Economics, Entrepreneurship, Management Vol. 12, No. 2. 2025

UDC 351:004:005.8 + 328.185 + 35.08
DOI: 10.56318/eem2025.02.074

ISSN 2312-3435
e-ISSN 2413-7634

Halyna Melnyk
PhD in Economics, Associate Professor
Yuriy Fedkovych Chernivtsi National University
58012, 2 Kotsiubynskoho Str., Chernivtsi, Ukraine
https://orcid.org/0000-0001-5386-5903

Viktor Rovinsky*
PhD in Technical Sciences, Associate Professor
Vasyl Stefanyk Carpathian National University
76018, 57 Shevchenka Str., Ivano-Frankivsk, Ukraine
https://orcid.org/0000-0001-8454-8580

Vasyl Melnyk
PhD in Physics and Mathematics
Yuriy Fedkovych Chernivtsi National University
58012, 2 Kotsiubynskoho Str., Chernivtsi, Ukraine
https://orcid.org/0009-0005-2880-6449

Organisational problems as the root cause of systemic failures of IT projects

Abstract. The relevance of the study was determined by the chronic failures of government information technology projects, which are accompanied by budget overruns and missed deadlines, representing a global problem. These failures are rarely purely technical; they are symptoms of deep organisational pathologies. Traditional frameworks for project management and business analysis focus on rational processes, often ignoring the irrational forces that deform them. The purpose of this study was to analyse and systematise the impact of four key organisational pathologies – dysfunctional formalisation, rent-seeking behaviour, favouritism, and autocratic management style – on the fundamental processes of project management and business analysis in government IT projects. The primary research method was thematic analysis using the 6-phase model. The empirical base consisted of M = 18 publicly available documents from 2019-2025, selected according to the principles of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA). Sources included audit reports from supreme audit institutions official reports from law enforcement agencies, which underwent triangulation. Data analysis revealed three main mechanisms of deformation in project management and business analysis processes: (1) formalisation and ritualisation, which transforms risk management and metrics into mere formality; (2) inversion and sabotage (through rent-seeking behaviour), which turns project management and business analysis into tools for falsifying procurements and embezzling funds; (3) the dominant autocratic management style, which replaces systematic processes with the leader's will. A conceptual matrix has been formed that details this impact. The work offers a set of criteria for early identification of pathologies and practical recommendations for countermeasures (in particular, using open data and strengthening rational standardisation). The practical significance of the proposed matrix lies in its function as a diagnostic tool for project managers, business analysts, and auditors

Keywords: project management; business analysis; organisational pathology; procurement corruption; bureaucracy

Article's History:
Received: 18.08.2025
Revised: 01.12.2025
Accepted: 23.12.2025
Published: 29.12.2025

Suggested Citation:
Melnyk, H., Rovinsky, V., & Melnyk, V. (2025). Organisational problems as the root cause of systemic failures of IT projects. *Economics, Entrepreneurship, Management*, 12(2), 74-85. doi: 10.56318/eem2025.02.074.

*Corresponding author

INTRODUCTION

The persistent failure of government information technology (IT) projects has become a significant concern for public administration worldwide. These failures have been characterised by chronic budget overruns, catastrophic schedule delays, and the inability to achieve declared goals. Such outcomes have rarely resulted from technical shortcomings alone; instead, they have reflected entrenched organisational dysfunctions that undermine the effectiveness of project management (PM) and business analysis (BA). The urgency of addressing these organisational factors has been underscored by recent public audits and academic studies, which highlighted the critical need for reform in public sector IT governance.

Recent researches have increasingly focused on the organisational roots of IT project failures. J. Schmidt (2023) analysed risk mitigation mechanisms, finding that bureaucratic inertia and lack of stakeholder engagement are recurrent barriers. In the Ukrainian context, the Accounting Chamber (2024) documented similar patterns, noting the absence of standardised methodologies and the prevalence of formalism in project oversight. I.J. Borges do Nascimento *et al.* (2023) and M. Bader *et al.* (2024) further explored the impact of process rigidity and insufficient user involvement on project outcomes. Previous researches, conducted by A.K. Albarzanji & A.Y. Alsabawy (2021) and K. Balka *et al.* (2022) have identified multiple causes for the failure of IT and e-government projects, including technical, organisational, and user-related factors. These findings have been also echoed in the work of M. Chen *et al.* (2025), who identified integration challenges and unrealistic expectations as key contributors to project failure.

Ukrainian scholars have also contributed to this discourse: the Ministry of Digital Transformation's audits (The Accounting Chamber, 2024) and regulatory reforms (Resolution of the Cabinet of Ministers of Ukraine No. 893, 2025) have provided empirical evidence of both progress and persistent challenges in the national context. As noted by M. Halushchak *et al.* (2023), Ukraine has made considerable progress in digital government services, climbing significantly in global e-government rankings; however, challenges in citizen engagement and participation remain. Effective risk management in the public sector was recognised as a key component in preventing project failure, particularly where management dysfunction and lack of transparency are present (Butenko, 2024). Despite these advances, the literature has revealed a gap in the systematic analysis of how specific organisational pathologies – such as dysfunctional formalisation, rent-seeking behaviour, favouritism, and autocratic management – distort the core processes of project management and business analysis in government IT projects. In the context of IT project implementation in Ukraine, researchers emphasised the need for comprehensive project governance, supported by modern tools like Enterprise Resource Planning (ERP) systems, Artificial intelligence (AI) integration, and proactive scenario planning (Koval *et al.*, 2023).

Building on the analysis of these studies, this research aimed to systematise the impact of key organisational pathologies on project management and business analysis within government IT projects. The study addressed the following questions: which organisational pathologies are most frequently identified in recent audits and investigations and how do these pathologies specifically deform or neutralise standard project management and business analysis processes. By integrating models of IT project failure, organisational pathology theory, and critiques of standard frameworks, this work sought to develop a diagnostic matrix for early identification and mitigation of these dysfunctions.

MATERIALS AND METHODS

The study employed a qualitative design; the primary method was thematic analysis based on the approach of N. Carter *et al.* (2014) and V. Braun & V. Clarke (2021). The empirical base consisted exclusively of publicly available documents with several inclusion criteria. By type, it incorporated official reports prepared by supreme audit institutions, including Audit Scotland (2017), the Accounting Chamber (2024), UK National Audit Office (2024; 2025), as well as documents issued by the US Government Accountability Office (2025). It also covered official reports from verified media reporters, such as I. Sitnikova (2025). The temporal scope of the study covered publications released between 2019 and 2025. Thematically, the selected documents addressed the management of government IT projects, digital transformation processes, IT-related public procurement, and instances of project failure in these areas. Document selection (based on PRISMA principles) included the following steps:

- Identification: N = 45 documents were identified through searches in databases.
- Screening: N = 29 documents were excluded (duplicates, lack of focus on PM/BA).
- Eligibility: N = 16 documents were assessed for full-text eligibility.
- Inclusion: M = 18 documents were selected for detailed coding.

Coding and triangulation were carried out by two independent analysts using the 6-phase model. In the first phase (coding), the text of the documents was analysed to identify semantic descriptions of problems (e.g., semantic code: "lack of quality assessment methodologies", "failure to report minimally required metrics", "delays in plan approval" etc.). In the second phase (theme generation), these codes were grouped into latent interpretive themes; for example, the code "lack of metrics" was grouped into the theme "Metrics Sabotage", which, in turn, fell under the pathology "Dysfunctional Formalisation". To mitigate the bias inherent in non-peer-reviewed media sources, their factual data (company names, amounts, dates) were cross-verified and triangulated with official data from audit bodies and court registries, where possible. Unverified data were

excluded from consideration. Table 1 presents the sources and cases selected for detailed coding, including document type, date, originating organisation, and the main coded themes identified in each.

Table 1. Examples of data sources

Source/Case	Document type	Date	Organisation	Coded themes
GAO "Legacy Systems"	Audit Report	2025	GAO (USA)	"Dysfunctional formalisation, PM paralysis"
GAO "DoD IT Projects"	Audit Report	2025	GAO (USA)	"Dysfunctional formalisation, lack of metrics"
NAO "Digital Transformation"	Audit Report	2023-2025	NAO (UK)	"Integration failure, "Red" rating"
"Derzhspetszviazok"	NABU Report / Media Report	2025	NABU (Ukraine)	"Rent-seeking, cronyism, PM/BA inversion"
Mintsyfra Reform	Regulatory Act Analysis	2025	CMU (Ukraine)	Rational standardisation (as a solution)
Accounting Chamber Audit (Accounting Chamber of Ukraine, 2024)	Audit Report	2024	Accounting Chamber (Ukraine)	"Dysfunctional formalisation, lack of methodologies"

Note: GAO – Government Accountability Office; NAO – National Audit Office; NABU – National Anti-Corruption Bureau of Ukraine; CMU – Cabinet of Ministers of Ukraine

Source: developed by the authors based on UK National Audit Office (2024), Resolution of the Cabinet of Ministers of Ukraine No. 893 (2025), US Government Accountability Office (2025), I. Sitnikova (2025)

This table summarises the empirical material underpinning the thematic analysis and the development of the diagnostic matrix. This approach relied on triangulation techniques to ensure validity and consistency of identified themes, as recommended in prior methodological studies. The emphasis on methodological transparency and structured use of heterogeneous data sources is consistent with approaches applied in contemporary Ukrainian economic research (Khudoliy, 2025). By structuring heterogeneous sources across institutional contexts, the table enhances transparency in data selection and supports the traceability of analytical decisions linking empirical evidence to higher-level thematic interpretations.

RESULTS AND DISCUSSION

Systemic governance failures in public sector IT projects

The results of the analysis revealed that systemic issues in public sector IT projects – including inadequate use of metrics, poor requirements elicitation, weak stakeholder engagement, and dysfunctional formalisation – are widespread across multiple national contexts (US, UK, and Ukraine). These patterns were consistently identified in the reviewed audit reports and triangulated sources. Despite incremental improvements in audit and oversight capabilities, the absence of robust methodologies and objective performance indicators has enabled project failures to remain concealed, allowing misallocation of resources and reduced accountability. These findings highlight common vulnerabilities in project governance and reinforce the need for rational standardisation, strong project management structures, and early stakeholder alignment to mitigate the effects of organisational dysfunction.

The experience of the US federal government is illustrative due to the transparency of its audit bodies. The US government invests over $100 billion annually in IT. However, these investments have often failed or have experienced cost overruns and schedule delays. As a result of this systemic issue, federal IT investment management has been on the GAO's "High Risk List" since 2015. As of January 2025, 463 of more than 1,800 GAO recommendations issued since 2010 to improve IT management remained unimplemented. A GAO analysis of the Department of Defense's (DoD) IT programs revealed systemic failures; planned expenditures were projected to reach $10.9 billion by fiscal year 2025 (US Government Accountability Office, 2025).

The 2025 report on 24 large IT programs demonstrated classic symptoms of project management failure; specifically, weak and inconsistent performance tracking was noted in metrics management. Out of 19 programs with operational investments, five failed to provide reports on minimally required performance metrics, such as customer satisfaction or financial outcomes. Only one program met all performance goals, while another met none. The data presented in the Table 2 summarise key challenges identified in major public sector IT programmes, as evidenced by audit reports from the US Government Accountability Office (2025) and the UK National Audit Office (2025).

Table 2. Summary of key challenges in major public sector IT programmes

Factor	Observed issue	Implications	Best practice reference
Budget and schedule management	Half of analysed programmes experienced cost overruns ($6.1M to $815.5M). Seven programmes had schedule delays up to 4 years.	Significant financial inefficiency; extended delivery timelines.	Scope management, robust planning, and cost control.
Stakeholder engagement	Insufficient involvement of end-users and clients in project decisions.	Requirements not fully understood, leading to misaligned solutions and poor user satisfaction.	Proactive stakeholder engagement, effective requirements elicitation (PMBOK®, BABOK®).
Risk/cybersecurity management	Two of four largest DoD IT programmes lacked approved cybersecurity strategies; none had plans for "zero trust" architecture by 2027.	Increased vulnerability and non-compliance with mandates.	Comprehensive risk response planning, cybersecurity best practices (PMI risk response principle).
Complexity of digital transformation	Digital projects in the UK faced integration challenges with legacy systems and unrealistic expectations.	Projects rated "critical condition"; common need for "resetting" projects.	Integration with legacy environments, realistic goal setting, strong project sponsorship (NAO reports).

Note: PMI – Project Management Institute; BABOK – Business Analysis Body of Knowledge
Source: developed by the authors based on US Government Accountability Office (2025), UK National Audit Office (2025), PMBOK Guide (n.d.)

Under the category of budget and schedule management, the table draws from findings that half of the analysed US federal IT programmes experienced significant cost overruns, with additional expenditure ranging from $6.1 million to $815.5 million. Furthermore, seven programmes faced delays, with timelines extended by up to 4 years. These issues reflect substantial financial inefficiency and prolonged delivery of outcomes, underscoring the importance of robust scope management and planning, as recommended by project management best practices (PMBOK Guide, n.d.).

For stakeholder engagement, the table highlights the insufficient involvement of end-users and clients in project decision-making processes, a pattern that is consistent with prior findings in the literature (Anthopoulos *et al.*, 2016). This lack of engagement meant that requirements were often defined without a comprehensive understanding of actual business needs, resulting in misaligned solutions. The table references established professional standards and guides, such as the PMBOK® Guide and BABOK®, which emphasise proactive stakeholder engagement and effective requirements elicitation as essential for project success and customer satisfaction.

In the area of risk and cybersecurity management, the Table 2 reflects audit findings that two of the four largest US Department of Defense IT programmes lacked approved cybersecurity strategies, and none had plans to implement the mandated "zero trust" architecture by 2027. These gaps highlight vulnerabilities in risk planning and the need to adhere to recognised principles in cybersecurity and risk response. Finally, the Table 2 incorporates data from the UK National Audit Office, which recorded similar patterns of difficulty in digital transformation projects. Many initiatives within the Government's Major Projects Portfolio were found to be in "critical condition", often due to the complexities of integrating new digital solutions with legacy systems and unrealistic expectations regarding project outcomes. The frequent need to "reset" or revise these programmes is also reflected as a recurring theme in the table.

Audit insights and overcoming dysfunctional formalisation in Ukrainian IT project management

Ukraine's audit bodies, although still developing specialised IT competencies, are already recording the same fundamental problems. An audit by the Accounting Chamber (2024) of the Ministry of Digital Transformation and the "DIIA" enterprise for 2022-2024 revealed significant achievements, including an economic effect of ₴59.7 billion and an anti-corruption effect of ₴6.5 billion. At the same time, the audit pointed to a fundamental problem identical to that identified by the GAO in the US: "the lack of approved methodologies for assessing service quality does not allow for proper monitoring of progress achieved and timely response to challenges".

The recognition of systemic risks in government IT projects has prompted both the State Audit Service of Ukraine and the Accounting Chamber to strengthen their IT audit capabilities. In particular, the State Audit Service has introduced a formal procedure for conducting state financial audits of investment projects (formerly referred to as "IT audits"), as established by Resolution of the Cabinet of Ministers of Ukraine No. 740 (2018). At the same time, the Accounting Chamber (2024) has initiated institutional capacity-building by recruiting specialised staff, including positions such as Head of the IT Processes and Systems Audit Sector, with the aim of developing appropriate audit methodologies.

A comparative analysis of these findings and corresponding evidence from the US Government Accountability Office (2025) reports revealed an identical, recurring symptom: the systemic absence or inadequacy of metrics

for assessing the effectiveness and quality of IT projects. In project management, metrics are the foundation of the "Monitoring and Control" phase. Without objective data, the project manager and stakeholders cannot adequately assess the project's status, its alignment with goals, or end-user satisfaction.

This phenomenon should be viewed as a functionally protective mechanism for the system. In a formalised organisation, where project failure can mean the end of a career, the absence of clear metrics becomes a form of insurance. If no objective, approved data record low user satisfaction or lack of progress, the project cannot be officially declared a failure (UK National Audit Office, 2024). This allows the project to exist in a state of simulated usefulness: it continues to consume budgets, simulate activity, and avoid accountability or radical decisions, such as a reset.

The management pathology of "dysfunctional formalisation" is often mistakenly reduced solely to its negative manifestation – red tape. In reality, formalised management is the fundamental operating system of any large organisation. Its impact is twofold: it can act as a rational tool for organisation or as an irrational brake, leading to the dominance of form over substance. In its positive (Weberian, rational-legal) sense, rational standardisation is a system of rational organisation. If standardisation remains within defined limits, it "will help increase the level of organisational management, promote accuracy, and speed up managerial work". It ensures a clear division of functions, a management hierarchy, and the presence of rules and standards.

However, it is important to distinguish between unnecessary rules and directives that create additional administrative burdens and complicate production processes. Often, such directives and instructions are issued as a formal response to emerging situations, aimed primarily at demonstrating managerial reaction rather than resolving underlying problems, as they are not accompanied by adequate resources for implementation. As a result, staff may become engaged in symbolic or superficial implementation, lacking the capacity to address the problem even at a theoretical level. Furthermore, management personnel organisationally distant from production processes and therefore fail to understand their actual operational requirements. This tendency is particularly evident when managers lack relevant education (e.g., individuals trained in psychology or history overseeing complex IT or robotics projects) and consequently avoid engagement with technical details.

However, even useful regulations inevitably involve certain costs, as organisations need time to adapt to new rules. Problems arise when formalisation exceeds rational limits. This phenomenon, commonly referred to as dysfunctional formalisation (or bureaucratism), reflects a situation in which formal procedures begin to dominate over the actual content of management. As a result, time is wasted, decision-making slows down, and opportunities for informal or corrupt practices may emerge, as managerial activity becomes focused on formal compliance rather than real problem-solving. In such conditions, substantive work is pushed to the background, and organisational effectiveness declines.

A clear example of addressing dysfunctional formalisation – rather than formalisation itself – in favour of rational standardisation is the reform of approaches to developing state IT systems in Ukraine, introduced by Resolution of the Cabinet of Ministers of Ukraine No. 893 (2025). Under the previous system, project initiation required five to seven separate documents, lengthy approval procedures, and compliance with outdated Soviet-era norms. The new resolution replaced the old system: instead of 5-7 documents, only technical requirements and a technical specification are required. It also replaced obsolete standards with international ones, notably ISO and IEEE, introduced more flexible modern information security systems instead of cumbersome comprehensive security frameworks (KSZI), and allowed the use of cloud technologies and open-source solutions. As a result, the expected development time for state IT systems was reduced from months to weeks.

International perspectives:
Lessons from the UK and Ukraine

Analysis shows that the vacuum created by the absence of rational standardisation is extremely dangerous. The absence of standards leads to chaotic requirements generation. Research on formalised management also confirms that insufficient use of standardisation tools leads to "disorganisation" and "reduced responsibility". This kind of organisational analysis benefits from robust qualitative research practices, including attention to intercoder reliability for ensuring consistency in thematic findings (O'Connor & Joffe, 2020). The vacuum is instantly filled either by dysfunctional formalisation or by rent-seeking behaviour, a phenomenon extensively analysed in the context of modern institutional inefficiencies (Krueger, 1974). Dysfunctional formalisation and organisational inertia directly disrupt the core of production processes. They turn tools intended to achieve goals (risk management, quality) into formal, ritualistic practices devoid of real content. Modern PM requires a proactive approach to risk management, for example, through RAID analysis (Risks, Assumptions, Issues, Dependencies), to "predict and prevent" problems. However, in a deeply formalised system, a PM can identify a risk (e.g., "delays in obtaining permits") but cannot "manage" the administrative risk, as they lack the authority.

In an environment dominated by formalism, publicly raising fundamental risks (e.g., "this "legacy" system is vulnerable") can be perceived as disloyalty, forcing the PM to ignore real risks. The interaction between dysfunctional formalisation, organisational inertia, and rent-seeking behaviour creates a self-reinforcing loop that undermines project management and business analysis processes. These dynamics are illustrated in Figure 1, which maps how each pathology contributes to inflated documentation, delays, and distorted procurement mechanisms, ultimately leading to systemic project failure.

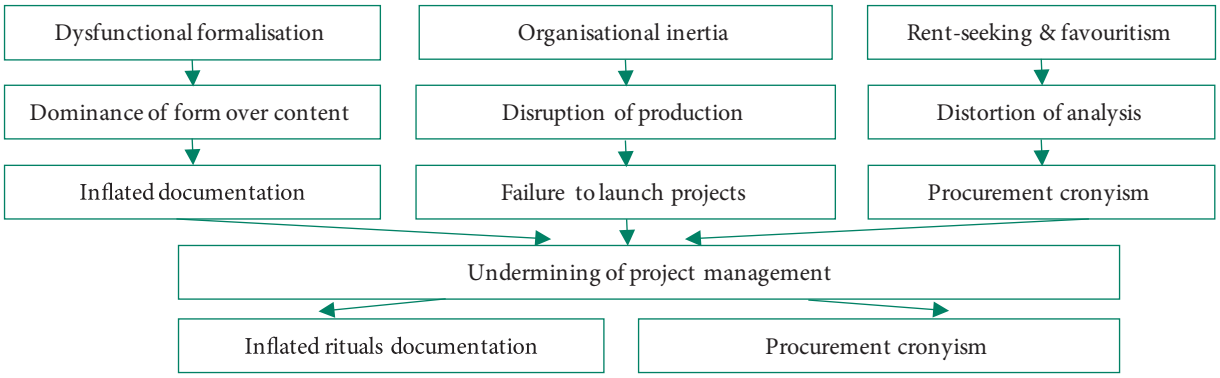

Figure 1. Systemic management pathologies in public sector projects
Source: developed by the authors

The most destructive impact of organisational inertia on PM is demonstrated by GAO reports on the modernisation of legacy IT systems in the US government. According to GAO assessments, six years ago ten legacy systems were identified as the most critical, yet by 2025 seven of them had still not been modernised. These systems were between 23 and 59 years old, relied on outdated programming languages such as COBOL and Assembler, operated on unsupported hardware, and, most critically, contained known cybersecurity vulnerabilities (US Government Accountability Office, 2025).

The failure to modernise these systems is a fundamental failure of project management at the initiation phase, caused by organisational inertia. Such inertia echoes broader structural issues in government IT project management, where outdated processes and risk-averse culture hinder innovation from the start (Yaraghi, 2015). This observation is consistent with long-standing case-based analyses, in which C. Sauer (1993) demonstrated that deep-rooted organisational failures are at the heart of many unsuccessful information systems initiatives. From this perspective, the situation reflects what organisational failure diagnosis models describe as systemic breakdowns occurring at early stages of planning and structural design, as conceptualised by A.M. Goulielmos (2005). Similar conclusions are echoed in consulting evidence, with PricewaterhouseCoopers (2017) identifying weak project foundations and unclear accountability as key root causes of early-stage failure in public sector projects.

Ultimately, GAO pointed directly to the cause: agencies failed to fully document their modernisation plans (US Government Accountability Office, 2025). Without these plans, initiatives have an "increased likelihood of cost overruns, schedule delays, and overall project failure", which aligns with empirical findings on the heavy-tailed, power-law distribution of IT project cost overruns identified by H. Mulder (1994) and later confirmed by B. Flyvbjerg *et al.* (2022). Such outcomes are often rooted in various forms of uncertainty inherent in software development projects, including scope ambiguity, stakeholder misalignment, and shifting requirements (Zhang *et al.*, 2025). This means that the administrative complexity of launching a new modernisation project (obtaining countless approvals) is so high that it is easier for agencies to continue spending hundreds of millions of dollars supporting old, vulnerable systems than to initiate their replacement (US Government Accountability Office, 2025). This represents a typical example of how unfavourable enterprise environmental factors can obstruct decision-making and progress in public sector projects, as discussed by M. Romanelli (2022). Moreover, R. Syed *et al.* (2023) noted that Such systemic stagnation is often intensified in developing countries, where digital transformation efforts face institutional, regulatory, and cultural resistance.

In formalised systems, the tracking of actual performance metrics is frequently undermined. Audit reports by the US Government Accountability Office (2025) and the Accounting Chamber (2024) of Ukraine document systematic deficiencies in performance measurement practices. The PM is forced to report on formal metrics ("10 meetings held") rather than substantive ones ("user satisfaction level"). Similar issues were observed in recent evaluations of digital transformation initiatives, where focus on documentation and procedure overshadowed meaningful performance outcomes (Szedmák *et al.*, 2025). A product is considered "quality" not when it meets user needs, but when it has collected signatures from all responsible parties. This represents the "dominance of form over content", a hallmark of organisational pathology as described in the Sustainability Directory (2025), in which procedures and rituals overshadow actual performance and purpose. In the context of public sector IT projects, M. Lerner (2020) argued that such systemic conditions frequently result in chronic failure when formality overtakes functionality.

In a normal IT project, BA is a process of discovering and validating real business needs. In organisations afflicted by management pathologies, the BA function degrades, becoming either a ritualistic filling out of documents or a tool for rent-seeking sabotage. In a system dominated by dysfunctional formalisation, the business analyst's focus shifts. This dysfunction reflects challenges frequently observed in developing countries, where poor governance

and institutional weaknesses undermine e-government initiatives (Nyansiro *et al*., 2021). The main stakeholder for the BA is not the end-user, but the approval procedure. Requirements are gathered and analysed not so the future product solves a real problem, but so the requirements document (Technical Specification) successfully passes all necessary committees. This leads to the creation of bloated, unrealistic technical specifications. Business analysis transforms into "paperwork". When rent-seeking interest is added to dysfunctional formalisation, a complete inversion of the very essence of business analysis occurs.

The goal changes from finding the best solution to justifying a predetermined (rent-seeking) solution. If organisational inertia leads to the passive failure of projects (paralysis, delays), the synergy of rent-seeking behaviour and favouritism leads to active sabotage. The project becomes a special operation to siphon funds, a pattern often linked to low procurement maturity and systemic vulnerabilities in public sector processes (Hua, 2022), reflecting how high transaction costs and limited administrative capacity can directly lead to procurement failure and project cancellations (Casady *et al*., 2023). Dysfunctional formalisation is a necessary prerequisite for rent-seeking behaviour. As UNODC (n.d.) researchers note, "the presence of regulatory acts and permits grants a certain monopoly power to officials". Officials and managers may intentionally introduce new, complex regulations to be able to demand illicit benefits (bribes) for their passage, a practice documented by A. Vasilev (2013) in analyses of administrative corruption. This mechanism reflects the classical theory of rent-seeking originally articulated by G. Tullock (1967), where regulatory control is leveraged for personal gain rather than public benefit. When rent-seeking opportunities are combined with favouritism, the system becomes closed. In such cases, the appointment of relatives/friends and "insiders" occurs largely regardless of their qualifications. Appointing an unqualified relative or associate to the role of PM is a guarantee of failure. Studies confirm a strong negative correlation between the presence of family ties and the efficiency of large institutions. In procurement, cronyism manifests in the creation of "VIP lanes" for politically connected suppliers, a mechanism that has been empirically linked to favouritism and distortions in auction outcomes (Dastidar & Jain, 2023).

The NABU investigation into the activities of the Derzhspetszviazok (State Service of Special Communications and Information Protection of Ukraine) illustrates the full synergy of all three pathologies. The investigation uncovered a large-scale scheme involving senior officials, resulting in the embezzlement of over ₴90 million during the procurement of unmanned aerial vehicles (UAVs) for the Defence Forces. A department head planned to embezzle part of the ₴30 billion allocated by "supplying drones at inflated prices". Investigation, conducted by I. Sitnikova (2025), revealed that procurement decisions favoured preselected companies linked to the brother of an entrepreneur with close business relations to the official involved. The crime was committed using a formal tender procedure. A clear inversion of key management and analytical processes is observed: the tender mechanism was organised to create an illusion of competition by involving controlled firms, while the business analysis and requirements definition process was subordinated to rent-seeking interests. As a result, specific models were purchased (DJI Mavic 3 and Autel Evo Max 4T), the choice of which, according to analysis, was likely based not on the end-user's operational needs, but on the possibility of suppliers earning super-profits; the purchases were made at prices 70-90% above market rates. Although the project was formally considered "completed", from the perspective of effective resource use, it must be seen as a failure, causing over ₴90 million in losses to the state.

Similar long-term failures of large government IT systems have been well documented. R.N. Charette (2019) showed that such projects often persist despite being technically outdated or poorly aligned with user needs. The autocratic management style, or authoritarian leadership, is considered a separate management pathology. It differs from dysfunctional formalisation and rent-seeking behaviour in that it does not slow or sabotage the project through bureaucracy or selfish interests, but rather forces it, systematically ignoring or destroying established processes of project management and business analysis. In the political dimension, this phenomenon is described as the dominance of the executive branch relying on a police-bureaucratic apparatus and a "cult of the leader"; in the corporate context, autocracy means the concentration of complete control over decision-making in the hands of one person, who disregards the team's input and demands unquestioning obedience.

Historical and modern illustrations of this leadership type (e.g., Jobs, Musk) are cited as examples, yet its effectiveness proves paradoxical: in narrow, specialised tasks or crisis scenarios (especially in defence structures), an autocrat can provide rapid, decisive solutions, minimising delays. However, in the long term and in systems requiring teamwork and stable procedures, this style undermines organisational culture, leads to demoralisation, and increases staff turnover. Recent studies by J. Crusoe *et al*. (2024) describe this phenomenon as "digital transformation decoupling", where managerial inertia and wilful ignorance prevent meaningful structural change. In an autocratic management model, the business analysis process is effectively annihilated: requirements are formulated and imposed as a monologue from the sole leader, mechanisms for gathering and validating requirements with stakeholders are absent, and the role of the business analyst is reduced to that of a "scribe" documenting the leader's vision. Any attempt at validation or critical review of requirements is interpreted as a waste of time or a manifestation of disloyalty, fostering a "culture of fear". As a result, systemic project management (PMBOK, Agile, etc.) loses its efficacy: planning is dictated by the leader's will, the risk management (RAID) process is blocked, and the sole metric of success becomes the leader's subjective approval. Although this style sometimes allows "breaking through" administrative paralysis to achieve a

quick result, it simultaneously destroys rational standardisation and stable PM and BA processes, undermining the organisation's long-term effectiveness.

The analysis of open sources, audit conclusions, and investigations indicates that the four identified organisational pathologies create a toxic and unviable environment for IT projects. First, dysfunctional formalisation breeds inertia and administrative paralysis, focusing PM and BA work on procedures instead of target outcomes, causing delays and an inability to initiate or adapt projects (The Accounting Chamber of Ukraine, 2024; US Government Accountability Office, 2025). Second, rent-seeking behaviour, along with favouritism/cronyism, inverts the purpose of PM and BA processes, turning projects into tools for illicit enrichment. According to investigative reporting by I. Sitnikova (2025), business analysis is used to formulate artificial requirements, and project management to rig tenders in favour of connected suppliers. Finally, an autocratic management style annihilates systemic management practices, replacing them with the leader's will, which fosters a "culture of fear" and makes realistic planning impossible. In sum, these phenomena undermine rational standardisation and long-term effectiveness, as detailed in the synthesis matrix, shown in Table 3. As summarised in Table 3, the identified organisational pathologies manifest through recurring deformation mechanisms that jointly undermine PM and BA functionality, reinforcing the systemic nature of project failure discussed above. On this basis, practical recommendations aimed at increasing the resilience of PM and BA through the systematic application of open data, identification of problem indicators, and introduction of mechanisms to protect project integrity.

Table 3. Matrix of the impact of organisational pathologies on PM and BA

Pathology	Impact on PM	Impact on BA
Dysfunctional formalisation	Paralysis and ritualisation. • Paralysis of decision-making due to endless approval cycles. • Administrative paralysis at initiation (Case: "Legacy Systems". • Sabotage or ignorance of real performance metrics. • Risk management becomes a formality (inability to influence administrative risks).	Ritualisation of the process. • Focus shifts from the user to the approval committee. • Requirements are gathered for "correct" documentation, not to solve a business problem. • "Dominance of form over content".
Rent-seeking behaviour	Inversion and falsification. • PM Goal: Not "within budget", but "spending the budget" with maximum markup (70-90% in Derzhspetszviazok case). • Falsification of procurement processes: "distorted market research", "simulated competition".	Inversion and sabotage. • Inversion of the process: Requirements (choice of drone models) are dictated by corruption margins, not business needs (Derzhspetszviazok case).
Favouritism / cronyism	Degradation of competencies. • Appointment of unqualified PMs (relatives, "associates"). • Creation of "VIP lanes" for "insider" suppliers, ignoring procedures.	Ignorance or incompetence. • Appointment of incompetent individuals to the role of customer (product owner). • BA cannot obtain clear, logical requirements. • Requirements are based on personal connections.
Autocratic management style	Annihilation of processes. • Planning: Replaced by the leader's will; deadlines are unrealistic. • Risk Management: Impossible. Reporting risks = "disloyalty" ("culture of fear"). • Metrics: The only metric is the leader's subjective approval.	Annihilation of the process. • The leader is the sole source of requirements. • Validation of requirements with users is forbidden or ignored. • BA is reduced to the role of "scribe".

Source: developed by the authors based on US Government Accountability Office (2025), I. Sitnikova (2025)

Project management and business analysis specialists must master tools for analysing public data (including the Ukrainian Open Data Toolkit (Resolution of the Cabinet of Ministers of Ukraine No. 893, 2025) and use them for preliminary analysis of similar tenders before formulating requirements and for market price analysis during budgeting (to counter inflation, as in the Derzhspetszviazok case). It is advisable to formalise a set of indicators for typical problems: signs of dysfunctional formalisation (prioritising procedures over results, lengthy approvals, refusal of objective metrics), rent-seeking behaviour and favouritism (illogical requirements in the technical specification, "VIP lanes", involvement of connected suppliers), and autocratic practices (prohibition of direct contact with users, punitive reactions to risk reporting).

Defence strategies should combine several complementary elements. First, they should insist on rational standardisation by implementing international standards such as ISO and IEEE, as well as recognised methodologies including BABOK and PMBOK as a legal shield against corruption (Project Management Institute, 2021). Second, they should emphasise the economic justification of procedures by translating administrative delays into measurable monetary losses. Finally, defence strategies should promote the development of an internal corporate legal environment that supports whistle-blowers and provides secure

channels for reporting risks, as formalised in Ukraine's regulatory framework for state IT projects (Resolution of the Cabinet of Ministers of Ukraine No. 893, 2025). Taken together, these measures form a preventive framework for maintaining PM and BA functionality.

In response to the research questions, three principal deformation mechanisms were identified. The first one (1) is paralysis and ritualisation: formalism manifests as excessive proceduralism that substitutes real action with bureaucratic rituals. This undermines adaptive project planning, impedes stakeholder alignment, and delays project initiation. Such patterns reflect the anti-patterns warned against in PMBOK's principle of "Tailoring" – which emphasises adjusting project practices to context rather than rigidly applying processes.

The second principle (2) is inversion and sabotage: rent-seeking behaviours and cronyism invert the intended logic of project work. Business analysis becomes a tool to justify predetermined vendor preferences (e.g., through artificially inflated or misaligned requirements), while project management is reduced to a mechanism for procurement manipulation. These behaviours violate core BABOK principles such as requirements validation, solution assessment, and stakeholder collaboration.

The third principle (3) is annihilation of controls: under autocratic leadership models, critical decision-making processes become centralised and opaque. Business needs are replaced by executive monologues, while risk management and validation functions are suppressed, often creating a "culture of fear". This contradicts PMBOK's emphasis on "Stewardship" and "Team Empowerment" – which promote shared ownership and open communication as enablers of successful outcomes.

Addressing these organisational pathologies requires more than technical fixes. Based on these findings, it is recommended to embed risk-based thinking throughout project life cycles, ensuring alignment with the PMBOK® principle to "Optimise Risk Responses". Additionally, it is important to institutionalise stakeholder engagement and validation mechanisms, which is consistent with BABOK's requirement lifecycle and engagement standards. Finally, fostering a culture of accountability and transparency remains essential, in line with PMBOK's principles of "Value Delivery" and "Holistic Thinking". These corrective actions are not only grounded in empirical evidence but also reflect global best practices in public project governance.

CONCLUSIONS

This study demonstrated that four recurring organisational pathologies – dysfunctional formalisation, rent-seeking behaviour, favouritism/cronyism, and autocratic management – systematically distort core processes of PM and BA within government IT projects. These dysfunctions were identified through thematic analysis of authoritative public data sources, including audit reports by the GAO, NAO, the Accounting Chamber of Ukraine, and verified investigative media. Collectively, these mechanisms not only sabotage project delivery but also erode the foundations of institutional learning, long-term digital capability, and public trust. The result is a systemic failure of rational standardisation, where formal PM and BA frameworks exist in name only and are used selectively to legitimise dysfunctional practices.

As echoed in broader literature on digital government and project failure, enhancing organisational maturity, enforcing ethical standards, and aligning PM/BA practices with strategic goals are essential for restoring effectiveness in public sector IT initiatives. Ultimately, this research underscores that effective digital transformation depends not solely on technical capacity or funding – but on resolving entrenched organisational dysfunctions that corrupt the very systems designed to deliver.

Looking forward, further research should explore the effectiveness of specific interventions aimed at mitigating organisational pathologies within public sector IT projects. Longitudinal studies could assess how sustained implementation of international standards and risk-based governance frameworks influence project outcomes over time. Additionally, comparative analyses across different governmental contexts would help identify universal and context-specific factors that facilitate or hinder digital transformation. Examining the role of emerging technologies and agile methodologies in overcoming entrenched dysfunctions may also provide valuable insights for future public sector reforms.

ACKNOWLEDGEMENTS

None.

FUNDING

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Albarzanji, A.K., & Alsabawy, A.Y. (2021). Causes of IT project failure: A systematic review. *Tanmiyat Al-Rafidain*, 40(132), 135-168. doi: 10.33899/tanra.2021.170354.

[2] Anthopoulos, L., Reddick, C.G., Giannakidou, I., & Mavridis, N. (2016). Why e-government projects fail? An analysis of the Healthcare.gov website. *Government Information Quarterly*, 33(1), 161-173. doi: 10.1016/j.giq.2015.07.003.

[3] Audit Scotland. (2017). *Principles for a digital future: Lessons learned from public sector ICT projects*. Retrieved from https://audit.scot.

[4] Bader, M., Antony, J., Jayaraman, R., Swarnakar, V., Goonetilleke, R.S., Maalouf, M., Garza-Reyes, J.A., & Linderman, K. (2024). Why do process improvement projects fail in organizations? A review and future research agenda. *International Journal of Lean Six Sigma*, 15(3), 664-690. doi: 10.1108/IJLSS-07-2023-0126.

[5] Balka, K., Heslin, B., & Risse-Tenk, S. (2022). *Unlocking the potential of public-sector IT projects*. Retrieved from https://www.mckinsey.com.
[6] Borges do Nascimento, I.J., Abdulazeem, H., Vasanthan, L.T., Martinez, E.Z., Zucoloto, M.L., Østengaard, L., Azzopardi-Muscat, N., Zapata, T., & Novillo-Ortiz, D. (2023). Barriers and facilitators to utilizing digital health technologies by healthcare professionals. *Npj Digital Medicine*, 6, article number 161. doi: 10.1038/s41746-023-00899-4.
[7] Braun, V., & Clarke, V. (2021). *Thematic analysis: A practical guide*. New York: SAGE Publications Ltd.
[8] Butenko, H.Ya. (2024). Risk management technology in the public sector: Challenges and opportunities. *Economics. Finance. Law*, 9, 9-13. doi: 10.37634/efp.2024.9.2.
[9] Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A.J. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum*, 41(5), 545-547. doi: 10.1188/14.onf.545-547.
[10] Casady, C.B., Petersen, O.H., & Brogaard, L. (2023). Public procurement failure: The role of transaction costs and government capacity in procurement cancellations. *Public Management Review*, 1-28. doi: 10.1080/14719037.2023.2231945.
[11] Charette, R.N. (2019). Three enduring government IT failures: Costly consequences continue for years – [Spectral Lines]. *IEEE Spectrum*, 56(8), 4-4. doi: 10.1109/MSPEC.2019.8784108.
[12] Chen, M., Martins, T.S., Zhang, L., & Dong, H. (2025). Digital transformation in project management: A systematic review and research agenda. *Systems*, 13(8), article number 625. doi: 10.3390/systems13080625.
[13] Crusoe, J., Magnusson, J., & Eklund, J. (2024). Digital transformation decoupling: The impact of willful ignorance on public sector digital transformation. *Government Information Quarterly*, 41(3), article number 101958. doi: 10.1016/j.giq.2024.101958.
[14] Dastidar, K.G., & Jain, S. (2023). Favouritism and corruption in procurement auctions. *Mathematical Social Sciences*, 123, 10-24. doi: 10.1016/j.mathsocsci.2022.12.005.
[15] Flyvbjerg, B., Budzier, A., Lee, J.S., Keil, M., Lunn, D., & Bester, D.W. (2022). The empirical reality of IT project cost overruns: Discovering a power-law distribution. *Journal of Management Information Systems*, 39(3), 607-639. doi: 10.1080/07421222.2022.2096544.
[16] Goulielmos, A.M. (2005). Applying the organizational failure diagnosis model to the study of information systems failure. *Disaster Prevention and Management: An International Journal,* 14(3), 362-377. doi: 10.1108/09653560510605027.
[17] Halushchak, M., Halushchak, O., & Mashliy, H. (2023). Electronic Ukraine in the digital world. *Galician Economic Journal*, 85(6), 174-182. doi: 10.33108/galicianvisnyk_tntu2023.06.174.
[18] Hua, S.Y. (2022). Procurement maturity and IT failures in the public sector. *Transforming Government: People, Process and Policy*, 16(4), 554-566. doi: 10.1108/TG-07-2022-0097.
[19] Khudoliy, L. (2025). Methodology for researching the banking services market in Ukraine. *Economics and Business Management*, 16(1), 92-107. doi: 10.31548/economics/1.2025.92.
[20] Koval, V.V., Mikhno, I.S., & Metil, T.K. (2023). The complex project risk management technologies in IT companies. *Business Inform*, 10, 389-396. doi: 10.32983/2222-4459-2023-10-389-396.
[21] Krueger, A. (1974). The political economy of the renk-seeking society. *American Economic Review*, 64, 291-303.
[22] Lerner, M. (2020). *Government tech projects fail by default. It doesn't have to be this way*. Retrieved from https://www.belfercenter.org.
[23] Mulder, H. (1994). *The chaos report*. Retrieved from https://www.researchgate.net.
[24] Nyansiro, J.B., Mtebe, J.S., & Kissaka, M.M. (2021). E-government information systems (IS) project failure in developing countries: Lessons from the literature. *The African Journal of Information and Communication*, 28, 1-29. doi: 10.23962/10539/32210.
[25] O'Connor, C., & Joffe, H. (2020). Intercoder reliability in qualitative research: Debates and practical guidelines. *International Journal of Qualitative Methods*, 19. doi: 10.1177/160940691989922.
[26] PMBOK Guide. (n.d.). *Underneath the surface*. Retrieved from https://pmbok.guide.
[27] PricewaterhouseCoopers (PwC). (2017). *Are public projects doomed to failure from the start? Transformation assurance*. Retrieved from https://www.pwc.ch.
[28] Project Management Institute. (2021). *The standard for project management and a guide to the project management body of knowledge (7th ed.)*. Newtown Square: Project Management Institute.
[29] Resolution of the Cabinet of Ministers of Ukraine No. 740 "On Approval of the Procedure for Conducting Investment Projects by the State Audit Service, its Interregional Territorial Bodies of State Financial Audit". (2018, September). Retrieved from https://zakon.rada.gov.ua.
[30] Resolution of the Cabinet of Ministers of Ukraine No. 893 "On Amendments to the Mandatory Requirements for the Creation (Modernisation, Modification, Development), Administration and Ensuring the Functioning of an Information System". (2025, July). Retrieved from https://www.kmu.gov.ua.
[31] Romanelli, M. (2022). *Understanding enterprise environmental factors*. Retrieved from https://projecttimes.com.

[32] Sauer, C. (1993). *Why information systems fail: A case study approach*. Oberkirch: Alfred Waller Ltd., Publishers.
[33] Schmidt, J. (2023). Mitigating risk of failure in information technology projects: Causes and mechanisms. *Project Leadership and Society*, 4, article number 100097. doi: 10.1016/j.plas.2023.100097.
[34] Sitnikova, I. (2025). *Case of embezzlement on drones: Preventive measures chosen for two officials of the State Service of Special Communications*. Retrieved from https://hromadske.ua.
[35] Sustainability Directory. (2025). *Organizational pathology*. Retrieved from https://pollution.sustainability-directory.com.
[36] Syed, R., Bandara, W., & Eden, R. (2023). Public sector digital transformation barriers: A developing country experience. *Information Polity*, 28(1), 5-27. doi: 10.3233/IP-220017.
[37] Szedmák, B., Varga, L., & Szabó, R.Z. (2025). Digital transformation of public services: The case of the document management application. *International Journal of Public Administration*, 1-18. doi: 10.1080/01900692.2024.2520522.
[38] The Accounting Chamber. (2024). *Accounting Chamber's annual report for 2023*. Retrieved from https://rp.gov.ua.
[39] Tullock, G. (1967). The welfare costs of tariffs, monopolies, and theft. *Western Economic Journal*, 5(3), 224-232.
[40] UK National Audit Office. (2024). *Lessons learned: Delivering value from government investment in major projects*. Retrieved from https://www.nao.org.uk.
[41] UK National Audit Office. (2025). *Government's approach to technology suppliers: Addressing the challenges*. Retrieved from https://www.nao.org.uk.
[42] UNODC. (n.d.). *Module 4: Public sector corruption*. Retrieved from https://www.unodc.org.
[43] US Government Accountability Office. (2025). *High-risk series: Critical actions needed to urgently address IT acquisition and management challenges*. Retrieved from https://www.gao.gov.
[44] Vasilev, A. (2013). *On the cost of rent-seeking by government bureaucrats in a Real-Business-Cycle framework*. Retrieved from https://www.econstor.eu.
[45] Yaraghi, N. (2015). *Doomed: Challenges and solutions to government IT projects*. Retrieved from https://www.brookings.edu.
[46] Zhang, M., Antwi-Afari, M.F., Wang, C., Sun, W., Mohandes, S.R., & Abdulai, S.F. (2025). Uncertainty in software development projects: A review of causes, types, challenges, and future research directions. *Systems*, 13(8), article number 650. doi: 10.3390/systems13080650.

Галина Мельник

Кандидат економічних наук, доцент
Чернівецький національний університет імені Юрія Федьковича
58012, вул. Коцюбинського, 2, м. Чернівці, Україна
https://orcid.org/0000-0001-5386-5903

Віктор Ровінський

Кандидат технічних наук, доцент
Карпатський національний університет імені Василя Стефаника
76018, вул. Шевченка, 57, м. Івано-Франківськ, Україна
https://orcid.org/0000-0001-8454-8580

Василь Мельник

Кандидат фізико-математичних наук
Чернівецький національний університет імені Юрія Федьковича
58012, вул. Коцюбинського, 2, м. Чернівці, Україна
https://orcid.org/0009-0005-2880-6449

Організаційні проблеми як першопричина системних невдач IT-проектів

Анотація. Актуальність дослідження зумовлена хронічними провалами державних проєктів у сфері інформаційних технологій, які супроводжуються перевищенням бюджетів і зривами термінів виконання, що становить глобальну проблему. Ці провали рідко мають суто технічний характер; вони є симптомами глибоких організаційних патологій. Традиційні підходи до управління проєктами та бізнес-аналізу зосереджені на раціональних процесах, часто ігноруючи ірраціональні сили, що їх деформують. Метою цього дослідження були аналіз і систематизація впливу чотирьох ключових організаційних патологій – дисфункційної формалізації, рентного поведінкового типу, фаворитизму та автократичного стилю управління – на основні процеси проєктного менеджменту та бізнес-аналізу у державних IT-проєктах. Основним методом дослідження був тематичний аналіз за шестистадійною моделлю. Емпіричну базу склали M = 18 відкритих документів за 2019-2025 рр., відібраних відповідно до принципів бажаних звітних елементів для систематичних оглядів та метааналізів (PRISMA). Джерела включали аудиторські звіти вищих органів аудиту та офіційні звіти правоохоронних органів, що пройшли тріангуляцію. Аналіз даних виявив три основні механізми деформації процесів в управлінні проектами та бізнес-аналізу: (1) формалізація та ритуалізація, що перетворює управління ризиками та метриками на формальність; (2) інверсія та саботаж (через рентну поведінку), що перетворює проєктний менеджмент та бізнес-аналіз на інструменти фальсифікації закупівель та розтрати коштів; (3) домінуючий автократичний стиль, що замінює системні процеси волею лідера. Сформовано концептуальну матрицю, що деталізує цей вплив. У роботі запропоновано набір критеріїв для раннього виявлення патологій та практичні рекомендації щодо протидії (зокрема, шляхом використання відкритих даних та посилення раціональної стандартизації). Практична значущість запропонованої матриці полягає в її функції діагностичного інструмента для менеджерів проєктів, бізнес-аналітиків та аудиторів

Ключові слова: проєктний менеджмент; бізнес-аналіз; організаційна патологія; корупція у закупівлях; бюрократія