



MEASURING STUDENTS' INFORMATION SECURITY COMPETENCE IN THE CONTEXT OF ARTIFICIAL INTELLIGENCE: CRITERIA, INDICATORS AND RELIABILITY OF THE DIAGNOSTIC TOOLKIT

Mustafojev Shahzod

Bukhara International University

E-mail: shahzod@buxdpi.uz

ORCID: <https://orcid.org/0009-0007-8584-1237>

Abstract. *The rapid integration of artificial intelligence (AI) into higher education has created new opportunities for learning while increasing the complexity of information security risks faced by university students. These risks include phishing, identity theft, unauthorized disclosure of personal data, manipulated digital content, and the uncritical use of AI-generated information. Consequently, assessing students' information security competence requires an approach that extends beyond theoretical knowledge and incorporates practical skills, risk assessment, responsible digital behaviour, and the critical evaluation of AI-generated outputs. This article proposes a multidimensional diagnostic assessment framework for measuring students' information security competence in AI-supported educational environments. The framework comprises five criteria: cognitive, operational, analytical, behavioural, and ethical-legal. For each criterion, observable indicators and appropriate assessment methods are specified. The article also outlines procedures for evaluating the reliability and validity of the proposed diagnostic instruments, including internal consistency analysis, test-retest reliability, expert evaluation, and construct validation. The framework is informed by established digital competence and AI competence frameworks, as well as recognized principles of educational measurement. Since the proposed model has not been empirically validated within the scope of this article, its psychometric properties are presented as matters for future investigation rather than established findings. The proposed approach provides a methodological basis for developing evidence-based assessment instruments for higher education.*

Keywords: *artificial intelligence, information security competence, higher education, diagnostic assessment, assessment criteria, performance indicators, reliability, validity, digital competence, AI literacy.*

Introduction

Artificial intelligence has become an increasingly important component of contemporary higher education. Students use AI-based applications to search for information, generate text, summarize



academic materials, translate documents, analyse data, and support problem-solving. Although these applications can facilitate learning, their use also introduces new challenges related to information security, privacy, data integrity, and responsible digital participation. The growing dependence on digital platforms requires university students to possess more than basic computer skills. They must understand potential security threats, recognize suspicious digital communications, protect personal information, evaluate the reliability of digital content, and make informed decisions when interacting with AI systems. In particular, generative AI may produce convincing but inaccurate information, reproduce sensitive information, or facilitate the creation of deceptive content. Students therefore need the ability to assess both the technical and informational risks associated with digital technologies.

The European Digital Competence Framework for Citizens, known as DigComp 2.2, provides an established reference for understanding digital competence through knowledge, skills, and attitudes. It includes digital safety, cybersecurity, privacy, and responsible engagement with emerging technologies, including AI (Vuorikari et al., 2022). Similarly, the UNESCO AI Competency Framework for Students identifies human-centred thinking, AI ethics, AI techniques and applications, and AI system design as important dimensions of student competence (Miao et al., 2024). These frameworks offer complementary perspectives for developing an assessment model that addresses information security in AI-supported educational environments. However, defining competence does not automatically provide a reliable means of measuring it. A student may correctly answer questions about cybersecurity while failing to identify a phishing message in a realistic situation. Another student may report confidence in protecting personal data but demonstrate unsafe behaviour when using an AI application. Consequently, an assessment instrument should combine different sources of evidence rather than rely exclusively on self-reported knowledge or attitudes.

The central research problem addressed in this article is the methodological challenge of measuring students' information security competence through clearly defined criteria, observable indicators, and reliable diagnostic procedures. The purpose of the article is to propose a multidimensional diagnostic assessment framework for evaluating students' information security competence in the age of artificial intelligence and to establish a methodological approach for examining the reliability and validity of the associated assessment instruments. The article addresses three research questions: which criteria and indicators can adequately represent students' information security competence in AI-supported learning environments; which diagnostic methods can provide evidence of students' actual knowledge, skills, and behaviour; and which psychometric procedures are necessary to establish the reliability and validity of the proposed assessment framework?

Theoretical Background and Literature Review



Information security competence can be understood as the integrated capacity to recognize information-related risks, apply appropriate protective measures, evaluate digital information critically, and behave responsibly when accessing, processing, storing, and sharing information. This definition distinguishes competence from knowledge alone. Knowledge concerns the understanding of relevant concepts and principles, whereas competence also involves applying that knowledge in practical situations and making appropriate decisions under changing conditions. For university students, information security competence encompasses several interconnected areas, including authentication and account protection, recognition of social engineering, personal data protection, secure use of digital services, evaluation of information sources, and appropriate responses to suspected security incidents.

The National Institute of Standards and Technology Cybersecurity Framework 2.0 provides a structured approach to understanding and managing cybersecurity risks. Its six core functions are Govern, Identify, Protect, Detect, Respond, and Recover (Pascoe et al., 2024). Although this framework was developed primarily to support organizational cybersecurity risk management, its concepts can inform the design of educational scenarios in which students identify threats, select protective measures, and determine appropriate responses to security incidents. Nevertheless, organizational cybersecurity frameworks should not be treated as direct measures of individual student competence. Their principles must be adapted to the educational context, students' responsibilities, and the specific outcomes that an assessment instrument is intended to measure. The integration of AI into education changes the conditions under which students access, evaluate, and share information. Generative AI tools can produce text, images, audio, and other digital outputs that appear credible even when they contain errors or misleading claims. AI-generated content can also be used in impersonation, fraudulent communications, and social engineering. Another important concern is the disclosure of sensitive information. Students may unintentionally submit personal identifiers, confidential academic documents, research data, or information belonging to other individuals to external AI services. The consequences depend on the service, its configuration, its data-handling practices, and the nature of the information submitted. AI-related risks therefore require students to understand data minimization, confidentiality, source verification, authentication, and the limitations of automated systems. They should also recognize that AI-generated content is not automatically accurate, secure, unbiased, or suitable for academic use. The UNESCO AI Competency Framework for Students emphasizes ethical, human-centred, and informed engagement with AI technologies (Miao et al., 2024). DigComp 2.2 also incorporates examples related to emerging technologies and the responsible, critical, and safe use of digital systems (Vuorikari et al., 2022). These publications support the inclusion of AI-related information evaluation, privacy protection, and ethical decision-making in a broader information security



assessment model. However, AI literacy and information security competence are not identical constructs. AI literacy includes understanding and using AI systems, whereas information security competence focuses more specifically on recognizing and managing risks to information, systems, and individuals. An appropriate diagnostic framework should therefore integrate relevant AI-related competencies without treating all aspects of AI literacy as information security outcomes.

The development of a diagnostic assessment instrument requires a clear definition of the construct being measured. Without such a definition, assessment items may represent different abilities inconsistently, resulting in scores that are difficult to interpret. Educational measurement distinguishes reliability from validity. Reliability concerns the consistency or precision of scores under specified conditions, whereas validity concerns the extent to which evidence and theory support the intended interpretations and uses of assessment results. Cronbach's alpha is a widely used coefficient for examining the internal consistency of multi-item scales (Cronbach, 1951). However, a high alpha coefficient does not independently establish that an instrument measures the intended construct, nor does it demonstrate that all items measure a single dimension. Its interpretation depends on the structure of the instrument, the properties of the items, and the assumptions underlying the analysis.

For multidimensional competence assessment, it may be more appropriate to examine the internal consistency of each theoretically coherent subscale rather than calculate a single coefficient for all items. McDonald's omega can provide an additional estimate of reliability when its underlying measurement assumptions are appropriate. Reliability can also be examined through repeated administration, agreement between assessors, and the consistency of scoring procedures. Construct validity requires evidence that the proposed dimensions adequately represent the intended competence and that observed score patterns are consistent with theoretical expectations. These principles imply that a diagnostic framework should be evaluated through several complementary procedures. No single coefficient or statistical test can establish the overall quality of an assessment instrument.

Research Methodology

This article adopts a conceptual and methodological research design. It develops a proposed framework for measuring students' information security competence by synthesizing established digital competence, AI competence, cybersecurity risk management, and educational measurement principles. The framework is intended for adaptation and empirical testing in higher education institutions. It is not presented as an already validated psychometric instrument. Its final structure, item composition, scoring rules, and measurement properties should be established through systematic research. The proposed development process consists of defining the construct,



identifying assessment criteria and indicators, developing diagnostic instruments, collecting pilot data, and evaluating reliability and validity.

For measurement purposes, students' information security competence is defined as their demonstrated ability to understand information security principles, apply protective procedures, evaluate digital information critically, adopt secure behaviours, and make responsible ethical and legal decisions when using digital and AI-based technologies. This operational definition identifies five proposed dimensions: cognitive competence, operational competence, analytical competence, behavioural competence, and ethical-legal competence. These dimensions constitute a proposed analytical model rather than an empirically confirmed factor structure. Their adequacy must be examined through expert review and empirical investigation.

The cognitive criterion concerns students' understanding of information security principles and common threats. Relevant indicators include knowledge of authentication, password security, phishing, malware, privacy, data protection, and the limitations of AI-generated information. A structured knowledge test can be used to measure this dimension. The operational criterion concerns the ability to apply security principles in practical situations. Indicators include identifying suspicious links, selecting appropriate account protection measures, configuring privacy settings, and choosing suitable actions when a security incident is suspected. Performance-based tasks and simulated scenarios are appropriate assessment methods.

The analytical criterion concerns the critical evaluation of information and digital content. Indicators include checking the credibility of sources, comparing claims across independent sources, identifying inconsistencies in AI-generated outputs, and recognizing the limitations of automated content detection. Scenario-based tasks can provide evidence of students' reasoning and verification practices. The behavioural criterion concerns the extent to which students demonstrate safe digital practices. Indicators include avoiding unnecessary disclosure of personal information, using appropriate authentication procedures, reviewing data-sharing permissions, and following institutional security guidance. Because self-reported behaviour may differ from actual behaviour, questionnaires should be supplemented by scenario-based or performance-based evidence wherever feasible and ethically appropriate.

The ethical-legal criterion concerns students' ability to make responsible decisions about data use, privacy, intellectual property, academic integrity, and the appropriate use of AI. Indicators include identifying confidentiality concerns, respecting the rights of other individuals, recognizing inappropriate disclosure, and explaining the ethical implications of specific digital actions. Each indicator should be associated with an observable response or performance outcome. Vague statements such as "understands cybersecurity" are insufficient unless translated into assessable behaviours, such as identifying a fraudulent login request and explaining the appropriate response.



The proposed diagnostic instrument should combine multiple assessment methods to reduce dependence on any single source of evidence. The first component should be a knowledge test containing objectively scored questions about information security principles, common threats, privacy, and AI-related risks. The second component should consist of practical tasks. Students might be asked to examine a simulated email, identify warning signs, choose an appropriate authentication procedure, or determine which information should not be entered into a public AI service. The third component should contain analytical scenarios requiring students to evaluate AI-generated claims, verify sources, and justify their decisions. The fourth component may be a behavioural questionnaire examining students' reported security practices. Its results should be interpreted cautiously because respondents may overestimate their own competence or provide socially desirable answers. The fifth component should consist of ethical and legal case studies requiring students to explain how they would respond to situations involving confidential data, academic work, or the inappropriate use of digital content. The tasks should be reviewed to ensure that they are understandable, relevant to the target student population, accessible to students with different levels of digital experience, and aligned with the intended assessment criteria.

A criterion-referenced scoring system can be used to assess each dimension separately. For example, a knowledge test may be scored according to the number of correct responses, while practical tasks may be evaluated using an explicit performance rubric. A four-level descriptive scale can support interpretation. At the basic level, the student demonstrates limited understanding of security principles and requires substantial guidance when responding to common threats. At the developing level, the student recognizes common threats and applies basic protective measures in familiar situations but has difficulty dealing with unfamiliar or complex scenarios. At the competent level, the student independently applies appropriate security practices in common situations, evaluates information sources, and justifies decisions using relevant security principles. At the advanced level, the student critically analyses complex scenarios, anticipates potential risks, compares alternative protective measures, and provides well-reasoned explanations for security-related decisions. These descriptions are provisional performance standards. They should be refined using expert judgment, pilot testing, and a systematic standard-setting procedure before they are used for consequential decisions. The five dimensions should initially be reported as separate scores. If a composite score is subsequently proposed, the weighting scheme must be justified theoretically and empirically. A single total score may conceal important differences between knowledge, practical performance, and behavioural competence.

Reliability and Validity of the Diagnostic Assessment Framework

Content validity concerns whether the assessment adequately represents the construct and its intended domain. To examine content validity, the proposed criteria, indicators, and assessment



tasks should be reviewed by experts in information security, educational assessment, AI, and higher education. Experts should evaluate the relevance, clarity, representativeness, and suitability of individual items. Their assessments can be summarized using a content validity index or Aiken's V, provided that the selected procedure and its assumptions are clearly specified. For Aiken's V, the calculation is based on expert ratings relative to the minimum rating on the chosen scale. Its interpretation should consider the number of experts, the rating scale, and the uncertainty associated with the estimate. A numerical value should not be treated as definitive evidence without considering these factors. Expert review should also examine whether the assessment includes both conventional cybersecurity threats and risks specifically associated with AI-supported learning. Particular attention should be given to privacy, misleading AI-generated content, identity impersonation, and responsible data handling.

Internal consistency analysis examines the degree to which items within a scale provide consistent information about the intended dimension. Cronbach's alpha may be calculated for appropriate multi-item scales. McDonald's omega can be considered as a complementary measure, particularly when a factor model is available and its assumptions are adequately supported. A coefficient around 0.70 is often used as a preliminary reference in some research settings, but it is not a universal acceptance threshold. Appropriate values depend on the purpose of the instrument, the stakes of the assessment, the number of items, the dimensionality of the construct, and the consequences of measurement error. Very high internal consistency does not necessarily indicate a superior instrument. It can also reflect redundant items that assess nearly identical content. Conversely, a multidimensional competence framework may not produce a high overall coefficient because its components represent distinct but related abilities. For this reason, internal consistency should be examined separately for theoretically coherent subscales. Item-total relationships, response distributions, and the consequences of removing items should also be evaluated.

Test-retest reliability examines the stability of scores across two administrations when the underlying competence is expected to remain reasonably stable. The diagnostic instrument can be administered to the same participants on two occasions separated by an appropriate interval. The interval should be long enough to reduce recall of specific responses but short enough to limit substantial changes in competence. Depending on the data and measurement design, an intraclass correlation coefficient or an appropriate correlation-based statistic may be used. Absolute agreement and consistency should be distinguished when selecting an intraclass correlation model. The interpretation must account for learning effects, changes in students' exposure to security threats, and differences in testing conditions. If students receive training between administrations, score changes may reflect genuine learning rather than poor reliability.



Performance-based assessment often requires human judgment. For example, assessors may evaluate students' explanations of why a message is suspicious or how they would respond to a data disclosure incident. To improve scoring consistency, each task should have a detailed rubric specifying the expected evidence and scoring rules. Assessors should receive training and practise applying the rubric to sample responses. Cohen's kappa may be appropriate for agreement between two assessors classifying responses into categories. Weighted kappa can be considered when categories are ordinal. Intraclass correlation coefficients may be appropriate for numerical ratings, depending on the design and assumptions. Agreement statistics should be selected according to the number of assessors, the scale of measurement, and the assessment design. Raw percentage agreement alone may be insufficient because it does not account for agreement expected by chance. Construct validity concerns whether the collected evidence supports the intended interpretation of assessment scores. The proposed five-dimensional model should first be examined through theoretical analysis and expert review. Exploratory factor analysis may be used when the factor structure is uncertain and sufficient pilot data are available. Confirmatory factor analysis may then be used to examine a specified measurement model in an appropriate sample. These procedures require careful attention to sample size, item characteristics, the measurement scale, factor identification, and model fit. A five-dimensional structure should not be declared valid merely because it was proposed theoretically.

Evidence may also be collected by examining relationships between diagnostic scores and other relevant measures. For example, practical performance may be compared with results from a separately developed cybersecurity knowledge test. Such relationships should be interpreted according to the theoretical expectations established before analysis. Convergent and discriminant evidence may help establish whether the proposed dimensions relate to relevant constructs while remaining distinguishable from other abilities. However, correlations alone cannot establish validity, and independent evidence should be considered whenever possible.

Reliability and validity must also be considered in relation to the intended population. Students may differ in prior cybersecurity education, digital experience, language proficiency, disability-related accessibility needs, and familiarity with specific AI tools. An assessment that relies heavily on knowledge of one commercial platform may measure platform familiarity rather than general information security competence. Similarly, poorly written scenarios may disadvantage students because of language complexity rather than security-related deficiencies. The diagnostic framework should therefore use clear language, culturally and educationally appropriate scenarios, and accessible assessment procedures. Where sample size and research design permit, measurement invariance or differential item functioning can be examined to identify potential differences in how



items operate across relevant groups. Such analyses should be interpreted cautiously and should not be used to make unsupported claims about individual students or demographic groups.

Proposed Results and Discussion

The principal outcome of the present conceptual and methodological analysis is a proposed structure for measuring information security competence through five related dimensions. These dimensions address knowledge, practical application, critical information evaluation, secure behaviour, and ethical-legal decision-making. The framework extends conventional knowledge-based assessment by incorporating practical and scenario-based evidence. This is important because students' ability to describe a security principle does not necessarily demonstrate their ability to apply it in practice.

The inclusion of an analytical dimension reflects the need to evaluate information generated or processed by AI systems. Students should be able to distinguish between a plausible statement and a verified claim, consult appropriate sources, and recognize that automated content may contain errors or misleading information. The behavioural dimension addresses the difference between knowing security principles and following them consistently. Self-report measures can provide useful information about attitudes and reported practices, but they should not be interpreted as direct proof of actual behaviour. Practical tasks and other ethically collected evidence can provide complementary information.

The ethical-legal dimension recognizes that information security decisions often involve obligations beyond technical protection. Students must consider privacy, confidentiality, intellectual property, academic integrity, and the rights of other individuals when using digital and AI-based tools. The proposed framework is consistent in its general orientation with DigComp 2.2, the UNESCO AI Competency Framework for Students, and the risk-oriented approach of the NIST Cybersecurity Framework 2.0. However, it is an educational measurement proposal rather than a reproduction or officially endorsed extension of any of these frameworks. Its practical contribution lies in connecting competence dimensions to observable indicators, assessment methods, and a planned process of psychometric evaluation.

Nevertheless, several limitations should be acknowledged. First, the proposed dimensions and their relationships have not been empirically confirmed in this article. Second, the optimal number and wording of assessment items remain to be established. Third, the reliability and validity of the instrument may differ across disciplines, institutions, educational levels, and language contexts. Fourth, AI technologies and associated security risks evolve rapidly. The instrument should therefore be reviewed periodically to maintain the relevance of its scenarios and indicators. Finally, reliability coefficients cannot substitute for evidence that the assessment supports the interpretations and decisions for which it is intended. Future empirical research should develop a complete



instrument, obtain expert feedback, conduct pilot testing, and analyse the resulting data. Such research would establish whether the proposed dimensions can be measured reliably and whether the assessment provides meaningful evidence of students' information security competence.

Recommendations for Empirical Validation

The proposed framework can be developed through a systematic empirical study. First, researchers should prepare an initial item pool based on the five criteria and relevant cybersecurity and AI competence literature. Each item should be linked to a specific indicator and an intended scoring rule. Second, subject-matter experts should evaluate the content coverage, clarity, and relevance of the items. Items that are ambiguous, redundant, or unrelated to the intended construct should be revised or removed. Third, cognitive interviews or a small pilot study should be conducted to determine whether students understand the questions and scenarios as intended. This stage can identify problems that are not apparent during expert review.

Fourth, the revised instrument should be administered to a sufficiently diverse student sample. The sample size should be determined in relation to the planned statistical analyses, model complexity, and anticipated data quality rather than by applying an arbitrary universal rule. Fifth, researchers should examine item performance, score distributions, missing responses, internal consistency, and the reliability of performance-based scoring. Factor analysis should be conducted when the research design and available data support it. Sixth, the proposed performance levels should be established through a documented standard-setting process. Score boundaries should not be selected solely because they produce convenient categories. Finally, the assessment should be evaluated for fairness, accessibility, and practical usefulness. The results should inform improvements to cybersecurity education rather than be used to label students without sufficient evidence.

An empirical study should report its participant characteristics, sampling procedures, instrument development process, statistical methods, coefficients, uncertainty estimates where appropriate, and limitations transparently. Any numerical results must come from collected and analysed data.

Conclusion

Measuring students' information security competence in the age of artificial intelligence requires an assessment approach that captures more than theoretical knowledge. Students must be able to understand security principles, apply protective measures, evaluate information critically, demonstrate safe digital practices, and make responsible ethical and legal decisions. This article has proposed a five-dimensional diagnostic framework comprising cognitive, operational, analytical, behavioural, and ethical-legal criteria. Each dimension is associated with observable indicators and suitable assessment methods. The proposed approach combines knowledge tests, practical tasks, analytical scenarios, behavioural questionnaires, and ethical case studies.



The article has also outlined a methodological approach for examining the quality of the diagnostic instrument. Content review, internal consistency analysis, test–retest reliability, inter-rater agreement, construct validation, and fairness analysis can provide complementary evidence about the instrument’s measurement properties. A central conclusion is that reliability and validity must be established through empirical evidence rather than assumed from the theoretical quality of a proposed framework. No single coefficient can demonstrate that an assessment instrument is suitable for every population or purpose.

The proposed framework should therefore be regarded as a foundation for instrument development and subsequent empirical validation. Its implementation in higher education may support more systematic identification of students’ information security strengths and learning needs, provided that the resulting assessment is tested rigorously and interpreted within its documented limitations.

References

1. Загвязинский В.И., Атаханов Р. Методология и методы психолого-педагогического исследования. – М.: Академия, 2005. – 208 с.
2. Беспалько В.П. Слагаемые педагогической технологии. – М.: Педагогика, 1989. – 192 с.
3. Новиков Д.А. Статистические методы в педагогических исследованиях (типовые случаи). – М.: МЗ-Пресс, 2004. – 67 с.
4. Богатырева Ю.И. Подготовка будущих педагогов к обеспечению информационной безопасности школьников: дис. ... д-ра пед. наук. – Тула, 2014. – 405 с.
5. Привалов А.Н., Богатырева Ю.И. Модель формирования компетентности будущих педагогов в области информационной безопасности // Информатика и образование. – 2013. – № 5. – С. 45–49.
6. Hadlington L. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours // Heliyon. – 2017. – Vol. 3, № 7. – Article e00346.
7. Vuorikari R., Kluzer S., Punie Y. DigComp 2.2: The Digital Competence Framework for Citizens. – Luxembourg: Publications Office of the European Union, 2022. – 133 p.
8. Laupichler M.C., Aster A., Schirch J., Raupach T. Artificial intelligence literacy in higher and adult education: A scoping literature review // Computers and Education: Artificial Intelligence. – 2022. – Vol. 3. – Article 100101.
9. Ng D.T.K., Leung J.K.L., Chu S.K.W., Qiao M.S. Conceptualizing AI literacy: An exploratory review // Computers and Education: Artificial Intelligence. – 2021. – Vol. 2. – Article 100041.



10. O'zbekiston Respublikasining "Shaxsga doir ma'lumotlar to'g'risida"gi Qonuni. 2019-yil 2-iyul, O'RQ-547-son.
11. OWASP Top 10 for Large Language Model Applications. Version 1.1. – OWASP Foundation, 2023. – 33 p.
12. Tolipov O'.Q., Usmonboyeva M. Pedagogik texnologiyalarning tatbiqiy asoslari. – Toshkent: Fan, 2006. – 261 b.