Received 27 November 2021
Revised 30 July 2022
4 February 2023
9 April 2023
11 June 2023
Accepted 12 June 2023

Information security awareness maturity: conceptual and practical aspects in Hungarian organizations

Andrea Kő
*Institute of Data Analytics and Information Systems,
Corvinus University of Budapest, Budapest, Hungary*
Gábor Tarján
Magicom, Budapest, Hungary, and
Ariel Mitev
*Institute of Data Analytics and Information Systems,
Corvinus University of Budapest, Budapest, Hungary*

Abstract

Purpose – This paper aims to provide a maturity model for information security awareness (MMISA), based on the literature, expert interviews and feedback. In addition to developing the MMISA, the authors investigate the role of the three decisive factors that affect ISA maturity level: risk management mechanism, organizational structure and ISA.

Design/methodology/approach – The research methodology is a combined one; qualitative and quantitative methods were applied, including surveying the literature, interviews and developing a survey to collect quantitative data about decisive factors that affect ISA maturity level. The authors perform a variance-based partial least squares-structural equation modeling (PLS-SEM) investigation of the relationships between these factors.

Findings – The investigation of decisive factors of ISA maturity levels revealed that if the authors identify a strong risk assessment mechanism (through a documented methodology and reliable results), the authors can expect a high level of ISA. If there is a well-defined organizational structure with clear responsibilities, this supports the linking of a risk management mechanism with the level of ISA. The connection between organizational structure and ISA maturity level is supported by ISA activities: an increased level of awareness actions strengthens an organizational structure via the best practices learned by the staff.

Originality/value – The main contribution of the proposed MMISA model is that the model offers controls and audit evidence for maturity levels. Beyond that, the authors distinguish in the MMISA model controls supporting knowledge and controls supporting attitude, emphasizing that this is not enough to know what to do, but the proper attitude is required too. The authors didn't find any other ISA maturity model which has a similar feature. The contribution of the authors' work is that the authors provide a method for solving this complex measurement problem via the MMISA, which also offers direct guidance for the daily practices of organizations.

Keywords Information management, Security, Risk, Structural equation modeling, Audit, Capability maturity model (CMM)

Paper type Research paper

1. Introduction

Increasing information security awareness (ISA) and knowledge of its maturity measurement are key components of creating an information security culture (AlGhamdi *et al.*, 2020;

Information Technology & People
Vol. 36 No. 8, 2023
pp. 174-195
Emerald Publishing Limited
0959-3845
DOI 10.1108/ITP-11-2021-0849

AlMindeel and Martins, 2020; Bulgurcu *et al.*, 2010; Siponen, 2000; Tam *et al.*, 2022). A proper security culture is the main means of protecting an organization's information and assets (Da Veiga and Martins, 2015). Reliably measuring an enterprise's level of information security awareness (ISA) is critical, as information assets and their protection are becoming increasingly important. This is at once a competitiveness issue, on one hand, and, on the other hand, a compliance criterion that is mandated by numerous international standards and regulations for profit-seeking and non-profit organizations (see, e.g. HIPAA, 1996; GLBA, 1999; PCI DSS, 2016; ISO 27001, 2013 and other standards). Most information security and other incidents are due to human error, negligence or intent, which we can best prevent through suitable ISA. For this reason, it is a key interest for the managers of enterprises to increase this awareness at the individual and organizational levels. However, there is no common understanding of ISA, its maturity or its decisive factors. Information security maturity is discussed in previous literature by several researchers (Greene *et al.*, 2022; Lopez-Leyva *et al.*, 2020; Nasir *et al.*, 2019; Schmitz *et al.*, 2021), but ISA maturity requires further study (Fertig *et al.*, 2020). We found only one article and one conference paper in Scopus with the "information security awareness maturity" keyword search.

This paper aims first to analyze the decisive factors of ISA maturity levels with a variance-based structural equation model. The second goal is to provide an ISA maturity framework – the maturity model for information security awareness (MMISA). The main contribution of the MMISA model is that it offers controls and audit evidence for maturity levels. Beyond that, we distinguish in the MMISA model controls supporting knowledge and controls supporting attitude, emphasizing that it is not enough to know what to do, but the proper attitude is required too. The MMISA model details five maturity levels, with the relevant controls and audit evidence providing valuable practical and theoretical support for Information Technology (IT) auditors and Information Systems (IS) managers to assess the ISA maturity of their company. We didn't find any other ISA maturity model which has a similar feature. The contribution of our work is that we provide a method for solving this complex measurement problem, and our MMISA offers direct support for the daily security and IT audit practices of organizations. The MMISA model is based on the literature review and the experiences of expert teams (IT auditors and IS managers). We involved the members of the Hungarian Information Security Community in MMISA model validation and testing (members of the Budapest Chapter of ISACA (Information Systems Audit and Control Association) and other IS associations, bodies or authorities). A total of 122 respondents evaluated the MMISA model; their feedback was positive regarding the application of the model in ISA maturity assessment.

This article first presents a theoretical background, including the hypotheses formulation regarding the decisive factors of ISA maturity levels and the corresponding relationship model. Section three details the research method and steps. Section four discusses the results of the quantitative analysis and hypotheses testing with PLS-SEM related to the relationship model. The following section provides an overview of the proposed maturity model, MMISA. The final section is the conclusion.

2. Theoretical background

2.1 Information security awareness

ISA is a topic of interest in the literature; several previous studies (Greene *et al.*, 2022; AlMindeel and Martins, 2020; van der Schyff and Flowerday, 2021; Stefaniuk, 2020; Lebek *et al.*, 2014; Parsons *et al.*, 2014; Bulgurcu *et al.*, 2010; Sasvári *et al.*, 2015; Maqousi *et al.*, 2013; Siponen, 2000) investigate ISA and its related challenges. "Information security awareness" keyword search results in 188 articles in Scopus on the 29th of July 2022. Most of the papers (153) were published in the previous ten years, and there is a rapidly growing research interest in ISA. There is no commonly accepted definition for ISA. Safa *et al.* (2015) approach ISA as the perception and the information security-related knowledge that the employees may hold, knowing what kind of behaviors and attitudes are dangerous. Tam *et al.* (2022) investigate the impact of poor or non-existing security awareness and/or the lack of job satisfaction and have used a combined model of the congruence model, the theory of planned behavior model and the security behavior concept. They prove that ISA is decisive and influential and companies should invest in promoting security behaviors. Maqousi *et al.* (2013) discusses ISA from a process-oriented view as an ongoing process of learning that results in behavioral change. Lebek *et al.* (2014) draws attention to the fact that effective security awareness programs (SAPs) depend on several behavioral influencing factors. Nemeslaki and Sasvári (2015) differentiate between and discuss the three dimensions of ISA: the organizational, infrastructural and individual dimensions. Siponen (2000) begins his study by reconfiguring the doctrines of awareness into a framework via their parts. Jaeger (2018) details the antecedents and outcomes of ISA.

Individual antecedents, which originate from employees' organizational antecedents, are the policies, procedures and information security communications that can influence individual behaviors. Social-environmental antecedents originate from individuals' interactions with their social environments. Technological antecedents are the factors represented by the technologies used by individuals. The outcomes are beliefs, which are formed by perceived responses, sanctions and their severity, personal norms and attitudes, behavioral intentions and actual behaviors. Based on these inputs and outputs, Jaeger (2018) provides an integrated framework for studying ISA, emphasizing the roles of organizational factors and knowledge (training). The greatest threat to IS security is the human user; the investigation of IS security is emphasized in recent studies by both academic and industry researchers (Tam *et al.*, 2022; Jansson and von Solms, 2013). Several studies discuss ISA from a user perspective (Zhao *et al.*, 2010; Jansson and von Solms, 2013). Soomro *et al.* (2016) argue that information security management (ISM) needs a more holistic approach based on their literature review. They indicate that awareness has a significant impact on the quality of management of information security. Diesch *et al.* (2020) suggest a comprehensive model of management success factors (MSFs) for information security decision-makers, in which awareness has a direct impact on information security. Based on our literature review and the identified conceptual gaps, we define ISA by emphasizing the most important layers of it: *ISA is the knowledge and attitude of interested parties of an organization regarding the protection of information assets that are owned or managed by the organization.* Our definition of ISA covers a wide range of interested parties who can influence ISA status in an organization (i.e. we also expect a level of ISA among our clients in the finance sector because the following best practice has a great impact on the security status of a financial institution: password management and secure PIN usage by card holders). Knowledge is a key component of the definition, defined as a crucial understanding of the rules, procedures and instructions related to ISA; however, we emphasize that this type of knowledge does not provide a direct, active defense for information assets. In this context, knowledge also involves those skills that provide the ability to complete the actions required by an existing control in an organization. Attitude has a decisive role in ISA as well; it entails an active and positive approach to security-related controls and countermeasures. People must understand not only what to do and why an action is correct, but also why they need to be actively involved in preventive and corrective actions. They report suspicious activities they observe, they are involved in backup and recovery activities and they follow the rules and actively advise each other when there are unexpected challenges. The ownership of the information (owned or managed information assets) is important but it is not the only factor determining ISA. The current era of data processing typically creates a situation where the processor is responsible for information security-related issues, but the data at risk are owned by someone else (e.g. cloud technologies or any agencies responsible for data processing). These special cases have a serious impact on the ISA programs and campaigns completed by relevant organizations. To prevent personal conflicts generated by audit events, professional auditors must provide a realistic picture of ISA at the organizational level rather than the individual level. This person-neutral approach has some benefits for every party because individuals are not accused or punished based on IS audit statements. An auditor does not violate any ethical standard of auditing, and the company receives a holistic picture of its ISA status (as an organization). Additionally, managers obtain a clear picture of missing or malfunctioning controls and/or areas for improvement. There are several conflicting research opinions about the decisive factors of the maturity level of ISA; in the next section, we discuss the role of risk management and organizational structure in more detail.

2.2 Risk management and organizational structure

Risk management is defined as the coordinated activities to direct and control an enterprise regarding risk (ISACA, 2020); we apply this definition. According to several studies, guidelines and standards, a risk-based approach should be the principal mechanism organizations use to manage information security (ISACA, 2017; Peltier, 2001; Fletcher *et al.*, 1995). Risk management is a key component of the IT governance framework suggested by ISACA (2017). The more risk management mechanisms are implemented in organizations, the more likely it is that organizations will have a higher level of ISM (ISACA, 2017; Dzazali and Zolait, 2012). Risk management is one of the core functions of ISM systems (Hong *et al.*, 2003). ISACA uses its RiskIT approach to facilitate risk management activities in organizations, while the latest version of Control Objectives for IT and Related Technology (COBIT) emphasizes risk management, both as a process model and as a holistic framework. Diesch *et al.* (2020) propose a comprehensive model of relevant MSFs for organizational information security. Risk assessment is the main element in building an information security culture (AlGhamdi *et al.*, 2020) and is, therefore, a key factor in protecting an organization's information and assets (Da Veiga and Martins, 2015). Risk is positioned as a basic input for security management by Diesch *et al.* (2020). Wangen (2017) compare several risk assessment methods to a specific framework called the core unified risk framework (CURF). They focus on risk assessment in their study and assume that risk management influences information security. Dzazali and Zolait (2012) discuss how organizational structure is a supportive environment for information security. In an ideal situation, organizational structure facilitates individual involvement and increased management participation and, therefore, directly impacts information security. Diesch *et al.* (2020) point out that organizational factors influence information security. They define organizational factors as the properties of an organization that influence its security. We apply this definition. Several authors describe the impact of organizational factors, such as organization identification, organization size, industry type or the internal structure and external framework of an organization, on information security (Tam *et al.*, 2022; ISACA, 2019; Hong *et al.*, 2003; Dzazali and Zolait, 2012; Diesch *et al.*, 2020). Based on the literature review in this section and our experiences related to risk assessments of information security, we establish the following three hypotheses on risk management:

H1. Risk management has a positive impact on organizational structure.

H2. Risk management has a positive impact on ISA.

H3. Risk management has a positive impact on the maturity level of ISA.

Examining the influencing role organizational structure plays in ISA and in the ISA maturity of an organization, we establish two hypotheses on organizational structure:

H4. Organizational structure has a positive impact on ISA.

H5. Organizational structure has a positive impact on the maturity level of ISA.

2.3 Measuring ISA: an overview of maturity models

Regarding our focus on measuring the level of ISA, there is an established basis and conceptual background for completing this task: several maturity models provide maturity grades, defining improvement paths for organizations. The ISA capability model (ISACM) is strongly control-based, and previous research examines ISO/IEC 27002 from the view of ISA (Poepjes and Lane, 2012). Three identified dimensions of awareness are affected by the controls in the referred standard. Awareness importance refers to how important or influential awareness is in the successful and correct functioning of a process or control. Awareness capability refers to how capable a person is when confronted by a decision and awareness risk; a gap that results when the required amount of awareness (awareness importance) is greater than the awareness that is actually displayed (awareness capability). In the model, these three dimensions are linked to the controls required by the ISO/IEC standard. As a part of the model, the stakeholder groups are also identified and linked to controls. The user awareness maturity model (UAMM) assesses IT users through five grades (Kruse and Pankey, 2010), from a blissfully unaware (grade 1) status to a competent and practiced (grade 5) one. The UAMM uses two dimensions for placing individuals into the appropriate grade of maturity (Kruse and Pankey, 2010). It assesses user behavior according to a user's level of discretion (first dimension) and allows for more flexibility for user behaviors as user maturity increases. The second dimension involves actors according to their knowledge and motivations. The UAMM defines maturity levels as related to people, and its approach strengthens our commitment to using additional dimensions while modeling ISA maturity. Previous studies discuss only IT staff ("IT user") when they refer to an organization's personnel. We suggest that ISA is not only related to those individuals who work directly with IT assets or equipment. We utilize the UAMM's two-dimensional approach in creating our MMISA (detailed in the following section). The SANS Institute Awareness Maturity Model provides a "five-grade" approach similar to the UAMM (Spitzner, 2012). The five grades (from levels 1 to 5) focus on the existence and quality of SAPs in an organization. At level 1, there is no SAP and no attempt to train or educate the staff of an organization. As a result, people do not know or understand the organization's policies and procedures, do not realize that they can be a target and are rather vulnerable to most human-based attacks. "Level 2" is compliance focused: the SAP is designed to meet specific compliance or audit requirements. Training is limited to annual or ad hoc events. As a result, employees are unsure of organizational policies, and they do not truly understand the role they play in protecting their organization's information assets or how to prevent, identify or report a security incident. "Level 3" focuses on promoting awareness to shift organizational culture and reduce risk in organizations. At this level, the existing and operating awareness program identifies the training topics that have the greatest impact on supporting the organization's mission and focuses on those key topics. In addition, the program moves beyond simple annual training to include continual reinforcement. "Level 4" refers to long-term sustainment, which builds on an existing program promoting awareness and change. Processes and resources are available for a long-term life cycle, including, at a minimum, an annual review and update of both training content and communication methods. The top-level ("Level 5") connects metrics to a SAP to track progress and measure impact. As a result, the program is continuously improving and able to demonstrate return on investment. This formal metrics program integrates all the benefits of the model's lower levels. The detailed model is presented in the SANS Institute Security Awareness Report of 2019, with some slight changes in grade names (SANS, 2019).

Our hypothesis on the relationship between ISA and maturity level is as follows:

H6. An increased ISA has a positive impact on the maturity level of ISA.

We also identify certain indirect (mediation) effects among the constructs we apply. These mediation effects indirectly influence one another. Given these mediation effects, we establish the following three hypotheses:

H7. Organizational structure mediates the relationship between risk management and ISA.

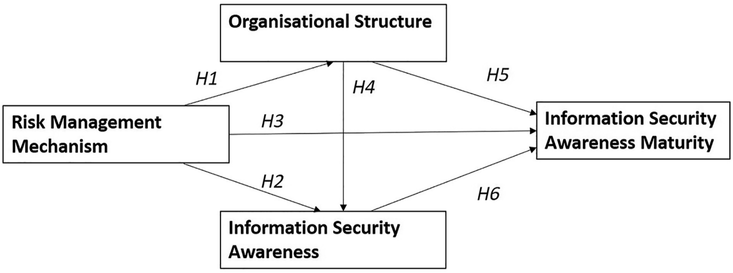
H8. Information security awareness mediates the relationship between organizational structure and the maturity level of ISA.

H9. Organizational structure and ISA mediate the relationship between risk management and the maturity level of ISA.

These mediation effects are discussed in detail in section 4.4. The model and the hypotheses are presented in Figure 1.

3. Research method

Our research has seven phases, which we summarize in Figure 2. The research method is a combined one; both qualitative and quantitative methods were applied. First, we performed a literature review, targeting ISA maturity, the decisive factors of the maturity level of ISA and the role of risk management and organizational structure. The main sources of the literature review were Scopus and Web of Science. Next, using the result of the literature review, we developed a relationship model for analyzing the relation between organizational structure, risk management mechanism, ISA and ISA maturity and for hypotheses formulation. In step 3, we developed a survey to collect quantitative data. Data collection and processing in step 4 were performed with the support of the Hungarian Information Security Community, and we contacted the members of the Budapest Chapter of ISACA and other IS associations, bodies or authorities. Two of the authors are active and certified members (Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM) and Certified in the Governance of Enterprise IT (CGEIT)) of these communities. The Hungarian Information Security Community (IS experts, auditors, IS managers, etc.) consists of approximately 2,200 people; an estimated 300 of them play active roles in different associations. These people engage with ISA programs in their organizations, and they confront ISA challenges as internal or external actors. This active portion of the community (about 600 people) was asked to take part in our research. A total of 122 people answered the online questionnaire; only 92 responses were fully assessable, although the questionnaire was open for several


Organisational Structure
H1
H4
H5
Risk Management Mechanism
H3
Information Security Awareness Maturity
H2
H6
Information Security Awareness

Source(s): Authors’ own work

Figure 1.
The relationship model

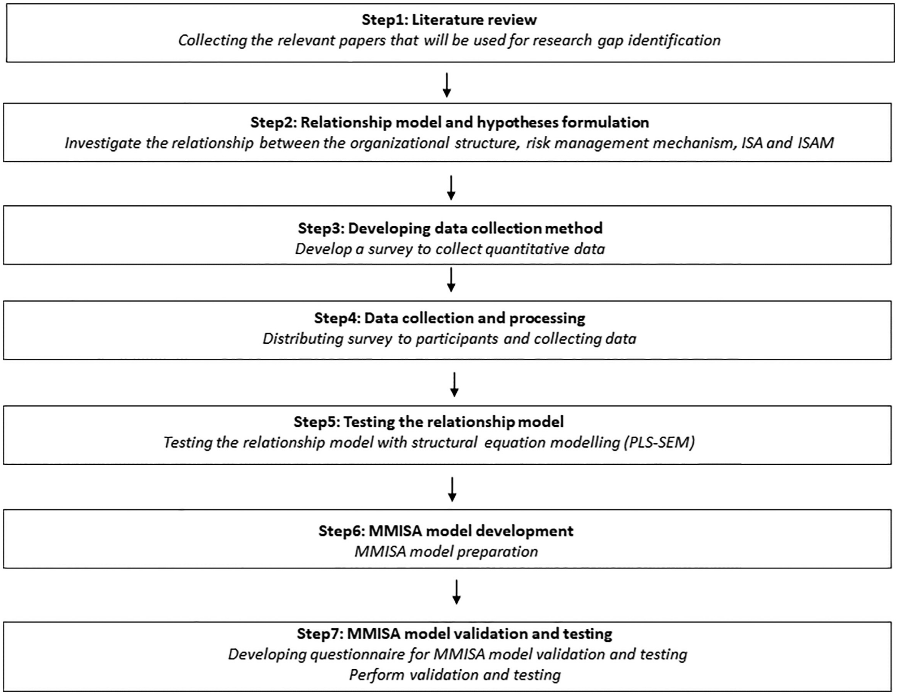

Step1: Literature review
Collecting the relevant papers that will be used for research gap identification
Step2: Relationship model and hypotheses formulation
Investigate the relationship between the organizational structure, risk management mechanism, ISA and ISAM
Step3: Developing data collection method
Develop a survey to collect quantitative data
Step4: Data collection and processing
Distributing survey to participants and collecting data
Step5: Testing the relationship model
Testing the relationship model with structural equation modelling (PLS-SEM)
Step6: MMISA model development
MMISA model preparation
Step7: MMISA model validation and testing
Developing questionnaire for MMISA model validation and testing
Perform validation and testing

Figure 2.
Research steps

Source(s): Authors' own work

months. The related relationship model was tested using partial least squares-structural equation modeling (PLS-SEM) in step 5, which is suitable when a theory is under-developed (Hair *et al.*, 2017a, 2017b). Because of the limited number of valid responses (92), we applied PLS-SEM, a variance-based, SEM that has a relatively low required sample size (Hair *et al.*, 2017a, 2017b). The use of PLS-SEM was justified by (1) the exploratory nature of this study, (2) the small (92) sample size and (3) the scale's development, assessed in this study, where items are measured on a seven-point Likert-type scale (Hair *et al.*, 2017a, 2017b).

The relationship model doesn't provide customized and suitable support for IS professionals, especially for the IT auditors, because it doesn't deal with the controls and audit evidence of the maturity levels. To overcome these challenges in step 6, we developed MMISA, our model. The last step was MMISA validation and testing. To test the MMISA model, we prepared interview questions. Responders, IT auditors, IS experts, consultants and IS officers were from the Hungarian Information Security Community; we asked again for the support of the Budapest Chapter of ISACA and other IS associations, bodies or authorities. We organized three dedicated events in the monthly meetings of ISACA Hungarian Chapter, where we presented the MMISA model and discussed it with the participants. We asked the participants to fill in the online questionnaire about the MMISA model and its usability. According to the MMISA model description (see Table 5), they needed to read and understand the scale grades, they needed to assess their organization on this 5-grade scale and they also were asked to give feedback about their difficulties on the assessment. Altogether we got 122 responses. Nobody presented extra controls, initiatives or evidence as a part of his or her answer during the inquiry period.

4. Results

In this section, we summarize the findings of step five, testing the relationship model with PLS-SEM. A structured questionnaire survey with multi-item scales for construct measurement was employed as a research instrument. We provide a rationale for the selection and definition of each construct in section 2. The four constructs (risk management mechanism, organizational structure, ISA and ISA maturity level) this study uses are based on a literature review of ISA and maturity models. The scales of the four constructs are described in Appendix.

4.1 Measurement scales

Three internationally pre-tested (to measure risk management mechanism, organizational structure and ISA) scales (a streamlined version of Dzazali and Zolait's (2012) scales) and a newly developed construct are used in this study (see Appendix). Each item is measured on a seven-point Likert scale, ranked from 1 = strongly disagree to 7 = strongly agree. The maturity level is measured on a five-point scale according to the MMISA. Mark 5 represents the highest level of maturity ("robust metrics framework") and mark 1 shows an initial state of maturity ("non-existent"). *Risk management* is measured by a four-item scale developed by Dzazali and Zolait (2012) to measure the risk management mechanism and procedure. The scale reliability is good (Cronbach $\alpha = 0.92$). *To measure the organizational structure,* a simplified version (three items) of the Dzazali and Zolait (2012) model is used. The scale reliability is good (Cronbach $\alpha = 0.85$). The *IS awareness* scale derives from the awareness and training scale developed by Dzazali and Zolait, but this model is focused only on the awareness segment (three items) because awareness and training are distinct constructs. The scale reliability is good (Cronbach $\alpha = 0.85$). The *ISA Maturity Level* is a one-item construct study (via MMISA, defined and developed earlier in this study), which focuses on the five different levels of maturity.

4.2 Data analysis

PLS-SEM was applied using ADANCO software (Dijkstra and Henseler, 2015). The small sample size and the exploratory nature of the research justified the use of PLS-SEM (Hair *et al.*, 2012). PLS-SEM works efficiently with small sample sizes and complex models without an additional assumption about the underlying data (Hair *et al.*, 2017a, 2017b). It can handle reflective and formative measurement models and be applied in various research situations. There are no distributional assumptions; PLS-SEM is a nonparametric method. Hair *et al.* (2017a, 2017b) and Cohen (1992) support calculating the minimum required sample size, which is 37. Based on Kock and Hadaya's (2018) inverse square root method, the minimum sample size is 59. According to both procedures, the minimum sample element size criterion is satisfied. Standardized factor loadings should be more than 0.5, but ideally 0.7 should be reached (Hair *et al.*, 2012). Appendix lists Dijkstra-Henseler's rho values, i.e. the index of internal consistency and reliability measure of constructs, which was well above the favorable 0.7 value in each case (Dijkstra and Henseler, 2015). Convergent validity was measured using average variance extracted (AVE), where values should be more than 0.5 in each construct (Hair *et al.*, 2017a, 2017b). The AVE is illustrated through the diagonal of Table 1. The data met the required criteria. Discriminant validity was measured by Fornell and Larcker's test (1981): in all cases, the AVE measure should be larger than the squared latent variable correlations of all other constructs. As Table 1 demonstrates, this requirement was met.

Discriminant validity was also measured by the heterotrait-monotrait ratio of correlations (HTMT), where each pair of constructs must be significantly lower than 0.85; this criterion was met in our study (see Table 2).

In sum, sufficient statistical evidence was found that verified the existence of the four constructs, that the measured variables are appropriate indicators of the related factors and that the constructs are different.

4.3 Structural model and results

Only one model-based criterion, the standardized root mean square residual (SRMR), is applied in PLS modeling, and its cut-off value is 0.08 (Hu and Bentler, 1999). The model delineated in this study has an appropriate model fit because SRMR = 0.057. The results (see Table 3 and Figure 3) demonstrate that not every hypothesis was accepted.

This model highlights the crucial role risk management plays in this context; risk management has a positive impact on organizational structure (b (beta value) = 0.73), IS awareness ($b = 0.41$) and ISA maturity level ($b = 0.28$), which means that hypotheses H1. H2 and H3 are supported. In other words, the better the risk management mechanisms are, the more pronounced information security can be within a level of organizational structure and the more effective an IS awareness-improving process is. Risk management also has a direct impact on ISA maturity level, which highlights its decisive, motivating role. Organizational

Table 1.
Discriminant validity: a Fornell–Larcker criterion

Construct	Risk management mechanism	Organizational structure	IS awareness	ISA maturity
Risk Management Mechanism	0.8085			
Organizational Structure	0.5337	0.7707		
IS Awareness	0.4286	0.4055	0.7779	
ISA Maturity	0.3276	0.2988	0.2801	1.0000

Note(s): Squared correlations; AVE in the diagonal
Source(s): Authors' own work using ADANCO software

Table 2.
Discriminant validity: an HTMT criterion

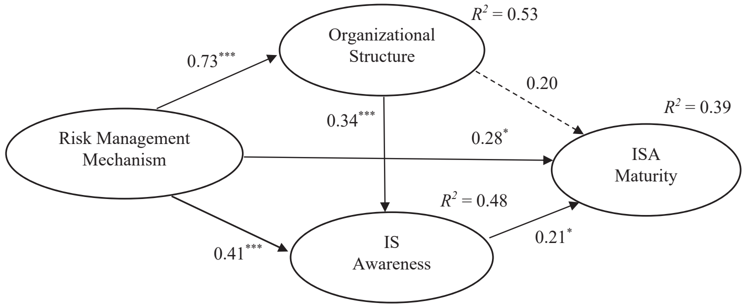
Construct	Risk management mechanism	Organizational structure	IS awareness	ISA maturity
Risk Management Mechanism				
Organizational Structure	0.8236			
IS Awareness	0.7360	0.7414		
ISA Maturity	0.5963	0.5917	0.5743	

Source(s): Authors' own work using ADANCO software

Table 3.
Direct effects on the model

Effect	Coeff.	*t*-value	*p*-value
Risk Management Mechanism → Organizational Structure	0.7305	9.5988	0.0000
Risk Management Mechanism → IS Awareness	0.4064	3.3668	0.0004
Risk Management Mechanism → ISA Maturity	0.2841	1.8675	0.0309
Organizational Structure → IS Awareness	0.3399	3.1863	0.0007
Organizational Structure → ISA Maturity	0.2027	1.4528	0.0732
IS Awareness → ISA Maturity	0.2141	2.2726	0.0115

Source(s): Authors' own work using Adanco software



Note(s): All coefficients are standardized (*$p < 0.05$; ***$p < 0.001$). The dotted lines represent the rejected hypotheses
Source(s): Author's own work

Figure 3. The structural model and results

structure has a positive impact on IS awareness ($b = 0.34$), which draws attention to the fact that organizational support is effective. IS awareness improvement can be achieved at a higher level (H4 is accepted). At the same time, the organizational structure does not have a significant impact on ISA maturity level (H5 is rejected), which means that organizational structure alone is not enough to increase the level of ISA maturity. This fact also mirrors our personal experiences. IS awareness has a positive impact on ISA maturity level ($b = 0.21$), which means that if the importance of ISA is raised to a high level, then it is able to foster a higher level of ISA maturity in an organization (H6 is accepted). Figure 3 shows that in addition to the direct effects of ISA, there are also certain indirect effects.

4.4 Mediation effects analysis

For a mediation effects analysis, according to Iacobucci (2008) and Zhao *et al.* (2010), SEM approaches should outperform the "causal steps" approach of Baron and Kenny (1986), because they estimate everything simultaneously. Hair *et al.* (2017a, 2017b, p. 239) also suggest that "to test mediation effects, use bootstrapping instead of the Sobel test, which is not applicable in a PLS-SEM context".

A mediation effects analysis was conducted using the logic of Zhao *et al.* (2010) and Hair *et al.* (2017a, 2017b). Table 4 shows that all mediating effects are complementary, which means that both mediated effects and a direct effect exist (a partial mediation) and point in the same direction.

	Total effect		Direct effect		Indirect effect			
Path	Coeff.	t-value	Coeff.	t-value	Point est.	CI 95%	Mediation	
RM → A	0.6547***	7.4365	0.4064***	3.3668	0.2483***	[0.0945. 0.4086]	Partial (compl.)	H7
OS → ML	0.2755*	2.0406	0.2027	1.4528	0.0728*	[0.0069. 0.1662]	Full	H8
RM → ML	0.5724***	7.2613	0.2841*	1.8675	0.1843***	[0.0937. 0.5597]	Partial (compl.)	H9

Note(s): (***$p < 0.001$; *$p < 0.05$); RM: Risk Management, A: Awareness, OS: Organizational Structure and ML: Maturity Level
Source(s): Authors' own work

Table 4. Summary of mediating effect tests

Maturity level	Brief description of the level	Controls supporting knowledge	Controls supporting attitude	Audit evidence
1 - Non-Existent	ISA practically does not exist	No supporting controls	No supporting controls	None
2 - Compliance Focused	ISA programme already exists but is designed primarily to meet specific compliance or audit requirements	Regular (annual) and documented awareness training events. General ISA training materials (contents) are available (e.g. videos, newsletters, or presentation materials). Regular (annual) internal audits. As a part of the onboarding process, the employees receive initial training with generic information security content	Documented disciplinary process	Training materials and training records; documented procedures for identifying customer needs, supplier management, and initial and regular ISA training; signed NDAs with employees and suppliers; 3rd party audit reports; certificates of compliance issued by customers and/or third parties; and risk assessment reports
3 - Promoting Awareness & Behavior Change	This ISA grade is based on a detailed risk assessment, which identifies the topics that have the greatest impact on supporting the organization's mission and ISA efforts to focus on those key topics	Based on the risk assessment of the organization, there are available, organization-specific ISA training materials (contents)	During the traditional disciplinary process, there is a defined and documented incentive system, i.e. prizes, trophies, presents, or campaigns related to information security	List of relevant ISA-related topics linked to a detailed risk assessment; management review meeting minutes; ISA project-related documents (PID, project plan, action plan, reports, etc.); regular management communications about emerging risks, actions, countermeasures and results via e-mail, blog, video, etc.

(*continued*)

Table 5.
The proposed model, explained by grades in detail

Maturity level	Brief description of the level	Controls supporting knowledge	Controls supporting attitude	Audit evidence
4 - Long-Term Sustainment & Culture Change	There is an ISA-related programme, which has the processes, resources, and leadership support in place for a long-term life cycle, including, at a minimum, an annual review and update of the programme. The programme and security are an established and updated part of the organization's culture	Documented procedures for the regular review of the communicated contents and for defining the learning objectives for target groups. Regular knowledge assessments by tests	IS-related goals are integral parts of the regular personal appraisal system for individuals as a part of performance assessments	Program-related documentation (set of projects, project and programme reports) and a detailed ISA budget for a longer period (i.e. three years)
5 - Robust Metrics Framework	The ISA programme has a robust metrics framework to track progress and measure impact. Consequently, the programme is continuously improving and able to demonstrate a return on investment	Documented and implemented procedures for measuring ISA (metrics, measurement method, and use of the measurement results)	Personalized, tailored to the organizational unit, "SMART" (specific, measurable, attainable, realistic and timely) objectives	Documented, traceable KGIs (Key Governance Indicators), KPIs and ROI (ROSI (Return On Security Investment)) calculations

Source(s): Authors' own work

Table 5.

The following are the hypotheses on the mediation effects in our model:

H7. Organizational structure mediates the relationship between risk management and IS awareness.

H8. IS awareness mediates the relationship between organizational structure and ISA maturity level.

H9. Organizational structure and IS awareness mediate the relationship between risk management and ISA maturity level.

First, the organizational structure has a mediating effect on the relationship between risk management and IS awareness. As reported in Table 4, the results demonstrate a significant indirect path from risk management through organizational structure to IS awareness. The direct path from risk management to IS awareness is also significant. It indicates the partial mediating effect (i.e. a complementary mediation) of organizational structure on the relationship between risk management and IS awareness (H7 is supported). Higher levels of risk management increase IS awareness directly and increase organizational structure, which drives IS awareness. Hence, certain risk management effects on IS awareness are explained by organizational structure.

Second, the mediating effects of IS awareness on the relationship between organizational structure and ISA maturity level are shown in Figure 3 and Table 4. IS awareness influences ISA maturity level indirectly. The indirect path from organizational structure through IS awareness to ISA maturity level is significant, but the direct path from organizational structure to ISA maturity level is non-significant. This indicates the full mediating effect of awareness on the relationship between organizational structure and ISA maturity level (H8 is supported). High levels of organizational structure cannot increase ISA maturity level directly but rather increase IS awareness, which in turn drives ISA maturity level. Hence, the organizational structure effects on the ISA maturity level are fully explained by IS awareness.

Third, the mediating effects of organizational structure and IS awareness on the relationship between risk management and ISA maturity level are shown in Figure 3 and Table 4. The results indicate that there is a significant influence of risk management, through organizational structure and IS awareness on ISA maturity level. The direct path from risk management to ISA maturity level is also significant. This finding also indicates partial mediating effects (i.e. a complementary mediation) of organizational structure and IS awareness on the relationship between risk management and ISA maturity level (H9 is supported).

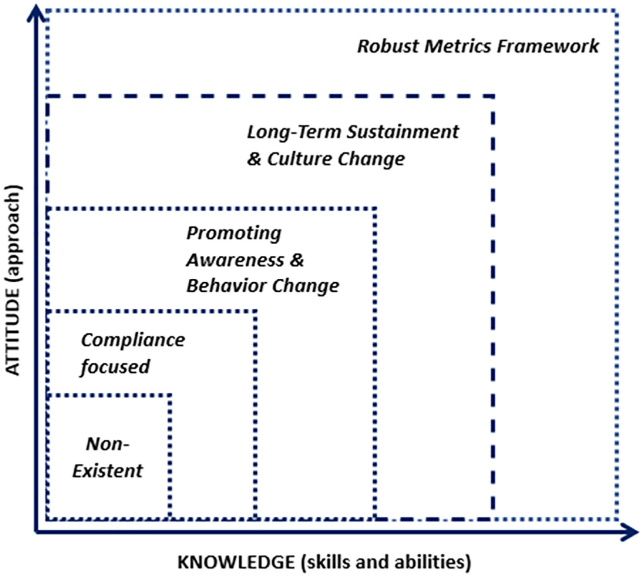
5. Discussion

ISA maturity investigated in the relationship model (Figure 3) provides information about ISA maturity key factors but doesn't detail several important issues from IT audit aspects, such as controls and audit evidence of the maturity levels. Without this information, IT auditors don't know the deficiencies in the control set, and there is no guideline about what controls should be developed and why or which audit evidence is relevant at a certain control set. Beyond that, we distinguish in the MMISA model controls supporting knowledge and controls supporting attitude, emphasizing that it is not enough to know what to do, but the proper attitude is required too, and because of that, we extend our investigation; we propose our MMISA, which includes the abovementioned details as well. Many organizations, to achieve continuous improvement in information security, use maturity models to assess the abilities of employees and other interested parties. The assessment results are used to define continuous improvement actions for changing and enhancing many different aspects of the relevant staff, such as their knowledge, attitudes and habits. Based on these considerations and the maturity model overview, we define ISA maturity level as an indicator of the quality of an organizational approach to managing and measuring complex awareness programs to improve staff knowledge, attitudes and habits via an IS-related focus. Maturity level means a well-defined grade of ISA-related activities and practices in an organization. The different grades represent different levels of the ISA programs, initiatives, applicable tools and campaigns that improve the skills and abilities of the interested parties (employees, subcontractors, partners, managers, etc.).

Based on the literature review and the experience of expert teams, we build our own ISA maturity model, the MMISA model (Table 5). We use the SANS Maturity Model (SANS, 2019) as a basis for defining maturity grades. Compared with SANS model, the main contribution of the MMISA model is an inventory of controls we construct to establish the level of existing ISA in each grade, and we include certain requisite comments and/or audit evidence to facilitate a common understanding and deployment of each grade. Our goal is to provide a framework that supports an IT audit through a measurable model; we define objective evidence that can be used for assessing ISA maturity in an organization (Table 5). The MMISA details five maturity levels, with the relevant controls and audit evidence, providing valuable support for IT auditors and IS managers to assess the ISA maturity of their company. Additionally, we distinguish controls required in each maturity level by knowledge and attitude, referring to the fact, that knowledge and attitude have a decisive but different role in ISA. People must be familiar not only with what to do and why an action is appropriate but also why they need to be actively involved in preventive and corrective actions. The two-dimension approach illustrated in Figure 4 helps to make differences among organizations and provides improvement directions for the model users. If we have a high level of knowledge and a low level of attitudes, then we get a clear message about what to do: we need to focus on motivation factors, how we can achieve, that people will follow the internal instructions for securing their working activities.

The grades of the MMISA are explained in detail in Table 5, where each maturity level has a brief description. At all levels, we define those controls that support knowledge (skills and abilities) and those controls that support staff attitudes (approach) to IS. From an auditor's perspective, the potential audit proofs are listed to provide objective evidence for the achievement of a certain level of ISA.

To test the MMISA, we asked IT auditors, IS experts, consultants and IS officers to grade their organization based on the current levels of IS controls and evidence (Table 5). We obtained feedback from 122 respondents from the Hungarian Information Security Community who play different roles in different associations. Each grade (maturity level) had a short description, and there was a list of controls supporting knowledge (skills and abilities) and attitude (approach). Potential evidence was also listed for each grade. The respondent made his or her own judgment on the existence and operability of the listed controls and evidence in his or her organization. If there were organization-specific control mechanisms in the assessed organization, then the respondent had the freedom to upgrade or downgrade the ISA maturity level in his/her response. In this case, a short explanation was also expected. Nobody presented extra controls, initiatives or evidence as a part of his or her answer during


Robust Metrics Framework
Long-Term Sustainment & Culture Change
Promoting Awareness & Behavior Change
Compliance focused
Non-Existent
ATTITUDE (approach)
KNOWLEDGE (skills and abilities)

Source(s): Authors' own work

Figure 4. The role of knowledge and attitude for information security awareness maturity

the inquiry period. Accordingly, we concluded that the MMISA is sufficiently detailed and suited to its purpose.

Here, we compare the MMISA model with the other maturity models discussed (see Table 6). The MMISA model is based on IT audit best practices and IS manager expertise. Its specialty compared with the other maturity models is that it has defined controls and audit evidence by grade. Its unique feature is that, beyond the maturity level description, it supports audit work as well.

6. Study implications

The current study considers several theoretical and practical implications for researchers of the IT security and audit field, IT auditors, IT security managers and experts, teachers, trainers, as well as designers of IT control environments, companies and the relevant entities associated with IT audit and security.

6.1 Theoretical implications

The present study has outlined several contributions to the theory and literature. The current study expands the prior literature on ISA and ISA maturity. The literature on ISA maturity models remains scarce. Information security maturity is discussed by several researchers (Greene *et al.*, 2022; Lopez-Leyva *et al.*, 2020; Nasir *et al.*, 2019; Schmitz *et al.*, 2021) but ISA maturity is not. Scopus search using "information security awareness" and "maturity models" resulted in two publications, only one article and one conference paper. Results extend our understanding of the decisive factors of ISA maturity levels with a variance-based

Table 6.
Comparison of the maturity models

Comparing factors	Information security awareness maturity models ISACM	UAMM	SANS	MMISA
Referred Standard	ISO 27002 (2005)	None	ISO 27002, PCI DSS, SOX, GLBA, HIPAA, NERC, NIST 800, ENISA	None
Focus	IT Stakeholder Groups (IT Staff, Senior Management, End Users)	IT Users	Awareness Programme	Interested Parties
Dimensions of Maturity	Importance, Capability, Risk (Three)	Threat and Countermeasure, Prescription and Discretion (Two)	(One)	Attitude (Approach), Knowledge (Skills and Abilities) (Two)
Number of Maturity Grades	7	5	5	5
Defined Controls, by Grade	Yes	None	None	Yes
Defined Audit Evidence, by Grade	None	None	None	Yes
Supports Audit Work	Partly	None	Partly	Yes

Source(s): Authors' own work

SEM (relationship model). Based on a literature review of ISA and maturity models, we prepared a relationship model, which uses four constructs (risk management mechanism, organizational structure, ISA and ISA maturity level). According to the relationship model, a strong risk assessment mechanism (through a documented methodology and reliable results) leads to a high level of ISA. These results confirm the study of Dzazali and Zolait (2012), Diesch *et al.* (2020) and Tam *et al.* (2022).

The most significant contribution of the current study is the MMISA model as an ISA maturity model providing controls and audit evidence for maturity levels. We distinguish in the MMISA model controls supporting knowledge and controls supporting attitude, emphasizing that it is not enough to know what to do, but the proper attitude is required too. We didn't find any other ISA maturity model with a similar feature. Fertig *et al.* (2023) developed a MMISA, similar to our model in some dimensions. Their proposed maturity model has five maturity levels, determined mathematically with the help of a polytomous extension of the Rasch model and hierarchical cluster analysis. They collected data for the calculations through a survey and applied design science as a research method. Their model, however, sets expectations at a more general level than we do in the MMISA model and does not provide specific guidance for assessing the control environment and related evidence. Kour and Karim (2021) aimed to estimate cybersecurity maturity level and awareness risk for workforce management in railways using Railway-Cybersecurity Capability Maturity Model (R-C2M2) and ISACM, respectively (Kour and Karim, 2021). Their approach differs from ours because it aims to reveal and identify cybersecurity awareness risks, and the research focuses on the railway. Analyzing the ISA measuring approaches and the related maturity models, we revealed that they don't offer controls and audit evidence for maturity levels, which is crucial for auditors and security professionals; additionally, they don't distinguish knowledge and attitude in IS context in their model. Our proposed MMISA model overcomes these deficiencies, and it provides a suitable framework for not only assessing an organization's current ISA maturity level, but also identifying the steps needed to reach a higher ISA maturity level. One crucial issue is that maturity in information technology can change over time (Mettler and Pinto, 2018). MMISA can manage this time dependency.

6.2 Practical implications

The findings of the current study present several practical implications for IT security managers, IT auditors, IT security experts, companies and control designers as well as teachers and trainers.

One of the most important practical benefits of our research is that it provides a structured guideline on how to improve ISA within organizations; it helps to identify gaps in the control environment, points to the evidence and shows the steps needed to improve it. Using MMISA model, auditors can get feedback about their control set; they know which control should be developed and how they are connected to audit evidence (so how to perform the audit). Repeating the assessment exercise using the MMISA model at the same companies over three or five-year, we can collect evidence on changes, trends and tendencies in information security practices. This feedback can be very useful for companies in improving the control environment and related regulatory procedures to reach a higher level of maturity. The MMISA model, with its well-defined grades, is useful for auditors, assessors and companies being assessed. The model is applicable for "quick tests" of ISA and helps companies to define their improvement paths to security awareness and to identify the company practices that foster ISA progression. Application of MMISA model can help and assist ISA development and organization development from ISA aspects. It provides an overview for managers of ISA status and gives feedback about the available controls in the organization. This outcome can be compared with the requirements of the regulatory frameworks and adjusted according to that. MMISA provides practical support for planning and designing controls based on the maturity level of a company. Creating a proper information security culture is crucial to protecting information assets. MMISA can be used to enrich it through leveraging knowledge related to ISA in security awareness training. Finally, the insights from the relationship model highlight that strengthening the risk assessment mechanism (through a documented methodology and reliable results) can result in a higher level of ISA.

7. Limitations and future work

The most important limitation of the research is the size and composition of the data. Furthermore, another limitation is that the data were collected in Hungary, and we tested our model in Hungary. For generalization purposes, we suggest testing MMISA in other countries. Results do not present the situation of a specific industrial sector. An additional extension of the research is the application and customization of MMISA model for some highly privacy-sensitive industries like finance and the healthcare sector. These sectors are assumed to have higher levels of ISA maturity. Future work includes additional tests of MMISA model involving a larger group of IS security professionals and IT auditors in real-life situations and scenarios. Based on their feedback, MMISA model could be improved. Repeating the assessment exercise at the same companies over three or five years, we can collect evidence on changes, trends and tendencies in information security practices. This feedback can be very useful for companies in improving the control environment and related regulatory procedures. Applying the MMISA model to other Information Security Communities in other countries provides an opportunity for comparison possibilities. Despite the limitations, our study represents a new approach to ISA maturity and could be a starting point for future studies.

8. Conclusion

This paper has two main goals; first, to analyze the decisive factors of ISA maturity levels with a variance-based structural equation model (we call it the relationship model), and second, to provide an ISA maturity framework – the MMISA model. From a practical view, based on the results of the relationship model, if we identify a strong risk assessment mechanism (through a documented methodology and reliable results), we can expect a high level of ISA. This means that we need to foster the implementation of a well-established risk assessment methodology because this can have a direct influence on ISA. On the other hand, we can also identify certain side effects:

(1) If there is a well-defined organizational structure with clear responsibilities, this supports the linking of a risk management mechanism with the level of ISA.

(2) The connection between organizational structure and ISA maturity level is supported by ISA activities: An increased level of awareness actions strengthens an organizational structure via the best practices learned by the staff.

(3) The relationship between risk management mechanism and ISA maturity level is also supported by organizational structure and ISA-related activities.

In short, the results of a well-elaborated risk assessment facilitate ISA maturity through an increased level of ISA activities. The process leads to a solid organizational structure that helps improve ISA-related tasks. Researchers can transform their findings into better company practices if they integrate the mechanism described above. Based on our research, to increase the level of ISA, organizations should introduce controls that support risk management mechanisms (e.g. the introduction and operation of a risk management procedure). Additionally, strengthening the role of an information security organization within an organizational structure is effective; it can have a measurable impact on the systematic and targeted training of staff.

According to our investigation related to the ISA measuring approaches and the corresponding maturity models, we found that they don't offer controls and audit evidence for maturity levels, which is crucial for auditors and security professionals; additionally, they don't distinguish knowledge and attitude in IS context in their model. Our proposed MMISA model eliminates these deficiencies it provides a suitable framework for not only assessing an organization's current ISA maturity level, but also identifying the steps needed to reach a higher ISA maturity level.

References

AlGhamdi, S., Win, K.T. and Vlahu-Gjorgievska, E. (2020), "Information security governance challenges and critical success factors: systematic review", *Computers and Security*, Vol. 99, 102030.

AlMindeel, R. and Martins, J.T. (2020), "Information security awareness in a developing country context: insights from the government sector in Saudi Arabia", *Information Technology and People*, Vol. 34 No. 2, pp. 770-788.

Baron, R.M. and Kenny, D.A. (1986), "The Moderator-Mediator variable distinction in social psychological research: conceptual, strategic, and statistical considerations", *Journal of Personality and Social Psychology*, Vol. 51, pp. 1173-1182.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, pp. 523-548.

Cohen, J. (1992), "Quantitative methods in psychology: a power primer", *Psychological Bulletin*, Vol. 112, pp. 1155-1159.

Da Veiga, A. and Martins, N. (2015), "Improving the information security culture through monitoring and implementation actions illustrated through a case study", *Computers and Security*, Vol. 49, pp. 162-176.

Diesch, R., Pfaff, M. and Krcmar, H. (2020), "A comprehensive model of information security factors for decision-makers", *Computers and Security*, Vol. 92, 101747.

Dijkstra, T.K. and Henseler, J. (2015), "Consistent partial least squares path modeling", *MIS Quarterly*, Vol. 39 No. 2, pp. 297-316.

Dzazali, S. and Zolait, A.H. (2012), "Assessment of information security maturity: an exploration study of Malaysian public service organizations", *Journal of Systems and Information Technology*, Vol. 14 No. 1, pp. 23-57.

Fertig, T., Schütz, A.E., Weber, K. and Müller, N.H. (2020), "Towards an information security awareness maturity model", in Zaphiris, P. and Ioannou, A. (Eds.), *Learning and Collaboration Technologies. Human and Technology Ecosystems. HCII 2020. Lecture Notes in Computer Science*, Springer, Cham, pp. 587-599.

Fertig, T., Schütz, A. and Weber, K. (2023), "Developing a maturity model for information security awareness using a polytomous extension of the Rasch model", *Proceedings of 1995 New Security Paradigms Workshop*, IEEE, pp. 66-74.

Fletcher, S.K., Halbgewachs, R., Jansma, R.M., Murphy, M.D., Lim, J.J. and Wyss, G.D. (1995), "Software system risk management and assurance", *Proceedings of the 56th Hawaii International Conference on System Sciences*, IEEE, pp. 6830-6840.

Fornell, C. and Larcker, D.F. (1981), "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol. 18 No. 1, pp. 39-50.

GLBA, The Gramm–Leach–Bliley Act (1999), "Financial services modernization act of 1999".

Greene, L., Hur, I., Levy, Y., Wang, L. and Kang, K. (2022), "Assessing effects of media affordances and information security awareness on knowledge-sharing in global software development", *Journal of Information Systems*, Vol. 36 No. 1, pp. 111-132.

Hair, J.F., Sarstedt, M., Ringle, C.M. and Mena, J.A. (2012), "An assessment of the use of partial least squares structural equation modeling in marketing research", *Journal of the Academy of Marketing Science*, Vol. 40 No. 3, pp. 414-433.

Hair, J.F., Hult, G.T.M., Ringle, C.M. and Sarstedt, M. (2017a), *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 2nd ed., Sage, Thousand Oaks.

Hair, J.F., Jr, Sarstedt, M., Ringle, C.M. and Gudergan, S.P. (2017b), *Advanced Issues in Partial Least Squares Structural Equation Modeling*, Sage, Los Angeles.

HIPAA (1996), "The health insurance portability and accountability act of 1996".

Hong, K.S., Chi, Y.P., Chao, L.R. and Tang, J.H. (2003), "An integrated system theory of information security management", *Information Management and Computer Security*, Vol. 11 No. 5, pp. 243-448.

Hu, L.T. and Bentler, P.M. (1999), "Cutoff criteria for fit indexes in covariance structure analysis: conventional criteria versus new alternatives", *Structural Equation Modeling: A Multidisciplinary Journal*, Vol. 6 No. 1, pp. 1-55.

Iacobucci, D. (2008), *Mediation analysis (No. 156)*, Sage.

ISACA (2017), *CISA Review Manual*, ISACA., Illionois. USA.

ISACA (2020), "Glossary", available at: https://www.isaca.org/resources/glossary (accessed 20 August 2020).

ISO/IEC 27001:2013 (2013), "Information technology – security techniques – information security management systems – requirements".

Jaeger, L. (2018), "Information security awareness: literature review and integrative framework", *Proceedings of the 51st Hawaii International Conference on System Sciences.*

Jansson, K. and von Solms, R. (2013), "Phishing for phishing awareness", *Behaviour and Information Technology*, Vol. 32 No. 6, pp. 584-593.

Kock, N. and Hadaya, P. (2018), "Minimum sample size estimation in PLS-SEM: the inverse square root and gamma-exponential methods", *Information Systems Journal*, Vol. 28 No. 1, pp. 227-261.

Kour, R. and Karim, R. (2021), "Cybersecurity workforce in railway: its maturity and awareness", *Journal of Quality in Maintenance Engineering*, Vol. 27 No. 3, pp. 453-464.

Kruse, S. and Pankey, B. (2010), "Assessing the effectiveness of security awareness training. RSA and tunitas group", available at: http://www.securitymetrics.org/attachments/Metricon-6.5-Kruse.pdf (accessed 05 March 2019).

Lebek, B., Uffen, J., Neumann, M., Hohler, B. and Breitner, M.H. (2014), "Information security awareness and behavior: a theory-based literature review", *Management Research Review*, Vol. 37 No. 12, p. 1049.

Lopez-Leyva, J.A., Kanter-Ramirez, C.A. and MoralesMartinez, J.P. (2020), "Customized diagnostic tool for the security maturity level of the enterprise information based on ISO/IEC 27001", *2020 8th International Conference in Software Engineering Research and Innovation (CONISOFT)*, IEEE, pp. 147-153.

Maqousi, A., Balikhina, T. and Mackay, M. (2013), "An effective method for information security awareness raising initiatives", *International Journal of Computer Science and Information Technology*, Vol. 5 No. 2, p. 63.

Mettler, T. and Pinto, R. (2018), "Evolutionary paths and influencing factors towards digital maturity: an analysis of the status quo in Swiss hospitals", *Technological Forecasting and Social Change*, Vol. 133, pp. 104-117, doi: 10.1016/j.techfore.2018.03.009.

Nasir, A., Arshah, R.A., Ab Hamid, M.R. and Fahmy, S. (2019), "An analysis on the dimensions of information security culture concept: a review", *Journal of Information Security and Applications*, Vol. 44, pp. 12-22.

Nemeslaki, A. and Sasvari, P. (2015), "Empirical analysis of information security awareness in the business and public sectors of Hungary", *Central and Eastern European eDem and eGov Days 2015. Time for a European Internet?*, Österreichische Computer-Gesellschaft, Wien, pp. 405-418.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014), "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)", *Computers and Security*, Vol. 42, pp. 165-176.

PCI (2016), "PCI DSS - payment card industry data security standard – requirements and security assessment procedures", Version 3.2, available at: https://www.pcisecuritystandards.org/document_library (accessed 20 May 2020).

Peltier, T.R. (2001), *Information Security Risk Analysis*, Auerbach Publications, New York. NY.

Poepjes, R. and Lane, M. (2012), "An information security awareness capability model (ISACM)", available at: https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1136&context=ism (accessed 30 June 2021).

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A. and Herawan, T. (2015), "Information security conscious care behaviour formation in organizations", *Computers and Security*, Vol. 53, pp. 65-78.

SANS (2019), "SANS the rising era of awareness training – SANS security awareness report", available at: https://www.sans.org/security-awareness-training/resources/reports/(accessed 20 July 2018).

Sasvari, P., Nemeslaki, A. and Rauch, W. (2015), "Old monarchy in the new cyberspace: empirical examination of information security awareness among Austrian and Hungarian enterprises", *Academic and Applied Research in Military and Public Management Science*, Vol. 15 No. 1, pp. 63-78.

Schmitz, C., Schmid, M., Harborth, D. and Pape, S. (2021), "Maturity level assessments of information security controls: an empirical analysis of practitioners assessment capabilities", *Computers and Security*, Vol. 108, 102306.

Siponen, M.T. (2000), "A conceptual foundation for organizational information security awareness", *Information Management and Computer Security*, Vol. 8 No. 1, pp. 31-41.

Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016), "Information security management needs more holistic approach: a literature review", *International Journal of Information Management*, Vol. 36 No. 2, pp. 215-225.

Spitzner, L. (2012), "Security awareness maturity model", available at: https://securingthehuman.sans.org/blog/2012/05/22/security-awareness-maturity-model (accessed 22 December 2017).

Stefaniuk, T. (2020), "Training in shaping employee information security awareness", *Entrepreneurship and Sustainability*, Vol. 7 No. 3, pp. 1832-1846.

Tam, C., de Matos Conceição, C. and Oliveira, T. (2022), "What influences employees to follow security policies?", *Safety Science*, Vol. 147, 105595.

van der Schyff, K. and Flowerday, S. (2021), "Mediating effects of information security awareness", *Computers and Security*, Vol. 106, 102313.

Wangen, G. (2017), "Information security risk assessment: a method comparison", *Computer*, Vol. 50 No. 4, pp. 52-61.

Zhao, X., Lynch, J.G., Jr and Chen, Q. (2010), "Reconsidering Baron and Kenny: myths and truths about mediation analysis", *Journal of Consumer Research*, Vol. 37 No. 2, pp. 197-206.

Further reading

Henseler, J., Hubona, G. and Ray, P.A. (2016), "Using PLS path modeling in new technology research: updated guidelines", *Industrial Management and Data Systems*, Vol. 116 No. 1, pp. 2-20.

ISACA (2012), "COBIT five: a business framework for the governance and management of enterprise IT", Rolling Meadows. IL 60008 USA.

ISACA (2018), *COBIT2019 Framework: Introduction and Methodology*, Schaumburg, IL 60173 USA.

ISO/IEC 27032:2012 (2012), "ISO 27032 – international standard ISO/IEC 27032:2012. Information technology – security techniques – guidelines for cybersecurity".

ITGI (2007), *COBIT 4.1 Control Objectives for Information Technology*, IT Governance Institute, available at: www.itgi.org.

Kruse, S. and Pankey, B. (2018), "User awareness maturity model (UAMM)", available at: http://securitymetrics.org/attachments/Metricon-6.5-Kruse.pdf (accessed 05 March 2022).

NIST (2013), *NIST Special Publication 800-53. Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations*, National Institute of Standards and Technology, 100 Bureau Drive (Mail Stop 8930) Gaithersburg. MD 20899-8930. USA, available online at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf (accessed 30 June 2020).

Sarbanes, S.P. and Oxley, M.G. (2002), "Sarbanes-Oxley act of 2002", *The Public Company Accounting Reform and Investor Protection Act*, p. 55, Washington DC, US Congress.

Appendix

Table A1. Measurement and reliability of the model constructs

Construct (Dijkstra-Henseler rho)	Item (scale)	Loading	Mean	Std. Dev
Risk Management (ρA = 0.944)	Information about risks across business processes is considered	0.9147	5.74	1.357
	Information and technical assets critical to the organization are identified	0.8609	6.19	1.095
	Management controls that provide sufficient protection against threats are defined	0.9158	5.54	1.294
	Vulnerabilities in the information systems and related processes are identified regularly	0.9040	5.68	1.389
Organizational Structure (ρA = 0.910)	Information security unit/personnel play important roles in decision-making processes about information security	0.8869	5.69	1.473
	The operation of the overall information security structure is evaluated and adjusted to adapt to changing conditions	0.8909	5.38	1.373
	Information security unit/personnel receive business objectives and needs from relevant unit head	0.8554	5.47	1.478
IS Awareness (ρA = 0.913)	Users are provided with instructions on classifying data in digital operation	0.9192	5.05	1.566
	Users are provided with instructions on classifying data in manual operation	0.9253	4.98	1.633
	Information security awareness briefing is standardized and formalized	0.7953	4.86	1.941
ISA Maturity Level (ρA = 1.000)	Existence of ISA programs. initiatives. applicable tools. and campaigns for improving the skills and abilities of the interested parties (employees. subcontractors. partners. managers. etc.)	1.0000	2.81	0.893

Note(s): Each item was measured on a seven-point scale. where 1 = strongly disagree. and 7 = strongly agree
Source(s): Authors' development

About the authors

Andrea Kő is Fulltime Professor and Director of the Institute of Data Analytics and Information Systems at Corvinus University of Budapest. She has an MSc in mathematics and physics from Eötvös Lóránd University of Budapest, a doctoral degree in computer science from Corvinus University of Budapest and a Ph.D. in management and business administration from Corvinus University of Budapest. She has published over 100 journal and conference papers. Her main research interests include IT audit, business intelligence and business analytics, knowledge management and semantic technologies and has participated in several international and national research projects. Andrea Kő is the corresponding author and can be contacted at: andrea.Kő@uni-corvinus.hu

Gábor Tarján, PhD, MBA, Certified Management Consultant (ICMCI CMC), ISO 27001 Lead Auditor, working as Information Security Officer (ISO) and Data Protection Officer (DPO), dealing with information security awareness related challenges for more than 20 years. He is a university lecturer at Metropolitan University Budapest and University of Public Affairs at Budapest and Corvinus University of Budapest. He is a project manager of information security management system implementation projects in various industries and he provides regularly information security trainings for managers.

Dr Ariel Mitev is Associate Professor at Corvinus University of Budapest. He is the author/co-author of several books on qualitative and quantitative research methodology and he has widely published on tourism and marketing issues in referred journals. His current research interests include research methodology, scale development and innovation diffusion of new technologies.