

A METHODOLOGY FOR IDENTIFYING AND CLASSIFYING CRITICAL INFORMATION INFRASTRUCTURE OBJECTS

Makhmudov Mirshod Bahodir ugli
*Leading specialist, Angren University;
applicant for the basic doctoral program (PhD)*
mirshodmakhmudov0515@gmail.com

Abstract:

Uzbekistan's rapid digital transformation has increased the dependence of public administration, finance, energy and healthcare on state information systems, while cyber threats against government information resources have grown. The Cybersecurity Strategy for 2026–2030 prioritizes the protection of critical information infrastructure, yet existing legislation does not provide clear, measurable criteria for deciding which systems qualify as critical. This paper aims to develop a practical, criteria-based methodology for identifying critical information infrastructure objects among state information systems and classifying them into tiers. Drawing on international risk-based practice (ISO/IEC 27001, NIST SP 800-53 and the EU's EPCIP programme), the methodology has three steps: compiling a unified register of information systems; scoring each system from 1 to 5 against six weighted criteria (socio-economic impact, national-security impact, interdependency, redundancy, threat exposure and recovery time objective); and classifying it by its total weighted score. Weights are to be set by an expert panel through a Delphi-style consensus process. The model separates systems into Tier I (critical, 4.00–5.00), Tier II (significant, 2.50–3.99) and Tier III (limited, 1.00–2.49), each linked to a proportionate level of oversight, from mandatory audits to baseline self-assessment. Unlike general impact-categorization schemes, it explicitly accounts for interdependency and national-security considerations. The proposed weights and thresholds remain a methodological proposal requiring empirical validation and sensitivity analysis. The methodology gives agencies a transparent, shared framework for directing limited resources to the systems that matter most

Keywords: information security, critical information infrastructure, state information systems, risk assessment, classification methodology

Introduction

Uzbekistan's push toward digital transformation over the past several years has dramatically expanded how public administration, finance, energy, and healthcare rely on information systems. Alongside that growth, the number and sophistication of cyberattacks aimed at government information resources have risen as well. On March 10, 2026, Presidential Decree No. PF-38 approved the country's Cybersecurity Strategy for 2026–2030, which names the protection of state information systems and critical information infrastructure from cyber threats as one of its priorities [1]. The Law "On Cybersecurity" sets out general principles for protecting state information resources, but it stops short of establishing clear, workable criteria for deciding which systems actually count as critical infrastructure in the first place [2].

Not every government information system carries the same weight. Some, if disrupted, could produce serious consequences at a national scale, while others are essentially local in their reach. Treating them all the same tends to spread resources too thin — low-priority systems get attention that comes at the expense of the ones that genuinely matter. This paper sets out to build a practical, criteria-based methodology for identifying and tiering critical information infrastructure objects among a government's information systems [3].

Materials and Methods

Protecting critical infrastructure has been studied internationally for quite some time. Uzbek scholarship covers the theoretical side of information security reasonably well — B.N. Tahirov's textbook, for instance, lays out the core concepts and threat models— but there has been little dedicated work on how to sort government information systems into tiers using measurable criteria. International practice, by contrast, leans heavily on risk-based classification. ISO/IEC 27001 requires organizations to inventory their assets and assess their value [4]; NIST SP 800-53 sorts information systems into low, moderate, and high impact levels under FIPS 199 [5]; and the EU's EPCIP programme singles out cross-border impact as a criterion of its own.

Building on this, we propose a three-step methodology: (1) inventory the objects, (2) score each one against a set of weighted criteria, and (3) classify based on the total score.

Step 1 — Inventory. Every state information system and resource is entered into a single register, recording its owner, function, user base, and technical infrastructure.

Step 2 — Scoring. Each object is rated from 1 to 5 against the six criteria below, and each rating is multiplied by a weight coefficient (w_i):

Table 1. Assessment Criteria and Weight Coefficients Used in the Proposed Scoring Model

No.	Assessment criterion	Weight (w_i)	Scale
1	Socio-economic impact on the population	0.25	1–5
2	Impact on national security	0.25	1–5
3	Interdependency with other systems	0.15	1–5
4	Availability of redundancy/backup	0.10	1–5 (reverse scale)
5	Exposure to cyberattacks (threat level)	0.15	1–5
6	Recovery time objective (RTO) after disruption	0.10	1–5 (reverse scale)

The total score is calculated as:

$S = \sum(w_i \times x_i)$, where $i = 1 \dots 6$, w_i is the weight of criterion i , and x_i is the score (1–5) assigned to it.

We recommend that the weight coefficients be set by an expert panel drawn from national security, digital technology, and network specialists, ideally through a Delphi-style consensus process rather than by a single agency acting alone.

Step 3 — Classification. Based on its total score (S), each object is placed into one of three tiers, described in the Results section below.

Results

Applying the proposed scoring model produces a three-tier classification of information systems according to the potential severity of cybersecurity-related disruption. The resulting classification is presented in Table 2.

Table 2. Three-Tier Classification of Information Systems Based on the Proposed Cybersecurity Scoring Model

Tier	Score range (S)	Description	Oversight level
Tier I (critical)	4.00 – 5.00	Disruption would have severe consequences at national scale	Enhanced (state oversight, mandatory audits)
Tier II (significant)	2.50 – 3.99	Disruption would have serious consequences at regional/sectoral scale	Standard (periodic audits)
Tier III (limited)	1.00 – 2.49	Disruption has localized impact, quick to recover	Baseline (self-assessment)

The results demonstrate that the proposed model differentiates information systems according to the potential consequences of disruption rather than applying the same cybersecurity requirements to all systems. Tier I systems represent the highest level of criticality because disruption may affect essential public services, economic activity, national-level functions, or national security [4]. Accordingly, these systems require enhanced oversight, including mandatory security assessments, penetration testing, continuous monitoring, and appropriate redundancy measures.

Tier II systems represent an intermediate level of criticality. Their disruption may significantly affect a particular sector, region, or group of interconnected organizations, but the expected consequences are more limited than those associated with Tier I systems. Periodic audits and structured risk assessments are therefore appropriate for this category [5].

Tier III systems have comparatively limited consequences in the event of disruption and can generally be managed through baseline cybersecurity controls and periodic self-assessment. However, a Tier III classification does not mean that such systems are free from cybersecurity risks. Their classification should be reconsidered if their functions, dependencies, threat exposure, or operational importance change.

The distribution of systems across these tiers is determined by the combined effect of the six assessment criteria rather than by a single indicator. In particular, socio-economic impact and national-security impact receive the highest weights, while interdependency, cyber-threat exposure, redundancy, and recovery requirements provide additional dimensions for distinguishing systems with similar functional importance. This allows the model to account for both the potential impact of disruption and the ability of an organization to withstand and recover from such disruption [6].

The proposed thresholds broadly correspond to the low-, moderate-, and high-impact logic used in established international cybersecurity approaches. However, the present model extends this general approach by explicitly incorporating interdependency between systems and national-security considerations. These factors are particularly relevant to government information infrastructure because disruption may propagate from one system to other dependent services.

The results therefore support the research objective of establishing a measurable and transparent basis for identifying systems that require different levels of cybersecurity protection. Classification should be reviewed at least annually, or earlier when substantial changes occur in system architecture, functionality, interdependencies, or threat exposure. Coordination through a unified national register can further support consistent application of the classification framework [7].

Discussion

The main significance of the results is that they provide a structured alternative to case-by-case identification of critical information infrastructure. Instead of relying exclusively on institutional judgment, the proposed scoring model establishes a common set of criteria through which the relative criticality of government information systems can be assessed [8].

The findings also indicate that criticality should be understood as a multidimensional characteristic. A system may be significant because of its socio-economic role or national-security importance, but its overall risk can also be affected by its dependence on other systems, exposure to cyber threats, availability of backup mechanisms, and expected recovery time. Consequently, two systems with similar functions may require different levels of oversight if their interdependencies and resilience characteristics differ.

This finding is consistent with the impact-based approach used in international cybersecurity frameworks. NIST, for example, categorizes information systems according to the potential impact of the loss of confidentiality, integrity, or availability and distinguishes low, moderate, and high impact levels [9]. The proposed model follows the same general principle of proportionality between potential impact and security requirements, but extends it by considering interdependency, national-security impact, threat exposure, and recovery characteristics. The model is therefore oriented specifically toward the identification of critical information infrastructure rather than general security categorization [10].

The inclusion of system interdependency has particular practical importance. In a highly interconnected digital environment, disruption of one information system may affect other services that depend on its data, authentication, communication, or processing functions. Therefore, assessing systems independently may underestimate their broader systemic significance. Including interdependency in the scoring model helps address this limitation and provides a more comprehensive basis for identifying critical systems [11].

From a theoretical perspective, the findings support a multidimensional approach to information-infrastructure criticality. The proposed model links criticality not only to the consequences of disruption but also to the structural and resilience characteristics of the system. This provides a basis for further research into quantitative approaches to critical-infrastructure classification.

From a practical perspective, the three-tier classification can support differentiated cybersecurity governance. Tier I systems can be prioritized for enhanced monitoring, mandatory audits, penetration testing, and stronger continuity and redundancy requirements. Tier II systems can be subject to periodic audits and structured risk assessments, while Tier III systems can primarily rely on baseline controls and self-assessment. Such differentiation may help institutions concentrate limited technical and financial resources on systems where disruption could produce the greatest consequences [12].

The proposed model also has relevance to Uzbekistan's broader digitalization objectives. As public services increasingly depend on interconnected information systems, maintaining cybersecurity is closely related to service continuity and institutional resilience. A differentiated classification

framework can therefore complement national cybersecurity and digital-transformation initiatives by helping institutions identify which systems require stronger protection [13].

Nevertheless, the results should be interpreted with several limitations in mind. The weighting coefficients and score thresholds represent a methodological proposal and require further empirical validation. Expert judgment may also introduce subjectivity into the assessment process. Future research should therefore test the model using real government information systems and historical cybersecurity incidents, as well as conduct sensitivity analysis to determine how changes in the weighting coefficients affect the final classification [14].

Overall, the results demonstrate that the proposed scoring model can provide a practical foundation for risk-based identification and classification of critical information infrastructure. Its main contribution is the creation of a transparent mechanism for linking the potential consequences of disruption with an appropriate level of cybersecurity oversight, while allowing the framework to be further refined through empirical testing and periodic review [15].

Conclusion

Identifying and classifying critical information infrastructure on objective grounds is one of the more practical levers available for improving how state information systems are protected. The methodology proposed here offers one way of doing that: it directs limited resources toward the systems that matter most, gives agencies a shared framework to work from, and supports the goals set out in the 2026–2030 Cybersecurity Strategy.

References

- [1] President of the Republic of Uzbekistan, “On defining the Cybersecurity Strategy of the Republic of Uzbekistan and improving the system for preventing cybercrime,” Decree No. PF-38, Mar. 10, 2026. [Online]. Available: <https://lex.uz/>
- [2] Republic of Uzbekistan, “On cybersecurity,” Law of the Republic of Uzbekistan. [Online]. Available: <https://lex.uz/>
- [3] International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 27001:2022: Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements*, 3rd ed. Geneva, Switzerland: ISO, 2022.
- [4] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, NIST Special Publication 800-53, Rev. 5. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2020.
- [5] C. Pascoe, S. Quinn, and K. Scarfone, *The NIST Cybersecurity Framework (CSF) 2.0*, NIST Cybersecurity White Paper 29. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2024, doi: 10.6028/NIST.CSWP.29.
- [6] European Commission, “European Programme for Critical Infrastructure Protection (EPCIP),” Directorate-General for Migration and Home Affairs, Brussels, Belgium. [Online]. Available: <https://eur-lex.europa.eu/>.
- [7] Ministry of Digital Technologies of the Republic of Uzbekistan, “Digital Uzbekistan—2030 strategy.” [Online]. Available: <https://digital.gov.uz/>.
- [8] European Commission, “Critical infrastructure resilience at EU-level,” Directorate-General for Migration and Home Affairs, Jan. 13, 2026. [Online]. Available: <https://home-affairs.ec.europa.eu/>.
- [9] European Commission, “On a European Programme for Critical Infrastructure Protection,” COM(2006) 786 final, Dec. 12, 2006. [Online]. Available: <https://eur-lex.europa.eu/>.
- [10] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, *Computer Security Incident Handling Guide*, NIST Special Publication 800-61, Rev. 2. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2012. [Online]. Available: <https://csrc.nist.gov/>.
- [11] K. Rigopoulos, S. Quinn, C. Pascoe, J. Marron, A. Mahn, and D. Topper, *NIST Cybersecurity*

- Framework 2.0: Resource & Overview Guide*, NIST Special Publication 1299. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2024, doi: 10.6028/NIST.SP.1299.
- [12] National Institute of Standards and Technology, *Cybersecurity Framework 2.0*. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2024. [Online]. Available: <https://www.nist.gov/cyberframework>.
- [13] B. N. Tahirov, *Fundamentals of Information Security: A Textbook*. Bukhara, Uzbekistan: Fan va Ta'lim, 2022, 156 p.
- [14] President of the Republic of Uzbekistan, “On the strategy ‘Uzbekistan—2030’,” Presidential Decree. [Online]. Available: <https://president.uz/>.
- [15] European Commission, “Commission issues guidance to strengthen resilience of critical infrastructure,” Directorate-General for Migration and Home Affairs, Jul. 10, 2026. [Online]. Available: <https://home-affairs.ec.europa.eu/>