Journal of Secure Digital Technologies
Volume 1 (№2) September 2026

ISSN (E): 3136-9340
Sertificate № KZ19VPY00128988, date of issue: 25.12.2025

The journal is published 4 times a year
(March, June, September, December)

EDITORIAL TEAM
Editor-in-Chief
Dr. Leila Rzayeva, Association prof., PhD, Digital government support center (Kazakhstan)

Deputy Editor-in-Chief
Dr. Ali Myrzatay, PhD, Digital government support center (Kazakhstan)

Executive Secretary
Dr. Abdenova Zhuldyz, PhD, Digital government support center (Kazakhstan)

EDITORIAL BOARD MEMBERS (KAZAKHSTAN)
Seitkulov E.N. – Candidate of Physical and Mathematical Sciences, Professor Computer Science, Computer Engineering and Control
Abdenova G.A. – PhD in Automation and Control, Candidate of Technical Sciences, Professor L.N. Gumilyov Eurasian National University
Atanov S.K. – Doctor of Technical Sciences, Professor.
Sergazin G.K. – PhD, Associate Professor Computer Science, Computer Engineering and Control
Satybaldina D.Zh. – Candidate of Physical and Mathematical Sciences, Professor Director, Research Institute of Information Security and Cryptology, L.N. Gumilyov Eurasian National University

INTERNATIONAL EDITORIAL BOARD MEMBERS
Ibraheem Shayea – PhD in Electrical and Electronic Engineering Istanbul Technical University (Turkey)
Yadigar Nasiboglu Imamverdiyev – DSc in Technical Sciences, Associate Professor Information Security, Computer Science and Computer Technology (Azerbaijan)
Erdal Irmak – PhD in Electrical and Electronics Engineering, Professor Gazi University (Turkey)
Korhan Kayisli – PhD in Electrical Electronics Engineering, Associate Professor Gazi University (Turkey)
Yonghao Wang – PhD in Electronic Engineering, Associate Professor Queen Mary, University of London (UK)
Amir Mosavi – PhD in Applied Informatics, Professor of AI Obuda University (Hungary)
Gerald Feldman – PhD in General Computing, Associate Professor Birmingham City University (UK)
Mohamed Ragab – PhD in Computer Science, Assistant Professor Birmingham City University (UK)
Seref Sagiroglu – PhD in System Engineering, Professor Gazi University (Turkey)

MANAGING EDITOR
Dr. Ali Myrzatay, PhD, Digital government support center (Kazakhstan)

TECHNICAL EDITOR
Dr. Ali Myrzatay, PhD, Digital government support center (Kazakhstan)

CONTENTS

Cyber Incident Damage Assessment for Public Digital Systems and Critical Infrastructure 3

Cyber Incident Damage Assessment for Public Digital Systems and Critical Infrastructure 37

Verifiable but Not Correct: Blockchain Trust Boundaries for Autonomous Agents 71

Calibrated Digital Twins and Geometry-based Perception for Automated Driving in Heavy Rain and Snowfall: Evidence From Research Testing in China and Implications for Kazakhstan. 88

Personal Data Protection in Kazakhstan's AI Enabled Public Services 109

Asking Another Jurisdiction What It Holds Without Telling It What You Hold: Private Artifact Matching with a Ledger-Anchored Transcript 131

On-Chain and Off-Chain Data Placement in Hybrid Blockchain Health Systems 143

An Integrated Project Management Maturity Model for Digital Qazaqstan Initiatives: Embedding Cybersecurity, AI Governance and Forward-Looking Cyber-Risk Requirements into ST RK ISO 21502-2022..... 158

Appendix A. Indicators and evidence for the baseline practice groups 181

Privacy Risks and Data Protection Readiness in AI Marketing in Kazakhstan..... 183

Supplementary Materials..... 205

Miraim Atanayeva*
Chief Senior Director, Project Monitoring and Management Center
Digital Government Support Center, Kazakhstan
m.atanayeva@govtec.kz; https://orcid.org/0000-0002-3067-356X
Ulzhan Ospanova
Senior Director, Project Monitoring and Management Center,
Digital Government Support Center, Kazakhstan
u.ospanova8@gmail.com, u.ospanova@govtec.kz; https://orcid.org/0000-0003-0427-7931
Zhanna Isabekova
Analyst at the Project Monitoring and Management Center
Digital Government Support Center, Kazakhstan
zh.issabekova@govtec.kz

AN INTEGRATED PROJECT MANAGEMENT MATURITY MODEL FOR DIGITAL QAZAQSTAN INITIATIVES: EMBEDDING CYBERSECURITY, AI GOVERNANCE AND FORWARD-LOOKING CYBER-RISK REQUIREMENTS INTO ST RK ISO 21502-2022

Abstract: The Nationwide Strategy "Digital Qazaqstan" until 2029, approved by Presidential Decree No. 1311 of 9 June 2026, and its Action Plan, approved by Government Resolution No. 760 of 26 August 2026, commit central and local state bodies and national companies to 136 measures, a large share of which deploy artificial intelligence (AI) in citizen-facing, business-facing and intra-governmental services. Project offices that are now translating these measures into implementation plans must simultaneously satisfy the project-management guidance of ST RK ISO 21502-2022, the information-security requirements of ST RK ISO/IEC 27001-2023 and the Unified Requirements on ICT and information security, and the emerging AI-management requirements of ST RK ISO/IEC 42001-2025, ISO/IEC 42005:2025, ISO/IEC 42006:2025 and the Law of the Republic of Kazakhstan "On Artificial Intelligence". Existing project-management maturity models are domain-neutral and contain no cybersecurity or AI-governance criteria, whereas cybersecurity and AI maturity models ignore the project life cycle. This article proposes an integrated project management maturity model (IPM3-DQ) that extends a ST RK ISO 21502-2022 practice-based baseline with three cross-cutting domains: cybersecurity (S), AI governance (A) and forward-looking cyber risk (F). The model uses a uniform 0–5 anchored scale, AHP-derived weights differentiated by project class, and a non-compensatory gating rule under which the maturity level of a project involving critically important digital objects or AI systems cannot exceed its security or AI-governance level by more than one level. A worked example of a G2C AI-assistant project shows that the conventional arithmetic-mean approach classifies the project as "Managed" (3.67), whereas the integrated model places it at "Defined" (2.67) with AI governance as the binding constraint. A validation protocol based on expert panels, Kendall's W, Cronbach's alpha and intraclass correlation is specified. The model gives project offices of state bodies a single instrument for self-assessment, audit

and semi-annual reporting under the Action Plan, and provides the regulator with a maturity-based lens for the national cybersecurity standardisation programme.

Keywords: *project management maturity; ST RK ISO 21502-2022; Digital Qazaqstan; cybersecurity; ISO/IEC 27001; ISO/IEC 42001; AI management system; AI impact assessment; cyber-risk forecasting; public sector; Kazakhstan.*

Интегрированная модель зрелости проектного управления для инициатив Digital Qazaqstan: встраивание требований кибербезопасности, управления искусственным интеллектом и прогнозной оценки киберрисков в СТ РК ISO 21502-2022

Аннотация: Общенациональная стратегия «Digital Qazaqstan» до 2029 года, утверждённая Указом Президента Республики Казахстан от 9 июня 2026 года № 1311, и План действий по её реализации, утверждённый постановлением Правительства Республики Казахстан от 26 августа 2026 года № 760, возлагают на центральные и местные государственные органы и национальные компании исполнение 136 мероприятий, значительная часть которых предусматривает внедрение искусственного интеллекта (ИИ) в сервисы для граждан, бизнеса и внутригосударственного взаимодействия. Проектные офисы, которые в настоящее время переводят эти мероприятия в планы реализации, должны одновременно соблюдать требования руководства по управлению проектами СТ РК ISO 21502-2022, требования информационной безопасности СТ РК ISO/IEC 27001-2023 и Единых требований в области ИКТ и обеспечения информационной безопасности, а также формирующиеся требования к управлению ИИ, установленные СТ РК ISO/IEC 42001-2025, ISO/IEC 42005:2025, ISO/IEC 42006:2025 и Законом Республики Казахстан «Об искусственном интеллекте». Существующие модели зрелости проектного управления нейтральны к предметной области и не содержат критериев кибербезопасности и управления ИИ, тогда как модели зрелости кибербезопасности и ИИ не учитывают жизненный цикл проекта. В статье предложена интегрированная модель зрелости проектного управления (IPM3-DQ), расширяющая базовый уровень, построенный на практиках СТ РК ISO 21502-2022, тремя сквозными доменами: кибербезопасность (S), управление ИИ (A) и прогнозная оценка киберрисков (F). Модель использует единую шкалу 0–5 с закреплёнными дескрипторами, весовые коэффициенты, полученные методом анализа иерархий (AHP) и дифференцированные по классам проектов, а также некомпенсаторное правило ограничения, согласно которому уровень зрелости проекта, затрагивающего критически важные цифровые объекты или системы ИИ, не может превышать уровень его кибербезопасности или управления ИИ более чем на один уровень. Рабочий пример проекта ИИ-ассистента G2C показывает, что традиционный подход на основе среднего арифметического относит проект к уровню «Управляемый» (3,67), тогда как интегрированная модель определяет его как

«Регламентированный» (2,67), при этом ограничивающим фактором выступает управление ИИ. Описан протокол валидации на основе экспертных панелей, коэффициента конкордации Кендалла (W), альфы Кронбаха и внутриклассовой корреляции. Модель предоставляет проектным офисам государственных органов единый инструмент самооценки, аудита и полугодовой отчётности в рамках Плана действий, а регулятору — основанный на зрелости взгляд на национальную программу стандартизации в сфере кибербезопасности.

Ключевые слова: *зрелость проектного управления; СТ РК ISO 21502-2022; Digital Qazaqstan; кибербезопасность; ISO/IEC 27001; ISO/IEC 42001; система менеджмента искусственного интеллекта; оценка воздействия ИИ; прогнозирование киберрисков; государственный сектор; Казахстан.*

Digital Qazaqstan бастамалары үшін жобалық басқарудың интеграцияланған кемелдік моделі: киберқауіпсіздік, жасанды интеллектті басқару және кибертәуекелдерді болжамды бағалау талаптарын ҚР СТ ISO 21502-2022 стандартына енгізу

Аңдатпа: Қазақстан Республикасы Президентінің 2026 жылғы 9 маусымдағы № 1311 Жарлығымен бекітілген 2029 жылға дейінгі «Digital Qazaqstan» жалпыұлттық стратегиясы және оны іске асыру жөніндегі Қазақстан Республикасы Үкіметінің 2026 жылғы 26 тамыздағы № 760 қаулысымен бекітілген Іс-шаралар жоспары орталық және жергілікті мемлекеттік органдар мен ұлттық компанияларға 136 іс-шараны орындауды жүктейді, олардың едәуір бөлігі азаматтарға, бизнеске және мемлекетішілік өзара іс-қимылға арналған сервистерге жасанды интеллектті (ЖИ) енгізуді көздейді. Қазіргі уақытта осы іс-шараларды іске асыру жоспарларына айналдырып жатқан жобалық офистер бір мезгілде ҚР СТ ISO 21502-2022 жобаларды басқару жөніндегі нұсқаулықтың талаптарын, ҚР СТ ISO/IEC 27001-2023 және Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптардың ақпараттық қауіпсіздік талаптарын, сондай-ақ ҚР СТ ISO/IEC 42001-2025, ISO/IEC 42005:2025, ISO/IEC 42006:2025 стандарттарымен және «Жасанды интеллект туралы» Қазақстан Республикасының Заңымен белгіленген, қалыптасып келе жатқан ЖИ-ді басқару талаптарын сақтауға тиіс. Жобалық басқарудың қолданыстағы кемелдік модельдері пәндік салаға бейтарап және киберқауіпсіздік пен ЖИ-ді басқару критерийлерін қамтымайды, ал киберқауіпсіздік пен ЖИ кемелдік модельдері жобаның өмірлік циклін ескермейді. Мақалада ҚР СТ ISO 21502-2022 практикаларына негізделген базалық деңгейді үш өтпелі доменмен — киберқауіпсіздік (S), ЖИ-ді басқару (A) және кибертәуекелдерді болжамды бағалау (F) — кеңейтетін жобалық басқарудың интеграцияланған кемелдік моделі (IPM3-DQ) ұсынылған. Модельде бекітілген дескрипторлары бар бірыңғай 0–5 шкаласы, иерархияларды талдау әдісімен (AHP)

алынған және жоба сыныптары бойынша сараланған салмақ коэффициенттері, сондай-ақ аса маңызды цифрлық объектілерді немесе ЖИ жүйелерін қамтитын жобаның кемелдік деңгейі оның киберқауіпсіздік немесе ЖИ-ді басқару деңгейінен бір деңгейден артық аса алмайтын өтемсіз шектеу ережесі қолданылады. G2C ЖИ-ассистенті жобасының жұмыс мысалы дәстүрлі орташа арифметикалық тәсіл жобаны «Басқарылатын» деңгейге (3,67) жатқызатынын, ал интеграцияланған модель оны ЖИ-ді басқару шектеуші фактор болып табылатын «Регламенттелген» деңгей (2,67) ретінде анықтайтынын көрсетеді. Сараптамалық панельдерге, Кендаллдың конкордация коэффициентіне (W), Кронбах альфасына және сыныпішілік корреляцияға негізделген валидация хаттамасы сипатталған. Модель мемлекеттік органдардың жобалық офистеріне Іс-шаралар жоспары шеңберінде өзін-өзі бағалаудың, аудиттің және жартыжылдық есептіліктің бірыңғай құралын, ал реттеушіге киберқауіпсіздік саласындағы ұлттық стандарттау бағдарламасына кемелдікке негізделген көзқарасты ұсынады.

Түйін сөздер: *жобалық басқарудың кемелдігі; ҚР СТ ISO 21502-2022; Digital Qazaqstan; киберқауіпсіздік; ISO/IEC 27001; ISO/IEC 42001; жасанды интеллект менеджменті жүйесі; ЖИ әсерін бағалау; кибертәуекелдерді болжау; мемлекеттік сектор; Қазақстан.*

1. Introduction

Public administration in Kazakhstan has moved decisively towards project-based delivery of strategic initiatives. The Model Regulation of Project Management of State Bodies, approved by Order No. 2 of the Minister of National Economy of 13 January 2022 and subsequently amended, designates ST RK ISO 21502-2022 as the reference guidance for project management in state bodies [4, 5]. The institutional importance of this shift was confirmed by a recent panel study of sixteen regions of Kazakhstan over 2005–2024, which found that the development of government project offices is positively and significantly associated with regional economic outcomes, while digitalisation on its own shows no robust causal effect unless it is matched by organisational capacity [36]. Technology, in other words, does not substitute for management maturity.

This finding acquires immediate practical weight with the adoption of the Nationwide Strategy for Large-Scale Digitalisation and Total Implementation of Artificial Intelligence Technologies "Digital Qazaqstan" until 2029 (Presidential Decree No. 1311 of 9 June 2026) [1] and of its Action Plan (Government Resolution No. 760 of 26 August 2026) [2]. The Action Plan comprises 136 measures grouped into three directions and twenty priority programmes ("icebreakers"). Responsible bodies must report on implementation twice a year, by 5 July and 20 December, to the Ministry of Artificial Intelligence and Digital Development, which consolidates the information for the Government Office. A large share of the measures are AI-intensive: a universal AI assistant eGov GPT (measure 26), AI assistants for civil servants in G2G, G2B and G2C interactions (measures 127–129), an AI

agent for the e-Otinish petition system (measure 136), AI-based functional analysis of state functions (measures 130–131), and sectoral targets such as a share of clinical decisions supported by AI of at least 80 % by 2028. In parallel, Icebreaker 19 "Cybersecurity" sets a target protection level of at least 90 % for critically important digital objects and tasks the Ministry, the National Security Committee, the Ministry of Trade and Integration and the Digital Government Support Centre with developing national cybersecurity standards through 2029 (measure 117), while Icebreaker 20 "State as a Platform" mandates the migration of state information systems to the QazTech platform (measure 125).

Project offices of state bodies and national companies are therefore drafting implementation plans for projects that are, at the same time, digital-transformation projects, information-security projects and—increasingly—AI projects. The guidance they are instructed to follow, ST RK ISO 21502-2022, is deliberately domain-neutral: it describes integrated and subject-specific management practices but says nothing about threat modelling, security attestation, AI impact assessment or supply-chain risk of machine-learning models. The relevant requirements exist, but in separate instruments: ST RK ISO/IEC 27001-2023 and ISO/IEC 27005:2022 for information security [8, 9]; the Unified Requirements on ICT and information security approved by Government Resolution No. 832 of 20 December 2016 [7]; ST RK ISO/IEC 42001-2025 for AI management systems [10], with national adoption of ISO/IEC 42005 (AI system impact assessment) and ISO/IEC 42006 (requirements for AI management system auditors) planned for 2026 and 2027 respectively [11, 12]; and the Law "On Artificial Intelligence" No. 230-VIII of 17 November 2025, which classifies AI systems by degree of impact and allocates responsibility across the life cycle [3]. No instrument tells a project office how mature its project management must be, as a whole, for these requirements to be met reliably.

The academic literature mirrors this fragmentation. Project management maturity models (PMMMs) such as OPM3, P3M3, CMMI-based models and the Kerzner PMMM have been compared extensively [13] but do not include cybersecurity or AI-governance dimensions; the single published attempt to add cybersecurity extensions to a PMMM for critical-infrastructure projects [21] predates ISO 21502:2020, NIST CSF 2.0 and ISO/IEC 42001. Cybersecurity maturity models [22, 23] and AI maturity models for the public sector [24] are organisational rather than project-oriented. Methods for forecasting cyber threats [27, 28] have not been embedded in project planning. For Kazakhstan, the only baseline measurement of project management maturity dates from 2015 [37], and recent work on the digital maturity of project offices of state bodies [38] contains no security or AI criteria. A further, methodological weakness is shared by most maturity instruments: scores are aggregated by simple arithmetic means with equal weights, without a test of expert agreement or scale reliability, so that a project with excellent scheduling and absent security governance can obtain a respectable "high" rating.

The objective of this article is to propose and specify an integrated project management maturity model for projects implemented under the Digital Qazaqstan Action

Plan—hereafter IPM3-DQ—that (i) retains ST RK ISO 21502-2022 as the normative baseline mandated for state bodies; (ii) embeds cybersecurity requirements derived from ST RK ISO/IEC 27001-2023, ISO/IEC 27005:2022 and the Unified Requirements as a cross-cutting domain; (iii) embeds AI-governance requirements derived from ISO/IEC 42001, 42005, 42006 and the Law on AI as a second cross-cutting domain; (iv) introduces a forward-looking cyber-risk domain that rewards the use of threat forecasting and probabilistic risk quantification in project planning; and (v) replaces the arithmetic-mean index with a weighted, non-compensatory aggregation whose parameters can be derived and validated with established expert-elicitation and psychometric procedures. The contribution is a design artefact: the model, its indicator system, its aggregation logic, a worked example, and a validation protocol.

The remainder of the article is organised as follows. Section 2 reviews related work and identifies the research gap. Section 3 summarises the regulatory and standards baseline of Kazakhstan on which the model is built. Section 4 specifies the model. Section 5 presents a worked example for an AI-assistant project under Icebreaker 20 and the validation protocol. Section 6 discusses implications, positioning and limitations, and Section 7 concludes.

2. Background and related work

2.1. Project management maturity models and the public sector

Maturity models describe an organisation's capability as a staged progression, typically across five levels inherited from the Capability Maturity Model. Nikolaenko and Sidorov [13] compared nine PMMMs (CMMI, OPM3, IPMA Delta, P3M3, SPICE, PM², Kerzner PMMM, ProMMM and PMMMsm) and concluded that the most robust models are those anchored in an international body of knowledge; this supports anchoring a national model in ISO 21502 rather than in a proprietary framework. Early cross-industry evidence showed median maturity of only level 2 in most assessed components [14], and later work in the public sector of Pakistan established, with PLS-SEM on 425 respondents, a significant link between project management maturity and the reputation of public organisations [15]. Žurga's Total Project Management Maturity Model for Slovenian public administration [16] remains one of very few PMMMs designed for government, and systematic reviews report a persistent scarcity of empirical studies on PMMM adoption in the public sector. Recent extensions add new dimensions to PMMMs—most visibly sustainability—which provides a methodological precedent for extending a PMMM with cybersecurity and AI governance. Risk-specific maturity assessment for IT projects has been operationalised by Nikolaenko and Sidorov [17], and fuzzy-AHP has been used to prioritise security-relevant practices in software development [18]; both demonstrate that weighting and consistency checking are feasible within maturity instruments.

2.2. Cybersecurity in project management and cybersecurity maturity models

A 2025 scoping review of 64 studies [19] found that cybersecurity is widely acknowledged as a critical element of project risk management, yet most project managers lack the competence to operationalise it and organisational culture is the dominant moderating factor. Al-Janabi et al. [20] proposed a cyber-resilient IT project management framework that aligns the cyber-risk management process with the stages of the IT project life cycle, from business case and charter to closure; it is the closest process-level precedent for the mapping proposed here. Payette et al. [21] derived six cybersecurity themes from NIST, C2M2 and CERT-RMM and proposed extensions to the project sub-model of P3M3 for critical-infrastructure projects. On the cybersecurity side, Büyüközkan and Güler [22] conducted a systematic review and bibliometric analysis of cybersecurity maturity models and proposed a model with five dimensions, fifteen factors and five levels, noting that earlier models rarely offer an end-to-end organisational assessment and are seldom validated. NIST CSF 2.0 [23] introduces the Govern function and four implementation tiers that are structurally comparable to maturity levels. The harmonised structure shared by ISO/IEC 27001:2022 and ISO/IEC 42001:2023 (clauses 4–10, Plan-Do-Check-Act) facilitates integrated management systems and, by extension, integrated assessment.

2.3. AI management standards and AI governance maturity

ISO/IEC 42001:2023 is the first certifiable management-system standard for AI; its Annex A lists controls grouped by control objectives and Annex C enumerates AI-specific risk sources [10]. ISO/IEC 42005:2025 provides guidance on AI system impact assessment for individuals, groups and society and is referenced by 42001 for high-impact systems [11]; ISO/IEC 42006:2025 specifies requirements for bodies auditing and certifying AI management systems, including auditor competence and audit-time calculation [12]. NIST AI RMF 1.0 structures AI risk management around the Govern, Map, Measure and Manage functions [25], and the NIST taxonomy of adversarial machine learning distinguishes evasion, poisoning, privacy and misuse attacks on predictive and generative AI [30]. For the public sector specifically, Dreyling et al. [24] developed an AI maturity model through a design-science process with iterative expert refinement, drawing on Estonian experience, and Vatamanu and Tofan [26] showed, using the technology–organisation–environment framework, that AI in public administration requires strong governance structures and comprehensive security measures. The European AI Act [43] and the Kazakh Law on AI [3] both adopt impact-based classification of AI systems. Empirical studies of ISO/IEC 42001 implementation remain scarce, and we found no study of an integrated 27001 + 42001 system in a government setting.

2.4. Forward-looking cyber-risk assessment

Project risk management in ISO 21502 is retrospective in practice: risks are registered when identified and re-assessed on request. The cybersecurity literature offers established means of anticipation. Wang, Neil and Fenton [27] implemented and extended the FAIR model with Bayesian networks, obtaining results consistent with Monte-Carlo benchmarks and enabling expected-loss estimates that can inform contingency reserves.

Landauer et al. [28] reviewed time-series methods in security analytics from intrusion detection to long-horizon attack prediction. Cheimonidis and Rantos [29] systematised dynamic risk assessment models, including fuzzy Bayesian networks, which justify re-assessment at project stage gates rather than at project start only. For AI projects, Cinà et al. [31] surveyed training-data poisoning and defences, Wang et al. [32] formalised the three-tier large-language-model supply chain, and practitioner taxonomies—the OWASP Top 10 for LLM Applications [33] and MITRE ATLAS [34]—provide threat catalogues suitable for scenario analysis. Annual threat landscapes such as ENISA's [35] supply empirical base rates. None of these sources has been integrated into a maturity instrument for project offices.

2.5. Kazakhstan context and research gap

Kazakhstan ranks 24th of 193 countries in the 2024 UN E-Government Development Index and first among landlocked countries [39], and its eGov portal offered more than 1,200 services to over 15 million registered users by the end of 2023. Narbaev's 2015 assessment using the project sub-model of P3M3 reported an average maturity of about 2.4 out of 5 across Kazakh organisations [37]. Descriptive studies of project offices in ministries and regions identify systemic shortcomings, and Taizhanova et al. [38] examined the digital maturity of project offices of state bodies, but neither strand includes security or AI criteria. Country-level indices (EGDI, OECD Digital Government Index [40]) do not measure project-management or security maturity at organisational level.

Five gaps follow. First, PMMMs, cybersecurity maturity models and AI-governance maturity models evolve in parallel and have not been integrated. Second, no maturity model is built on ISO 21502, although Kazakhstan's Model Regulation makes it the reference standard. Third, most maturity instruments are psychometrically weak and rely on additive indices without reliability testing. Fourth, forecasting of cyber threats is absent from project maturity assessment. Fifth, no instrument connects project maturity to the Kazakh regulatory architecture created by the Law on AI, the Unified Requirements and the Digital Qazaqstan Action Plan. IPM3-DQ addresses all five.

3. Regulatory and standards baseline

Table 1 lists the instruments on which IPM3-DQ is built and the role each plays in the model. The selection follows a simple rule: the baseline must be the instrument that state bodies are already obliged to apply, and cross-cutting domains must be derived from instruments that are either adopted as national standards or are planned for adoption within the Strategy's horizon.

Table 1. Normative instruments underlying IPM3-DQ

Instrument	Status in Kazakhstan	Role in IPM3-DQ
Decree No. 1311 of 9 June 2026 (Strategy "Digital Qazaqstan" until 2029) [1]; Resolution No. 760 of 26 August 2026 (Action Plan, 136 measures, 20 icebreakers) [2]	In force; semi-annual reporting	Defines the project population, horizon (2029) and reporting cycle; Icebreakers 17, 19, 20 supply targets for domains S, A, F
Model Regulation of Project Management of State Bodies (Order MNE No. 2 of 13.01.2022, as amended) [4]	In force	Mandates ST RK ISO 21502-2022 and 21503 for state bodies; justifies the baseline
ST RK ISO 21502-2022 (ISO 21502:2020, IDT) [5, 6]	National standard, 2022	Baseline: ten practice groups P1–P10
ST RK ISO/IEC 27001-2023 (ISO/IEC 27001:2022, IDT) [8]; ISO/IEC 27005:2022 [9]	National standard, 2023; 27005 adopted as ST RK	Domain S: ISMS scope, risk assessment, Annex A controls
Unified Requirements on ICT and information security (Resolution No. 832 of 20.12.2016, as amended) [7]	In force	Domain S: mandatory security requirements for state information systems and critically important digital objects; attestation
Law "On Artificial Intelligence" No. 230-VIII of 17.11.2025 [3]	In force since 18.01.2026	Domain A: impact-based classification, life-cycle responsibility, national AI platform
ST RK ISO/IEC 42001-2025 (ISO/IEC 42001:2023) [10]	National standard, 2025	Domain A: AI management system roles, risk and impact processes, Annex A controls
ISO/IEC 42005:2025 [11]; ISO/IEC 42006:2025 [12]	National adoption planned 2026 and 2027	Domain A: impact assessment at initiation; audit readiness at closure
NIST CSF 2.0 [23]; NIST AI RMF 1.0 [25]; NIST AI 100-2 [30]; OWASP LLM Top	International references (non-binding)	Domain F: threat catalogues, base rates and forecasting inputs

Instrument	Status in Kazakhstan	Role in IPM3-DQ
10 [33]; MITRE ATLAS [34]; ENISA Threat Landscape [35]		

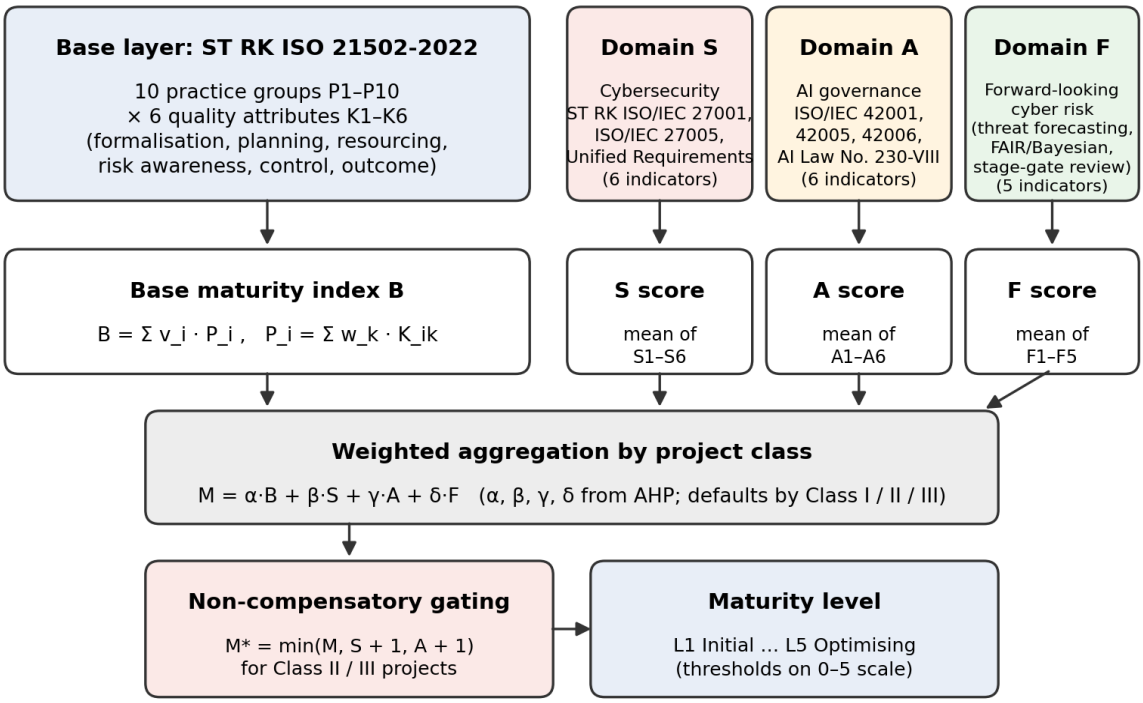
Note. Numbers of measures and icebreakers are cited from the text of Resolution No. 760 as published on adilet.zan.kz.

4. The IPM3-DQ model

4.1. Design approach and requirements

The model was developed as a design-science artefact. From the gaps identified in Section 2 and from the obligations of project offices under the Action Plan, five design requirements were derived: R1—the baseline must be ST RK ISO 21502-2022 without modification of its practice structure, so that the model is auditable against the standard state bodies already apply; R2—cybersecurity and AI governance must be assessed as cross-cutting domains along the project life cycle, not as additional practice groups, because they condition every practice; R3—the scale must be uniform and anchored, so that scores are comparable across practices, domains and assessors; R4—aggregation must be weighted and non-compensatory for projects whose failure has security consequences, so that strength in scheduling cannot mask weakness in security; R5—the instrument must be validatable with standard expert-elicitation and reliability procedures, and its weights must be re-derivable when standards change (for example upon national adoption of ISO/IEC 42005 and 42006). Figure 1 shows the resulting architecture.

Figure 1. Architecture of the IPM3-DQ model



4.2. Scope, assessment units and project classes

The object of assessment is the project management system of an organisation implementing measures of the Action Plan; the subject is the degree to which the practices of ST RK ISO 21502-2022 and the cross-cutting requirements are implemented. Assessment can be performed at three units: the organisation (central or local executive body, national company), its project office, or an individual project. Because the consequences of immaturity differ by project type, three project classes are distinguished and determine both the weights and the gating rule (Section 4.6):

- **Class I —** ordinary digital projects that do not process personal data at scale, do not involve critically important digital objects and do not deploy AI systems (e.g., measure 72, product identification system);
- **Class II —** projects involving state information systems, critically important digital objects or large-scale personal-data processing under the Unified Requirements (e.g., measure 125, migration of state IT systems to QazTech; measure 120, personal-data access control);
- **Class III —** projects deploying AI systems within the meaning of the Law on AI, with the sub-classification by degree of impact prescribed by that Law (e.g., measures 26, 127–129, 136; AI-supported clinical decision systems under Icebreaker 2).

4.3. Baseline layer: practice groups and quality attributes

The baseline layer preserves the practice structure of ST RK ISO 21502-2022. Ten practice groups P1–P10 are assessed: pre-project activities and initiation (P1); planning (P2); stakeholder engagement and communication (P3); resource and team management (P4); risk and issue management (P5); quality management (P6); schedule management (P7); cost management (P8); monitoring, control and change control (P9); and closure, reporting and lessons learned (P10). Each practice group is scored against six quality attributes K1–K6 that describe how well the practice is institutionalised rather than what the practice is—an important correction to earlier formulations in which "risk management" appeared simultaneously as an assessment criterion and as an assessed practice. The attributes are: K1 formalisation (documented procedure, templates, roles); K2 planning quality (completeness and currency of plans and baselines); K3 resourcing and competence (assigned, trained personnel and tooling); K4 risk awareness (practice-specific risks identified and owned); K5 measurement and control (metrics, reporting cadence, corrective action); K6 outcome (evidence that the practice produces its intended result). Appendix A gives the indicators and evidence sources for each practice group.

4.4. Uniform anchored scale

All practices, attributes and domain indicators are scored on the same 0–5 scale with anchored descriptors (Table 2). Using a single scale removes the inconsistency, common in practitioner instruments, between a 1–5 criterion scale, a 0–5 indicator scale and an interpretation table that begins at 0; it also makes the lowest level (absence of the practice) explicitly scorable.

Table 2. Anchored scoring scale

Score	Anchor	Generic descriptor
0	Absent	No evidence that the practice or control exists
1	Initial	Performed ad hoc by individuals; no documentation; results unpredictable
2	Forming	Partially documented; applied inconsistently across projects; roles informal
3	Defined	Documented, approved and applied in all projects; roles and templates defined
4	Managed	Applied systematically; measured with indicators; deviations trigger corrective action
5	Optimising	Continuously improved on the basis of measurements, audits, lessons learned and external benchmarks

4.5. Cross-cutting domains S, A and F

The three cross-cutting domains are assessed with indicators placed along the project life cycle, so that each indicator can be verified at the corresponding stage gate of the Model

Regulation. Table 3 specifies the indicators, their normative source and the evidence an assessor should request. Domain S (cybersecurity) translates ST RK ISO/IEC 27001-2023, ISO/IEC 27005:2022 and the Unified Requirements into six project-level indicators. Domain A (AI governance) translates ISO/IEC 42001, 42005 and 42006 and the Law on AI into six indicators and applies only to Class III projects. Domain F (forward-looking cyber risk) rewards practices that anticipate the threat landscape over the Strategy's horizon rather than registering threats already materialised; its five indicators are deliberately method-agnostic, accepting qualitative scenario analysis at lower scores and probabilistic quantification at higher scores.

Table 3. Indicators of the cross-cutting domains

Code	Indicator (life-cycle stage)	Normative source	Evidence; anchors 0 / 3 / 5
S1	Security classification and threat model at initiation	Unified Requirements; ISO/IEC 27005 cl. 7	Object classified (state IS / critically important digital object); threat model approved. 0 – none; 3 – classification only; 5 – approved threat model linked to charter
S2	Security requirements and ISMS scope in the project plan	ST RK ISO/IEC 27001 cl. 4, 6; Annex A	Security requirements traced to Annex A controls; ISMS scope covers project deliverables. 0 – none; 3 – generic checklist; 5 – traceable, risk-based requirements
S3	Secure procurement and supply-chain requirements	ISO/IEC 27001 A.5.19–5.23; Unified Requirements	Security clauses in tender documentation; supplier assessment. 0 – none; 3 – standard clauses; 5 – supplier risk assessment and acceptance tests
S4	Security testing and attestation before commissioning	Unified Requirements (compliance testing); ISO/IEC 27001 A.8.29	Penetration/compliance test reports; attestation certificate. 0 – none; 3 – testing without remediation tracking; 5 – attestation passed, residual risks accepted formally
S5	Incident-response and monitoring handover	ISO/IEC 27001 A.5.24–5.28; Action Plan measure 119	Connection to monitoring; incident playbooks; roles after go-live. 0 – none; 3 – playbooks exist; 5 – tested through exercises

Code	Indicator (life-cycle stage)	Normative source	Evidence; anchors 0 / 3 / 5
S6	Personal-data protection and access control	Law on Personal Data; Action Plan measure 120	Connection to "Personal-data access control" service; DPIA-type assessment. 0 – none; 3 – partial; 5 – connected and audited
A1	AI impact assessment and legal classification at initiation	ISO/IEC 42005; Law on AI No. 230-VIII	Impact assessment report; classification by degree of impact. 0 – none; 3 – classification without assessment; 5 – assessment approved, mitigations in charter
A2	AI management roles, policy and data governance	ISO/IEC 42001 cl. 5–6, Annex A; NIST AI RMF Govern/Map	Named AI owner; AI policy; training-data provenance and quality controls. 0 – none; 3 – roles only; 5 – documented data lineage, poisoning controls [30, 31]
A3	AI supply-chain and model provenance management	ISO/IEC 42001 A.10; LLM supply-chain [32]	Model/vendor register; licence and update terms; evaluation of third-party models. 0 – none; 3 – register; 5 – contractual controls and re-evaluation on update
A4	Adversarial and safety testing before deployment	NIST AI 100-2 [30]; OWASP LLM Top 10 [33]; MITRE ATLAS [34]	Red-team reports against the relevant threat catalogue. 0 – none; 3 – functional tests only; 5 – adversarial testing with remediation
A5	Human oversight, monitoring and incident handling in operation	ISO/IEC 42001 cl. 8–10; Law on AI	Oversight procedure; model performance and drift monitoring; AI incident process. 0 – none; 3 – oversight without monitoring; 5 – monitored with escalation
A6	Audit readiness of the AI management system	ISO/IEC 42006; ISO/IEC 42001 cl. 9	Internal audit records; readiness for third-party audit. 0 – none; 3 – internal review; 5 – audited by a competent body

Code	Indicator (life-cycle stage)	Normative source	Evidence; anchors 0 / 3 / 5
F1	Use of external threat intelligence in the risk register	ENISA Threat Landscape [35]; national monitoring (measure 119)	Risk register cites current threat landscape; refreshed each reporting period. 0 – none; 3 – cited once; 5 – refreshed semi-annually
F2	Probabilistic quantification of cyber risk	FAIR / Bayesian networks [27]	Expected-loss estimate for top cyber risks. 0 – none; 3 – qualitative likelihood–impact; 5 – quantified distribution
F3	Horizon scanning and scheduled re-assessment at stage gates	Dynamic risk assessment [29]; time-series prediction [28]	Re-assessment minutes at each gate; horizon to 2029. 0 – none; 3 – re-assessed on request; 5 – scheduled at every gate with trend data
F4	Scenario planning for emerging AI-specific threats	NIST AI 100-2; MITRE ATLAS	Documented scenarios (prompt injection, data poisoning, model theft) with triggers. 0 – none; 3 – generic; 5 – project-specific with indicators
F5	Budgeted cyber-risk reserve	ISO 21502 cl. 7.5–7.6; FAIR	Contingency reserve explicitly linked to cyber-risk estimates. 0 – none; 3 – lump-sum reserve; 5 – reserve derived from F2

4.6. Aggregation and interpretation

Scores are aggregated in four steps. First, the score of each practice group is the weighted mean of its six attributes:

$$P_i = \Sigma_k\, w_k \cdot K_{ik}, \quad \Sigma_k\, w_k = 1, \quad k = 1\ldots6 \tag{1}$$

Second, the baseline maturity index is the weighted mean of the ten practice groups:

$$B = \Sigma_i\, v_i \cdot P_i, \quad \Sigma_i\, v_i = 1, \quad i = 1\ldots10 \tag{2}$$

Third, each cross-cutting domain score (S, A, F) is the mean of its indicators, or a weighted mean where the expert panel has assigned indicator weights. Fourth, the integrated maturity index is a weighted combination whose weights depend on the project class:

$$M = \alpha \cdot B + \beta \cdot S + \gamma \cdot A + \delta \cdot F, \quad \alpha + \beta + \gamma + \delta = 1 \tag{3}$$

The weights w, v and (α, β, γ, δ) are derived by the Analytic Hierarchy Process [42] from pairwise comparisons made by an expert panel, with the consistency ratio of each comparison matrix required to be below 0.10. Default values proposed for use until a panel-

derived set is available are given in Table 4; they encode the policy judgement that security and AI governance should carry at least half of the weight for Class III projects.

Table 4. Default domain weights by project class

Project class	α (baseline B)	β (security S)	γ (AI governance A)	δ (forward-looking F)	Gating rule
Class I	0.70	0.20	—	0.10	none
Class II	0.50	0.30	—	0.20	M* = min(M, S + 1)
Class III	0.40	0.25	0.25	0.10	M* = min(M, S + 1, A + 1)

For Class II and Class III projects a non-compensatory gating rule is then applied: the final index M* cannot exceed the security score, or the AI-governance score, by more than one scale point:

$$M^* = \min(M, S + 1, A + 1) \quad (4)$$

The rationale is that a project whose security governance is "initial" cannot be "managed" as a whole, whatever its scheduling discipline; the one-point tolerance avoids the opposite error of reducing the whole assessment to its weakest indicator. Finally, M* is mapped to one of five maturity levels (Table 5). A single interpretation table is used for practices, domains and the integrated index, eliminating the duplicated and inconsistent level names found in earlier instruments.

Table 5. Interpretation of scores

Range of M* (or any score)	Level	Interpretation
0.00 – 1.49	L1 Initial	Practices largely absent or ad hoc; project outcomes unpredictable
1.50 – 2.49	L2 Forming	System being established; partial, inconsistent application
2.50 – 3.49	L3 Defined	Processes documented and applied; limited measurement
3.50 – 4.49	L4 Managed	Processes systematically applied and measured; corrective action routine
4.50 – 5.00	L5 Optimising	Continuous improvement; alignment with best international practice

4.7. Assessment procedure

The procedure follows five steps that map onto the stage gates of the Model Regulation: (1) scoping—select the assessment unit, determine the project class and the

applicable domains; (2) evidence collection—gather the documents listed in Table 3 and Appendix A, complemented by interviews; (3) scoring—at least two assessors score independently, after which disagreements are reconciled and inter-rater agreement is recorded; (4) computation—apply equations (1)–(4) with the current weight set; (5) reporting—produce the practice ranking, the domain profile and the level, together with prioritised recommendations, and feed the result into the semi-annual report under Resolution No. 760. Re-assessment is scheduled at each stage gate for Class II and III projects, which simultaneously satisfies indicator F3.

5. Worked example and validation protocol

5.1. Worked example: a G2C AI-assistant project

To illustrate the computation and the effect of the gating rule, consider a hypothetical Class III project of a central state body implementing measure 129 of the Action Plan (an AI assistant for civil servants in G2C interactions) on the QazTech platform. The scores below are illustrative values chosen to represent a project office with sound conventional project management and an immature AI-governance practice; they are not empirical data. Table 6 gives the attribute scores for the ten practice groups and Table 7 the domain indicator scores.

Table 6. Illustrative attribute scores of the baseline layer

Practice group	K1	K2	K3	K4	K5	K6	P_i
P1 Pre-project and initiation	4	4	4	4	4	4	4.00
P2 Planning	4	4	4	3	4	4	3.83
P3 Stakeholders and communication	4	4	3	3	4	4	3.67
P4 Resources and team	4	3	3	3	4	4	3.50
P5 Risk and issues	3	3	3	3	3	4	3.17
P6 Quality	4	4	3	3	4	4	3.67
P7 Schedule	4	4	4	4	4	4	4.00
P8 Cost	4	4	4	3	4	4	3.83
P9 Monitoring, control and change	4	3	3	3	4	4	3.50
P10 Closure and lessons learned	4	3	3	3	4	4	3.50
Baseline index B (equal weights)							3.67

Table 7. Illustrative domain indicator scores

Domain	Indicator scores	Domain score
S — cybersecurity	S1 = 3, S2 = 3, S3 = 2, S4 = 4, S5 = 3, S6 = 4	3.17
A — AI governance	A1 = 1, A2 = 2, A3 = 2, A4 = 1, A5 = 3, A6 = 1	1.67
F — forward-looking cyber risk	F1 = 2, F2 = 0, F3 = 1, F4 = 1, F5 = 1	1.00

Under the conventional approach—the arithmetic mean of practice scores with no security or AI component—the project obtains 3.67 and is classified as L4 "Managed". Under IPM3-DQ with the Class III default weights, equation (3) gives $M = 0.40 \times 3.67 + 0.25 \times 3.17 + 0.25 \times 1.67 + 0.10 \times 1.00 = 2.78$, and the gating rule (4) gives $M^* = \min(2.78, 4.17, 2.67) = 2.67$, i.e., L3 "Defined", with AI governance as the binding constraint. The domain profile makes the diagnosis explicit: the project has not performed an AI impact assessment (A1 = 1), has not tested the assistant against adversarial threat catalogues (A4 = 1) and has no audit trail (A6 = 1); the forward-looking domain shows that cyber risk is neither quantified nor budgeted (F2 = 0, F5 = 1). The recommendations that follow are concrete and standard-referenced: conduct an ISO/IEC 42005 impact assessment and classify the system under the Law on AI before the next stage gate; commission red-team testing against the OWASP LLM Top 10; and derive a cyber-risk reserve from a FAIR-type estimate. Had the same scores been treated as a Class I project, M would equal 3.30 (L3) without gating—showing that the class assignment, not only the scores, drives the result, which is the intended behaviour.

5.2. Validation protocol

Design requirement R5 demands that the instrument be validated rather than merely proposed. The following protocol is specified and is being implemented with project offices participating in the Action Plan; its results will be reported separately. (a) Content validity: a panel of 15–30 experts drawn from project offices of central state bodies, local executive bodies and national companies, from the Digital Government Support Centre and from information-security specialists, reviews the indicator set in two Delphi rounds; indicators are retained when at least 75 % of the panel rates them relevant. (b) Weights: the panel performs AHP pairwise comparisons for attributes, practice groups and domains separately for each project class; matrices with consistency ratio above 0.10 are returned for revision; group weights are obtained by geometric aggregation. (c) Expert agreement: Kendall's coefficient of concordance W is computed for the rankings of practices and domains, with $W \geq 0.5$ and $p < 0.05$ as the acceptance threshold. (d) Reliability: Cronbach's alpha is computed for the attribute scales within each practice group and for each domain (threshold

0.70). (e) Inter-rater agreement: the intraclass correlation coefficient ICC(2,k) is computed from independent scoring of the same projects by two or more assessors (threshold 0.75). (f) Pilot application: the instrument is applied to 3–5 projects of different classes drawn from Icebreakers 19 and 20, and the resulting profiles are compared with the outcomes of security attestation and with the semi-annual reports, providing a first test of criterion validity. The protocol follows the measurement-theory recommendations that recent psychometric evaluations of public-sector digital-maturity frameworks have shown to be routinely neglected.

6. Discussion

6.1. Positioning relative to existing models

Table 8 positions IPM3-DQ against the models reviewed in Section 2. Its distinctive features are the combination of a project-life-cycle baseline with security and AI domains, the forward-looking component and the non-compensatory aggregation. OPM3 and P3M3 provide richer process libraries but no security or AI content; C2M2 and NIST CSF 2.0 tiers describe organisational cyber capability without a project life cycle; the public-sector AI maturity model of Dreyling et al. [24] covers AI governance dimensions but not project delivery; the Secure-by-Design extensions of Payette et al. [21] are the closest precedent but predate the current standards, lack AI content and were not validated.

Table 8. Comparison of IPM3-DQ with related models

Model	Life-cycle baseline	Security domain	AI domain	Forward-looking	Gating	Public sector
OPM3 / P3M3 / Kerzner PMMM [13]	Yes (PMBOK / PRINCE2)	No	No	No	No	Generic
Secure-by-Design PMMM extensions [21]	Yes (P3M3)	Yes (NIST, C2M2)	No	No	No	Critical infra-structure
Cybersecurity maturity models [22]; NIST CSF 2.0 tiers [23]	No	Yes	Partial	Partial	No	Generic

Model	Life-cycle baseline	Security domain	AI domain	Forward-looking	Gating	Public sector
AI maturity model for the public sector [24]	No	Partial	Yes	No	No	Yes
Digital maturity of project offices of state bodies [38]	Partial	No	No	No	No	Yes (Kazakhstan)
IPM3-DQ (this article)	Yes (ST RK ISO 21502-2022)	Yes (27001/27005, Unified Requirements)	Yes (42001/42005/42006, Law on AI)	Yes	Yes (gating)	Yes (Kazakhstan)

6.2. Implications for project offices and the regulator

For project offices, the model converts a diffuse obligation—"take cybersecurity and AI requirements into account"—into eighteen verifiable indicators tied to the stage gates they already operate, and it produces a ranked list of practices to improve. Because the indicator evidence coincides with the documentation that attestation and audit bodies request, the assessment can be reused for compliance purposes. For the Ministry of Artificial Intelligence and Digital Development, the integrated index offers a candidate component of the digital development index of state bodies foreseen by measure 103 and a maturity-based lens for sequencing the national cybersecurity standardisation programme under measure 117: domains with persistently low scores across many bodies indicate where national standards, templates or training are most needed. For the Digital Government Support Centre, which is both a co-executor of measure 117 and the publisher of this journal, the model provides a basis for guidance material to project offices. The sectoral measures that already call for maturity and risk KPIs (measure 50 in the energy sector; measure 62 in agriculture; the data-governance maturity targets of Icebreaker 17) could adopt the same scale and aggregation logic, improving comparability across sectors.

6.3. Limitations

The study has four limitations. First, the model is presented with a worked example and a validation protocol, not with completed validation; the default weights in Table 4 are policy-informed proposals that the AHP procedure will replace. Second, the one-point

tolerance in the gating rule is a design choice whose sensitivity should be examined in the pilot. Third, the AI-governance domain depends on standards whose national adoption is still in progress (ISO/IEC 42005 and 42006), so indicators A1 and A6 will need to be re-anchored to the final texts of the national standards; the model's modular structure is intended to absorb such revisions. Fourth, self-assessment by project offices is exposed to optimism bias, which the two-assessor requirement and the ICC threshold mitigate but do not eliminate.

7. Conclusion

The Digital Qazaqstan Action Plan places 136 digital and AI measures in the hands of project offices that are obliged to follow ST RK ISO 21502-2022 but have no instrument for judging whether their project management is mature enough to meet the cybersecurity and AI-governance requirements those measures entail. This article has proposed IPM3-DQ, an integrated project management maturity model that keeps ST RK ISO 21502-2022 as its baseline and adds three cross-cutting domains—cybersecurity derived from ST RK ISO/IEC 27001-2023, ISO/IEC 27005 and the Unified Requirements; AI governance derived from ISO/IEC 42001, 42005, 42006 and the Law on AI; and forward-looking cyber risk—scored on one anchored scale, aggregated with class-specific weights and subjected to a non-compensatory gating rule. The worked example shows that the model changes conclusions in exactly the cases that matter: a project with strong conventional practices and weak AI governance is downgraded from "Managed" to "Defined", and the reason is made explicit. The validation protocol specifies how weights, agreement and reliability are to be established. Future work will report the results of the expert panel and pilot applications, examine the sensitivity of the gating tolerance, and extend the model to programme and portfolio level under ST RK ISO 21503, where the aggregation of project-level maturity into a portfolio-level cyber-risk posture is of direct interest to the Strategy's governance.

Acknowledgments

This research wasn’t funded by anyone.

Author Contributions

Conceptualization: Zh.I.; Methodology: Zh.I. and M.A.; Validation: Zh.I. and M.A.; Formal analysis: U.O.; Writing — original draft preparation: Zh.I. and M.A.; Writing — review and editing: Zh.I. and U.O.; Visualization: M.A.; Supervision: Zh.I.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] Decree of the President of the Republic of Kazakhstan No. 1311 of 9 June 2026 "On approval of the Nationwide Strategy for Large-Scale Digitalisation and Total Implementation of Artificial Intelligence Technologies 'Digital Qazaqstan' until 2029". Available at: https://adilet.zan.kz/rus/docs/U2600001311

[2] Resolution of the Government of the Republic of Kazakhstan No. 760 of 26 August 2026 "On approval of the Action Plan for the implementation of the Nationwide Strategy for Large-Scale Digitalisation and Total Implementation of Artificial Intelligence Technologies 'Digital Qazaqstan' until 2029". Available at: https://prg.kz/m/amp/document/37110361/

[3] Law of the Republic of Kazakhstan No. 230-VIII of 17 November 2025 "On Artificial Intelligence". Available at: https://adilet.zan.kz/rus/docs/Z2500000230

[4] Order of the Minister of National Economy of the Republic of Kazakhstan No. 2 of 13 January 2022 "On approval of the Model Regulation of Project Management of State Bodies" (as amended). Available at: https://adilet.zan.kz/rus/docs/V2300033371

[5] ST RK ISO 21502-2022. Project, programme and portfolio management — Guidance on project management (ISO 21502:2020, IDT). Astana: Committee for Technical Regulation and Metrology, 2022.

[6] ISO 21502:2020. Project, programme and portfolio management — Guidance on project management. Geneva: ISO, 2020.

[7] Resolution of the Government of the Republic of Kazakhstan No. 832 of 20 December 2016 "On approval of the Unified Requirements in the field of information and communication technologies and information security" (as amended).

[8] ST RK ISO/IEC 27001-2023. Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC 27001:2022, IDT). Astana, 2023.

[9] ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. Geneva: ISO/IEC, 2022.

[10] ISO/IEC 42001:2023. Information technology — Artificial intelligence — Management system. Geneva: ISO/IEC, 2023; adopted as ST RK ISO/IEC 42001-2025.

[11] ISO/IEC 42005:2025. Information technology — Artificial intelligence (AI) — AI system impact assessment. Geneva: ISO/IEC, 2025.

[12] ISO/IEC 42006:2025. Information technology — Artificial intelligence — Requirements for bodies providing audit and certification of artificial intelligence management systems. Geneva: ISO/IEC, 2025.

[13] Nikolaenko V, Sidorov A. Assessment of project management maturity models strengths and weaknesses. Journal of Risk and Financial Management. 2023;16(2):121. https://doi.org/10.3390/jrfm16020121

[14] Grant KP, Pennypacker JS. Project management maturity: an assessment of project management capabilities among and between selected industries. IEEE Transactions on Engineering Management. 2006;53(1):59–68. https://doi.org/10.1109/TEM.2005.861802

[15] Irfan M, Hassan M, Hassan N, Habib M, Khan S, Nasruddin AM. Project management maturity and organizational reputation: a case study of public sector organizations. IEEE Access. 2020;8:73828–73842. https://doi.org/10.1109/ACCESS.2020.2988511

[16] Žurga G. Project management in public administration. TPM — Total Project Management Maturity Model. The case of Slovenian public administration. Transylvanian Review of Administrative Sciences. 2018;14(53):144–159.

[17] Nikolaenko V, Sidorov A. Assessing the maturity level of risk management in IT projects. Sustainability. 2023;15(17):12752. https://doi.org/10.3390/su151712752

[18] Khan RA, et al. Securing software development through people maturity: a fuzzy-AHP decision-making framework. Journal of Software: Evolution and Process. 2025;37:e70045. https://doi.org/10.1002/smr.70045

[19] Lawal Y. Integrating cybersecurity into project management: a scoping review of current practices and gaps. Journal of Technology Studies. 2025. https://doi.org/10.21061/jts.430

[20] Al-Janabi S, Jabbar H, Syms F. Cybersecurity transformation: cyber-resilient IT project management framework. Digital. 2024;4(4):866–897. https://doi.org/10.3390/digital4040043

[21] Payette J, Anegbe E, Caceres E, Muegge S. Secure by design: cybersecurity extensions to project management maturity models for critical infrastructure projects. Technology Innovation Management Review. 2015;5(6):26–34.

[22] Büyüközkan G, Güler M. Cybersecurity maturity model: systematic literature review and a proposed model. Technological Forecasting and Social Change. 2025;213:123996. https://doi.org/10.1016/j.techfore.2025.123996

[23] National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg, MD: NIST, 2024. https://doi.org/10.6028/NIST.CSWP.29

[24] Dreyling R, Lemmik J, Tammet T, Pappel I. An artificial intelligence maturity model for the public sector: a design science approach. TalTech Journal of European Studies. 2024;14(2):217–239. https://doi.org/10.2478/bjes-2024-0023

[25] National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. Gaithersburg, MD: NIST, 2023. https://doi.org/10.6028/NIST.AI.100-1

[26] Vatamanu AF, Tofan M. Integrating artificial intelligence into public administration: challenges and vulnerabilities. Administrative Sciences. 2025;15(4):149. https://doi.org/10.3390/admsci15040149

[27] Wang J, Neil M, Fenton N. A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. Computers & Security. 2020;89:101659. https://doi.org/10.1016/j.cose.2019.101659

[28] Landauer M, Skopik F, Stojanović B, Flatscher A, Ullrich T. A review of time-series analysis for cyber security analytics: from intrusion detection to attack prediction. International Journal of Information Security. 2025;24(1):3. https://doi.org/10.1007/s10207-024-00921-0

[29] Cheimonidis P, Rantos K. Dynamic risk assessment in cybersecurity: a systematic literature review. Future Internet. 2023;15(10):324. https://doi.org/10.3390/fi15100324

[30] Vassilev A, Oprea A, Fordyce A, Anderson H, Davies X, Hamin M. Adversarial machine learning: a taxonomy and terminology of attacks and mitigations. NIST AI 100-2 E2025. Gaithersburg, MD: NIST, 2025. https://doi.org/10.6028/NIST.AI.100-2e2025

[31] Cinà AE, Grosse K, Demontis A, Vascon S, Zellinger W, Moser BA, Oprea A, Biggio B, Pelillo M, Roli F. Wild patterns reloaded: a survey of machine learning security against training data poisoning. ACM Computing Surveys. 2023;55(13s):294. https://doi.org/10.1145/3585385

[32] Wang S, Zhao Y, Hou X, Wang H. Large language model supply chain: a research agenda. ACM Transactions on Software Engineering and Methodology. 2025;34(5):147. https://doi.org/10.1145/3708531

[33] OWASP Foundation. OWASP Top 10 for LLM Applications 2025. 2024. Available at: https://genai.owasp.org

[34] MITRE Corporation. MITRE ATLAS: Adversarial Threat Landscape for Artificial-Intelligence Systems. Available at: https://atlas.mitre.org (accessed 21 October 2026).

[35] European Union Agency for Cybersecurity. ENISA Threat Landscape 2025. Athens: ENISA, 2025.

[36] Yessengeldina A, Taizhanova Z, Kuttybayeva N, Iskakova D, Khalbayev Y. Government project offices and the effectiveness of government programs: an empirical analysis based on panel data. Economies. 2026;14(7):267. https://doi.org/10.3390/economies14070267

[37] Narbaev, T. (2015). An assessment of project management maturity in Kazakhstan. *PM World Journal*, *4*(11), 1-20.

[38] Bekish, U., Yessengeldina, A., & Skrypko, T. (2025). FEATURES OF ASSESSMENT OF DIGITAL MATURITY OF THE PROJECT OFFICE OF STATE BODIES OF KAZAKHSTAN. Public Administration and Civil Service, 2(93), 31-41.

[39] United Nations Department of Economic and Social Affairs. United Nations E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development. New York: United Nations, 2024.

[40] OECD–IDB. (2023). 2023 OECD-IDB Digital Government Index of Latin America and the Caribbean: Results and key Findings. OECD Public Governance Policy Papers.

[41] Nerima, M., & Ralyté, J. (2021, May). Towards a digital maturity balance model for public organizations. In International conference on research challenges in information science (pp. 295-310). Cham: Springer International Publishing.

[42] Saaty TL. The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. New York: McGraw-Hill, 1980.

[43] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L, 12.7.2024.

Appendix A. Indicators and evidence for the baseline practice groups

The table lists, for each practice group of ST RK ISO 21502-2022, the key performance indicators and the evidence an assessor should examine when scoring attributes K1–K6 on the scale of Table 2. The list consolidates and corrects the practitioner matrix from which the model originated: all indicators now use the 0–5 scale and are mapped to the ten practice groups of Section 4.3.

Table A1. Baseline indicator matrix

Practice group	KPI	Evidence	Anchors (0 / 3 / 5)
P1 Pre-project and initiation	Project charter; business justification; stakeholder identification	Approved charter; business case; stakeholder register	0 – absent; 3 – partial; 5 – approved and linked to Action Plan measure
P2 Planning	Project management plan; schedule; resource plan; security and AI requirements included	Approved plan; baseline schedule; resource plan	0 – absent; 3 – approved without baselines; 5 – integrated plan with baselines
P3 Stakeholders and communication	Stakeholder map; communication plan; satisfaction	Stakeholder map; communication plan; survey results	0 – absent; 3 – plan exists; 5 – executed and measured
P4 Resources and team	Resource matrix; utilisation; role allocation; competence (incl. security and AI)	RACI; utilisation reports; training records	0 – absent; 3 – roles defined; 5 – competence verified
P5 Risk and issues	Risk register; probability–impact assessment; response plan; issue log	Risk register; risk matrix; response plan; issue log	0 – absent; 3 – register maintained; 5 – responses implemented and reviewed at gates
P6 Quality	Quality plan; quality control; defect rate	Quality plan; test and review records; defect statistics	0 – absent; 3 – plan approved; 5 – controls executed, defects minimal
P7 Schedule	Schedule variance; progress reporting; forecasting tools	Progress reports; schedule analysis	0 – variance > 20 %; 3 – variance 5–20 %; 5 – variance < 5 % with forecasting

Practice group	KPI	Evidence	Anchors (0 / 3 / 5)
P8 Cost	Budget approved; cost variance; financial reporting; cyber-risk reserve (F5)	Budget; cost reports	0 – variance > 20 % either way; 3 – 5–20 %; 5 – < 5 % with reserve analysis
P9 Monitoring, control and change	Reporting regularity; KPI control; change log	Reports; KPI dashboard; change log	0 – absent; 3 – periodic; 5 – systematic with corrective action
P10 Closure and lessons learned	Completion act; final report; knowledge base	Completion act; final report; lessons-learned repository	0 – absent; 3 – prepared; 5 – lessons reused in subsequent projects