

Electronic scientific and practical journal

INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT

#37(2026)
June '26



WWW.SMART-SCM.ORG

ISSN 2708-3195

DOI.ORG/10.46783/SMART-SCM/2026-37

ISSN 2708-3195



9 772708 319005

Electronic scientific and practical publication in economic sciences

Electronic scientifically and practical journal “Intellectualization of logistics and Supply Chain Management” included in the list of scientific publications of Ukraine in the field of economic sciences (category “B”): **Order of the Ministry of Education and Culture of Ukraine dated June 11, 2026 No. 928 (Appendix 13 item 205).**

Cluster: Economic Transformation, Business and Administration

Specialties: C1 – Economics and International Economic Relations (by specializations)

D3 – Management

D5 – Marketing

ISSN 2708-3195

DOI: <https://doi.org/10.46783/smart-scm/2026-37>

The electronic magazine is included in the international scientometric databases:

Index Copernicus, Google Scholar

Released 6 times a year

№ 37 (2026)

June 2026

Kyiv - 2026

Founder: Viold Limited Liability Company

Editor in Chief: Hryhorak M. Yu. – Doctor of Economics, Ass. Professor.

Technical editor: Harmash O. M. – PhD (Economics), Ass. Professor.

Assistant editor: Davidenko V. V. – PhD (Economics), Ass. Professor.

Members of the Editorial Board:

BUGAYKO Dmytro – Doctor of Economics, Professor, Academician of the Academy of Economic Sciences of Ukraine, Corresponding Member of the Transport Academy of Ukraine;
RELAWATI Rahayu – Doctoral Degree, Professor;
KRAUS Nataliia – Doctor of Economics, Professor;
MOSKVICHENKO Iryna – PhD in Economics, Associate Professor;
ILCHENKO Nataliia – Doctor of Economics, Professor;
GALKIN Andrii – Doctor of Technical Sciences, Professor;
ROMANENKOV Yuri – Doctor of Technical Sciences, Professor;
SIMONETTI Biagio – PhD, Associate professor;
SOKOLOVA Olena – PhD in Economics, Associate Professor;
HLYNSKYI Nazar – Doctor of Sciences in Economics;
LIESKOVSKÁ Vanda – Doctor of Sciences in Economics, Professor;
SHKURENKO Olga – Doctor of Economics, Professor;
LAZORENKO Larysa – Doctor of Sciences in Economics, Professor;
ALKEMA Viktor – Doctor of Economics, Professor;
ZAPOROZHETS Oleksandr – Doctor of Technical Sciences, Professor
DYMA Oleksandr – Doctor of Economics, Associate professor

The electronic scientific and practical journal is registered in international scientometric data bases, repositories and search engines. The main characteristic of the edition is the index of scientometric data bases, which reflects the importance and effectiveness of scientific publications using indicators such as quotation index, h-index and factor impact (the number of quotations within two years after publishing).

In 2020, the International Center for Periodicals (ISSN International Center, Paris) included the Electronic Scientific and Practical Edition “Intellectualization of logistics and Supply Chain Management” in the international register of periodicals and provided it with a numerical code of international identification: ISSN 2708-3195 (Online).

Recommended for dissemination on the Internet by the Academic Council of the Department of Logistics NAU (No. 7 of February 26, 2020). Released 6 times a year. Editions references are required. The view of the editorial board does not always coincide with that of the authors.

Electronic scientifically and practical journal “Intellectualization of logistics and Supply Chain Management” included in the list of scientific publications of Ukraine in the field of economic sciences (category "B"): **Order of the Ministry of Education and Culture of Ukraine dated June 11, 2026 No. 928 (Appendix 13 item 205).**

Cluster: Economic Transformation, Business and Administration

Specialties: C1 – Economics and International Economic Relations (by specializations); D3 – Management; D5 – Marketing

DOI: <https://doi.org/10.46783/smart-scm/2026-37>
e-mail: support@smart-scm.org

facebook.com/Smart.SCM.org
тел.: (063) 593-30-41
<https://smart-scm.org>

Contents

INTRODUCTION

6

GONCHARENKO K.V. WELL DIGIT LLC, CEO (Ukraine), **BUGAYKO D.O.** Doctor of Science (Economics), Professor, Academician of the Academy of Economic Sciences of Ukraine, Corresponding Member of the Transport Academy of Ukraine, Instructor of ICAO Institute, Professor (Full) of the Logistics Department Vice Director for International Cooperation and Education of National University "Kyiv Aviation Institute" (Ukraine)

AI IN AVIATION COMPLIANCE MONITORING: SAFETY BARRIERS, REGULATORY GAPS, AND ARCHITECTURAL CONDITIONS FOR TRUSTWORTHY DEPLOYMENT

7– 20

MARCHUK V.Ye. Doctor of Technical Sciences, Professor, Professor of the Department of International Business and Logistics, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute." (Ukraine), **ZELINSKA M.V.** Master's degree seeker of the Department of International Business and Logistics, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute» (Ukraine), **REZANKO O.V.** Master's degree seeker of the Department of International Business and Logistics, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute» (Ukraine)

IMPROVING CONTRACT PERFORMANCE IN THE DEFENSE PROCUREMENT SYSTEM BASED ON A RISK-ORIENTED APPROACH

21 – 35

HARMASH O.M. PhD (in Economics), Associate Professor Department of International Business and Logistics, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" (Ukraine), **TRUSHKINA N.V.** Ph.D. (in Economics), Senior Researcher Research Center for Industrial Problems of Development of the NAS of Ukraine (Ukraine), **KHOKHLOVA O.M.** Master's degree seeker of the Department of International Business and Logistics, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute» (Ukraine), **GVOZDOVA O.O.** Master's degree seeker of the Department of Information Warfare, National Defence University of Ukraine, (Ukraine)

DIGITAL PLATFORMS AS A MECHANISM FOR ENSURING THE ECONOMIC SECURITY OF ENTERPRISES IN THE CONTEXT OF CORPORATE GOVERNANCE

36 – 68

KYRYLENKO O.M. Doctor of Economic Sciences, Professor, Dean of the Faculty of Finance and Economics, National Academy of Statistics, Accounting and Audit, Kyiv (Ukraine), **BORYSIUK A.V.** PhD Student, Specialty D3 "Management", National University "Kyiv Aviation Institute", Kyiv (Ukraine)

THE READINESS OF HUMAN CAPITAL FOR DIGITAL AND GREEN TRANSFORMATION IN CONDITIONS OF INTERNATIONAL INSTABILITY

69 –79

HRYHORAK M.Yu. Doctor of Economics, Associate Professor, Professor of the Department of International Business and Logistics, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute." (Ukraine)	
Novosolova D.V. Master's degree student, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute." (Ukraine)	
ORGANIZATIONAL RESILIENCE OF LOGISTICS SYSTEMS IN A CONFLICT ENVIRONMENT: GAME THEORETICAL AND ADAPTIVE APPROACH	80 –95
KLYMENKO V.V. PhD (Economics), Associate Professor, Associate Professor of Transport Technologies and Systems Department, National University "Kyiv Aviation Institute" (Ukraine), DOKIIENKO L.M. PhD (Economics), Associate Professor, Associate Professor of Transport Technologies and Systems Department, National University "Kyiv Aviation Institute" (Ukraine), NOVALSKA N.I. PhD (Economics), Associate Professor, Associate Professor of Transport Technologies and Systems Department, National University "Kyiv Aviation Institute" (Ukraine), SOKOLOVA O. Ye. PhD (Economics), Associate Professor, Associate Professor of Transport Technologies and Systems Department, National University "Kyiv Aviation Institute" (Ukraine)	
HARMONIZATION OF CUSTOMS PROCEDURS IN THE INTERACTION OF TRANSPORT MODES AS A FACTOR FOR ENHANCING THE EFFICIENCY OF MULTIMODAL LOGISTICS CHAINS	96 –106
NESTERENKO S. S. Doctor of Economic Sciences, Professor, Professor of the Department of management and administration, Director of the Institute of Economics and Management, HEI "Open International University of Human Development "Ukraine", DUBAS R. H. Doctor of Economic Sciences, Professor, Head of the Department of management and administration, Institute of Economics and Management, HEI "Open International University of Human Development "Ukraine"	
MODERN THREATS TO THE ECONOMIC SECURITY OF ENTERPRISES AND WAYS OF THEIR NEUTRALIZATION	107–116
ANTONOVA A.O. PhD (in Economics), Associate Professor, Professor Transport Technologies and Systems Department of National University "Kyiv Aviation Institute" (Ukraine)	
ON POST-PANDEMIC SHORT-TERM FORECASTING OF QUARTERLY AIR PASSENGER TRAFFIC AT POLISH AIRPORTS	117 –124

DOI: <https://doi.org/10.46783/smart-scm/2026-37-2>

UDC 355.41:658.7:005.334
JEL Classification: H56, D81, L14, M11.

Received: 2026-04-27
Accepted: 2026-06-05
Published: 2026-06-30

Marchuk V.Ye. Doctor of Technical Sciences, Professor, Professor of the Department of International Business and Logistics, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute." (Ukraine)

ORCID – 0000-0003-0140-5416
Researcher ID S-6514-2018
Scopus author id: – 57212323045
E-Mail: v.marchuk.kpi@gmail.com

Zelinska M.V. Master's degree seeker of the Department of International Business and Logistics, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute» (Ukraine)

ORCID – 0009-0004-6614-1620
Researcher ID
Scopus author id: –
E-Mail: m.zelinska09@gmail.com

Rezanko O.V. Master's degree seeker of the Department of International Business and Logistics, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute» (Ukraine)

ORCID – 0009-0005-7220-8913
Researcher ID
Scopus author id: –
E-Mail: olyarezanko@gmail.com

IMPROVING CONTRACT PERFORMANCE IN THE DEFENSE PROCUREMENT SYSTEM BASED ON A RISK-ORIENTED APPROACH

Volodymyr Marchuk, Marharyta Zelinska, Olha Rezanko. «*Improving contract performance in the defense procurement system based on a risk-oriented approach*». The article examines the theoretical and applied foundations of forming a risk-oriented approach to ensuring contract performance within the defense procurement system under conditions of a wartime economy and high uncertainty. A comprehensive analysis of contemporary risk assessment models, including FMEA, its modifications, risk indicator systems, and security assessment models, was conducted, allowing the identification of their advantages and limitations in the context of defense logistics application. It was established that existing approaches insufficiently account for time criticality, risk controllability, detection complexity, and strategic significance, thereby reducing the effectiveness of contract management.



The necessity of improving risk assessment methods is substantiated, and an integrated model is proposed based on the extension of the classical approach through the introduction of additional coefficients reflecting the specific characteristics of the defense procurement system. A conceptual risk-oriented model for ensuring contract performance was developed, incorporating interconnected blocks of risk identification, assessment, and managerial decision-making, thereby providing a systematic and adaptive approach to risk management throughout all stages of the contract lifecycle.

The practical significance of the obtained results lies in the possibility of improving the validity of managerial decisions, increasing the effectiveness of contract performance assurance instruments, reducing the probability of contract non-performance, and enhancing the resilience of the defense procurement system to destabilizing factors.

Keywords: risk-oriented approach, defense procurement, risk management, contract performance, FMEA, risk assessment, military logistics, strategic significance, time criticality, managerial decision-making

Володимир Марчук, Маргарита Зелінська, Ольга Резанко. «Підвищення ефективності виконання контрактів у системі оборонних закупівель на засадах ризик-орієнтованого підходу». У статті досліджено теоретичні та прикладні засади формування ризик-орієнтованого підходу до забезпечення виконання контрактів у системі оборонних закупівель в умовах воєнної економіки та високої невизначеності. Здійснено комплексний аналіз сучасних моделей оцінювання ризиків, зокрема FMEA, її модифікацій, систем ризик-індикаторів та моделей оцінки захищеності, що дозволило виявити їх переваги та обмеження щодо застосування у сфері оборонної логістики. Встановлено, що існуючі підходи недостатньо враховують часову критичність, керованість ризиків, складність їх виявлення та стратегічну значущість, що знижує ефективність управління контрактами.

Обґрунтовано необхідність удосконалення методів оцінювання ризиків та запропоновано інтегровану модель, яка базується на розширенні класичного підходу шляхом введення додаткових коефіцієнтів, що відображають специфіку функціонування системи оборонних закупівель. Розроблено концептуальну ризик-орієнтовану модель забезпечення виконання контрактів, яка включає взаємопов'язані блоки ідентифікації, оцінювання та прийняття управлінських рішень і забезпечує системний та адаптивний підхід до управління ризиками на всіх етапах контрактного циклу.

Практичне значення отриманих результатів полягає у можливості підвищення обґрунтованості управлінських рішень, ефективності застосування інструментів забезпечення виконання контрактів, зниження ймовірності їх невиконання та підвищення стійкості системи оборонних закупівель до впливу дестабілізуючих факторів

Ключові слова: ризик-орієнтований підхід, оборонні закупівлі, управління ризиками, виконання контрактів, FMEA, оцінювання ризиків, воєнна логістика, стратегічна значущість, часова критичність, управлінські рішення

Introduction. Under the current conditions of the functioning of Ukraine's defense procurement system, characterized by a high level of uncertainty, increasing volumes of financing, and the critical importance of timely provision of the security and defense sector needs, the issue of

ensuring proper contract performance has become particularly relevant. Delays in deliveries, non-compliance of products with established requirements, and the financial instability of suppliers create significant risks to the effective functioning of the defense-industrial complex. Traditional approaches to

contract performance assurance, which are primarily based on the application of standard financial and legal instruments (bank guarantees, penalties, and security deposits), do not always take into account the specific risks inherent in defense procurement and are often applied without proper consideration of their level of criticality. This reduces the effectiveness of contract management and limits the possibilities for preventive influence on potential threats.

In this regard, the implementation of a risk-oriented approach becomes particularly important, as it provides for the systematic identification, assessment, and ranking of contract performance risks followed by a substantiated selection of instruments for their minimization. Such an approach makes it possible to increase the adaptability of the defense procurement system, ensure more efficient use of resources, and improve the reliability of contractual obligations fulfillment.

Literature Review and Previous Research. Contemporary approaches to risk management in procurement, particularly in defense procurement, are formed through an interdisciplinary combination of engineering reliability analysis methods, economic modeling, and institutional control mechanisms. Considerable attention in the scientific literature has been devoted to the development of tools for risk identification, assessment, and prioritization; however, the issue of their adaptation to the specific features of defense procurement, characterized by high uncertainty, time criticality, and strategic significance, remains insufficiently explored.

In particular, study [1] examines the current state of legal regulation of risk management in the field of defense product quality assurance and summarizes NATO experience, emphasizing the necessity of integrating standardized risk management procedures into national defense procurement systems. At the same time, paper [2] highlights the significant role of

corruption risks as one of the key factors affecting the efficiency and transparency of defense procurement processes and substantiates the need to improve mechanisms for their identification and mitigation.

Alongside this, considerable attention in scientific research has been devoted to the development of risk assessment models used for risk identification and prioritization. Traditionally, risk assessment in defense procurement contract performance is defined through the integration of probability and impact: $(R = P \times I)$ [3] where risk is determined as the product of probability and impact [3]. Such an approach provides a basic quantitative assessment of risk and enables its ranking according to significance for managerial decision-making. However, it has limited analytical potential because it does not account for the complexity of risk detection, controllability, and time criticality, which are crucial characteristics in the context of defense procurement.

To overcome the limitations of basic approaches based on the integration of probability and impact, scientific literature has developed more detailed assessment models that take into account additional risk characteristics and improve the accuracy of analysis. One of the most widely used risk analysis methods is Failure Mode and Effects Analysis (FMEA) [4, 5], which is based on calculating the Risk Priority Number (RPN):

$$RPN = O \times S \times D, \quad (1)$$

where:

O – probability of occurrence;

S – severity of consequences;

D – probability of detection.

This approach historically emerged in the aerospace and defense industries and was used to predict failures in complex technical systems, thereby enabling early identification of critical disruptions.

In applied research and process management practice, this model is often interpreted through a more practice-oriented



understanding of its components, according to which the Risk Priority Number is defined as the product of severity, frequency of occurrence, and the complexity of risk detection and control. Such an interpretation does not alter the essence of the classical FMEA model but expands the meaning of the Detection parameter by incorporating characteristics related to detection complexity and risk controllability, thereby bringing the model closer to modern risk management approaches [6].

The advantages of the FMEA model lie in its ability to systematize risks according to the structural elements of the system, determine priorities for corrective actions, and ensure compliance with quality standards. In particular, applied studies emphasize the effectiveness of FMEA in improving system reliability and process quality management [4].

At the same time, scientific research notes that FMEA has several methodological limitations, including a high dependence on expert judgments and the subjectivity of determining the parameters O, S, and D [4]. In the context of defense procurement, these limitations are amplified by additional factors such as the lack of consideration of risk controllability, the neglect of time criticality, and insufficient differentiation of threat detection levels. As a result, the basic FMEA model may underestimate the strategic consequences of risks, especially in the conditions of military logistics and dynamic supply chains.

To overcome the limitations of the classical model, scientific studies have proposed a number of modifications, particularly for logistics and procurement, involving the introduction of weighting coefficients that reflect the context of application [7–9]:

$$RPN_{mod} = O \times S \times D \times W, \quad (2)$$

where W is a weighting coefficient reflecting industry-specific characteristics or the context of risk.

Such approaches make it possible to improve the accuracy of risk assessment in non-manufacturing sectors, particularly in procurement, and to account for the characteristics of specific stages of the supply chain.

The advantages of modified models include flexibility in adapting to industry specifics, the possibility of ranking risks according to a hierarchy of importance, and the expansion of the analytical capabilities of the basic model. However, their main drawbacks are associated with the subjectivity of determining weighting coefficients, the absence of standardized approaches to their calculation, insufficient consideration of the strategic significance of risks, and the neglect of time sensitivity, which is critically important for defense contracts. Moreover, empirical results of such models are predominantly limited to manufacturing systems and are not fully adapted to high-risk procurement processes [7–9].

Another area of research is associated with the use of risk-indicator models in procurement systems applied for automated monitoring of procurement procedures. Within such approaches, risks are ranked according to predefined weighting coefficients, while the integral indicator is formed on the basis of the sum of indicator values with subsequent comparison against threshold values [10–12].

The advantages of this approach include the possibility of automated analysis of large data arrays, effectiveness in detecting procedural and corruption-related risks, and practical applicability within digital public procurement systems. In particular, the application of such indicators in electronic procurement systems makes it possible to identify a significant share of risky procedures and increase procurement transparency. However, the limitations of risk-indicator models lie in their static nature, focus

primarily on procedural and corruption-related risks, lack of consideration of time criticality, and neglect of the strategic significance of contracts. This reduces their effectiveness in the dynamic environment of defense procurement, where risks are complex and multidimensional [11].

In the field of security and defense, security assessment models are used in which risk is considered as a function of the totality of potential threats and their characteristics:

$$R = f(\omega, T), \quad (3)$$

where:

ω – number of threats;

T – parameters or characteristics of threats.

Scientific research in the field of information security and military systems additionally introduces a security coefficient reflecting the ability of the system to counter threats and minimize their impact [13–15]. In particular, relevant methodologies for assessing the security of information systems and military equipment define risk while taking into account not only the characteristics of threats but also the effectiveness of protective mechanisms [13]. Similar approaches are widely used in information security and cybersecurity systems, where risk assessment is integrated with threat analysis and evaluation of mitigation mechanisms [14, 16].

The advantages of such models include orientation toward complex threats, consideration of the specifics of the security environment, and the possibility of assessing the level of system protection. At the same time, their disadvantages manifest themselves in insufficient detailing of risk parameters, lack of consideration of risk controllability, neglect of time criticality, and limited applicability for analyzing contractual relations in procurement.

The conducted analysis of scientific approaches to risk assessment allows concluding that existing models, including FMEA, its modifications, risk-indicator

systems, and security assessment models, form an important methodological basis for risk identification and prioritization. However, their application in the field of defense procurement remains limited due to insufficient adaptation to conditions of high uncertainty, environmental dynamism, contract deadline criticality, and the strategic significance of outcomes.

In particular, the traditional FMEA model based on calculating the indicator $RPN=O \times S \times D$, is widely applied in the defense industry for failure prediction and ensuring the reliability of complex technical systems. However, its basic parameters do not fully reflect the specifics of contractual relations in defense procurement, where risks are complex and multi-level in nature.

Attempts to adapt this approach, particularly through the introduction of contextual weights ($RPN_{mod} = O \times S \times D \times W$), as well as through the use of risk-indicator systems, are aimed at increasing the relevance of risk assessment in procurement processes. Nevertheless, these approaches retain significant limitations associated with insufficient consideration of specific factors characteristic of defense logistics.

The generalization of the analysis results makes it possible to identify the key shortcomings of existing models, including:

- neglect of the time sensitivity of risks;
- limited consideration of their controllability;
- absence of integration of strategic impact factors;
- high subjectivity in parameter assessment under conditions of limited information.

In the context of defense procurement, these limitations become critically important because risks directly affect not only economic outcomes but also the level of national defense capability and security. This determines the necessity of improving existing risk assessment approaches while taking into account the specifics of military logistics and modern management standards,

particularly those applied in the practices of NATO member states.

Given the above, the need to develop an improved risk assessment model that would ensure a more comprehensive consideration of the operational conditions of the defense procurement system becomes increasingly relevant. Such a model should go beyond the traditional analysis of risk occurrence probability and impact scale by supplementing them with a number of critically important parameters.

In particular, under modern conditions of military logistics, accounting for risk controllability becomes fundamentally important, as it reflects the ability of the system to respond promptly to threats and minimize their consequences. Equally important is consideration of the complexity of risk detection, since under conditions of limited access to information, timely threat identification becomes significantly more difficult.

Furthermore, in the field of defense procurement, the strategic significance of risks becomes especially important, as it is determined by their impact on national defense capability and the functioning of critical systems. Ignoring this aspect may lead to underestimation of risks with indirect but critical consequences.

A separate role is played by time criticality, which characterizes the limited time available for responding to risk events. In the context of defense contracts, delays in fulfilling obligations may have not only economic but also security-related consequences, which significantly increases the requirements for the accuracy of risk assessment and prioritization.

Thus, existing approaches to risk assessment do not provide the required level of comprehensiveness and adaptability necessary for effective contract management in the field of defense procurement. This substantiates the expediency of developing an integrated risk assessment model that would take these parameters into account

and improve the validity of managerial decision-making. The proposed model and its methodological support will be presented in the subsequent sections of the study.

Purpose and Objectives of the Study.

The purpose of the study is to develop and scientifically substantiate an integrated risk-oriented approach to ensuring contract performance within the defense procurement system based on the improvement of risk assessment and prioritization methods, taking into account risk controllability, detection complexity, strategic significance, and time criticality.

To achieve the stated purpose, the following objectives were defined in the study:

1. To analyze existing scientific approaches to risk assessment (FMEA, its modifications, risk-indicator systems, and security assessment models) and determine their advantages and limitations in the field of defense procurement.
2. To identify the specific characteristics of risks within the defense procurement system, taking into account high uncertainty, environmental dynamism, limited resources, and the strategic nature of contracts.
3. To substantiate the necessity of improving existing risk assessment approaches by expanding the set of assessment parameters.
4. To develop an integrated risk assessment model based on the combination of basic parameters (probability and impact) with additional coefficients (controllability, detection, strategic significance, and time criticality).
5. To formulate a conceptual risk-oriented model for ensuring contract performance that integrates the processes of risk identification, assessment, and management within a unified approach.
6. To develop methodological approaches for determining the model parameters and coefficients based on expert evaluation and data analysis.



7. To conduct an approbation of the proposed approach using the example of a hypothetical contract in order to assess its practical applicability.

8. To evaluate the effectiveness of the proposed model in terms of improving the validity of managerial decision-making, the reliability of contract performance, and the resilience of the defense procurement system.

Research Results. Considering the identified limitations of existing risk assessment approaches and the necessity of their adaptation to the specific characteristics of defense procurement, this study proposes an integrated risk-oriented model for ensuring contract performance.

The proposed model (Fig. 1) is based on the principles of risk management, systems approach, and adaptive management, and is aimed at improving the reliability of contract performance in the field of defense procurement through the integration of procedures for risk identification, assessment, monitoring, and mitigation at all stages of the contract lifecycle. The model takes into account the specific features of the defense sector, including a high level of uncertainty, the strategic significance of contracts, time constraints, and increased requirements for quality and security.

The model consists of three interconnected blocks:

- Risk identification.
- Risk assessment.
- Managerial decision-making.

Risks in defense procurement should be interpreted as a function of the influence of external and internal environmental factors on the processes of planning, concluding, and executing contracts in the field of defense procurement.

$$R = f(E_{ext}, E_{int}), \quad (4)$$

where: E_{ext} – external (exogenous) environmental factors;

E_{int} – internal (endogenous) environmental factors.

The external environment forms the exogenous conditions for the functioning of the procurement system and includes political, economic, legal, and technological factors characterized by a high level of uncertainty and a low degree of controllability (Table 1). At the same time, the internal environment encompasses organizational, managerial, financial, and operational aspects of the activities of procurement entities and determines their ability to identify, assess, and mitigate risks. Such an approach makes it possible to systematically structure the sources of risks and improve the effectiveness of risk management throughout all stages of the contract lifecycle.

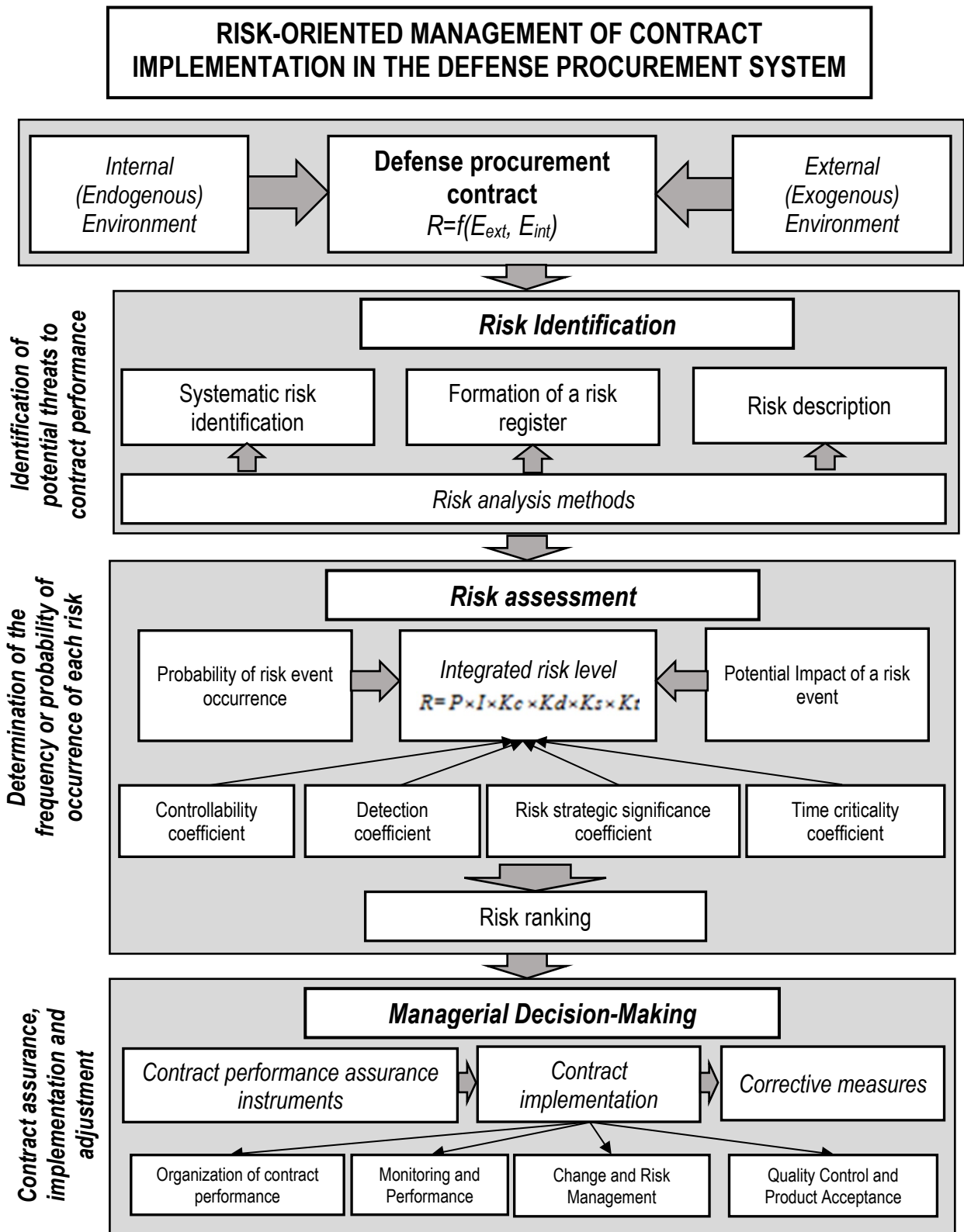


Figure 1 – Risk-Oriented Model for Ensuring Contract Performance

The first block of the model, "Risk Identification," is the initial and critically important stage of risk-oriented management, which involves the systematic

identification, description, and classification of potential events or conditions capable of negatively affecting the achievement of the system's operational objectives or the



implementation of a specific contract. In the context of defense procurement, this process becomes particularly significant due to the increased level of uncertainty, the strategic

nature of the products, the long duration of contract cycles, and the presence of security-related constraints.

Table 1 – Representation of Defense Procurement Risks Through the Environmental Perspective

Environment	Group of Factors	Source of Risk	Example of a Risk Event
External	<i>Political</i>	Geopolitical instability, changes in the state's foreign policy course, introduction of international sanctions, restrictions on military-technical cooperation	Disruption of an international contract due to sanctions restrictions or termination of interstate agreements
	<i>Legal</i>	Frequent changes in the regulatory and legal framework governing defense procurement, inconsistency between national and international legislation, existence of legal gaps	Recognition of a contract as invalid or its revision due to changes in legislation or regulatory requirements
	<i>Economic</i>	Macroeconomic instability, inflationary processes, exchange rate fluctuations, restrictions in budget financing	Increase in contract cost, growth of expenses related to contract performance, necessity to revise the budget
	<i>Technological</i>	Import dependence on critical components, limited access to advanced technologies, technological barriers, and export control restrictions	Absence of critical components, production delays due to the inability to supply high-tech elements
Internal	<i>Managerial</i>	Insufficient quality of strategic and operational planning, errors in needs assessment, ineffective managerial decisions	Unrealistic contract deadlines, exceeding resource constraints
	<i>Organizational</i>	Imperfections in organizational structure, low level of coordination between departments, absence of clearly regulated procedures	Disruptions in interaction between executors, duplication of functions, delays in decision approval
	<i>Financial</i>	Insufficient financial support, ineffective management of budget funds, cash flow gaps	Suspension of contract performance due to lack of financing or untimely payments
	<i>Contractual</i>	Imperfect contract terms, unclear definition of the rights and obligations of the parties, absence of liability mechanisms	Non-performance or improper performance of obligations by the parties, emergence of disputes and claims
	<i>Operational</i>	Disruptions in production processes, resource shortages, breakdowns in logistics chains, technical failures	Delay in product delivery, failure to meet work schedules, deterioration in product quality

In the process of risk identification, it is advisable to use a combination of qualitative and quantitative analysis methods, including expert assessments, historical data analysis, scenario modeling methods, SWOT analysis, PEST analysis, and process decomposition. Particular importance is attached to

stakeholder involvement, which makes it possible to consider different perspectives and improve the completeness of risk identification.

The result of the identification stage is the formation of a risk register containing a description of each risk, the source of its



occurrence, potential consequences, and an initial classification according to defined criteria (probability, impact, area of occurrence, etc.). In the defense procurement system, the typical groups of risks include:

- risks of non-performance or delayed performance of contracts;
- financial risks (changes in resource costs, currency fluctuations);
- technological risks (non-compliance with technical specifications);
- logistics risks (supply disruptions);
- risks related to information security and counterfeit products.

Thus, risk identification serves as the foundation for the subsequent stages of risk management and ensures the validity of managerial decision-making in the field of defense procurement. Its quality directly determines the effectiveness of the entire risk management system and the level of resilience of contractual activities to destabilizing factors.

The second block of the proposed model, "Risk Assessment," constitutes a key stage of risk-oriented contract performance management in the field of defense

procurement. Its purpose is to determine the significance level of identified risks based on the integration of the probability of their occurrence and the magnitude of their potential impact on contract outcomes. The basic approach involves the use of a multiplicative model of the following form: $R=P \times I$, which corresponds to generally accepted principles of risk management [17, 20].

At the same time, the specific characteristics of defense procurement (high uncertainty, deadline criticality, limited access to resources and technologies) necessitate the improvement of this model through the introduction of additional parameters that allow a more accurate reflection of the contract's operational context. This approach is consistent with the methodology of Failure Mode and Effects Analysis (FMEA), where the risk level is determined not only by probability and consequences but also by the ability to detect the risk [18].

Taking this into account, the improved risk assessment model can be represented as follows:

$$R=P \times I \times K_c \times K_d \times K_s \times K_t, \quad (5)$$

where:

- K_c – controllability coefficient;
- K_d – detection coefficient;
- K_s – risk strategic significance coefficient;
- K_t – time criticality coefficient.

The controllability coefficient K_c reflects the ability of management entities to influence a risk through its prevention or mitigation of consequences. Under conditions of high controllability, the value of the coefficient decreases, indicating a reduction in the integrated risk level. Conversely, for poorly controlled risks, the value of K_c increases, strengthening their weight within the overall assessment structure.

The detection coefficient K_d characterizes the possibility of timely identification of a risk before its realization. Its introduction represents an adaptation of FMEA approaches to the field of defense procurement and makes it possible to account for the latent nature of certain risks, particularly those related to technological or contractual aspects [18].

The strategic significance coefficient K_s reflects the impact of a risk on the



achievement of strategic objectives, particularly the maintenance of national defense capability. Its application is appropriate in cases where the consequences of a risk extend beyond a single contract and possess a systemic character.

A special role in the proposed model is played by the time criticality coefficient K_t , which takes into account the dependence of risk consequences on delays in response or contract execution. The introduction of this parameter corresponds to project risk management approaches, where the time factor is considered one of the key drivers of uncertainty [20]. The value of K_t should be determined on a scale from 0.9 to 2.0 depending on the level of deadline criticality: from situations where delays have insignificant impact to situations where disruptions in the contract schedule directly affect national defense capability.

The determination of correction coefficient values is carried out on the basis of expert evaluation, group decision-making methods (in particular, the Delphi method), and analysis of statistical data related to the implementation of similar contracts. Such an approach corresponds to the recommendations of international risk management standards, which provide for the adaptation of assessment tools to the specifics of the subject area [17].

Therefore, the proposed modification of the model makes it possible to improve the accuracy and relevance of risk assessment in the field of defense procurement, ensuring more substantiated prioritization of managerial decisions and enhancing the reliability of contract performance.

The third block, "Managerial Decision-Making," is the central element of the risk-oriented model for ensuring contract performance in the defense procurement system, ensuring the transformation of the results of risk identification, assessment, and prioritization into specific managerial actions. Its functioning is based on the principles of systemicity, adaptability, proportionality, and

validity of decisions. From a scientific perspective, this block may be interpreted as an integrated multi-level management subsystem combining instrumental, procedural, and analytical components aimed at minimizing the negative impact of risks on contract performance.

The selection of assurance instruments is a logical continuation of the risk assessment stage and involves the formation of an optimal set of financial, organizational-managerial, legal, and technological response mechanisms. This process should be considered as a multicriteria optimization problem within which the following are taken into account:

- risk level (probability and impact);
- specifics of the contract subject matter;
- lifecycle stage;
- characteristics of the counterparty;
- institutional and regulatory constraints.

The key principle is proportionality, according to which the complexity and intensity of assurance instruments increase together with the growth of the risk level. This ensures rational allocation of resources and avoidance of excessive regulatory burden.

Contract implementation represents the operational phase within which managerial decisions are materialized into specific results. It encompasses a set of interconnected organizational, production, logistics, and financial processes. In the context of the risk-oriented approach, contract implementation is characterized by high dynamism, dependence on external factors, and the necessity for continuous adaptation of managerial decisions.

The key elements include:

- organization of contract performance (management structure, allocation of responsibilities);
- planning and resource provision;
- change management;
- operational-level risk management;
- ensuring communication between the parties;



- quality control and acceptance of results;
- monitoring and control.

Monitoring and control perform the function of informational and analytical support for management and form the basis for informed decision-making. Monitoring is considered as a continuous process of data collection and analysis, whereas control is regarded as a procedure for assessing the compliance of actual results with planned parameters.

The effectiveness of this stage is determined by the ability of the system to ensure a balance between compliance with contractual conditions and flexibility in responding to environmental changes.

Corrective measures constitute the final yet cyclical stage, ensuring the adaptation of the management system to changing conditions. From the perspective of management theory, this process is an element of a closed-loop management cycle that ensures the alignment of the actual system state with its target parameters.

The prerequisites for corrective actions include deviations from planned indicators, changes in risk levels, emergence of new risks, changes in the external environment, and insufficient effectiveness of applied measures. The main directions of adjustment involve revision of risk assessments, modification of response instruments, adjustment of contract parameters, optimization of organizational processes, and updating of risk management plans.

The cyclical nature of this stage ensures continuous improvement of the management system and enhances its resilience to risks.

Thus, the managerial decision-making block acts as the core of the risk-oriented model for ensuring contract performance, within which an integrated approach to risk management is implemented. Its functioning ensures not only minimization of the probability of risk occurrence but also reduction of their consequences, which

ultimately increases the efficiency, reliability, and resilience of the defense procurement system.

Analysis and Discussion of Results

The obtained research results demonstrate the expediency of transitioning from fragmented approaches to risk assessment toward an integrated risk-oriented model adapted to the specific characteristics of defense procurement. Unlike traditional methods, particularly FMEA and its modifications, the proposed approach provides a comprehensive consideration of both classical risk parameters (probability and impact) and additional characteristics that are critically important under conditions of military logistics.

The key advantage of the developed model lies in its systemic nature, manifested in the integration of three interconnected blocks – identification, assessment, and managerial decision-making – within a unified management cycle. Such a structure ensures the continuity of the risk management process and the possibility of оперативного responding to changes in the external and internal environment.

Particular importance is attached to the improved risk assessment model, which, unlike classical approaches, takes into account controllability, detection complexity, strategic significance, and time criticality of risks. The inclusion of these coefficients makes it possible to increase the accuracy of risk prioritization and ensure a more substantiated selection of management instruments. In particular, consideration of time criticality enables an adequate assessment of risks associated with delays in contract performance, which is critically important for the defense sector. At the same time, the strategic significance parameter makes it possible to account for the systemic impact of risks on national defense capability, extending beyond the boundaries of a single contract.

The proposed approach also demonstrates a higher level of adaptability



compared to existing models, as it provides the possibility of adjusting assessment parameters depending on contract implementation conditions, counterparty characteristics, and changes in the external environment. This is consistent with modern principles of risk management and the requirements for managing complex systems under conditions of uncertainty.

At the same time, the research results also indicate certain limitations of the proposed approach. In particular, the determination of the values of additional coefficients (controllability, strategic significance, and time criticality) is largely based on expert evaluation, which preserves an element of subjectivity. This necessitates further development of methodological support, particularly the formalization of assessment scales and the use of analytical and digital tools to improve the objectivity of calculations.

In addition, the effectiveness of the model largely depends on the level of informational support and digitalization of management processes, which remains a significant challenge for the defense procurement system. In this context, a promising direction involves the integration of the proposed model with digital procurement management platforms and the use of data analytics to automate risk assessment processes.

Conclusions. As a result of the conducted research, the theoretical and methodological foundations of a risk-oriented approach to ensuring contract performance within the defense procurement system were developed. It was established

that existing risk assessment models, particularly FMEA, its modifications, risk-indicator systems, and security assessment models, have limited applicability in the field of defense procurement due to insufficient consideration of time criticality, controllability, and the strategic significance of risks.

The necessity of improving risk assessment approaches through the expansion of the classical model with additional parameters was substantiated, allowing a more adequate reflection of the specifics of military logistics and contractual relations in the defense sector.

An integrated risk-oriented model for ensuring contract performance was developed, combining the stages of identification, assessment, and managerial decision-making within a unified management cycle. The proposed risk assessment model, based on the use of controllability, detection, strategic significance, and time criticality coefficients, ensures increased accuracy of risk prioritization and greater validity of managerial decisions. It was demonstrated that the implementation of a risk-oriented approach will contribute to improving the efficiency, reliability, and resilience of the defense procurement system, reducing the probability of contract disruption, and minimizing their negative consequences.

Prospects for further research include the development of formalized methods for determining the model parameters, its approbation using real defense contract cases, as well as integration with digital procurement management systems.

References

1. Naumenko, M., Plynokos, D., Ivzhenko, I., & Kalinichenko, O. (2024). Risk management in the field of defense product quality assurance: state of legal regulation and NATO experience. *Testing and Certification*, 4(6), 30–37. <https://doi.org/10.37701/ts.06.2024.04>



2. Naumenko, M., Plynokos, D., Ivzhenko, I., & Kalinichenko, O. (2024). Risk management in the field of defense product quality assurance: state of legal regulation and NATO experience. *Testing and Certification*, 4(6), 30–37. <https://doi.org/10.37701/ts.06.2024.04>
3. Hres, O. (2021). Corruption risks in the implementation of defense procurement. *Information and Law*, 1(36), 128–133. [https://doi.org/10.37750/2616-6798.2021.1\(36\).238193](https://doi.org/10.37750/2616-6798.2021.1(36).238193)
4. Project Management Institute (2021). A Guide to the Project Management Body of Knowledge (PMBOK® Guide) (7th ed.). *Newtown Square, PA*: PMI.
5. Brian W. Schuller, Alyson Burns, Elizabeth A. Ceilley et al. (2017). Failure mode and effects analysis: a community practice perspective. *Journal of Applied Clinical Medical Physics*, 18(6), 258–267. <https://doi.org/10.1002/acm2.12190>
6. Dastjerdi, H. A., Khorasani, E., Yarmohammadian, M. H., & Ahmadzade, M. S. (2017). Evaluating the application of failure mode and effects analysis technique in hospital wards: a systematic review. *Journal of Injury and Violence Research*, 9(1), 51–60. <https://doi.org/10.5249/jivr.v9i1.794>
7. Risk identification tool and process quality assessment. (2026). Retrieved April 21, 2026, from <https://smart-eam.com/ua/news/instrument-vyjavlenija-riskov-ocenka-kachestva-processov/>
8. Hu-Chen Liu, Liu Liu, & Ning Liu (2013). Risk evaluation approaches in failure mode and effects analysis: A literature review. *Expert Systems with Applications*, 40(2), 828–838. <https://doi.org/10.1016/j.eswa.2012.08.010>
9. Ali Cevat Kutlu & Mehmet Ekmekçioğlu (2012). Fuzzy failure modes and effects analysis by using fuzzy TOPSIS-based fuzzy AHP. *Expert Systems with Applications*, 39(1), 61–67. <https://doi.org/10.1016/j.eswa.2011.06.044>
10. Ying-Ming Wang, Kwai-Sang Chin, Gary K. K. Poon, & Jian-Bo Yang (2009). Risk evaluation in failure mode and effects analysis using fuzzy weighted geometric mean. *Expert Systems with Applications*, 36(2), 1195–1207. <https://doi.org/10.1016/j.eswa.2007.11.028>
11. State Audit Service of Ukraine. (2026). Methodology for determining automatic risk indicators during public procurement monitoring. Retrieved April 21, 2026, from https://dasu.gov.ua/attachments/715be5a3-2202-486c-907a-7920dec062d5_%D0%BD%D0%B0%D0%BA%D0%B0%D0%B7_71%20%D0%B2%D1%96%D0%B4%2017.03.2026.pdf
12. Infobox Prozorro. (2026). Procurement monitoring: risk indicators and the most common violations identified by the State Audit Service of Ukraine. Retrieved April 21, 2026, from <https://infobox.prozorro.org/articles/monitoring-zakupivel-rizik-indikator-ta-naychastishi-porushennya-viyavleni-dasu>
13. Prozorro Risk Indicators (2026). Retrieved April 21, 2026. from <https://risks.prozorro.gov.ua/>
14. Krainov, V., Malanchuk, M., & Hrozovskyi, R. (2020). Methodology for assessing the effectiveness of an integrated information protection system. *Information and Analytical Activities in the Field of Security and Defense*, 1(37), 103–106. <https://doi.org/10.33099/2311-7249/2020-37-1-103-106>
15. Sulimovska, M. (2024). Improved methodology for assessing the security of restricted-access information. *Information and Analytical Activities in the Field of Security and Defense*, 3(51), 120–132. <https://doi.org/10.33099/2311-7249/2024-51-3-120-132>
16. Rybydailo, A., Fedoriienko, V., Kulchytskyi, O., & Oboznenko, Ye. (2022). Approaches to assessing the security of the information infrastructure of the Ministry of Defense of Ukraine. *Collection of Scientific Works of the Center for Military and Strategic Studies of the*



-
- Ivan Cherniakhovskyi National Defense University of Ukraine*, 1(74), 69–77.
<https://doi.org/10.33099/2304-2745/2022-1-74/69-77>
17. Toliupa, S., Parkhomenko, I., & Shtanenko, S. (2021). Model of an intrusion counteraction system in an information system. *Information and Communication Technologies, Electronic Engineering*, 1(1), 39–50. Retrieved April 21, 2026, from <https://science.lpnu.ua/sites/default/files/journal-paper/2021/dec/25671/stattya4stolyupaiparhomenkoshtanenko.pdf>
 18. International Organization for Standardization. (2018). ISO 31000:2018 Risk management – *Guidelines*. Geneva: ISO.
 19. State Standard of Ukraine. (2019). *DSTU IEC 60812:2019 Failure mode and effects analysis (FMEA and FMECA)*. Kyiv: UkrNDNC.
 20. NATO Standardization Office. (2013). AAP-48: NATO System Life Cycle Processes. *Brussels: NATO*.
 21. Project Management Institute. (2021). A Guide to the Project Management Body of Knowledge (PMBOK® Guide) (7th ed.). *Newtown Square, PA: PMI*.

