



**MULTI-COMPONENT STRUCTURE AND
INDICATOR-BASED DIAGNOSTIC MODEL OF
INFORMATION SECURITY COMPETENCE IN
STUDENTS**

Shukurov Dadanur Tohir ugli

*A lecturer of the Department of Engineering and Digital
Technologies, Sarbon University,*

dadanur0094@gmail.com

ARTICLE INFO:

Received: 25.10.2026

Revised: 26.10.2026

Accepted: 27.10.2026

KEY WORDS:

*information security
competence, structure,
criterion, indicator,
pedagogical diagnostics,
qualimetrics,
development level.*

ABSTRACT

The article investigates the operationalization of students' information security competence for pedagogical diagnostics. Domestic scientific sources, DigComp 2.2, the NICE Framework, and human-centric security assessment approaches were comparatively analyzed based on criterion-based content analysis, competency decomposition, and qualimetric modeling. As a result, a framework consisting of cognitive, risk-analytical, operational-technological, value-ethical, and reflexive-behavioral components, along with five criteria, twenty indicators, and four development levels, was developed. The diagnostic model integrates knowledge tests with situational tasks, digital work products, observation, and reflective evidence. The proposed approach makes it possible to evaluate competence not merely through theoretical awareness, but at the level of threat identification, execution of security controls, responsible decision-making, and transfer to novel situations.

INTRODUCTION

The expansion of the digital educational environment has substantially increased the volume and scope of students' interactions with information. E-learning platforms, cloud collaboration suites, mobile applications, videoconferencing, online libraries, generative artificial intelligence, and social media networks have become routine tools of educational practice. Concurrently, threats such as account takeover, phishing, malware files, misconfigured permissions, personal



data disclosure, corruption of academic records, and copyright infringement directly affect educational outcomes. Under these conditions, information security competence must be treated not merely as an accumulation of technical knowledge, but as an integrated system encompassing risk perception, selection of protective measures, responsible behavior, and self-monitoring capabilities.

Prior to cultivating competence, its structural composition and the evidence required for its assessment must be defined. Otherwise, educational objectives remain limited to the vague notion of "knows security," and assessment remains at the level of memorizing definitions. Ganiev, Karimov, and Tashev systematize the technical foundations of information security, including confidentiality, integrity, availability, authentication, access control, and security policies [1]. From a pedagogical standpoint, this content must be translated into the student's actual activity, values, and behavior.

Analyzing the factors and criteria for cultivating information competence, Karimova identifies knowledge, activity, motivation, and reflection as interrelated components [2; 3]. Boboqulova highlights the necessity of digital responsibility and awareness alongside technical skills within higher education security culture [4]. Tuxtabayeva and Ayitqulova examine the potential of gamification, simulation, and interactive methods in developing students' security behavior [5]. Boymanov substantiates that information culture, ethical values, and social responsibility are integral components of security education [6]. These perspectives demonstrate that assessing competence through knowledge-based testing alone is insufficient.

Ambiguity in criteria and indicators within pedagogical diagnostics causes two distinct errors. First, a student may be rated as competent simply for answering theoretical questions correctly, despite failing to identify a real phishing message or exposing a cloud document to the public. Second, a student proficient in technical actions may receive a high score while remaining oblivious to ethical and legal consequences. Consequently, diagnostics must maintain a balanced synthesis of evidence across knowledge, analysis, practical performance, values, and self-regulation.

DigComp 2.2 links digital safety to protecting devices, personal data and privacy, health and well-being, and the environment [10]. The NICE Framework outlines cybersecurity work roles through tasks, knowledge, and skills [11]. The HAIS-Q approach seeks to quantify the alignment among security knowledge, attitude, and behavior [12]. Their pedagogical integration enables the unification of general digital safety principles with concrete actions in academic and professional tasks.

The objective of this article is to design a multi-component structure for students' information security competence, operationalize its criteria and indicators, describe its levels of development, and propose a multi-evidence diagnostic model. The research question is formulated as follows: which components and forms of assessment evidence reliably capture a



student's information security awareness, practical readiness, responsible decision-making, and ability to transfer skills to novel situations?

MATERIALS AND METHODS

This study is theoretical and model-driven, examining nine domestic and three international sources. Three selection criteria were applied: coverage of structural dimensions of information security or information competence; inclusion of criteria and indicators suitable for pedagogical assessment; and applicability to higher education or digital learning contexts. Concepts across the bibliographic corpus were coded under "knowledge," "risk analysis," "practical protection," "ethical-legal responsibility," "behavior," and "reflection".

The first method is criterion-based content analysis. Definitions, constituent components, expected behaviors, and assessment evidence from each source were entered into a comparative matrix. Semantic units were grouped according to their recurrence and pedagogical significance. Consequently, partially overlapping terms such as "information literacy," "security culture," "cybersecurity skills," and "digital responsibility" were harmonized into a unified competence structure.

The second method is competency decomposition. The overarching outcome—"the student identifies risks in a digital scenario, makes reasoned decisions, implements protective measures, and evaluates the outcomes"—was decomposed into observable discrete actions. Each action was framed around guiding questions: "what do they know?", "what do they analyze?", "what can they perform?", "what values guide them?", and "how do they monitor their activity?"

The third method is qualimetric modeling. To maintain structural balance among the five components, weighting coefficients were established: cognitive — 0.20; risk-analytical — 0.20; operational-technological — 0.25; value-ethical — 0.15; and reflexive-behavioral — 0.20. The aggregate index is calculated using the formula:

$$\$I = 0.20K + 0.20R + 0.25O + 0.15Q + 0.20F\$$$

The purpose of these weights is to assign slight priority to practical execution while preventing knowledge, analytical thought, and behavioral ethics from being marginalized.

The fourth method is evidence triangulation. Each indicator is corroborated using at least two independent types of evidence: objective knowledge tests, situational choices, practical tasks, digital artifacts, direct observation, and self-assessments accompanied by reflective explanations. Rather than evaluating competence through an isolated test score, diagnostic consistency across evidence streams is evaluated. For example, a student must state the parameters of a strong password, generate one within a password manager, and articulate the rationale behind their implementation.

Four levels of development were defined: reproductive, situational-practical, independent-transfer, and reflexive-responsible. Level thresholds are determined by combining the overall index with mandatory critical indicators. Even if a student attains a high aggregate numerical score, demonstrating critical vulnerabilities—such as disclosing personal data or concealing a



security incident—precludes advancement to higher levels. This constraint preserves the ethical and functional integrity of the diagnostic framework.

RESULTS

Content analysis yielded a five-component structure of information security competence. The cognitive component denotes knowledge of fundamental terms, threats, security solutions, and regulatory guidelines. The risk-analytical component encompasses contextualizing assets, threats, vulnerabilities, and potential impacts to prioritize salient risks. The operational-technological component reflects the practical configuration and verification of security tools. The value-ethical component is grounded in respect for confidentiality, academic integrity, copyright compliance, and non-maleficence. The reflexive-behavioral component captures habitual security routines, self-monitoring, incident reporting, and the transfer of safety practices to new contexts.

The model operates along the structural continuum of "knowledge–analysis–action–responsibility–reflection". This sequence is non-linear in practice: when encountering a live threat, students draw upon previous experience and ethical values, execute technical measures, verify results, and calibrate subsequent behavior. Consequently, while components can be evaluated discretely, overall competence reflects their integrative performance.

Component	Criterion	Key Indicators	Priority Evidence
Cognitive	Substantive clarity	Distinguishes threats from vulnerabilities; explains CIA principles; identifies legal regulations; articulates functions of security tools.	Objective test, concept mapping.
Risk-analytical	Justified situational assessment	Identifies digital assets; evaluates likelihood and impact; verifies source credibility; selects prioritized mitigation measures.	Case study analysis, risk mapping.
Operational-technological	Technical accuracy of defense	Enables MFA; configures access controls; creates backups; executes initial incident response protocols.	Practical assignment, verified screenshot evidence.
Value-ethical	Responsible decision-making	Safeguards confidentiality; adheres to academic integrity; respects licensing and attribution; chooses non-harmful interventions.	Ethical dilemma task, reasoned justification statement.
Reflexive-behavioral	Consistent and transferable habits	Applies verification routines; acknowledges mistakes; reports incidents; adapts security rules to novel digital environments.	Direct observation, reflective logs, portfolio.

Indicators are intentionally formulated using operationalized action verbs. Vague, unobservable phrasing like "understands" was replaced with concrete actions that yield



verifiable evidence, such as "distinguishes," "justifies," "configures," "verifies," and "reports". This alignment bridges learning outcomes, learning tasks, and assessment metrics.

Level	Typical Student Performance	Diagnostic Indicators	Pedagogical Intervention
1.Reproductive	Recalls rules, relies on demonstrations, operates with guidance in simple situations.	Demonstrates isolated knowledge; behavioral consistency and transfer are low.	Visual step-by-step guides, guided micro-tasks.
2. Situational-practical	Executes security actions in routine contexts, provides partial explanations for choices.	Possesses technical skills; exhibits hesitation in complex scenarios.	Scenario-based cases, targeted feedback, iterative drills.
3. Independent-transfer	Analyzes risks in unfamiliar situations and selects appropriate measures independently.	Demonstrates sustained alignment across theoretical and practical evidence.	Multi-stage projects, authentic professional simulations.
4. Reflexive-responsible	Manages individual and peer digital safety, justifies decisions, promptly reports incidents.	Behavior is stable, ethical, and readily transferred across domains.	Peer mentoring roles, institutional security initiatives.

Differentiating performance solely through aggregate numerical marks introduces diagnostic vulnerabilities. Therefore, three indicators are designated as mandatory "critical gates": protecting personal data, halting active or suspicious operations, and promptly reporting incidents via official channels. Failure to satisfy any critical indicator automatically restricts a student from advancing to Level 3 or Level 4. This safeguard ensures that high theoretical scores cannot mask hazardous operational behavior.

Assessment Instrument	Weight	Target Construct	Implementation Example
Short objective test	15%	Knowledge of terminology, operational principles, and security controls.	Identifying phishing markers in email headers.
Situational task	25%	Risk evaluation, contextual reasoning, and decision justification.	Developing an action plan for a spoofed LMS communication.
Practical task	30%	Correct execution and technical configuration of security measures.	Setting up MFA and defining cloud file access permissions.
Digital portfolio	20%	Tangible artifacts, transfer of practices, and longitudinal	Curated risk maps, audit screenshots, incident logs.



		progression.	
Reflection and observation	10%	Habitual routines, responsibility, and metacognitive learning from errors.	Structured "What I verified and why" activity logs.

In this multi-evidence model, the weight of conventional testing is deliberately constrained, while practical and contextual evaluations are prioritized. The portfolio captures cumulative learning trajectories across the academic term rather than relying on an isolated examination snapshot. Structured reflection is employed not as a cosmetic exercise, but to inspect the underlying logic of a student's decisions and verify behavioral persistence.

The diagnostic sequence is organized across four distinct stages. First, initial diagnostic screening identifies baseline competencies, isolating strengths and weaknesses. Second, ongoing formative evaluations during regular coursework provide immediate, corrective feedback for every technical or procedural error. Third, capstone case simulations or integrative projects assess how the components function in unison. Fourth, students evaluate their completed portfolios, analyzing errors, remedies, and overall competency progression.

The composite index standardizes diagnostic decisions without replacing qualitative educator appraisal. For example, if $SK=80$, $SR=70$, $SO=90$, $SQ=75$, and $SF=65$, the aggregate index equals 78.25. While this composite score falls within the range for Level 3, failing the mandatory incident reporting indicator caps the student's rating at Level 2, prompting a targeted corrective assignment. Consequently, quantitative metrics remain tied to qualitative proof and safety-critical baselines.

To evaluate cohort-level outcomes, instructors construct aggregated "competence profiles". By plotting mean performance across components, profiles can highlight systemic discrepancies—such as high cognitive mastery coexisting with deficient reflexive behavior. In such instances, scheduling additional lectures is ineffective; instructional efforts must pivot toward simulation drills, peer risk audits, incident handling exercises, and verification checklists. Diagnostics thus functions as a driver of instructional design rather than an endpoint of grading.

DISCUSSION

The proposed framework integrates the dispersed domestic constructs of information competence, security culture, and digital responsibility into a cohesive educational outcome. While Karimova's criteria emphasize the integration of knowledge and practical activity [2; 3], Boymanov and Boboqulova underscore the cultural and axiological dimensions of security [4; 6]. The technical foundations systematized by Ganiev et al. anchor the operational indicators in technical precision [1]. As a result, the model bridges technical instruction and normative personal development without setting them in opposition.

In comparison to DigComp 2.2, this model preserves core general digital safety dimensions while introducing higher-education-specific requirements, such as academic integrity,



collaborative cloud data hygiene, scientific data stewardship, and formal incident reporting. The NICE Framework is valuable for standardizing task descriptions, but it does not specify pedagogical progressions or educational values. Consequently, NICE terminology was leveraged for competency decomposition, whereas DigComp served to establish comprehensive thematic scope.

A primary advantage of this model is its departure from the "one indicator—one test" approach in favor of evidence triangulation. Information security behaviors are highly susceptible to social desirability bias: students easily select compliant answers on surveys while bypassing security protocols in practice for convenience. Authentic scenarios, practical system interactions, and behavioral observations expose these discrepancies. While the HAIS-Q instrument highlights the interrelation of knowledge, attitude, and behavior [12], this model operationalizes those connections within concrete academic tasks and portfolio milestones.

A limitation of the model is that component weightings were derived theoretically and require empirical calibration across different academic disciplines. For computer science and software engineering students, the operational component may warrant higher weighting, whereas for humanities or pedagogical fields, indicators addressing ethical, communicative, and media security may require greater emphasis. Subsequent research must assess inter-rater agreement, run pilot tests, and verify internal consistency and criterion validity.

The administration of diagnostic instruments requires strict adherence to privacy and ethical standards. Instructors must never inspect students' personal credentials, private accounts, or authentic confidential records. All practical evaluations must occur within sandbox accounts, synthetic data repositories, and isolated environments, with results applied strictly for developmental learning. This structural safeguard reinforces the value-ethical component of the competence itself.

Requirements for instrument design. Situational tasks must measure security decision-making rather than testing reading speed through unnecessary technical jargon. Every scenario must articulate the asset, threat indicators, decision junctions, and expected evidence, utilizing distractors that reflect authentic threats without adding artificial complexity. If a scenario is linguistically burdensome for specific cohorts, performance will reflect reading comprehension gaps rather than security competence. Pilot testing must therefore assess linguistic accessibility and time burdens alongside content validity.

Inter-rater consistency. To mitigate subjectivity when scoring performance logs and reflective texts, evaluators require analytic rubrics, benchmark evidence, and borderline performance samples. Having two independent evaluators score identical student artifacts and resolve score variances sharpens criteria interpretation. Explicit performance descriptors are critical for complex constructs such as "justifies decisions" or "demonstrates responsible communication".



Integrating diagnostics into pedagogy. Returning an isolated numerical grade to students diminishes the formative potential of the assessment. Feedback is ideally organized into three concise elements: verified competencies, the single most critical security error, and a specific follow-up task to remediate it. For example, feedback such as: "You identified the phishing attempt accurately, but failed to verify it through official channels; complete the communication verification log in the next exercise" directs the student toward concrete behavioral change.

Curriculum-level utility. When anonymized competence profiles are evaluated across entire academic degree programs, faculty can detect which indicators are underperforming within specific courses or terms. If a recurring deficiency appears across cohorts, the curriculum, tools, or instructional environment must be adjusted rather than attributing the deficit to individual learners. In this manner, diagnostic assessment transitions from a compliance audit into an active mechanism of quality assurance.

CONCLUSION

This study designed a multi-component structure of students' information security competence comprising cognitive, risk-analytical, operational-technological, value-ethical, and reflexive-behavioral components. A diagnostic matrix establishing specific criteria, four operational indicators per component, and prioritized forms of evidence was defined.

Competency maturation is classified across four levels: reproductive, situational-practical, independent-transfer, and reflexive-responsible. The composite index weighs knowledge, analysis, practical skill, ethics, and habitual behavior, while mandatory critical indicators prevent inflated ratings when unsafe actions occur.

The diagnostic model synthesizes objective tests, contextual tasks, practical technical work, digital portfolios, direct observation, and self-reflection. Consequently, outcomes demonstrate not what a student memorizes, but how they identify risks in digital settings, what interventions they execute, how they defend decisions, and how they learn from operational mistakes. This framework provides an empirical basis for instructional planning, personalized remediation, cohort profiling, and longitudinal curriculum evaluation.

REFERENCES

1. G'aniyev S.K., Karimov M.M., Tashev K.A. Information security: textbook for higher education students. — Tashkent: Aloqachi, 2016.
2. Karimova N.B. Factors and criteria for developing information competence in students // Pedagogy and Psychology in the Modern World. — 2025. — 4(6). — pp. 15–18.
3. Karimova N.B. Developing students' information competence through digital educational technologies // Inter Education & Global Study. — 2024. — No. 8. — pp. 306–314.



4. Boboqulova A. The significance of information security culture in higher education // Academic Research in Modern Science. — 2025. — 4(38). — pp. 84–89. — DOI: 10.5281/zenodo.15746280.
5. Tuxtabayeva M., Ayitqulova G. Modern methods of developing information security culture in students // Young Scientists. — 2025. — 3(26). — pp. 41–43.
6. Boymanov J.I. The importance of information culture and social responsibility in integrating information security into the educational process // Science Shine. — 2025. — 1(14/49). — pp. 4–8. — DOI: 10.71337/inlibrary.uz.science-shine.126749.
7. Mahmudova M.H. Effectiveness and practical problems of modern educational technologies in enhancing media literacy // Foreign Languages in Uzbekistan. — 2025. — 11(5/64). — pp. 201–215. — DOI: 10.36078/1762334254.
8. Mirzayev T.T. Pedagogical models of developing information security competence based on blockchain technology // Pedagogical Skill. — 2025. — No. 5. — pp. 134–137.
9. Sattorov M. Didactic conditions for organizing independent study based on information and communication technologies. — Tashkent: Fan, 2020.
10. Vuorikari R., Kluzer S., Punie Y. DigComp 2.2: The Digital Competence Framework for Citizens. — Luxembourg: Publications Office of the European Union, 2022. — DOI: 10.2760/115376.
11. Petersen R., Santos D., Smith M.C., Wetzel K.A., Witte G. Workforce Framework for Cybersecurity (NICE Framework). NIST SP 800-181 Rev. 1. — Gaithersburg: NIST, 2020. — DOI: 10.6028/NIST.SP.800-181r1.
12. Parsons K., McCormac A., Butavicius M., Pattinson M., Jerram C. Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q) // Computers & Security. — 2014. — Vol. 42. — pp. 165–176. — DOI: 10.1016/j.cose.2013.12.003.