Author Accepted Manuscript version of the paper by Shao-Fang Wen and Basel Katt in Information and Computer Security, DOI: 10.1108/ICS-06-2023-0101

Exploring the Role of Assurance Context in System Security Assurance Evaluation: A Conceptual Model

Shao-Fang Wen*, Basel Katt

Department of Information Security and Communication Technology
Norwegian University of Science and Technology
Gjøvik, Norway

* Corresponding author.
Email address: shao-fang.wen@ntnu.no
ORCID: http://orcid.org/0000-0002-6228-8367

Abstract.

Purpose – Security Assurance Evaluation (SAE) is a well-established approach for assessing the effectiveness of security measures in systems. However, one aspect that is often overlooked in these evaluations is the assurance context in which they are conducted. This research paper aims to explore the role of assurance context in system SAEs and proposes a conceptual model to integrate the assurance context into the evaluation process.

Design/methodology/approach – The conceptual model highlights the interrelationships between the various elements of the assurance context, including system boundaries, stakeholders, security concerns, regulatory compliance, and assurance assumptions, and regulatory compliance.

Findings – By introducing the proposed conceptual model, this research provides a framework for incorporating the assurance context into SAEs and offers insights into how it can influence the evaluation outcomes.

Originality/value – By delving into the concept of assurance context, this research seeks to shed light on how it influences the scope, methodologies, and outcomes of assurance evaluations, ultimately enabling organizations to strengthen their system security postures and mitigate risks effectively.

Keyword. System security, security assurance, security evaluation, context model

1. Introduction

In today's interconnected world, Information and Communication Technology (ICT) has become the lifeblood of organizations across various sectors. It facilitates seamless communication, enables efficient operations, and empowers data-driven decision-making. Given the extensive dependence on ICT systems, it is of utmost for organizations to prioritize the adoption of comprehensive security measures to safeguard their ICT systems and maintain a strong security posture. These measures are instrumental in reinforcing defenses and mitigating the potential risks posed by unauthorized access, data breaches, service disruptions, and other harmful cyber incidents. However, the implementation of security measures alone is not sufficient. Organizations must also possess tangible evidence that validates the effectiveness and adequacy of their security implementation (Johnson 2006; Williams 2001). This evidence serves as a testament to the organization's commitment to security and assures stakeholders that appropriate measures are in place to protect valuable information and critical assets.

Security Assurance Evaluation (SAE) has emerged as a valuable approach for organizations to evaluate and ensure the trustworthiness and reliability of their systems (Katt and Prasher 2019). By conducting SAE, organizations can assess whether a system operates correctly and securely, thereby instilling confidence in its functionality and mitigating potential risks (Boyce and Jennings 2002). Specifically, SAE involves evaluating, documenting, and monitoring the security posture of systems to determine whether the implemented security features, practices, procedures, and architecture effectively align with the security objectives before dissemination or delivery to the intended users (Ross 2011). One of the key benefits of SAE is its contribution to regulatory compliance (Ezingeard et al. 2005). Organizations are often required to adhere to specific regulatory requirements, industry standards, and best practices to demonstrate compliance by evaluating their security measures against these benchmarks and identifying any gaps or non-compliance areas that need to be addressed (Hale and Gamble 2019).

In recent years, there has been a significant surge in research efforts dedicated to SAE methodologies (Shukla et al. 2021). This increased focus has led to the development of numerous frameworks, models, and techniques that are specifically designed to assess and enhance the security of systems. These advancements have greatly contributed to the understanding and evaluation of security measures across various domains. However, amidst the progress made, it is important to acknowledge a crucial aspect that is often overlooked in these evaluations—the *Assurance Context* in which evaluation activities are conducted. According to Suchman (Suchman 1987), work is a situated activity and, particularly, it is performed within a context. This implies that all the essential information required for a work process to accomplish its objectives must be encapsulated within the context itself. To have

a complete understanding of actions and events, stakeholders must have access to all the pertinent contextual information associated with those circumstances (Borges et al. 2005; Kwan and Balasubramanian 2003; Santoro and Brézillon 2005).

To enhance the overall effectiveness of SAEs, it is imperative to recognize and incorporate the assurance context into the evaluation methodologies and frameworks utilized during the evaluation process. By recognizing the specific context within which the SAE are conducted, organizations can ensure that their evaluations are comprehensive, accurate, and truly reflective of their security needs and objectives. This paper aims to explore the role of assurance context in system SAEs and proposes a conceptual model that highlights its significance. Our objective is to explore and address the research question: "*What are the principal attributes of the assurance context that define the process of evaluating System Security Assurance?*" By delving into the concept of assurance context, this research seeks to shed light on how it influences the scope, methodologies, and outcomes of system SAEs, ultimately enabling organizations to strengthen their system security postures and mitigate risks effectively.

The rest of this paper is organized as follows. In Section 2, an exploration of the concepts of security assurance evaluation and assurance context is conducted. Section 3 introduces the proposed conceptual model for assurance context. Following that, Section 4 delves into the interconnections between the context model and the assurance evaluation. Finally, the conclusion and future work are presented in Section 5.

2. Background

This section outlines the concepts of SAE and assurance contexts, and their relationships are briefly described. This is the first step towards ensuring reliable communication within this field.

2.1 Security Assurance Evaluation

As suggested by Anderson (Anderson 2020), *Assurance* can be defined as the evaluation of the likelihood of system failure in a specific manner. In the context of security, security assurance can be simply understood as our estimation that the system will remain uncompromised. From a substantive perspective, security assurance encompasses the degree of confidence in satisfying security requirements (Spears et al. 2013). It involves ensuring that the necessary security measures are in place to protect the system from potential threats, vulnerabilities, and attacks. The NIST Special Publication (Ross 2011) provides a formal definition of security assurance as "the measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediate and enforce the security policy" (Page 26). Organizations strive to achieve a high level of security assurance to minimize the risk of security breaches and maintain the integrity and

confidentiality of their systems and data. This paper adopts the definition of security assurance proposed by Katt and Prashe (Katt and Prasher 2019), which views security assurance as an attribute linked to the confidence that system requirements are fulfilled, while vulnerabilities and weaknesses are either tolerated or addressed. The term "evaluation", with this definition, signifies a systematic process that involves assessing the *Security Posture* of a system to determine its overall security status and conditions.

Security assurance evaluation typically follows a systematic approach that encompasses a range of activities, starting from the identification of relevant security policies and standards (Hecker and Riguidel 2009; Jaskolka 2020). These frameworks and methodologies provide a structured framework for conducting assessments, testing, and analysis of the system's security controls and practices. During the evaluation process, emerging threats are taken into consideration, reflecting the dynamic nature of the cybersecurity landscape. Compliance with applicable regulations and industry standards is also assessed to ensure that the system meets the necessary legal and industry requirements (Hale and Gamble 2019). The security assurance evaluation aims to provide an objective and unbiased assessment of the system's security posture by collecting and examining evidence. This involves identifying potential gaps or weaknesses in the security controls, practices, and architecture. Such findings are crucial in enabling stakeholders to make informed decisions regarding the system's security and to allocate resources effectively for risk mitigation (Peltier 2005). The ultimate objective of security assurance evaluation is to drive improvements in the system's security posture (Ouedraogo et al. 2012). Based on the evaluation findings and recommendations, stakeholders can prioritize remediation efforts, implement necessary security enhancements, and allocate resources efficiently to address identified weaknesses. This iterative process ensures that the system's security posture evolves and improves over time, keeping up with the evolving threat landscape and maintaining a strong defense against potential cyber threats (Peltier 2005; Sattarova Feruza and Kim 2007).

2.2 Context and Contextual Information

Context refers to the situation within which something exists or happens, and that can help explain it (CambridgeDictionary). Dey (Dey 2001) defines context as ‘‘any information that can be used to characterize the situation of entities that are considered relevant to the interaction between a user and an application, including the user and the application themselves”. This information set is named contextual information (Abowd et al. 1999). Context provides for two essential processes: on the one hand, it supports the particularization of meanings by restricting the cognitive process of meaning construction, and by eliminating ambiguities or concurrent meanings that do not seem to be adequate at a given moment; on the other hand, context also prevents this particularized meaning from being isolated as it brings about coherence with a larger whole (Van Oers 1998).

Contextual information includes elements such as time, location, historical background, social dynamics, and environmental factors that contribute to the nuances and complexities of a given situation. Contextual information is a crucial component of fully understanding knowledge (Klemke 2000; Brézillon 2002; Jafari et al. 2008). In various disciplines, from communication to problem-solving and analysis, grasping contextual information is essential for avoiding misunderstandings, making informed choices, and effectively addressing challenges (Brézillon 2002). The context can provide a major meaning to knowledge, promoting a more effective comprehension of a determined situation in collaborative work (Brézillon and Araujo 2005). Access to relevant contextual information enables stakeholders to comprehensively understand the work processes, make informed decisions, and effectively respond to the challenges and opportunities that arise (Silva et al. 2012).

3. Related Work

Within this section, we will explore the forefront proposition of methodologies, frameworks, and models that address contextual information in the SAE. Our goal is to create a curated collection of critical concepts concerning assurance contexts in this particular field. Our curation process entails a careful selection and analysis of recent scholarly articles that delve into the integration of contextual factors into SAE.

3.1 Security Assurance Evaluation Framework

During the evaluation of system security, it is a typical practice to consider diverse information security standards and maturity models. These resources provide structured and methodical strategies to progressively improve security practices over time. One of the most representative works is the Common Criteria for Information Technology Security Evaluation (often referred to as Common Criteria or CC) (ISO 2022). The CC is an international standard (ISO/IEC 15408) for the security evaluation of IT products. CC offers a comprehensive framework of guidelines and specifications that can support the definition of security functional requirements and security assurance requirements. By following a strict, standardized, and repeatable methodology, the CC ensures the effective implementation, evaluation, and operationalization of security products by the specific operational contexts they are intended for (Shukla et al. 2022). In the realm of CC, the assessment process of the target of evaluation (TOE) takes into consideration contextual information, including identifying potential security threats, establishing organizational security policies, and making necessary assumptions.

In addition to CC, various researchers have been working on the development of SAE models and frameworks. Valuable insights and contextual information about SAE can be derived from their research contributions. For instance, Deveci et al. (Deveci and Caglayan 2015) have proposed a model-driven security framework that is used for the analysis, design, and evaluation of security properties of information systems. This framework supports

developers and evaluation authorities in implementing the CC assurance process through formal methods based on UML. Katt and Prasher (2019) proposed a general-purpose security assurance framework and its assurance evaluation process. The basic components of the proposed framework included are the assurance scheme, assurance target, assurance metrics, assurance technique, and assurance level. They discussed the advantages of quantitative security assurance metrics considering both the security requirements and vulnerabilities. Villagrán-Velasco et al. (2020) evaluate system security based on threat enumeration and on verifying if these threats are not controlled in specific software architectures. They also consider the effect of policies and the use of weights according to their impact.

3.2 Ontology-Based Conceptual Modeling for Security Assurance Evaluation

Numerous research studies have made attempts to utilize *ontology*-based approaches in the conceptual modeling process for integrating various security assurance concepts and methodologies. The main benefit of the ontology-based model is the availability of a formal, encoded description of the domain knowledge: that is, all the concepts, their attributes, and their inter-relationships will be well-defined and represented (Berners-Lee et al. 2001). Within the field of ontology-based SAE, there exists a considerable body of research literature. Among them, we can highlight several recent papers aimed at modeling security assurance knowledge and security assessment methodologies.

Franco Rosa et al. (2018) have developed a security assessment ontology called SecAOnto, which serves to conceptualize the key knowledge in the field of security assessment. The primary objective is to provide support for security assessment methods that rely on assessment criteria. SecAOnto comprises various core concepts that can be broadly classified into three categories: system assessment, information security, and security assessment. Aman and Khan (2019) presented an ontology-based security model that aims to provide the necessary knowledge to evaluate the security performance of an application specifically in the context of its hosting infrastructure. The ontology consists of three domains: (1) The infrastructure domain contains the necessary vocabulary to set up a virtual operational environment for the target of evaluation, (2) the Testing profile domain is used to define, implement, and execute the test scope, requirements, and specifications, and (3) Security aptitude domain encompasses a list of all the known vulnerabilities that are assigned an impact score using the Common Vulnerability Scoring System (CVSS).

Gonzalez-Gil et al. (2019) proposed a context-based security evaluation ontology (IoTSecEv) to describe the different security preferences of the end-users of an IoT device, based on concerns and interests in different security elements, such as threats, vulnerabilities, security mechanisms or features. In that regard, it is possible to evaluate security from a context-based standpoint in which the different interests and concerns of the uses are properly addressed. In the domain of cloud security, Maroc and Zhang (2019) developed an ontology

(CS-CASEOnto) for cloud services security evaluation, which covered necessary security knowledge and relevant cloud concepts of significance to security measurement. The ontology includes concepts related to the evaluation target, criteria, yardstick reflecting stakeholders' requirements, and the related evaluation activities including data gathering techniques and data synthesis approaches.

In the automobile domain, Shaaban et al. (2019) presented an ontology (OnSecTa) for the security verification and validation process. The model verifies and validates security requirements in a vehicle to assure that these requirements are fulfilled according to the security status, and the actual security goal needs to be achieved. It creates an ontological view of vehicle components and detected potential threats and related security requirements (defined according to Common Criteria – Protection Profile). With logical queries to the ontology, one can determine whether or not the security requirements can handle risks in a vehicle. In addition, Powley et al. (2019) proposed an Evaluation Ontology (EO) that facilitate the modeling of evaluation processes and outcome in automobile industries, specifically for connected vehicles. For dealing with the complex systems of systems that are vulnerable to cyberattacks, it aims to integrate different types of evaluation into a single model for all activities at all levels of all organizations in an enterprise.

Lastly, Doynikova et al. (2020) propose a semantic model for the security evaluation of information systems in which an ontology of security metrics is developed to trace dependencies among available security knowledge sources, available raw security data, and metrics calculated on their base (divided by the security assessment goals) and security assessment goals. The key aspect of ontology is to process huge streams of gathered security-related data (both static, from open-source databases, and dynamic, from security monitoring tools).

Table 1 presents a thorough overview of the significant contextual details discussed in the chosen research paper. We acknowledge that previous research in this area has been limited and fragmented, making it difficult for scholars and practitioners to develop a comprehensive understanding of the assurance context. Hence, this paper seeks to address this research void and bridge the knowledge gap.

Table 1. Contextual information addressed in the SAE frameworks/models

SAE frameworks/models	Contextual information being addressed
Common Criteria (ISO 2022)	The target of evaluation, threat, organizational security policy, threat
Deveci and Caglayan (2015)	Asset, security policy, threat
Katt and Prasher (2019)	assurance target
Villagrán-Velasco et al. (2020)	security policy, threat
Franco Rosa et al. (2018)	Asset, system architecture, risk, scope of assessment, operational environment
Aman and Khan (2019)	Application, infrastructure (host, network, router, configuration), users
Gonzalez-Gil et al. (2019)	Asset, observer, evaluator, interest (security feature, security property, etc.), concern (threat)
Maroc and Zhang (2019)	Target (component, service, model), actor, threat, standards
Shaaban et al. (2019)	Target component, attack, threat, risk, common criteria (protection profile).
Powley et al. (2019)	The system under evaluation, stakeholder, purpose of evaluation (needs), standards (approved methods), environments
Doynikova et al. (2020)	Product, infrastructure (host, network), configuration, attacker

4. Context Modeling for Security Assurance Evaluation

To ensure the evaluation activities remain relevant, effective, and appropriate, SAE should operate within a well-defined boundary and specific parameter, known as the *Assurance Context*. We define the assurance context as the set of circumstances, factors, and conditions that surround and influence the process of security assurance evaluation. When conducting an SAE, the evaluation process takes into account the assurance context to assess the security posture. Figure 1 illustrates how assurance contexts interplay with SAE and security posture. The assurance context helps define the scope and criteria against which the security posture is evaluated. It provides the context-specific information and background necessary to ensure that the evaluation is relevant and targeted to the specific needs. It may include factors such as industry standards, regulations, and organizational-specific requirements, which also influents the choice of methodologies and approaches used in the evaluation process. By considering the context, the evaluation focuses on the specific areas that require attention, providing meaningful evaluation outcomes and recommendations. This facilitates decision-making by helping stakeholders interpret the security posture evaluation results and assess their relevance.

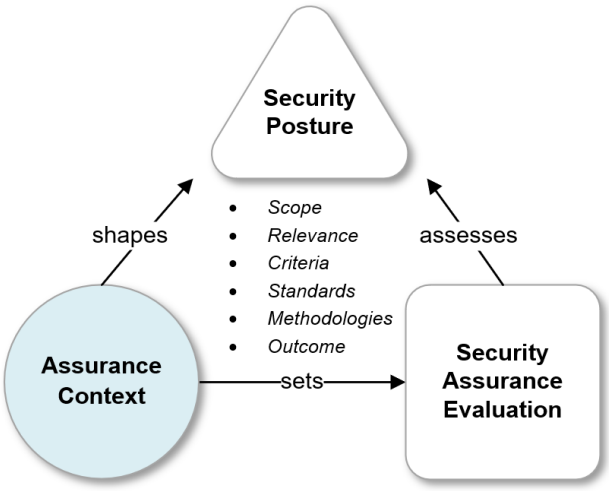

Figure 1. The relationships between the assurance context and assurance evaluation

The purpose of the context model is to encapsulate fundamental terms and concepts related to systems and their environment, providing a preliminary framework for comprehending SAE. In essence, our assurance context model focuses on addressing the following considerations:

Consideration 1: Evaluation Scope

When evaluating a system, it's important to consider the scope and parameters of the evaluation process. This includes understanding boundaries, extent, and any assumptions that may be involved (Jakeman et al. 2006). By doing so, one can determine the areas and components of the system that will undergo assessment, analysis, and validation within the context of the SAE.

Consideration 2: Security Problem

Security problems encompass specific issues, challenges, or areas of non-compliance that jeopardize the security of a system (Herrmann 2002; Kirlappos et al. 2014). They play a crucial role as catalysts, guiding and directing the evaluation process. It is imperative to address these security problems as an integral part of SAE.

Consideration 3: Stakeholder Influence

Stakeholders, with interests in the trustworthiness of the system, exert their influence to shape the activities, outcomes, and decisions of the evaluation process (Jaskolka 2020). Their perspectives, concerns, and requirements significantly impact the evaluation process and the measures taken to ensure the system's security.

Taking into account the aforementioned considerations, we recognize four pivotal elements within the assurance context: system context, assurance assumption, security concern, and

stakeholders. The interconnection between the context consideration and model elements is depicted in Figure 2. The subsequent sections will present an in-depth discussion of each context element.

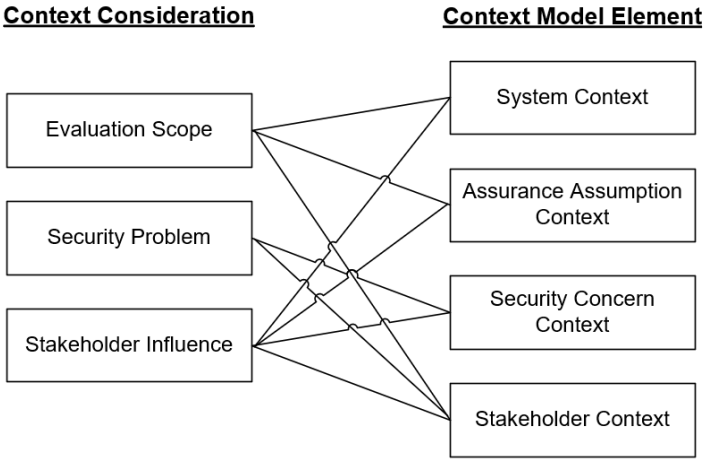

Figure 2. The relationships between the context consideration and model elements

4.1 System Context

In the context of SAE, the system context refers to the broader environment in which the *System of Interest* (SoI) operates, including its relationships, interactions, and dependencies with other entities. In our definition, an SoI is a system that draws interest from a set of stakeholders who want to focus their attention on assessing the system's security measures through the lens of SAE. The system context encompasses the system-wise factors that can influence the security of the system and the risks associated with its operation. Vested in the security and trustworthiness of the system, stakeholders need confidence that their interests are being met.

SoI represents the specific system, software, infrastructure, or network that is being assessed or evaluated for its security. The SoI could range from an entire organization's IT infrastructure to a specific application, device, or component within a larger system. To prevent ambiguity and ensures that the evaluation efforts are directed towards the SoI, it is crucial to take a wide-ranging approach to thoroughly view the system, which is often overlooked in SAE studies. Within this section, we commence by presenting the concept of SoI, which sets forth the groundwork for our proposed model.

Typically, an SoI includes components that have been deliberately subject to environmental influences and other factors within boundaries (e.g., the system boundary), as depicted in Figure 3. The system component is the core subset of SoI, meaning any essential constituent or the source code (in the software-system context) made to perform a specific task(s). The system component is influenced by the environment that it is installed, executed, or operated in. This environment consists of factors or elements that are not intrinsic to the component itself but can affect its behavior.

The system boundary delineates the scope of an SAE and discerns it from the exterior environment. We categorize such external spaces into two distinct subsections: system environment and operational environment. The former is included in the scope of SoI, while the latter is external to the system (depicted in Figure 4). In our definition, a system environment refers to the complete set of hardware and software (tools, resources, systems, and services) that are the necessities to secure build, maintain, and scale the system component. Simple examples of system environments are a hardware environment, a software-based execution environment, or some combination of these. On the other hand, the operational environment is where the SoI operates within and interacts with its components

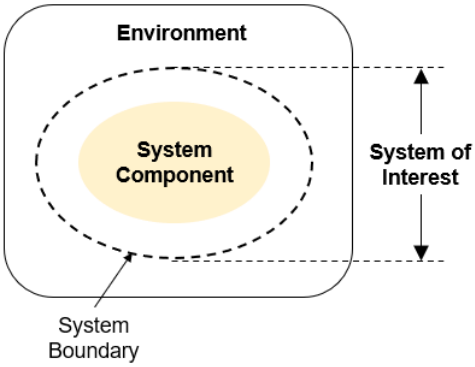

Figure 3. The system boundary of a system of interest

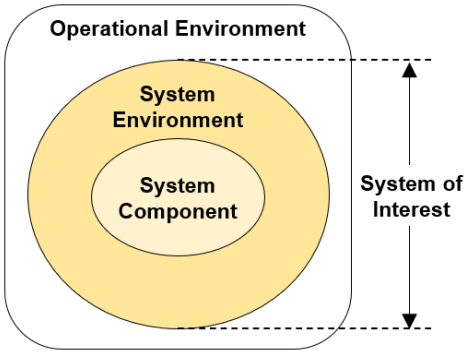

Figure 4. The structure of a system of interest in SAE

and other associated systems, for example, a user, a system administrator, an organization, a LAN, or a general office environment.

To provide a practical demonstration of the proposed system structure, Figure 5 illustrates the structural composition of an SoI with the type of Application Software. This application is designed to offer users a specific set of tasks or functions. It is installed and runs on a platform made up of an operating system and software-based runtime environment. It is optimally deployed within a virtual machine (VM) to create an isolation layer from the underlying hardware. The SoI includes all software that forms part of the application installation package, incorporating any enhancements or modifications to its underlying platform such as drivers in the runtime environment.

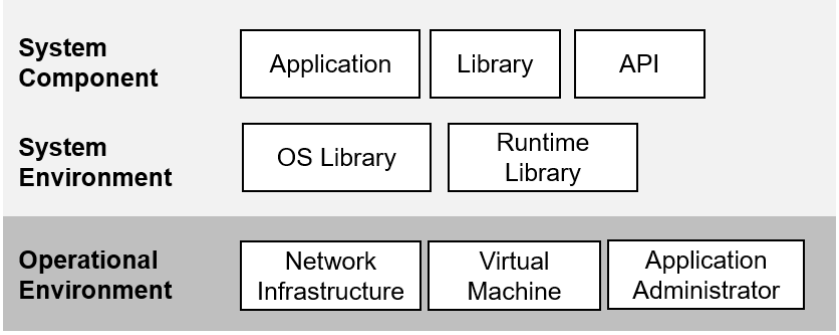

Figure 5. The structural composition of an application-software system

The SoI functions within a network infrastructure that encompasses components such as firewalls, switches, routers, and other networking elements. These components facilitate seamless communication between the application and other parts of the system. The administrator is in charge of access management, system backups, patch management, and system updates. Due to the security evaluation's exclusion of responsibility for security functionality implemented by abstracted platform layers, the network infrastructure, VM, and administrator fall outside the system boundary.

Based on the above definition, a conceptual model visualizing the system context is provided in Figure 6. The system context defines the limits and interactions of the SoI and plays a decisive role in defining the extent and characteristics of system properties. An SoI is comprised of *System Componen*t and *System Environment*, and it is situated within the broader *Operational Environment*, as discussed earlier. It is important for stakeholders who hold an interest in the SoI to briefly describes the usage of the SoI and its major functionalities (i.e., *System Description*), meanwhile, to define the *System Boundary* to provide a clear understanding of the system's context within its environment. *Security Measures* encompass the technical and procedural controls that are put in place to safeguard the SoI components and corresponding systems environments from potential threats. While security measures are

Author Accepted Manuscript version of the paper by Shao-Fang Wen and Basel Katt in Information and Computer Security, DOI: 10.1108/ICS-06-2023-0101

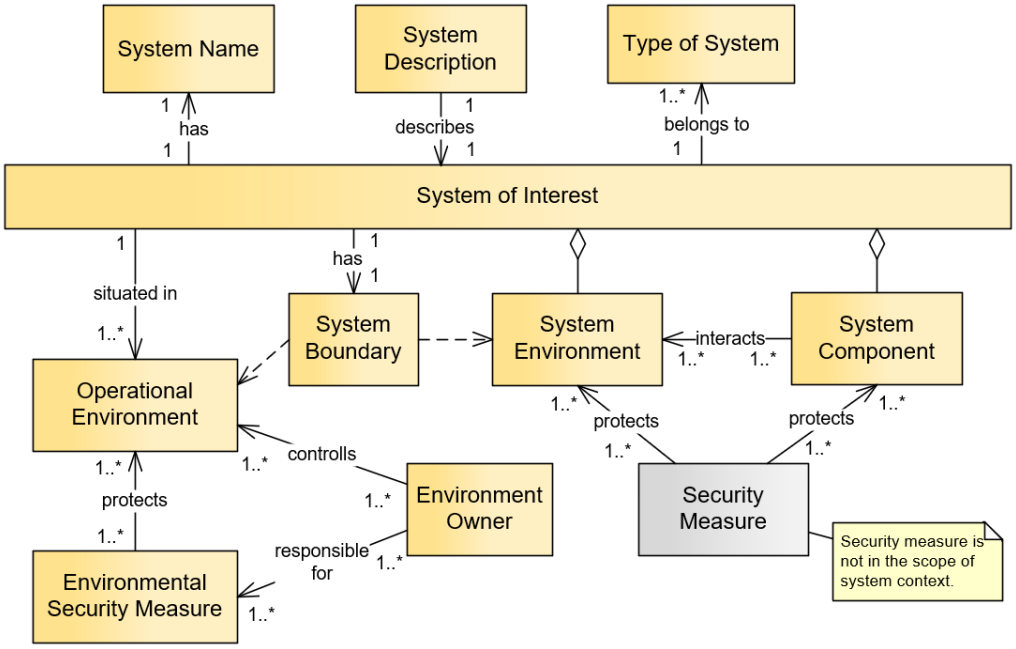

Figure 6. The conceptual model of system context

not explicitly outlined in the assurance context, they will be determined by the assurance context and assessed during the SAE process.

Type of System refers to the categorization based on systems' characteristics, behavior, or structures. Examples of these types of systems are web applications, databases, firewalls, and industrial control systems. By identifying the type of system, stakeholders can tailor their approach and focus on the specific security aspects that are relevant to that type of system. For example, the security considerations for a database will differ from those of a web application or a physical access control system.

The *Environment Owner* is the individual or organization responsible for managing and maintaining the operational environment. They are responsible for implementing and enforcing security policies and procedures, identifying potential threats and risks, and implementing countermeasures (i.e., *Environmental Security Measures*) to mitigate them.

These measures can include physical security measures, such as access control and surveillance, as well as technical measures, such as firewalls, intrusion detection systems, and system backup and recovery. In SAE, these measures are assumed to be true and will not be tested and verified (See Section 3.2 Assurance Assumption).

4.2 Assurance Assumption Context

Assurance Assumption in SAE refers to the explicit statements made about certain conditions, constraints, or factors that are considered to be true for the evaluation. Certain assumptions

Author Accepted Manuscript version of the paper by Shao-Fang Wen and Basel Katt in Information and Computer Security, DOI: 10.1108/ICS-06-2023-0101

may limit the evaluation scope to specific systems or environments. In our model, assurance assumptions are mainly made on the operational environment, considering the SoI boundary, as depicted in Figure 7. The assumption includes the security measures of the environment where the SoI is expected to operate. Table 2 presents the potential assurance assumptions made regarding the operational environments in the SoI.

To provide transparency and communicate any constraint associated with the evaluation, the stakeholder should explicitly formulate the assurance assumptions along with the assurance result. This helps decision-makers understand the context and potential uncertainties surrounding the assurance result. If assumptions utilized in the SAE are incorrect or insufficient, they can lead to inaccurate conclusions about the system's security posture.

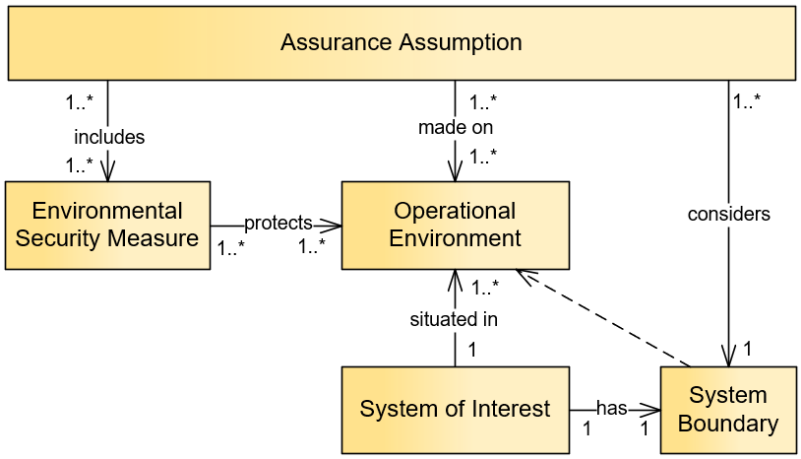

Figure 7. The conceptual model of assurance assumption context

Table 2. Assurance assumptions about the operational environment

Operational environment element	Assumption
Network Infrastructure	It is assumed that strong network measures are built, such as virtual private networks (VPNs), intrusion detection and prevention systems (IDPS), and network segmentation.
Virtual machine	It is assumed that there is a strong isolation between VMs
Application administrator	It is assumed that the administrator is not careless, willfully negligent, or hostile, and administers the application in compliance with the applied enterprise security policy.

4.3 Security Concern Context

Security Concern refers to expressing apprehension, interest, or a sense of responsibility regarding the security aspects of a system. Security concerns can arise from various sources such as experience/historical data, anticipated problems, or organizational requirements.

These concerns must be fully addressed in the evaluation process to provide stakeholders with a higher level of confidence in the system's security posture. Figure 8 illustrates the conceptual model for the assurance assumption context. In our model security concerns are identified by taking into account two key aspects: threat and compliance.

Threat Landscape is the major security concern in the context. Threats refer to potential dangers or hazards that can compromise the security of the SoI. A threat consists of an *Adverse Action* carried out by a *Threat Agent* on an SoI. Threat agents exploit vulnerabilities that exist in the SoI to cause damage or inflict harm to the SoI. One of the goals of SAE is to discover vulnerabilities before threat agents can take advantage of them. Table 3 displays the potential threats to the system of interest, outlining the corresponding threat actors and their adverse actions.

Another essential aspect of security concern is *Compliance Requirements*. In the context of SAE, compliance refers to adherence to relevant laws, regulations, standards, policies, and guidelines about security measures. The compliance concern is aimed at ensuring that the SoI operates within legal and regulatory boundaries and follows industry best practices for security, meanwhile, it helps demonstrate that appropriate security measures are in place to mitigate potential threats. The compliance is formulated and put into action by various *Entities* and results in various compliance frameworks, including Security Regulations, Security Standards, and Organizational Policies.

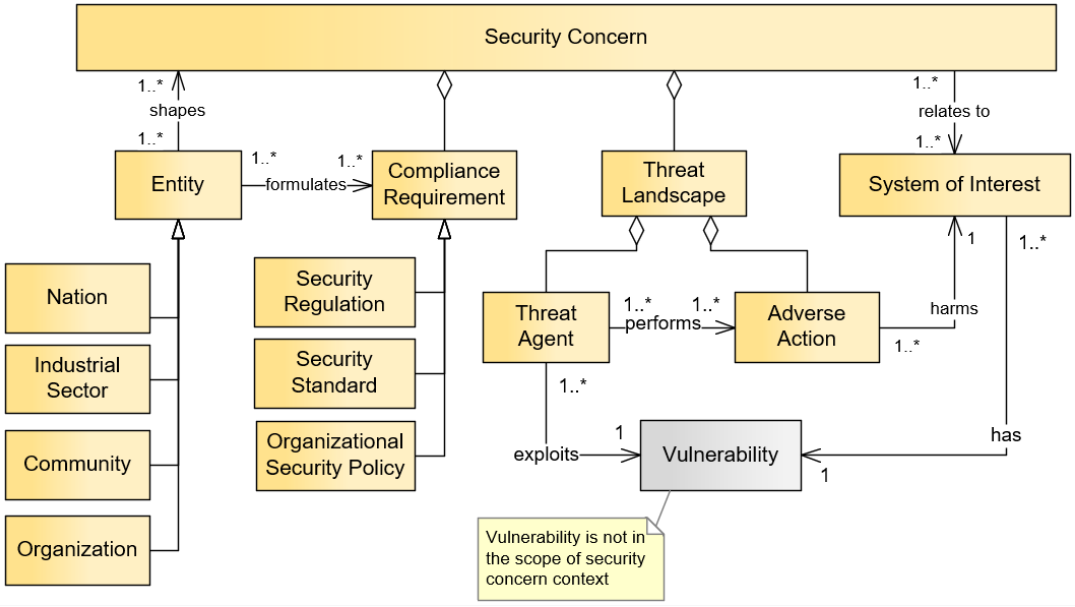

Figure 8. The conceptual model of security concern the context

Table 3. Possible threats to the SoI

Threat	**Threat actors and adverse actions**
Network attack	Attackers may actively engage in communication with the application or manipulate the communication between the application and other endpoints to compromise its security.
Networks eavesdrop	Attackers may monitor and gain access to data exchanged between the application and other endpoints.
Local attack	An attacker can act through unprivileged software running on the same platform as the application. They can potentially provide the application with maliciously formatted input, such as files or other local communications.
Physical access	An attacker may try to access sensitive data at rest.

Security Regulations are legal requirements imposed by governing bodies or regulatory authorities. They are external mandates that organizations must adhere to comply with the law. For example, the General Data Protection Regulation (GDPR) is a comprehensive data protection law implemented by the European Union (EU) to enhance the privacy rights and data security of individuals within the EU. *Security Standards*, on the other hand, are voluntary frameworks or guidelines developed by industry organizations, consortiums, or standards bodies. They provide recommendations, best practices, and requirements for achieving a desired level of security within a specific domain or industry. Examples of security standards include ISO/IEC 27001 for information security management, NIST Cybersecurity Framework, and the OWASP Application Security Verification Standard (ASVS) (OWASP 2021) for web applications. The *Organization Security Policy* is an internal document developed by the organization itself. It is a set of guidelines, rules, and principles that outline the organization's approach to security. It considers factors such as the industry sector, organizational culture, business goals, and the sensitivity of the information being protected. This contextual understanding helps tailor security assurance activities to the specific needs and priorities of the organization. Examples of organizational security policies are access control policies, password policies, and privacy policies.

4.4 Stakeholder Context

Stakeholders in SAE can be defined as individuals, groups, or entities who have a direct or indirect interest in SoI. The assurance context recognizes the expectations and requirements of various stakeholders. It ensures that security assurance activities address the concerns and priorities of these stakeholders and provide the necessary assurances regarding the security of the SoI. Figure 9 presents the conceptual model of the stakeholder context. The stakeholders in security assurance can be classified into three main categories:

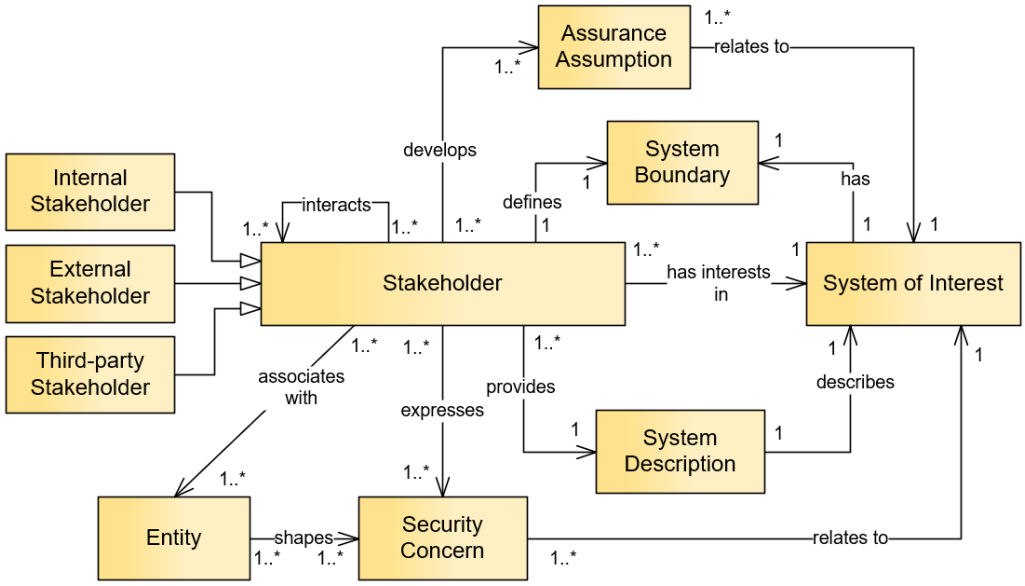

Figure 9. The conceptual model of stakeholder context

- *Internal Stakeholder*: Internal stakeholders are those individuals or groups within the organization that owns or operates the SoI being evaluated. These stakeholders have a direct connection to the system's security and are actively involved in its development, operation, or governance. They have a vested interest in the system depending on their specific roles and interactions with the system. Some examples of internal stakeholders include system developers, system owners, IT staff, security teams, and business units that handle sensitive data.
- *External Stakeholder*: External stakeholders typically refer to individuals, organizations, or entities that have a stake or interest in the SoI being evaluated but are not directly part of the organization that owns or operates the system. These stakeholders provide an external perspective and contribute to the SAE process. Some examples of external stakeholders include customers, partners, suppliers, regulatory agencies, and business partners.
- *Third-party stakeholder*: These stakeholders refer to individuals, organizations, or entities that are external to the organization that owns or operates the system being evaluated but have a direct involvement or influence on its security. Examples include security auditors, consultants, penetration testers, and vendors who provide security-related products or services.

In the context of SAE, stakeholders express significant security concerns that are informed by associated entities. Meanwhile, they define the system boundaries and develop assurance assumptions based on SoI. Stakeholders could also interact with each other in various ways in SAE. These interactions can include communication, collaboration, coordination, and

Author Accepted Manuscript version of the paper by Shao-Fang Wen and Basel Katt in Information and Computer Security, DOI: 10.1108/ICS-06-2023-0101

decision-making. The nature and extent of these interactions depend on the specific stakeholders involved and the objectives of the SAE.

5. Discussion

This section delves into how the assurance context impacts the assurance evaluation. We'll discuss how they are interconnected and how this interrelation can inform ways to assess security posture. By understanding the interconnectedness of these elements, we can gain valuable insights into evaluating security posture effectively. Figure 10 serves as an expanded representation of Figure 1, illustrating the interrelationships between the various context elements, the security posture of the system, and the assessment process.

In this model, the security posture is conceptualized using three elements: security measures, vulnerabilities, and the assurance level currently in place. These elements collectively define the system's overall security readiness. The assurance level reflects the degrees of confidence or trust that stakeholders can have in the system's ability to meet its intended objectives and protect against threats. A strong security posture is characterized by the presence of robust security measures, minimal vulnerabilities, and a higher assurance level.

The assurance context assumes a pivotal role in shaping the security posture of the SoI. The assurance context initially involves the identification of stakeholders participating in the evaluation process and their unique security concerns. The evaluation considers these concerns, guaranteeing that the assessment effectively addresses the pertinent security

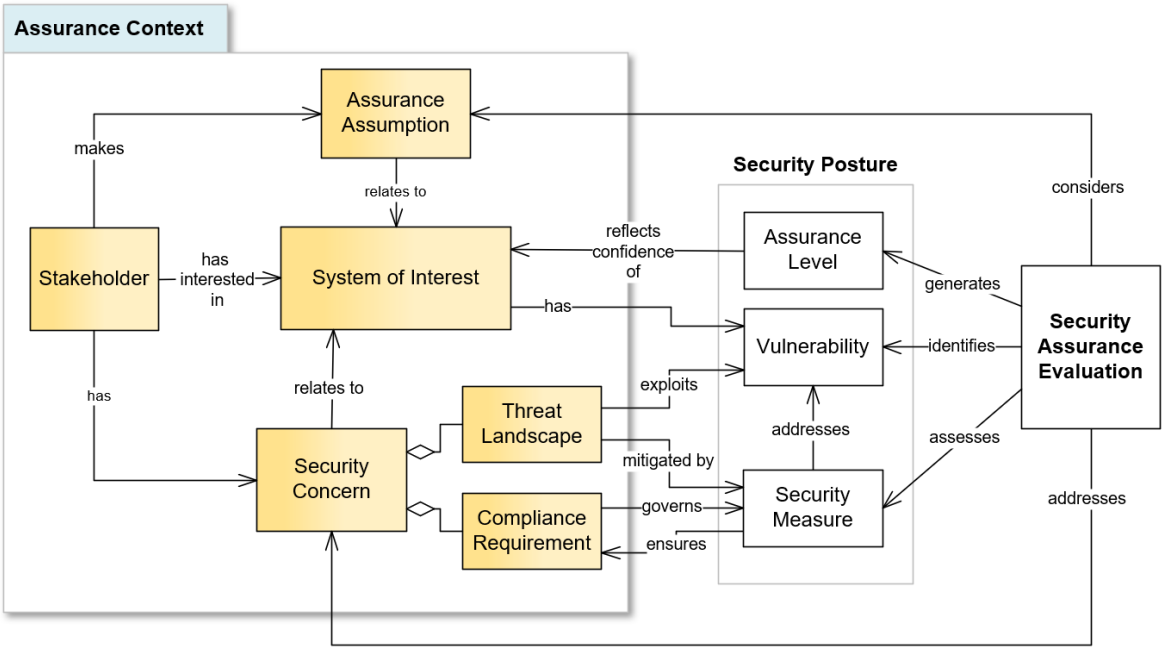

Figure 10. Interconnection between the assurance context, security posture, and the evaluation process

requirements, priorities, and expectations of the stakeholders. Moreover, the implementation of security measures is guided by these security concerns, which, in turn, are influenced by established standards and regulations. These standards and regulations provide a framework for determining the minimum level of security measures required. Organizations must provide security for their systems and meet the industry's standards. Compliance requirements are the guidelines that help stakeholders make sure they are meeting their security obligations and remaining compliant. By understanding and adhering to compliance requirements, organizations can ensure they are taking steps toward providing a secure system and avoiding potential risks. In this regard, the assurance context acts as a guiding principle in establishing the appropriate level of security measures to be implemented, providing a comprehensive and context-specific approach to security assurance.

In addition, SAE involves assessing the effectiveness of the implemented security measures in addressing the identified threats (Herrmann 2002). By thoroughly analyzing and understanding various threats, stakeholders can identify the specific vulnerabilities that need to be addressed. This knowledge allows them to design and implement appropriate security measures that directly target these vulnerabilities, effectively mitigating the associated threats. Such integration of the threat landscape into the assurance evaluation and analysis process enables organizations to prioritize their security efforts and allocate resources more effectively, thereby maximizing the effectiveness of their security measures.

Furthermore, assurance evaluation operates within the established boundary set by the assurance context and adheres to specific parameters outlined in the assurance assumption. Defining the system boundary enables stakeholders to determine the dependencies and interactions between the system and its external environments, meanwhile helping delineate the areas of responsibility, ownership, and accountability within the system. This ensures that the evaluation activities remain relevant and appropriate in addressing the security concerns of stakeholders. Based on the information, requirements, and considerations provided by the assurance context, assurance evaluation gathers the assurance evidence, generates the data and findings, meanwhile, interprets and analyzes that data to extract meaningful information. The insights derived from the assurance evaluation provide stakeholders with a clear understanding of the confidence level in the system's security posture. These insights serve as a foundation for informed decision-making processes, guiding stakeholders in determining the appropriate actions to enhance the security posture.

6. Limitations

While assurance context modeling holds promise for enhancing the accuracy and relevance of SAE, it's essential to acknowledge and address potential research limitations that could impact the effectiveness and applicability of the model. These limitations provide insights

into the boundaries and challenges associated with implementing assurance context modeling:

Complex and Dynamic Nature of Context: The complexities and nuances of real-world situations in the context of SAE can pose challenges when it comes to drawing broad conclusions or implementing the model in various industries or sectors. Additionally, with the continuous advancements in technology, changes in regulations, and shifts in the market, the proposed 'static' assurance context model may face challenges in adapting to rapid changes. Developing a model that comprehensively captures this complexity and dynamics might be challenging, leading to oversimplification or the omission of critical contextual factors. Additionally, the crucial contextual factors and their interrelationships were identified and synthesized through the literature review, combined with a subjective comprehension of context modeling within the realm of security assurance. Different stakeholders might have varying opinions about what constitutes relevant context, which can introduce bias and inconsistencies. To ensure accuracy and validity, it is crucial to engage in thorough review activities and iterative practices for the modeling approach.

Real-world Application/Framework Integration: While the model may seem promising in theoretical scenarios, its practical implementation could face unforeseen obstacles and unpredictable variations that are exceedingly challenging to foresee and account for during the validation process. Context models serve to provide a deeper understanding of the environment in which security measures are implemented, considering various factors such as system infrastructure, security threats, and organizational context. By integrating this model with established SAE frameworks, organizations aim to enhance their overall security posture. However, this integration requires careful consideration and analysis to ensure harmony between the different components. In some cases, there may be conflicts between the assumptions made by the context models and the existing SAE frameworks. Therefore, organizations must undertake a thorough assessment and alignment process to mitigate any potential inconsistencies or redundancies resulting from the integration of the context model with established security frameworks, methodologies, and compliance standards.

7. Conclusion

This paper focuses on the concept of assurance contexts in security assurance evaluation (SAE). Additionally, a conceptual model of assurance context is presented. This model highlights the importance of considering multiple dimensions of the assurance context during SAEs. These dimensions encompass aspects such as system boundaries, stakeholders, security concerns, assurance assumptions, as well as other pertinent factors that can significantly impact the evaluation outcomes. Furthermore, considerations such as regulatory compliance, industry-specific requirements, and the evolving threat landscape should be given due attention when assessing the security posture of a system. By introducing the proposed conceptual model, this research has provided a framework for incorporating the assurance context into SAEs. By incorporating these dimensions into the evaluation process,

organizations can achieve a more comprehensive and accurate understanding of the security landscape and make informed decisions to bolster their overall security measures.

Through this research, we aim to contribute to the advancement of system SAE methodologies and empower organizations to strengthen their system security postures in an ever-changing threat landscape. By exploring the role of assurance context, we strive to provide valuable insights that enable organizations to conduct more effective and relevant system SAEs. Considering the assurance context is not just a recommended practice but an essential aspect of conducting thorough and meaningful security evaluations. By taking into account the unique circumstances, requirements, and objectives of the organization, the evaluation process can be aligned to address the specific concerns and priorities at hand. Neglecting the assurance context, on the other hand, can result in incomplete or inaccurate evaluations, overlooking critical insights, and compromising the effectiveness of security measures. Therefore, embracing the assurance context as an integral part of the evaluation process enhances the overall quality and value of security assessments.

7.1 Implications for future research

The introduction of the proposed assurance context model in the realm of security assurance evaluations holds profound implications for future research endeavors. The main theoretical contribution of this paper is the development of a comprehensive conceptual framework for assurance context modeling in the domain of security assurance. This framework can be viewed as a "sensitizing device" (Klein and Myers 1999) allowing researchers and practitioners to examine the world from a specific perspective and enhancing conceptual clarity in discussions about context management. As organizations strive to enhance their cybersecurity posture by considering a broader spectrum of contextual factors, several key research directions emerge.

Firstly, there is a pressing need for comprehensive model validation and refinement across diverse industries and organizational scales. |Given that assurance context plays a crucial role in SAE, it is essential to understand how organizations can enhance their capabilities for the security evaluation process. While this paper has provided some insights into the challenges involved, it also acknowledges the need for further research to expand the empirical evidence base necessary to analyze and evaluate improvement efforts in this area. With a stronger empirical foundation, organizations can gain a deeper understanding of how to enhance their capabilities for SAE and improve their overall security practices.

Another research direction is to explore the development of automated tools or software solutions that can assist evaluators in integrating the assurance context into their evaluations. Context is dynamic, and automated tools can ensure that the assurance context model remains up to date. These tools can monitor changes in regulations, industry trends, and internal

factors, automatically updating the model to reflect the evolving context. This real-time synchronization helps evaluators consistently consider the most current contextual factors. Such automated tools can also generate context-specific recommendations based on assessment outcomes. These recommendations align security measures with the organization's context and provide evaluators with structured guidance to facilitate the identification and incorporation of the assurance context factors into the evaluation.

Furthermore, the absence of quantitative evaluation methods in security assurance presents an opportunity for further research (Shukla et al. 2022). A research frontier lies in the quantification of the influence of different contextual factors on security outcomes. Devising methods to objectively measure the impact of context could revolutionize resource allocation decisions and risk management strategies. This entails not only considering qualitative elements but also incorporating quantitative data, thus providing organizations with a more data-driven approach to addressing security vulnerabilities. By addressing these implications for further research, the cybersecurity community can significantly advance the field, paving the way for more tailored, efficient, and adaptive security assurance practices that mirror the intricate realities of today's complex assurance contexts.

Conflict of interests: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding. The Research Council of Norway financially supports this research work through the SFI-Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS, NFR project number: 310105).

Reference

Abowd, Gregory D, Anind K Dey, Peter J Brown, Nigel Davies, Mark Smith, and Pete Steggles. 1999. "Towards a better understanding of context and context-awareness." In *Handheld and Ubiquitous Computing: First International Symposium, HUC'99 Karlsruhe, Germany, September 27–29, 1999 Proceedings 1*, 304-07. Springer.

Aman, Waqas, and Fazlullah Khan. 2019. "Ontology-based dynamic and context-aware security assessment automation for critical applications." In *2019 IEEE 8th Global Conference on Consumer Electronics (GCCE)*, 644-47. IEEE.

Anderson, Ross. 2020. *Security engineering: a guide to building dependable distributed systems* (John Wiley & Sons).

Berners-Lee, Tim, James Hendler, and Ora Lassila. 2001. 'The semantic web', *Scientific american*, 284: 28-37.

Borges, Marcos RS, Patrick Brézillon, Jose Alberto Pino, and J -Ch Pomerol. 2005. "Groupware system design and the context concept." In *Computer Supported*

Cooperative Work in Design I: 8th International Conference, CSCWD 2004, Xiamen, China, May 26-28, 2004. Revised Selected Papers 8, 45-54. Springer.

Boyce, Joseph, and Daniel Jennings. 2002. *Information assurance: Managing organizational IT security risks* (Butterworth-Heinemann).

Brézillon, Patrick. 2002. "Modeling and using context: Past, present and future." In *Rapport de recherche interne LIP6*. Paris.

Brézillon, Patrick, and Renata Araujo. 2005. 'Reinforcing shared context to improve collaboration', *Revue des Sciences et Technologies de l'Information-Série RIA: Revue d'Intelligence Artificielle*, 19: 537-56.

CambridgeDictionary. 'context', Accessed May. 3, 2023. https://dictionary.cambridge.org/dictionary/english/context.

Deveci, Engin, and Mehmet U Caglayan. 2015. 'Model driven security framework for software design and verification', *Security and Communication Networks*, 8: 2768-92.

Dey, Anind K 2001. 'Understanding and using context', *Personal ubiquitous computing*, 5: 4-7.

Doynikova, Elena, Andrey Fedorchenko, and Igor Kotenko. 2020. 'A semantic model for security evaluation of information systems', *Journal of Cyber Security and Mobility*: 301–30-01–30.

Ezingeard, Jean-Noël, Elspeth McFadzean, and David Birchall. 2005. 'A model of information assurance benefits', *Information Systems Management*, 22: 20-29.

Franco Rosa, Ferrucio de, Mario Jino, and Rodrigo Bonacin. 2018. 'Towards an ontology of security assessment: a core model proposal.' in, *Information Technology-New Generations* (Springer).

Gonzalez-Gil, Pedro, Antonio F Skarmeta, and Juan Antonio Martinez. 2019. "Towards an ontology for iot context-based security evaluation." In *2019 Global IoT Summit (GIoTS)*, 1-6. IEEE.

Hale, Matthew L, and Rose F Gamble. 2019. 'Semantic hierarchies for extracting, modeling, and connecting compliance requirements in information security control standards', *Requirements engineering*, 24: 365-402.

Hecker, Artur, and Michel Riguidel. 2009. "On the operational security assurance evaluation of networked IT systems." In *Smart Spaces and Next Generation Wired/Wireless Networking: 9th International Conference, NEW2AN 2009 and Second Conference on Smart Spaces, ruSMART 2009, St. Petersburg, Russia, September 15-18, 2009. Proceedings*, 266-78. Springer.

Herrmann, Debra S. 2002. *Using the Common Criteria for IT security evaluation* (CRC Press).

ISO. 2022. 'ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security ', Accessed May. 3, 2023. https://www.iso.org/standard/72891.html.

Jafari, Mostafa, Mohammad Fathian, Alireza Jahani, and Peyman Akhavan. 2008. 'Exploring the contextual dimensions of organization from knowledge management perspective', *VINE*, 38: 53-71.

Jakeman, Anthony J, Rebecca A Letcher, and John P Norton. 2006. 'Ten iterative steps in development and evaluation of environmental models', *Environmental modelling & software*, 21: 602-14.

Jaskolka, Jason. 2020. "Recommendations for effective security assurance of software-dependent systems." In *Intelligent Computing: Proceedings of the 2020 Computing Conference, Volume 3*, 511-31. Springer.

Johnson, Everett C. 2006. 'Security awareness: switch to a better programme', *Network Security*, 2006: 15-18.

Katt, Basel, and Nishu Prasher. 2019. 'Quantitative security assurance.' in, *Exploring Security in Software Architecture and Design* (IGI Global).

Kirlappos, Iacovos, Simon Parkin, and M Angela Sasse. 2014. "Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security." In.

Klein, Heinz K, and Michael D Myers. 1999. 'A set of principles for conducting and evaluating interpretive field studies in information systems', *MIS quarterly*: 67-93.

Klemke, Roland. 2000. "Context Framework - an Open Approach to Enhance Organisational Memory Systems with Context Modelling Techniques." In *Proceedings of the Third International Conference on Practical Aspects of Knowledge Management (PAKM2000), 30-31 October 2000*. Basel, Switzerland.

Kwan, M Millie, and P Balasubramanian. 2003. 'KnowledgeScope: managing knowledge in context', *Decision support systems*, 35: 467-86.

Maroc, Sarah, and Jian Biao Zhang. 2019. "Context-aware security evaluation ontology for cloud services." In *2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, 1012-18. IEEE.

Ouedraogo, Moussa, Djamel Khadraoui, Haralambos Mouratidis, and Eric Dubois. 2012. 'Appraisal and reporting of security assurance at operational systems level', *Journal of systems and software*, 85: 193-208.

OWASP. 2021. 'Application Security Verification Standard (ASVS)', Accessed Jun. 3, 2022. https://owasp.org/www-project-application-security-verification-standard/.

Peltier, Thomas R. 2005. *Information security risk analysis* (CRC press).

Powley, Stephen, Simon Perry, Jon Holt, and Jeremy Bryans. 2019. "An Evaluation Ontology Applied to Connected Vehicle Security Assurance." In *INCOSE International Symposium*, 37-52. Wiley Online Library.

Ross, Ronald S. 2011. 'Managing information security risk: Organization, mission, and information system view'.

Santoro, Flávia Maria, and Patrick Brézillon. 2005. "Developing shared context within group stories." In *Groupware: Design, Implementation, and Use: 11th International Workshop, CRIWG 2005, Porto de Galinhas, Brazil, September 25-29, 2005. Proceedings 11*, 232-47. Springer.

Sattarova Feruza, Y, and Tao Hoon Kim. 2007. 'IT security review: Privacy, protection, access control, assurance and system security', *International journal of multimedia and ubiquitous engineering*, 2: 17-32.

Shaaban, Abdelkader Magdy, Christoph Schmittner, Thomas Gruber, A Baith Mohamed, Gerald Quirchmayr, and Erich Schikuta. 2019. "Ontology-based model for automotive security verification and validation." In *Proceedings of the 21st International Conference on Information Integration and Web-based Applications & Services*, 73-82.

Shukla, Ankur, Basel Katt, Livinus Obiora Nweke, Prosper Kandabongee Yeng, and Goitom Kahsay Weldehawaryat. 2021. 'System Security Assurance: A Systematic Literature Review', *arXiv preprint arXiv:2110.01904*.

Shukla, Ankur and Basel Katt. 2022. 'System security assurance: A systematic literature review', *Computer Science Review*, 45: 100496.

Silva, Douglas Machado, Renata Mendes de Araujo, Flávia Maria Santoro, and Gabriel Alonso Peña Pascual. 2012. "Defining context in a business process collaborative elicitation approach." In *Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, 861-68. IEEE.

Spears, Janine L, Henri Barki, and Russell R Barton. 2013. 'Theorizing the concept and role of assurance in information systems security', *Information & Management*, 50: 598-605.

Suchman, Lucy A. 1987. "PLANS AND SITUATED ACTIONS: The problem of Human-Machine Communication." In.: Cambridge University Press.

Van Oers, Bert. 1998. 'From context to contextualizing', *Learning and instruction*, 8: 473-88.

Villagrán-Velasco, Olga, Eduardo B Fernández, and Jorge Ortega-Arjona. 2020. "Refining the evaluation of the degree of security of a system built using security patterns." In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 1-7.

Williams, Paul. 2001. 'Information security governance', *Information security technical report*, 6: 60-70.