteria	Possible indicator
Accuracy	Validity of the document hash for the given IDHolder
Availability	Existence of the IDDocument in the SEDAM database
Believability	Required number of Credentials with the valid value
Completeness	Required number of Credentials with no null value
Reputation	Validity of the IDIssuer
Consistent representation	Conformance of the document template (e.g. valid number of information blocks)
Concise Representation	Existence of all metadata for security control
Currency	Valid document issue date
Ease of manipulation	Automated Quality check score obtained without contacting the document issuing entity
Interoperability	Access to the stored EOD on an IS node) for check
Relevancy	Valid document type
Restricted access	Secure identification and authentication for exchange with the SEDAM cluster

4.3.4. Trust and Reputation Layer

The SEDAM architecture is designed in alignment with the Group models. For this reason, the GTrust model is suggested for this case study. Key concepts of the model are an entity, group, group leader, context, Trust and Reputation values.

Entity

An entity may be a single server hosting an e-service (IS nodes and EDC) or security operations.

Group

The group is a collection of entities with particular affinities and capabilities.

Group leader

The leader is one of the group entities (SEDAM cluster), the representative entity for new group members and the outside environment. The group leader knows every context.

Trust and/or Reputation values of entity A used by B for data exchange are calculated depending on the context (interaction). A threshold value (based on Threat scenario analysis) can be set to define when a transaction is possible or not between the cluster and a specific node. The threshold value for an IS node can differ from the threshold value of the controller node.

4.3.5. Compliance Layer

The SEDAM provides two different compliance operations: one on the Cluster–ISnode interface and another on the Cluster–EDC interface.

Compliance on the Cluster–ISnode interface. When an IS node initiates an indexing process, the control level of the SEDAM runs the security control algorithm by checking all required OED Information quality criteria. The current OED is indexed only when the assessment result is successful.

Compliance on the Cluster–EDC interface. A document authentication process can be initiated only by an authorized EDC. To validate the OED authentication, the SEDAM cluster runs the eDocument authenticity control algorithm. The obtained assessment result is communicated to the concerned EDC at the end of the operation.

5. Discussion and Future Work

The proposed Information Security Architecture provides some important outcomes to address certain shortcomings and limit security risks in settings with low organizational and digital culture levels. The simplified layered structure of the architecture allows managers to monitor the information security deployment easily.

The implementation of the ELISA model requires the creation of security policy documentation. This high-level document must specify all security arrangements (Information quality criteria, security extensions, security rules, mechanisms, processes, auditing and continuous monitoring operations, normative documents, trust and reputation algorithms, and compliance measures) covering all layers.

All specifications should be aligned with the e-Government Strategic Program (eGSP) to achieve the required capability levels for governance and management objectives. The policy document should help to:

Table 4. Comparative analysis

	ISO 27001	SABSA	COBIT 2019	TISA	ELISA
Information security governance guidance	No*	Yes	Yes	No	Yes
Information security management	Yes	Yes	Yes	Yes	Yes
CIA triad and Security extensions	Yes	Yes	Yes	Yes	Yes
Defined Trust framework and assessment measures	No	Yes	No	Yes	Yes
Tracking with regulation change	Yes	Yes	Yes	Yes	Yes
Regulation control harmonization	Yes	Yes	Yes	Yes	Yes
Recommendations for remedial actions	Yes	Yes	Yes	Yes	Yes
Security compliance assessment at the system level (regulatory)	Yes	Yes	Yes	No	Yes
Guidance for information security compliance in the operating (external) environment	No	No	No	No	Yes

**The Information Security Governance guidance for ISO 27001 is emphasized in the ISO 27014 Standard*.

- identify and hire qualified human resources;
- define the different work teams to secure effectively Government IS;
- plan, execute, evaluate and improve security processes.

Creating an independent Information Security Compliance team that should report reviews to the eGSP Executive Management should help improve the daily services of all Operational Information Security Departments, managing the security of national Information Systems.

A comparative analysis of ELISA and four frameworks are provided in table 4. Considering the business alignment criteria, ELISA is closer to SABSA and COBIT frameworks. These two frameworks sufficiently address the questions of Information Security Governance and Information Security Management to meet business needs. The architectural structure and Trust modelling approach of TISA are considered in the ELISA model. However, ELISA added the Reputation concept to the TISA Trust layer. On top of this, the security meta-model and the compliance layered developed in ELISA make it different from the TISA architecture. All Standards focus on compliance with regulatory security requirements neglecting the information quality outside the Information Systems.

This negligence is compromised when official government documents are edited in digital form. Digitized information can be easily modified. For this reason, ELISA considers Information Security Compliance in the information systems and in their external operating environment as an essential principle to increase the level of information security in countries with low organizational and digital culture.

The SEDAM case study, presented in section 4, demonstrated the applicability of the ELISA model and outlined how to align Information security with e-Government objectives using a cost-effective approach. Considering the provided description of each layer, the information security reference documentation can be elaborated and help to improve the information security in Benin. For instance, the tax registration certificate (TRC) is edited online. Every TRC is secured by a QR code and protected against modification.

Currently, two compliance assessment methods are available in the operational environment: (*i*) scanning the QR code or (*ii*) checking the TRC number on the official website. In response, the last and first names of the registered person appear. Despite the protective measures, the actual Compliance methods are insufficient to guarantee a TRC document's reliability in the operational environment. Because person B, with the same last name and first name as another person A, can use a falsified document with the QR code of A. Therefore, he can do business without paying taxes. But, the use of the SEDAM cluster for Compliance assessment based on the appropriate security credentials can help to detect automatically the falsified document which is not indexed.

However, the ELISA model remains a tool whose efficiency depends on several factors, including the awareness of the end users and the will of Government authorities.

In perspective, further research will be carried out to address a general e-Government Risk Profile for settings with a low level of organizational and digital culture to achieve resilient security goals. Also, considering the resources (technical resources and workforce) limitations in developing countries, future research works will be devoted to developing cost-effective tools to automate security management and governance tasks as much as possible.

6. Conclusion

In this work, an Extended Layered Information Security Architecture (ELISA) is introduced for e-Government, focusing on settings with limited resources and low organizational and digital culture levels. The main novelty in

the recommended model consists in separating the security management activities from the governance tasks to strengthen the compliance controls in the Information Systems and outside them. A meta-model, based on a set of six information security criteria, including the CIA triad, and various security concepts, is developed to achieve the security objectives. The proposed model suggests two specific side layers (Trust and Reputation layer and Compliance layer) in addition to the conventional layers of Information Systems Architectures. The Trust and Reputation layer is designed to provide a Trust/Reputation measurement mechanism that can be easily implemented. The Compliance layer addresses an approach that can be automated as much as possible, including controlling the information quality in the operating environment.

A System for Electronic Documents Authentication Management (SEDAM) was discussed as a case study of the proposed model. All layers of the architecture are described, and a list of security sub-criteria is provided with possible measurable Information quality indicators.

The SEDAM case demonstrated the implementation advantages of the proposed ELISA architecture.

In developing countries, an Information Security Strategy based on the proposed set of Information quality criteria and the ELISA model's simplified structure should help develop solutions for secure data processing, storage and transmission, thereby improving the efficiency of e-Government services.

Conflicts of Interest

The author declared no potential conflicts of interest for this work's research, authorship, and publication.

References

[1] *Federal Information Security Modernization Act*, USA Public Law 113–283, pp. 1-16, 2014.

[2] Stephen Gantz, and Daniel Philpott, *Risk Management: FISMA and the Risk Management Framework*, Elsevier, pp. 329-365, 2013.

[3] *Systems and Software Engineering – Recommended Practice for Architectural Description of Software-Intensive Systems*, ISO/IEC 42010, 2007.

[4] *Managing Information Security Risk: Organization, Mission, and Information System View*, National Institute of Standards and Technology, pp. 1-36, 2011.

[5] Nir Kshetri, "Cybercrime and Cybersecurity in Africa," *Journal of Global Information Technology Management*, vol. 22, no. 2, pp. 77-81, 2019. *Crossref*, https://doi.org/10.1080/1097198X.2019.1603527

[6] *Software Management: Security Imperative, Business Opportunity*, Business Software Alliance, 2018.

[7] Mouna Jouini, Latifa Ben Arfa Rabai, and Anis Ben Aissa, "Classification of Security Threats in Information Systems," *Procedia Computer Science*, vol. 32, pp. 489-496, 2014. *Crossref*, https://doi.org/10.1016/j.procs.2014.05.452

[8] J. A. Zachman, "A Framework for Information Systems Architecture," *IBM Systems Journal*, vol. 26, no. 3, pp. 276-292, 1987.

[9] Sead Muftic, and Morris Sloman, "Security Architecture for Distributed Systems," *Computer Communications*, vol. 17, no. 7, pp. 492-500, 1994. *Crossref*, https://doi.org/10.1016/0140-3664(94)90104-X

[10] Gustavo A. Santana Torrellas, "A Security Architectural Approach for Risk Assessment Using Multi-agent Systems Engineering," *Lecture Notes in Computer Science*, pp. 110-124, 2003. *Crossref*, https://doi.org/10.1007/978-3-540-40010-3_10

[11] Rose-Mharie Åhlfeldt, Paolo Spagnoletti, and Guttorm Sindre, "Improving the Information Security Model by Using TFI," *New Approaches for Security, Privacy and Trust in Complex Environments*, pp. 73-84, 2007. *Crossref*, https://doi.org/10.1007/978-0-387-72367-9_7

[12] Rossouw de Bruin, and S H von Solms, "Modelling Cyber Security Governance Maturity," *EEE International Symposium on Technology and Society*, pp. 1-8, 2015. *Crossref*, https://doi.org/10.1109/ISTAS.2015.7439415

[13] Nguyen Ai Viet et al., "Toward Cyber-Security Architecture Framework for Developping Countries: An Assessment Model," *Proceedings of Advances in Intelligent Systems and Computing*, pp. 652-658, 2016. *Crossref*, https://doi.org/10.1007/978-3-319-49073-1_69

[14] Robson de Oliveira Albuquerque et al., "A Layered Trust Information Security Architecture," *Sensors*, vol. 14, no. 12, pp. 22754-22772, 2014. *Crossref*, https://doi.org/10.3390/s141222754

[15] George Farah, *Information Systems Security Architecture – A Novel Approach to Layered Protection*, SANS Institute, pp. 4-10, 2005.

[16] Alfonso Avila, "Identity Theft in Developing Countries' Online Banking Industry, Real Threat or Artificial Technological Need?," *Global Internet Governance Academic Network*, 2007. *Crossref*, http://dx.doi.org/10.2139/ssrn.2798296

[17] Ali Hedayati, "An Analysis of Identity Theft: Motives, Related Frauds, Techniques and Prevention," *Journal of Law and Conflict Resolution*, vol. 4, no. 1, pp. 1-12, 2012. *Crossref*, https://doi.org/10.5897/JLCR11.044

[18] *Framework for Improving Critical Infrastructure Cybersecurity*, NIST USA, pp. 1-55, 2018.

[19] *Information Technology – Security Techniques – Information Security Management Systems – Requirements*, ISO/IEC 27001, 2nd Edition, pp. 1-22, 2013.

[20] John Sherwood, Andrew Clark, and David Lynas, *Enterprise Security Architecture a Business-Driven Approach*, Ed. Taylor & Francis Group, pp. 1-43, 2005.

[21] *The TOGAF Standard*, The Open Group, Version 9.2, pp. 1-48, 2018.

[22] *Model Curriculum for Information Security Management*, ISACA, 2nd Edition, pp.1-33, 2012.

[23] Razieh Sheikhpour, and Nasser Modiri, "An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls," *International Journal of Security and its Applications*, pp. 13-28, 2012.
[24] Christopher Oparaugo, "ISO 27001 Process Mapping to COBIT 4.1 to Derive a Balanced Scorecard for IT Governance," *COBIT Focus*, 2015.
[25] Iis Hamsir Ayub Wahab, and Assaf Arief, "An Integrative Framework of COBIT and TOGAF for Designing IT Governance in Local Government," *2nd International Conference on Information Technology, Computer, and Electrical Engineering*, pp. 36-40, 2015. *Crossref*, http://doi.org/10.1109/ICITACEE.2015.7437766
[26] Heru Susanto, Mohammad Nabil Almunawar, and Yong Chee Tuan, "Information Security Management System Standards: A Comparative Study of the Big Five," *International Journal of Electrical & Computer Sciences*, vol. 11, no. 5, pp. 23-29, 2011.
[27] ISACA Glossary. [Online]. Available: https://www.isaca.org/resources/glossary
[28] *COBIT 2019 Framework: Introduction and Methodology*, ISACA, pp. 1-68, 2018.
[29] *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, NIST SP 800-161, p. 276, 2022. *Crossref*, http://dx.doi.org/10.6028/NIST.SP.800-161r1
[30] Daniel Makupi, and Nelson Masese, "Determining Information Security Maturity Level of an Organization based on ISO 27001," *SSRG International Journal of Computer Science and Engineering*, vol. 6, no. 7, pp. 5-11, 2019. *Crossref*, https://doi.org/10.14445/23488387/IJCSE-V6I7P102
[31] Audun Jøsang, Roslan Ismail, and Colin Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," *Decision Support Systems*, vol. 43, no. 2, pp. 618-644, 2007. *Crossref*, https://doi.org/10.1016/j.dss.2005.05.019
[32] Audun Jøsang, "The Right Type of Trust for Distributed Systems," *Proceedings of New Security Paradigms Workshop*, pp. 119-131, 1996. *Crossref*, https://doi.org/10.1145/304851.304877
[33] Audun Jøsang, "Trust and Reputation Systems," *Aldini and R. Gorrieri (Eds.), Foundations of Security Analysis and Design IV*, FOSAD, vol. 4677, pp. 209-245, 2007. *Crossref*, https://doi.org/10.1007/978-3-540-74810-6_8
[34] Andreas Gutscher, Jessica Heesen, and Oliver Siemoneit, "Possibilities and Limitations of Modeling Trust and Reputation," *Proceedings of WSPI*, 2008.
[35] Félix Gómez Mármol, and Gregorio Martínez Pérez, "Towards Pre-Standardization of Trust and Reputation Models for Distributed and Heterogeneous Systems," *Computer Standards & Interfaces*, vol. 32, no. 4, pp. 185-196, 2010. *Crossref*, https://doi.org/10.1016/j.csi.2010.01.003
[36] Jordi Sabater, and Carles Sierra, "Regret: Reputation in Gregarious Societies," *Proceedings of International Conference on Autonomous Agents*, no. 5, pp. 194-195, 2001. *Crossref*, https://doi.org/10.1145/375735.376110
[37] Evans Mwasiaji, and Kenneth Iloka, "Cyber Security Concerns and Competitiveness for Selected Medium Scale Manufacturing Enterprises in the Context of Covid-19 Pandemic in Kenya," *SSRG International Journal of Computer Science and Engineering*, vol. 8, no. 8, pp. 1-7, 2021. *Crossref*, https://doi.org/10.14445/23488387/IJCSE-V8I8P101
[38] Robson de Oliveira Albuquerque, Luis Javier García Villalba, and Tai-Hoon Kim, "GTrust: Group Extension for Trust Models in Distributed Systems," *International Journal of Distributed Sensor Networks*, vol. 10, no. 2, 2014. *Crossref*, https://doi.org/10.1155/2014/872842
[39] S. H. Von Solms, "Information Security Governance – Compliance Management vs Operational Management," *Computers & Security*, vol. 24, no. 6, pp. 443–447, 2005. *Crossref*, https://doi.org/10.1016/j.cose.2005.07.003
[40] S. H. Von Solms, and Rossouw von Solms, "The Control Part of the Model – An Information Security Compliance Management Environment," *Information Security Governance*, pp. 1-13, 2008. *Crossref*, https://doi.org/10.1007/978-0-387-79984-1_7
[41] Shayak Sen et al., "Bootstrapping Privacy Compliance in Big Data Systems," *IEEE Symposium on Security and Privacy*, pp. 327-342, 2014. *Crossref*, https://doi.org/10.1109/SP.2014.28
[42] Zsolt István, Soujanya Ponnapalli, and Vijay Chidambaram, "Software-Defined Data Protection: Low Overhead Policy Compliance at the Storage Layer is Within Reach!," *Proceedings of VLDB Endowment*, vol. 14, no. 7, pp. 1167-1174, 2021. *Crossref*, https://doi.org/10.14778/3450980.3450986
[43] Aristeidis Chatzipoulidis, Theodosios Tsiakis, and Theodoros Kargidis, "A Readiness Assessment Tool for GDPR Compliance Certification," *Computer Fraud & Security*, vol. 2019, no. 8, pp. 14-19, 2019. *Crossref*, https://doi.org/10.1016/S1361-3723(19)30086-7
[44] Wilson Goudalo, Christophe Kolski, and Vanderhaegen Frédéric, "Towards Advanced Security Engineering for Enterprise Information Systems: Solving Security, Resilience and Usability Issues Together within Improvement of User Experience," *Proceedings of ICEIS*, pp. 436-459, 2016. *Crossref*, https://doi.org/10.1007/978-3-319-62386-3_20
[45] *Information Technology - Security Techniques - Code of Practice for Information Security Controls*, ISO/ICE 27002, 2nd Edition, pp 1-80, 2013.
[46] *A Business Framework for the Governance and Management of Enterprise IT*, ISACA, pp. 1-94, 2012.
[47] Ryan Hand, Michael Ton, and Eric Keller, "Active Security," *Proceedings of ACM Workshop on Hot Topics in Networks*, no. 17, pp. 1-7, 2013. *Crossref*, https://doi.org/10.1145/2535771.2535794
[48] N. Lodonou oke, "*Implementation of a Layered Information System Security Architecture: Case of the DGI*," University of Abomey-Calavi, Abomey-Calavi, Rep. Benin, 2020.
[49] *A Profile for U.S. Federal Cryptographic Key Management Systems*, NIST SP 800-152, p. 146, 2015. *Crossref*, http://dx.doi.org/10.6028/NIST.SP.800-152
[50] Piero Bonatti et al., "On the Integration of Trust with Negotiation, Argumentation and Semantics," *The Knowledge Engineering Review*, vol. 29, no. 1, pp. 31-50, 2014. *Crossref*, https://doi.org/10.1017/S0269888913000064