Статья поступила в редакцию: 05.07.2026
Статья принята к публикации: 29.07.2026
Статья опубликована: 28.08.2026

УДК 004.9+658.5

DOI: 10.32743/UniTech.2026.149.8.23252

Methodological approach to risk management in IT projects through identification, assessment and minimization of project deviations

Mineeva Iuliia
Project manager Sibedge
Russia, Moscow
E-mail: mineevayi@sibedge.com

Методический подход к управлению рисками в IT-проектах путем выявления, оценки и минимизации проектных отклонений

Минеева Юлия Игоревна
руководитель
проектов Sibedge
Российская Федерация, г. Москва

Abstract

The article examines the problem of risk management in IT projects based on the identification, assessment and minimization of project deviations. The relevance of the study is determined by the growing uncertainty in the development of software products, digital services and corporate information systems. The purpose of the study is to develop and substantiate a methodological approach to IT project risk management based on the early identification, quantitative assessment, and minimization of project deviations. A methodological approach is proposed in which risk assessment is based on measurable deviations of the actual project state from planned, target, or acceptable values. The classification of project deviations is substantiated, the causes of their occurrence are revealed, and a methodology for early diagnosis and integrated risk assessment is proposed. Special attention is paid to the use of AI tools for anomaly detection, prediction of critical deviations and preparation of response options. The practical significance of the study lies in the possibility of applying the proposed approach in IT project management, project offices and development teams.The methodological novelty of the study lies in linking risk management with a system of regular monitoring of project data, including the backlog, sprint backlog, issue tracker, CI/CD, test reports, and team performance indicators. The proposed model

Библиографическое описание: Минеева Ю.И. Методический подход к управлению рисками в IT-проектах путем выявления, оценки и минимизации проектных отклонений // Universum: технические науки : электрон. научн. журн. 2026. 8(149). URL: https://7universum.com/ru/tech/archive/item/23252

For citation: Mineeva I. Methodological approach to risk management in IT projects through identification, assessment and minimization of project deviations // Universum: Technical Sciences : electronic scientific journal. 2026. No. 8(149). Available at: https://7universum.com/ru/tech/archive/item/23252

makes it possible not only to record risk events that have already occurred, but also to identify early signals of their escalation, rank deviations by probability, impact, and response urgency, and develop a well-founded mitigation plan. The proposed approach enhances the transparency of managerial decision-making and can serve as a basis for standardizing risk control procedures in IT teams.

Аннотация

В статье рассматривается проблема управления рисками в IT-проектах на основе выявления, оценки и минимизации проектных отклонений. Актуальность исследования определяется повышением неопределенности в сфере разработки программных продуктов, цифровых сервисов и корпоративных информационных систем. Цель исследования состоит в разработке и обосновании методического подхода к управлению рисками IT-проектов на основе раннего выявления, количественной оценки и минимизации проектных отклонений. В качестве основы предложен методический подход, при котором риск рассматривается через измеримое отклонение фактического состояния проекта от планового, целевого или допустимого уровня. Обоснована классификация проектных отклонений, раскрыты причины их возникновения, предложена методика ранней диагностики и интегральная оценка риска. Отдельное внимание уделено применению AI-инструментов для выявления аномалий, прогнозирования критических отклонений и подготовки вариантов мер реагирования. Практическая значимость исследования состоит в возможности применения предложенного подхода в управлении IT-проектами, проектных офисах и командах разработки. Методическая новизна работы заключается в увязке риск-менеджмента с системой регулярного мониторинга проектных данных: backlog, sprint backlog, issue tracker, CI/CD, отчетов о тестировании и показателей командной производительности. Предложенная модель позволяет фиксировать наступившие рисковые события, а также выявлять ранние сигналы их эскалации, ранжировать отклонения по вероятности, влиянию и срочности реагирования, а также формировать обоснованный mitigation plan. Предложенный подход способствует повышению прозрачности управленческих решений и может быть использован как основа для стандартизации процедур контроля рисков в IT-командах.

Keywords: IT project, risk management, project deviations, project management, AI, machine learning, mitigation plan.

Ключевые слова: IT-проект, управление рисками, проектные отклонения, проектное управление, AI, machine learning, mitigation plan.

Introduction

Risk management in IT projects is one of the most important areas of project management. The development of digital products is characterized by a high degree of uncertainty regarding final requirements, the need for rapid adaptation to changing requirements, and the continuous evolution of technologies, while also being highly dependent on team competencies, budget constraints, and project schedules. As a result, IT projects are exposed to elevated risks associated with changing requirements, external integrations, contractor performance, information security requirements, and

stakeholder expectations. A distinctive feature of IT projects is the delayed manifestation of risk events. The delayed and cumulative effects of project risks remain one of the major challenges in IT project management, the effective resolution of which requires the application of scientifically grounded approaches [1]. Classical software risk management also emphasizes proactive identification and elimination of risk items before they become sources of project failure [2].

The aim of the study is to develop a methodological approach to risk management in IT projects through the identification, assessment, and minimization of project deviations.

Research methodology

The study is based on the analysis of scientific publications on software project risk management, the identification of risk factors, the diagnosis of project deviations, the application of Scrum artifacts, and the use of machine learning in project risk management.

The methodological procedure combines the classification of observable project deviations, their early diagnosis based on operational project data, identification of the underlying risk factor, integrated risk scoring, selection of a response measure, and subsequent reassessment. In the proposed approach, a project deviation is not equated with risk itself. It is treated as an observable early signal indicating that a risk may materialize or escalate. This distinction makes it possible to move from the identification of abstract risk factors to the monitoring of measurable changes in the actual state of an IT project.

For the quantitative prioritization of identified deviations, an integrated risk score is proposed:

$$R = P \cdot I \cdot U,$$

where R is the integrated risk score associated with the identified project deviation; P is the estimated probability that the detected deviation will lead to further risk escalation or an adverse project event; $I$is the normalized degree of impact on project objectives; and U is the urgency of managerial response. All parameters take values from 0 to 1.

The value of P can be determined from historical project data, the observed frequency of similar deviations, or predictive estimates generated from previous project cases. The value of I reflects the expected effect of the deviation on schedule, cost, scope, quality, or other critical project objectives. The value of U characterizes the time sensitivity of the deviation and increases as the admissible period for managerial response decreases.

For operational interpretation, the following working intervals are used: $R < 0.125$ – low risk; $0.125 \leq R < 0.343$ – moderate risk; $0.343 \leq R < 0.512$ – high risk; and $R \geq 0.512$ – critical risk. The threshold values correspond to the simultaneous achievement of benchmark levels of 0.5, 0.7, and 0.8 by the three assessment parameters ($0.5^3 = 0.125$; $0.7^3 = 0.343$; $0.8^3 = 0.512$). The thresholds may subsequently be calibrated using historical data from a specific organization or project portfolio.

All parameters are assessed on a scale from 0 to 1. A value close to 1 indicates a high level of the corresponding parameter. The assessment also incorporates the response urgency parameter, which makes it possible to account for the time sensitivity of the deviation.

Results and discussion

Risks in IT projects are traditionally characterized by the simultaneous presence of organizational, technical, managerial, and user-related factors. Risks in IT projects arise as a result of changing requirements, planning errors, reduced team performance, an increasing number of defects, limited customer involvement, delays in approvals, integration issues, and insufficient project data. A project deviation can serve as one of the earliest observable signals of risk materialization or escalation. By its nature, risk reflects the probability of an adverse outcome, whereas a deviation captures an existing discrepancy between the planned and the actual project state. Within the context of IT project management, it is advisable to focus on the analysis of project deviations, as they are measurable and can be incorporated into a project monitoring system.

Accordingly, the proposed approach does not replace conventional risk identification with deviation analysis. Rather, it introduces project deviation as an intermediate observable element between a risk factor and a possible adverse project outcome. The resulting relationship can be represented as follows: 1) risk factor; 2) measurable project deviation; 3) risk escalation; 4) adverse project outcome. This makes it possible to identify a developing risk before its consequences become fully manifested in project schedule, cost, scope, or quality indicators.

Unlike classifications focused primarily on sources and categories of software project risks [3; 4; 10], the proposed classification describes the detected deviation simultaneously from several managerial perspectives: the affected project area, the source of the deviation, the project stage at which it occurs, the indicator through which it can be detected, and the urgency of response. Therefore, the classification presented in Figure 1 performs not only a descriptive function but also supports the subsequent selection of diagnostic indicators and response measures.

Risk factors should be considered within the following groups: requirements, customer, team, technologies, planning, external environment, and change management [3]. In the context of IT projects, different groups of risk factors are often interrelated. The main types of project deviations are presented in Figure 1.

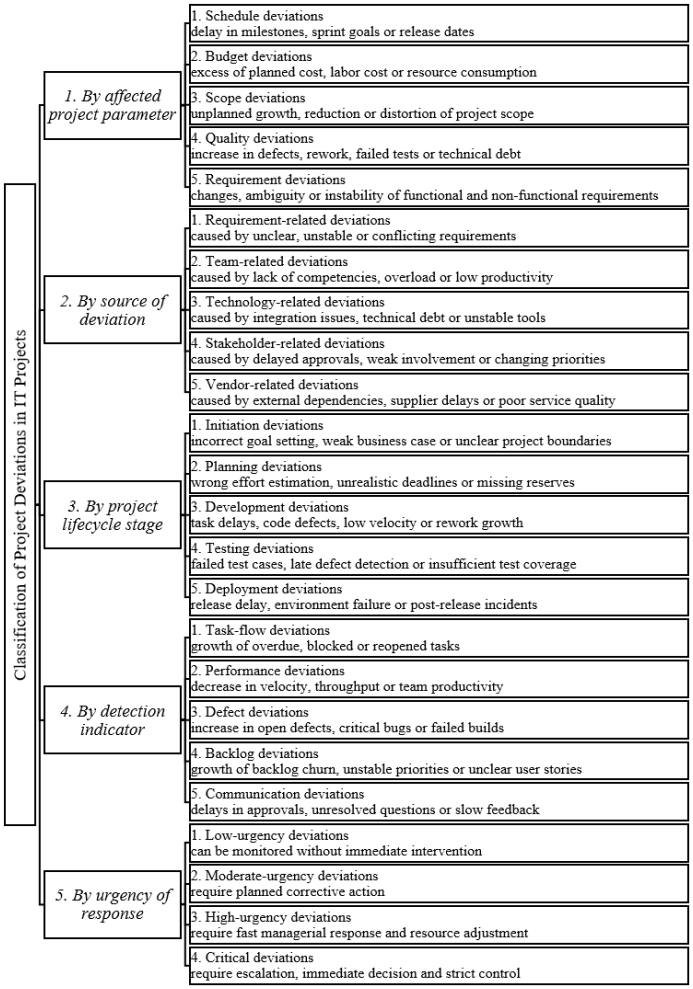

Figure 1. Classification of project deviations in IT projects

The determinants of risk occurrence in IT projects can be divided into several groups:

1. requirements-related determinants, including poorly defined requirements, frequent backlog changes, the absence of acceptance criteria, and conflicting customer expectations;

2. team-related determinants, including competency gaps, team member overload, ineffective role distribution, and a low task completion rate;

3. planning-related determinants, including underestimated effort estimates, insufficient task decomposition, the absence of time reserves, and inadequate assessment of external dependencies;

4. technology-related determinants, including complex integrations, increasing technical debt, an unstable development environment, CI/CD issues, late defect detection, and insufficient test coverage;

5. customer- and external stakeholder-related determinants, including delays in approvals, changing priorities, dependence on contractors, and a gap between business expectations and the team's capabilities.

Previous studies identify user involvement, management support, requirements management, team experience, and change control among the significant factors affecting software project risks [4]. Risks in IT projects rarely arise from a single source; rather, they more often emerge at the intersection of organizational decisions, technical conditions, and the quality of communication. The impact of risks is reflected in the deterioration of project performance, as they may lead to schedule delays, budget overruns, reduced quality, loss of functionality, an increase in the number

of defects, and reduced team effectiveness. Moreover, different dimensions of risk affect project schedule, cost, and quality in different ways [5]. Therefore, risk assessment should also take into account the magnitude of a risk's impact on project outcomes.

The traditional risk matrix, based on probability and impact, is useful for the initial assessment of risks. However, IT projects often require the introduction of an additional parameter-response urgency. This parameter reflects how quickly a decision must be made and is particularly important when managing sprints, release cycles, integration dependencies, and critical defects. General project management and risk management standards also emphasize the need to integrate risk-related decisions into planning, monitoring, response selection and stakeholder communication [6; 7].

Based on the above, the methodology for the early diagnosis of project deviations includes four interrelated stages:

1. Data collection. Project information is obtained from the backlog, sprint backlog, issue tracker, burndown chart, testing reports, CI/CD systems, task statuses, defect logs, overtime records, requirement change history, and data on external dependencies. At this stage, the objective is to create a unified set of operational data suitable for subsequent diagnostic analysis.

2. Diagnostic analysis. The collected data are used to calculate indicators reflecting schedule deviation, the proportion of overdue and blocked tasks, changes in velocity, growth in open defects, reopened issues, backlog churn, deviation of actual effort from estimated effort, approval delays, and the proportion of tasks without acceptance criteria. A deviation is recorded when the actual value exceeds an established project threshold or demonstrates a persistent negative trend.

3. Risk evaluation. The root cause and the corresponding risk factor are identified for each detected deviation. The values of P, I, and U are then estimated, after which the integrated risk score $R=P \cdot I \cdot U$ is calculated and the deviation is assigned to a low, moderate, high, or critical risk category.

4. Response preparation. The calculated value of R, together with the type and root cause of the deviation, is used to determine the required managerial response. Low-risk deviations remain under monitoring; moderate risks require planned corrective actions; high risks require a formal mitigation plan; and critical risks require immediate intervention and escalation.

Modern software risk management requires a reconsideration of the role of risk management within a project, as risks should be analyzed throughout the entire project lifecycle rather than only during the planning phase [8; 9]. Early diagnosis of project deviations thus becomes a continuous management process (Figure 2).

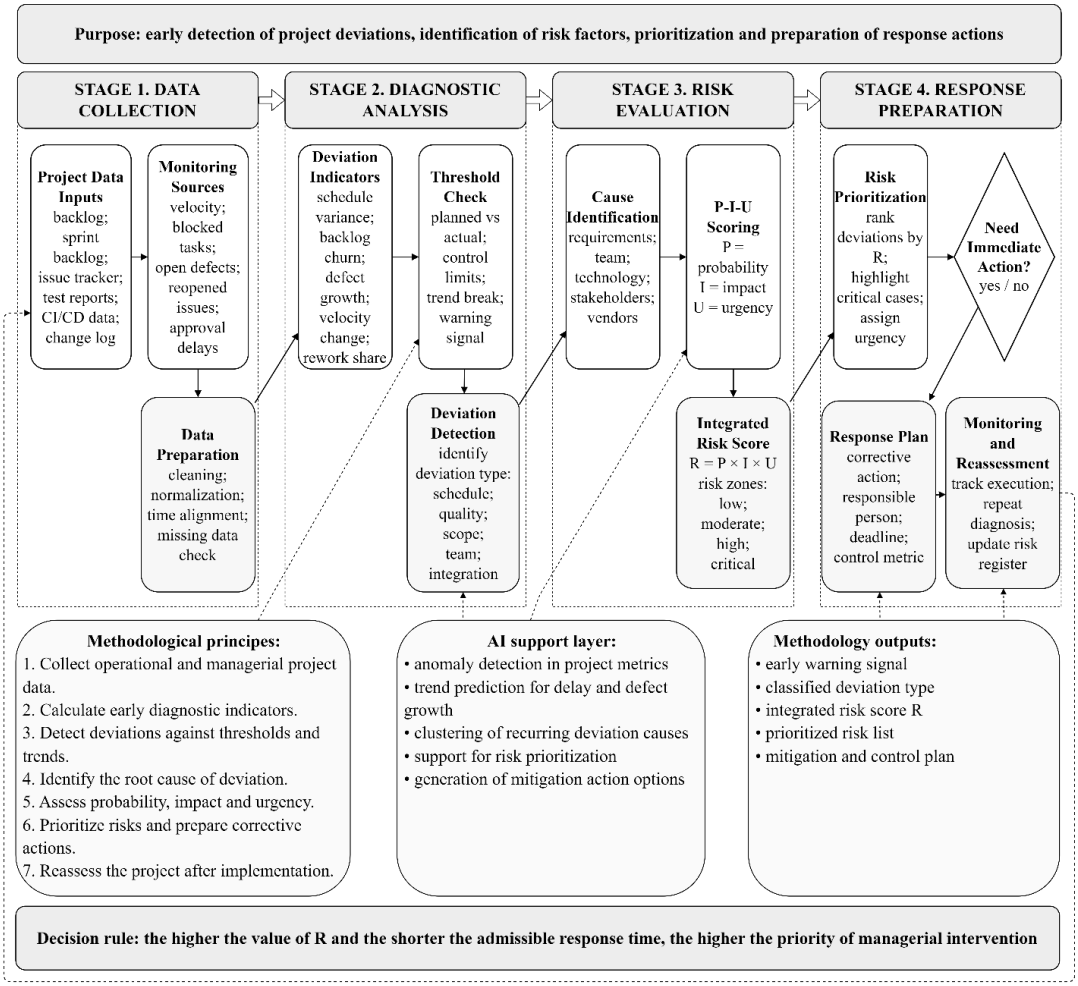

Figure 2. Methodology for the early diagnosis of project deviations

The proposed sequence extends the conventional probability–impact approach by introducing two additional elements. First, risk assessment is initiated by an observable deviation detected in current project data rather than solely by periodic expert identification of potential risks. Second, the inclusion of response urgency U distinguishes situations with similar probability and impact but different admissible response times. This distinction is particularly relevant to IT projects, where a blocked deployment pipeline, a critical security defect, or an unresolved integration dependency may require substantially faster intervention than another risk with a comparable expected impact. Thus, the proposed score does not replace the traditional probability–impact assessment reflected in project and risk management standards [6; 7], but operationalizes it for continuous monitoring of IT projects.

Within the proposed methodology, AI tools can support four analytical operations associated with the processing and interpretation of project data:

1. at the data collection stage, AI helps process information from the issue tracker, backlog, testing reports, and task statuses.

2. at the deviation detection stage, AI tools can identify anomalies in task dynamics, team velocity, the number of defects, and the frequency of requirements changes.

3. at the root cause analysis stage, clustering techniques can be applied to identify recurring problems.

4. at the risk assessment stage, AI can support the prediction of whether a deviation is likely to escalate to a high- or critical-risk level.

Within the proposed methodology, AI is therefore treated as a supporting analytical layer rather than as an independent risk assessment dimension. Its principal functions are anomaly detection in operational project metrics, identification of recurring deviation patterns, estimation of escalation probability, and analytical support for the selection of response options. The final values of I and U, as well as the managerial decision concerning the mitigation measure, remain subject to project management assessment. Thus, AI support influences the quality and speed of risk diagnosis but does not replace the integrated risk score R or managerial responsibility for the final decision.

The risk mitigation model is based on the transition from identifying a project deviation to taking a management action (Figure 3). Once a deviation has been identified, its cause is determined, after which the value of R is calculated and the risk is assigned to a priority category. An appropriate response measure is then selected, such as reducing the probability of occurrence, reducing the impact, decreasing response urgency, extending the schedule, reallocating resources, refining requirements, conducting additional testing, performing a technical review, carrying out a security review, or escalating the issue.

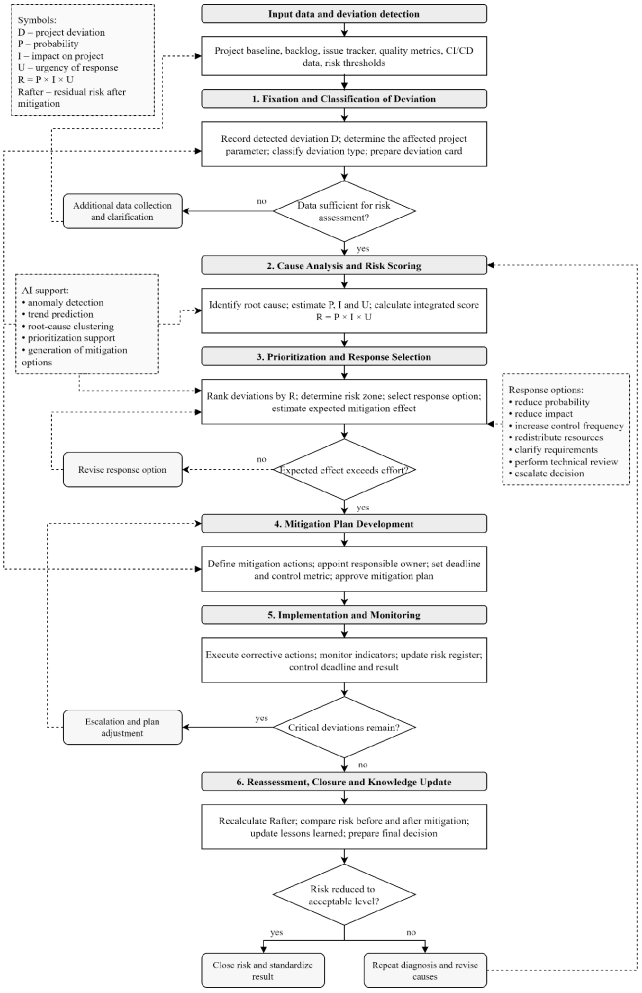

Figure 3. Risk mitigation and project deviation management model

To demonstrate the application of the proposed methodological approach, an illustrative reassessment of eight groups of project deviations was performed (Figure 4). The assessment compares the integrated risk score R before and after the implementation of mitigation measures.

The purpose of this comparison is to demonstrate how the proposed indicator can be used not only for initial risk prioritization but also for subsequent control of the effectiveness of managerial intervention. The difference between the initial and reassessed values is determined as follows:

$$\Delta R = R_{before} - R_{after}.$$

A positive value of ΔRindicates a reduction in the integrated risk score after mitigation. The relative effectiveness of mitigation can additionally be determined as:

$$E_R = \frac{R_{before} - R_{after}}{R_{before}} \times 100\%.$$

This indicator makes it possible to compare the effectiveness of risk response measures across deviation groups with different initial levels of R.

Deviation group	R before	R after	Risk reduction
Requirement deviations	0,574	0,312	0,261
Schedule deviations	0,476	0,276	0,200
Quality deviations	0,390	0,221	0,169
Team productivity deviations	0,384	0,228	0,156
Integration deviations	0,351	0,208	0,143
Security deviations	0,365	0,194	0,170
Vendor dependency deviations	0,228	0,139	0,088
Communication deviations	0,250	0,139	0,112

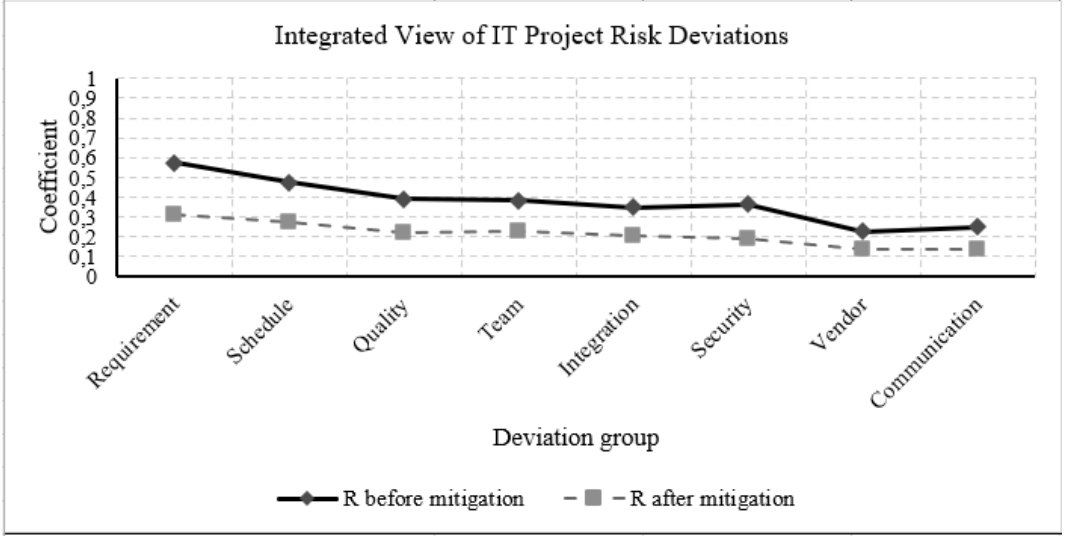

Figure 4. Changes in integrated risk scores before and after mitigation measures
Source: prepared by the author.

The results presented in Figure 4 demonstrate a decrease in the integrated risk score for all eight groups of project deviations. The average value of R decreased from 0.377 before mitigation to 0.215 after mitigation. The average relative reduction amounted to approximately 42.8 %, indicating that the application of corrective and mitigation measures produced a consistent decrease in the assessed level of project risk across the analyzed deviation groups.

The largest absolute reduction was observed for requirement deviations, for which R decreased from 0.574 to 0.312 ($\Delta R = 0.262$). According to the proposed scale, this corresponds to a transition from the critical to the moderate risk category. The result indicates that deviations related to unstable or conflicting requirements can be substantially reduced when the response is directed toward requirement clarification, backlog stabilization, specification of acceptance criteria, and coordination with stakeholders.

A substantial reduction was also recorded for security deviations, where R decreased from 0.365 to 0.194, corresponding to a relative reduction of approximately 46.8 %. Schedule, quality, team productivity, and integration deviations initially belonged to the high-risk category and moved to the moderate-risk category after mitigation. This result demonstrates the practical role of repeated risk scoring: the methodology makes it possible to determine whether the implemented measures have changed the priority of a detected deviation rather than merely documenting that a corrective action has been performed.

Vendor dependency deviations demonstrated the smallest absolute reduction ($\Delta R = 0.089$) and remained within the moderate-risk category. This result may be explained by the limited ability of an internal project team to directly influence external suppliers and dependencies. In such cases, mitigation measures can reduce the consequences and improve response preparedness but may have a weaker effect on the underlying probability of the risk event.

The comparison therefore indicates that the effectiveness of mitigation depends on the controllability of the underlying risk factor. Deviations caused by internal project processes, including requirements management, quality control, scheduling, and team coordination, are more directly affected by managerial intervention. Risks associated with external dependencies may require contractual, organizational, or escalation mechanisms beyond the boundaries of the project team. This distinction should be considered when interpreting changes in R and selecting subsequent response measures.

The obtained results also clarify the methodological distinction between the proposed approach and conventional risk factor analysis. Existing studies emphasize the identification of software project risk sources and their classification [3; 4; 10], while proactive risk management focuses on detecting and addressing risk items before they lead to project failure [2]. The proposed methodology develops this direction by introducing measurable project deviations as operational signals connecting risk factors with current project performance. In this respect, continuous monitoring of backlog, issue tracker, testing, and CI/CD data complements lifecycle-oriented approaches to software risk management [8; 9] and provides a quantitative basis for repeated risk reassessment.

At the same time, the proposed approach has limitations. The values of P, I, and U depend on the availability and quality of project data and may require calibration for different organizations and types of IT projects. The threshold values proposed in this study should therefore be considered working reference points rather than universal boundaries. Further research should focus on validating the methodology using longitudinal data from multiple IT projects and comparing expert-based and machine-learning-based estimates of risk escalation probability.

Based on the proposed methodology and the results of repeated risk assessment, the approach can be applied in project offices, product teams, development teams, and digital transformation units. Its practical value lies in linking a risk assessment to a specific measurable project deviation

and expressing the required management priority in quantitative terms. This enables the project manager to compare heterogeneous project deviations, identify priority areas for intervention, select appropriate mitigation measures, and subsequently assess whether the implemented actions have reduced the integrated risk score.

Conclusion

The study resulted in the development of a methodological approach to risk management in IT projects based on the transition from the detection of measurable project deviations to risk assessment, prioritization, mitigation, and repeated evaluation. The proposed approach distinguishes between a risk factor, an observable project deviation, and an adverse project outcome, which makes it possible to use current project data as early signals of possible risk escalation.

The methodological contribution of the study consists in combining a multi-criteria classification of project deviations with the integrated risk score $R = P \cdot I \cdot U$, where risk probability and impact are supplemented by the urgency of managerial response. The proposed assessment scale connects the quantitative value of $R$with differentiated management actions ranging from monitoring to immediate escalation. This makes the indicator applicable both to initial risk prioritization and to repeated assessment after mitigation measures have been implemented.

The illustrative application of the approach to eight groups of project deviations demonstrated a decrease in the integrated risk score across all analyzed categories. The average value of R decreased from 0.377 to 0.215, while the average relative reduction was approximately 42.8 %. The largest absolute decrease was observed for requirement deviations, whereas vendor dependency deviations showed a more limited reduction, indicating differences between risks arising from internally controllable project processes and those associated with external dependencies.

AI tools can support the proposed methodology through anomaly detection, identification of recurring deviation patterns, prediction of risk escalation, and preparation of response alternatives. However, AI is considered a supporting analytical layer, while the final assessment of impact and response urgency and the selection of mitigation measures remain the responsibility of the project manager.

The practical significance of the proposed approach lies in its applicability to project offices, software development teams, product teams, and digital transformation units using operational data from backlog management systems, issue trackers, testing environments, and CI/CD pipelines. The principal limitation of the study is the need to calibrate the parameters and threshold values using historical data from specific organizations. Further research should therefore focus on empirical validation of the approach across multiple IT projects and on evaluating the accuracy of AI-supported prediction of project deviation escalation.

References

1. Barki, H. Toward an assessment of software development risk. Barki, S. Rivard, J. Talbot // Journal of Management Information Systems. – 1993. – T. 10, № 2. – DOI: 10.1080/07421222.1993.11518006.
2. Boehm B.W. Software risk management: Principles and practices // IEEE Software. – 1991. – T. 8, № 1. – DOI: 10.1109/52.62930.

3. Keil, M. A framework for identifying software project risks. Keil P.E. Cule, K. Lyytinen R.C. Schmidt // Communications of the ACM. – 1998. – T. 41, № 11. – DOI: 10.1145/287831.287843.
4. Schmidt, R. Identifying software project risks: an international Delphi study. Schmidt, K. Lyytinen, M. Keil, P. Cule // Journal of Management Information Systems. – 2001. – T. 17, № 4. – DOI: 10.1080/07421222.2001.11045662.
5. Wallace, L. How software project risk affects project performance: an investigation of the dimensions of risk and an exploratory model. Wallace, M. Keil, A. Rai // Decision Sciences. – 2004. – T. 35, № 2. – DOI: 10.1111/j.0011–7315.2004.02059.x.
6. Project Management Institute. A Guide to the Project Management Body of Knowledge (PMBOK® Guide). – 7th ed. – Newtown Square, PA: Project Management Institute. – Newtown Square, PA: Project Management Institute. – 2021.
7. International Organization for Standardization. ISO 31000:2018 Risk management – Guidelines. – Geneva: International Organization for Standardization, 2018.
8. Bannerman P.L. Risk and risk management in software projects: A reassessment // Journal of Systems and Software. – 2008. – T. 81, № 12. – DOI: 10.1016/j.jss.2008.03.059.
9. Alhawari, S. Knowledge-Based Risk Management framework for Information Technology project. Alhawari, L. Karadsheh, A. Nehari Talet, E. Mansour // International Journal of Information Management. – 2012. – T. 32, № 1. – DOI: 10.1016/j.ijinfomgt.2011.07.002.
10. Menezes, J. Risk factors in software development projects: a systematic literature review. Menezes Jr., C. Gusmão, H. Moura // Software Quality Journal. – 2019. – T. 27, № 3. – DOI: 10.1007/s11219-018-9427-5.