
Advancing information system testing: challenges, methods, and practical recommendations

Nona Otkhзорia

Faculty of Informatics and control systems, Georgian Technical University, Tbilisi, Georgia
ORCID 0000-0002-5837-5345

Lily Petriashvili

Faculty of Informatics and control systems, Georgian Technical University, Tbilisi, Georgia
ORCID 0000-0003-3593-4877

Taliko Zhvania

Faculty of Informatics and control systems, Georgian Technical University, Tbilisi, Georgia
ORCID 0000-0003-1238-5211

Ana Imerlishvili

Faculty of Informatics and control systems, Georgian Technical University, Tbilisi, Georgia
ORCID 0009-0001-6736-3514

To cite this article:

Otkhзорia Nona, Petriashvili Lily, Zhvania Taliko, Imerlishvili Ana. Advancing information system testing: challenges, methods, and practical recommendations. International Science Journal of Engineering & Agriculture. Vol. 4, No. 2, 2025, pp. 203-214. doi: 10.46299/j.isjea.20250402.13.

Received: 01 28, 2025; **Accepted:** 03 05, 2025; **Published:** 04 01, 2025

Abstract: The rapid advancement of technology has made information systems indispensable in various industries, increasing their complexity and the demand for effective testing methodologies. This article investigates the challenges and solutions associated with testing information systems, focusing on quality assurance processes. A structured survey involving 82 professionals, predominantly from the Georgian market, was conducted to assess current practices, identify gaps, and propose improvements. The survey revealed significant challenges in areas such as test planning, environment stability, and the adoption of automated testing tools. Key findings highlight that although 75% of organizations have experienced testers, only 41.5% have well-defined test cases, underscoring the need for better planning. Additionally, while 59.8% of respondents reported stable test environments, a considerable portion still faces instability, affecting testing efficiency. Automated testing, adopted by 31% of respondents, is viewed as highly effective, yet many organizations struggle with its implementation due to resource constraints. Performance and security testing practices also showed variability in frequency and effectiveness, with Apache JMeter being the dominant tool for stress testing. To address these challenges, this article recommends several strategies, including regular training for testing staff, improving test planning with clearer requirements, and investing in stable test environments. Automated testing adoption should be encouraged through targeted training and better tool utilization, while resource optimization can alleviate constraints. Risk-based prioritization of testing tasks is suggested to maximize efficiency under limited resources. These recommendations aim to enhance testing practices, ensuring higher reliability and performance of information systems. The study concludes that further research is

needed to explore emerging testing technologies and methodologies, ensuring continuous improvement in quality assurance processes in the evolving landscape of information systems.

Keywords: information systems, quality assurance, testing methods, Regression testing, automated testing, performance testing, security testing, testing challenges.

1. Introduction

Information systems have become the backbone of the modern world in many industries, supporting critical operations and enhancing business efficiency. From banking and healthcare to manufacturing and logistics, organizations rely on complex information systems to manage large volumes of data, streamline processes, and improve decision-making. As technology continues to advance at an unprecedented pace, these systems are constantly evolving, becoming more sophisticated and interconnected. This rapid development not only enhances functionality but also introduces new challenges related to system reliability, security, and performance.

In this context, quality control becomes indispensable in the field of information systems, ensuring that these complex systems function as intended and meet end-user expectations. Effective testing methods are essential to maintain high-quality standards, minimize defects, and mitigate potential risks. However, testing information systems is often a challenging task due to the complexity of modern software architectures and the dynamic technological landscape. Even when the system itself is relatively simple in terms of content and technical implementation, testing can be complicated by various factors.

One of the primary challenges is the intricate dependencies between system components, which can lead to unexpected interactions and issues during integration testing. Additionally, emerging technologies such as cloud computing, artificial intelligence, and the Internet of Things (IoT) introduce unique testing requirements and complexities. These advanced technologies necessitate rigorous testing methodologies to ensure security, scalability, and interoperability. Furthermore, the growing need to comply with strict security and performance standards adds another layer of complexity to the testing process.

Another critical aspect is the increasing frequency of software updates and patches, which make continuous testing and integration crucial for maintaining system integrity. The integration of agile development practices has introduced rapid development cycles, necessitating more frequent and adaptive testing strategies to keep pace with these fast-moving changes. This ongoing evolution of information systems demands testing approaches that are not only thorough but also flexible enough to adapt to changing requirements and new technological landscapes.

To address these challenges, organizations must adopt comprehensive and adaptive testing strategies. By doing so, they can enhance the efficiency and effectiveness of their quality assurance processes, ensuring that information systems are reliable, secure, and capable of meeting evolving business needs. In this paper, we will explore the key challenges in information system testing, discuss the most effective methods for overcoming them, and offer practical recommendations for improving testing practices to meet the demands of modern business environments.

2. Object and subject of research

The object of this study is information systems used in various industries, which are becoming increasingly complex with technological advances. The subject of the study is the problems, methodologies and best practices of testing these information systems, emphasizing quality assurance processes to improve their reliability and performance.

3. Target of research

The aim of this study is to conduct a comprehensive comparative analysis of complex methods for testing information systems in the context of various challenges. It seeks to evaluate the effectiveness, scalability, and value of these methods, as well as to develop recommendations and ideas for organizations aiming to optimize their testing processes.

The research will focus largely on performance testing, automated testing, security testing, usability testing, and accessibility testing. A thorough analysis of the strengths and weaknesses of each method in different contexts will be provided.

Based on this comparative analysis, the study will explore the intricacies and nuances of each testing methodology. It aims to unpack the technical characteristics of performance testing, which evaluates the speed, responsiveness, and stability of a system—crucial factors in today's fast-paced digital world. Stress testing, a technique used to push a system to its limits in order to assess its performance under extreme conditions, will also be discussed.

The study will also delve into the importance and challenges of security testing in an era where data breaches, cyber threats, and data losses are significant risks. Furthermore, the growing role of automated testing in modern quality assurance departments will be explored. As businesses strive to deliver high-quality software faster and more efficiently, automation has become an essential tool, but it is not without its challenges. This study will examine the difficulties of creating and managing automated tests, as well as possible solutions.

Additionally, the study will examine usability and accessibility testing in detail. With an increasing emphasis on user experience and inclusivity in software design, these testing methodologies have become indispensable. However, they also present unique challenges, which will be highlighted and discussed.

Finally, the study will address common constraints that arise during testing, such as limited resources and tight deadlines, and examine how these constraints impact the success of testing efforts. Overall, this study aims to provide a comprehensive understanding of the challenges associated with monitoring different testing methodologies in real-world environments.

4. Literature analysis

There are several complex methods of information system testing that serve different purposes. These methods include Functional Testing, Non-Functional Testing, Specialized Testing, Automated Testing, Risk-Based Testing, End-to-End Testing, Data Migration Testing, and Operational Testing (FIG.1). Since organizations face numerous challenges in monitoring the quality of their information systems, selecting the most appropriate testing methods is essential to ensure quality, reliability, and performance while addressing the unique challenges of each situation (Otkhozoria, Petriashvili, Kudukhashvili, & Nino, 2023; Otkhozoria, Zhvania, Petriashvili, & Lortkipanidze, 2024).



Figure 1. Information Systems Testing Methods.

Establishing a dedicated Quality Assurance (QA) department reflects a company's commitment to product quality and customer satisfaction. The QA department plays a critical role in ensuring that products, services, and software meet specified requirements before market release. During the initial stages of QA implementation, documentation is a priority. This includes defining processes, establishing protocols, and creating test cases to maintain product quality. These documents serve as a roadmap for the QA team, guiding their work, outlining tasks, setting timelines, and detailing methodologies. This structured approach facilitates the identification of anomalies and defects in the product (Rose, 2023; Satoshi, Yasuharu, Nishi, & Suzuki, 2020).

The literature review underscores the increasing importance of information systems across industries, necessitating robust quality assurance mechanisms. Previous studies identify multiple testing methods—functional, non-functional, automated, and risk-based testing—each addressing specific challenges. However, gaps remain in test planning, environment stability, and automated testing tool implementation. This research builds upon existing studies by analyzing these challenges within the Georgian market, contributing new insights into the effectiveness of various testing methodologies.

Types of Software Testing and Their Importance

Software testing plays a crucial role in ensuring the reliability, performance, and security of information systems. As organizations increasingly rely on digital infrastructure, testing methodologies have evolved to address emerging technological challenges. This literature review explores different types of software testing, their significance, and ongoing research efforts aimed at improving their effectiveness.

Performance Testing and Its Significance

Performance testing evaluates how a system performs under specific load conditions, assessing key attributes such as speed, responsiveness, stability, reliability, scalability, and resource utilization. This type of testing is critical for identifying system bottlenecks and establishing benchmarks for future testing efforts. A crucial subset of performance testing is **stress testing**, which examines system durability, availability, and error handling under extreme load conditions.

The importance of performance testing has become increasingly evident in the digital era, where businesses depend on seamless digital services to maintain their reputation and operational efficiency. The case of the U.S. government's Healthcare.gov website in 2013 serves as a prime example of performance testing failures. Researchers (Anthopoulos, Reddick, & Giannakidou, 2016) attribute the system's initial failure to poor planning, insufficient resources, and inadequate load testing. A key issue was the discrepancy between the test environment and real-world conditions, leading to misinterpreted results and system instability.

Research dating back to 1998 (Vokolos & Weyuker, 1998) already recognized challenges in performance testing, emphasizing the disproportionate focus on functional testing over performance testing. Their findings demonstrated that investing in performance testing early in the development process allows organizations to detect and resolve critical software defects before they escalate into major system failures.

A recent 2023 study by Nokia (Stradowski & Madeyski, 2023) examines performance testing challenges at the **gNB system level in 5G networks**, revealing critical gaps in user scenario testing, competency enhancement, and industry-wide implementation difficulties. These findings highlight the persistent gap between industry needs and academic research solutions, underscoring the necessity for targeted research in this area. To address these issues, Nokia has invested in **sophisticated test labs** equipped with hundreds of base stations and aerial cameras to ensure accurate performance testing of 5G networks.

Stress Testing in the Banking Sector

Stress testing is particularly valuable in the banking industry, where it helps estimate capital requirements under adverse conditions and assesses system performance during peak loads. A study by Sahin, Haan, and Neretina (2020) highlights the role of stress testing in identifying system vulnerabilities and ensuring long-term stability. The researchers emphasize that stress test results are most valuable in unstable environments, suggesting that improved transparency in the stress testing process can enhance reliability and decision-making capabilities in financial institutions.

Automated Testing: Benefits and Challenges

Automated testing involves the use of specialized tools to execute test cases, reducing manual effort and improving overall testing efficiency. This approach is particularly beneficial for large-scale systems with complex test scenarios. However, automated testing also presents challenges, including high initial setup costs and the need for continuous maintenance.

A study by Masuda, Nishi, and Suzuki (2020) examines testing difficulties in highly complex systems, emphasizing the necessity of software-test architecture and pre-production testing environments. Their research suggests that organizations that invest in **pre-production testing** can achieve substantial cost savings and improved system performance by identifying and mitigating issues before deployment.

A comprehensive 2013 survey (Garousi & Zhi, 2013) on software testing practices across industries revealed an increasing adoption of **Agile methodologies and test automation**. However, manual testing remains prevalent due to the complexity of automation and the difficulties in maintaining test scripts. A 2019 study (Wang et al., 2020) found that organizations implementing Agile and DevOps methodologies experience **more cost-effective test automation results**. A more recent 2021 study (Nass, Alégroth, & Feldt, 2021) explores GUI-based test automation challenges, identifying common issues such as **synchronization problems** and **regression testing difficulties** caused by frequent UI changes.

Security Testing: Addressing Cyber Threats

Security testing assesses system vulnerabilities and ensures that sensitive data is protected against cyber threats. A key area of concern in web security is **Cross-Site Scripting (XSS) vulnerabilities**. Research by Salas and Martins (2014) identifies major challenges in detecting XSS vulnerabilities, emphasizing the complexity of **Web Services Security (WS-Security)** mechanisms and the need for

advanced testing tools. Their study highlights the importance of collaboration between development and security teams to enhance security awareness and mitigate emerging cyber risks.

Accessibility Testing: Ensuring Inclusive Software Design

Accessibility testing ensures that software is usable for individuals with disabilities. Compliance with accessibility regulations, such as **Section 508 of the U.S. Rehabilitation Act** and the **Web Accessibility Directive in the European Union**, is critical for organizations aiming to create inclusive digital environments. Zhong et al. (2021) recommend **integrating accessibility testing throughout the software development lifecycle**, utilizing assistive technologies, and training development teams on usability best practices.

Usability Testing: Enhancing User Experience

Usability testing evaluates software from a user-centric perspective, assessing ease of use, navigation, and overall user satisfaction. Historically, Microsoft's extensive usability testing in the late 1990s led to the introduction of the **Ribbon interface** in its Office Suite, significantly improving user efficiency and accessibility. Despite its benefits, usability testing presents challenges, such as **subjective data interpretation and the diverse needs of users**.

A study by Rose (2023) suggests that organizations can improve usability testing by defining **clear test scenarios**, incorporating **user story-driven testing**, and leveraging **expert evaluations**. These strategies can help ensure that software meets user expectations and enhances the overall digital experience.

Conclusion and Future Research Directions

This literature review highlights the critical role of software testing in ensuring the reliability, security, and usability of modern information systems. While various methodologies exist, challenges such as **test planning, automation difficulties, security vulnerabilities, and usability concerns** remain prominent.

Addressing these issues requires ongoing research, industry collaboration, and investment in robust testing environments. Future research should explore **the integration of artificial intelligence (AI) in automated testing**, the development of **adaptive testing frameworks for dynamic software systems**, and **enhanced security testing techniques** to mitigate evolving cyber threats. Additionally, greater emphasis should be placed on **real-world testing environments**, as demonstrated by Nokia's investment in sophisticated test labs for 5G networks.

By advancing research in these areas, organizations can improve the effectiveness of software testing methodologies, ensuring that digital systems remain **resilient, secure, and user-friendly** in an increasingly complex technological landscape.

In conclusion, the literature review highlights the significance of information system testing across various domains. While numerous methodologies exist, challenges such as test planning, automation, security vulnerabilities, and usability persist. Addressing these issues through targeted research, industry collaboration, and investment in robust testing environments is essential for advancing information system testing practices.

5. Research methods

A structured survey was the primary research method used, targeting both software testing specialists and technical department representatives. The questionnaire was developed using the Ishikawa diagram and insights from an initial survey. A total of 82 professionals, predominantly from the Georgian market, participated, providing comprehensive data on testing practices, challenges, and effectiveness. The study employed both qualitative and quantitative analysis to evaluate the state of information system testing.

6. Research results

The survey revealed key insights into the state of information system testing across organizations. A significant majority (75%) of organizations have experienced testers. However, only 41.5% of respondents believe their teams have well-defined test cases, indicating a gap between the availability of skilled testers and the quality of test planning. About half of the respondents perceive their testers as highly qualified, suggesting opportunities for improvement through targeted training programs. Regarding test environment stability, 59.8% of respondents reported mostly stable environments, while 34.2% reported instability, highlighting the need for more reliable testing conditions. Additionally, while 59.8% of respondents found requirements to be clearly defined, 19.5% considered them vague, which may hinder testing efficiency (Fig.2).

Performance testing is conducted weekly by 11 % of respondents and monthly by 24.4%, with smaller proportions conducting it quarterly or as needed—potentially insufficient for critical systems. The effectiveness of security testing methods was rated moderately by most respondents, with 32% giving it a score of 4, 31% a score of 3, and 30% a score of 5 on a 5-point scale. Stress testing tools were predominantly represented by Apache JMeter (62.7%), with LoadRunner used by 12.5%. Other tools collectively accounted for less than 2% of usage. Automated testing was reported as implemented and very effective by 31% of respondents, while 30% found it implemented but not as effective as desired. Meanwhile, 13.4% had not adopted automated testing, often citing resource constraints (Fig.3, Fig.4). Resource constraints remain a recurring issue, with 13.5% of respondents constantly facing them, 38% experiencing them very often, and 30% occasionally. When dealing with such constraints, 60% of respondents prioritize test tasks based on project needs, while 17.1% rely on risk analysis.

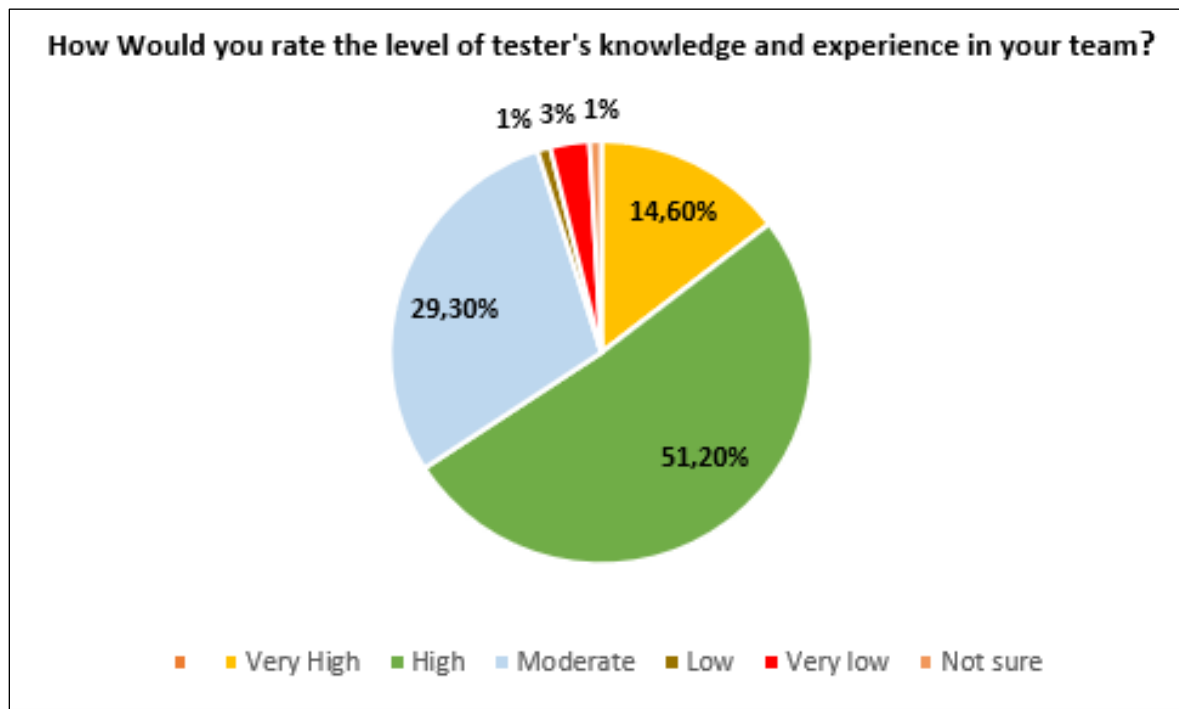


Figure 2. Survey results - Assessing the tester's knowledge and experience level.

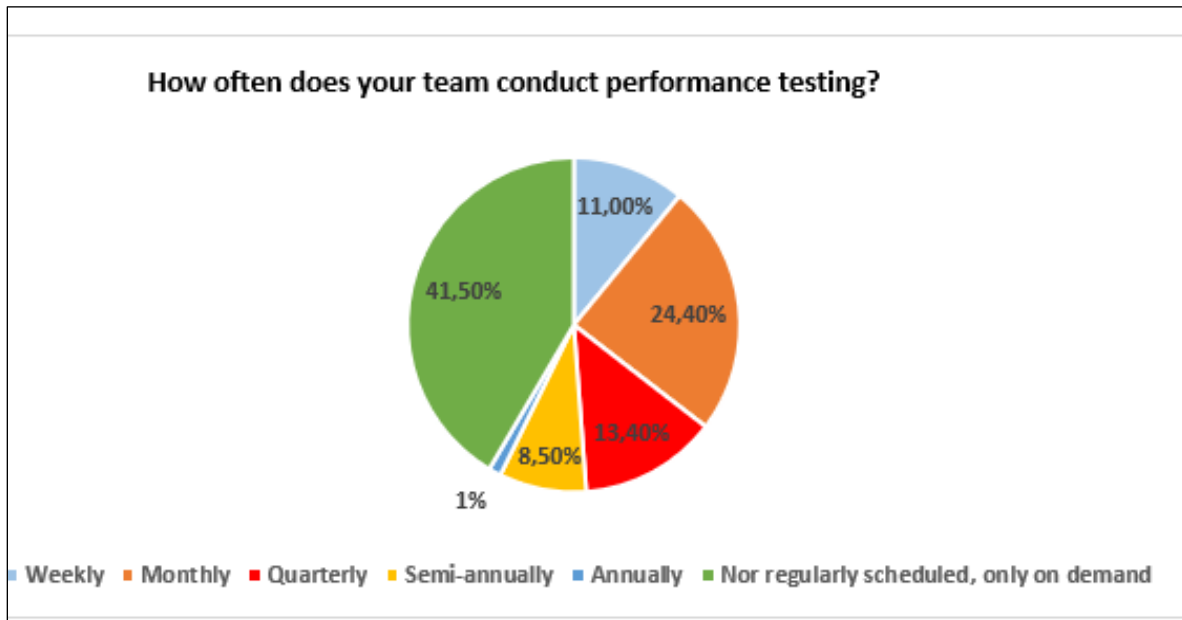


Figure 3. Performance testing frequency.

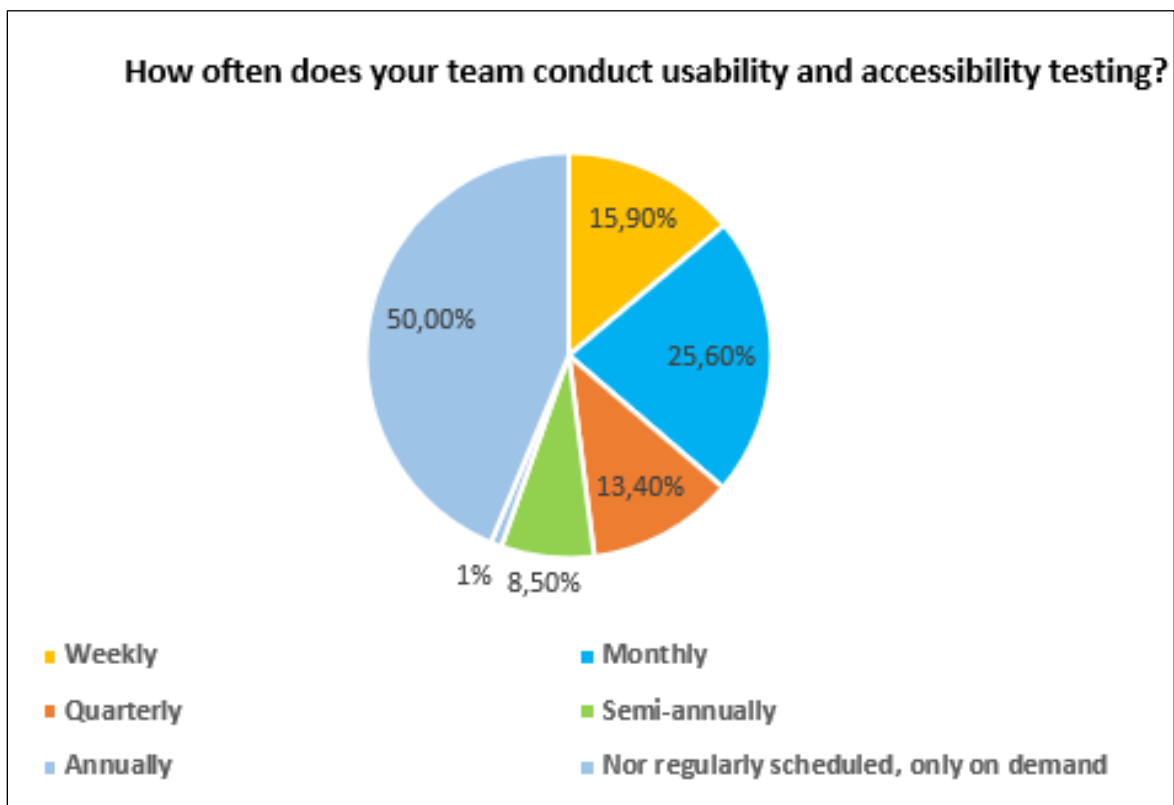


Figure 4. conduct usability and accessibility testing frequency.

The survey results provide important insights into the current state of software testing, the use of complex testing methods, and the challenges facing professionals in the field.

Geographically, the distribution of participants provides a broad perspective, reflecting experiences and practices within and outside Georgia. This diversity helps ensure that the findings are not overly localized and adds validity to the study.

In terms of roles within organizations, the distribution across QA, management, development, operations, and other categories offers a comprehensive view of the software testing landscape, including the perspectives of those directly involved in testing, process managers, and others who impact quality in various ways.

Responses to the sufficiency of experienced testers and clarity of communication within teams indicate important aspects of team dynamics and resource allocation. These are key elements to consider to understand the effectiveness of current testing methods and potential areas for improvement.

The answers to the questions about the stability of the test environment and the level of tester knowledge provide insights into the technical and human factors. These answers help to paint a clearer picture of the infrastructure supporting the testing process and the skills and experience of the people performing it.

The frequency with which different types of testing are conducted, such as performance and usability testing, provides insight into how often these complex methods are used. Variations in frequency can be driven by a number of factors, including the nature of the projects, resource availability, or specific client requirements.

The reported effectiveness of current security testing methods and the implementation and effectiveness of automated testing suggest the use of these complex methods. Understanding perceived effectiveness can shed light on areas where processes are perceived to be performing well and those that need improvement.

The answers to the questions about testing time and prioritizing testing tasks offer a perspective on the challenges that testers face in real-world scenarios.

The challenges reported during real-time monitoring of implementation results provide a deeper understanding of the issues that may arise during this crucial phase. These insights can help develop strategies to mitigate such issues in the future.

It is noteworthy that clear trends in the field of testing have been identified. According to the Pareto principle, five main problems have been identified, namely: the effectiveness of security testing methods, the implementation of automated testing, stable test environments, testing constraints (time, resources, etc.), and a good description of test cases.

It is noteworthy that clear trends in the field of testing have been identified. According to the Pareto principle, five main problems have been identified, namely: the effectiveness of security testing methods, the implementation of automated testing, stable test environments, testing constraints (time, resources, etc.), and a good description of test cases.

7. Prospects for Further Research Development

Future research should explore emerging testing technologies and methodologies to address the evolving challenges of information system quality assurance. Investigating the integration of advanced automation tools and AI-driven testing approaches can further enhance testing efficiency. Additionally, expanding the study to include international markets would provide a comparative perspective, enabling the development of globally applicable testing strategies.

8. Conclusion

The present study provides a comprehensive analysis of complex testing methods in information systems, identifying key challenges and offering actionable recommendations for improvement. Through a combination of qualitative and quantitative data analysis, this research examined performance testing, automated testing, security testing, accessibility testing, and usability testing. The findings revealed that while these methods play a crucial role in ensuring system reliability, security, and user satisfaction, their

implementation is often hindered by various challenges, including resource constraints, gaps in skills development, communication inefficiencies, and limitations in testing environments.

One of the most pressing issues identified in this study is the need for enhanced test planning. Organizations should prioritize defining clear and comprehensive test cases, ensuring that experienced testers can maximize their efficiency. This can be achieved through structured training programs, workshops, and certification courses designed to keep testing staff up to date with the latest methodologies and tools. Regular training sessions should be held to improve the skills of testing teams, equipping them to handle evolving challenges more effectively.

Additionally, investments should be made in stabilizing test environments. Reliable hardware, networks, and software configurations should be maintained to minimize inconsistencies in test results. Unstable environments can introduce errors that do not originate from the system itself but rather from fluctuating test conditions. By standardizing testing environments and ensuring consistency, organizations can improve the reliability of their testing outcomes.

Clearer requirements should be established through close collaboration with stakeholders. Often, miscommunication between development and testing teams leads to inefficiencies, delays, and incomplete test coverage. Implementing requirement management tools and adopting structured documentation approaches can enhance clarity and ensure that all team members have a shared understanding of testing goals.

Organizations conducting critical system testing should aim to perform performance and usability tests on a regular basis, ideally weekly or monthly. Continuous monitoring of system performance ensures early detection of potential problems, allowing for timely corrective actions and overall improvement in system quality and user satisfaction.

Security testing is another area requiring significant enhancement. As cyber threats continue to evolve, adopting advanced security testing methodologies and tools is essential to mitigate vulnerabilities and prevent data breaches. While Apache JMeter remains a dominant tool for stress testing, organizations should explore other tools to diversify their capabilities and tailor testing to specific security needs. Advanced penetration testing tools and vulnerability assessment techniques should be integrated into security testing frameworks to provide comprehensive protection.

Automated testing presents significant advantages in improving testing efficiency, but organizations must address common challenges associated with automation. These include configuration difficulties, script optimization issues, and the need for adequate training. Organizations that have not yet implemented automated testing should be encouraged to do so, with clear guidance on its benefits and strategies for effective integration. Moreover, teams should regularly review and refine their automation scripts to ensure optimal performance and adaptability to evolving system requirements.

Resource allocation remains a key factor influencing the effectiveness of testing efforts. Many organizations struggle with limited budgets, tight schedules, and insufficient manpower. Implementing strategic resource management frameworks can help alleviate these constraints. Organizations should adopt risk-based prioritization strategies, focusing on high-risk areas early in the testing process. This approach ensures that critical vulnerabilities and performance issues are addressed before they escalate into significant problems.

To improve real-time monitoring of testing results, organizations should develop strategies that enhance system visibility and responsiveness. Advanced monitoring tools, dashboard visualization techniques, and real-time alert mechanisms can help teams track system performance and detect anomalies promptly. Implementing artificial intelligence-driven monitoring solutions can further optimize testing by providing predictive analytics and automated issue resolution.

Mitigating the challenges of accessibility and usability testing is another crucial consideration. With increasing emphasis on inclusivity in software development, organizations must ensure that their products are accessible to a diverse user base. Usability testing should be conducted with real users from

varied demographic backgrounds to gain accurate insights into user experience challenges. Accessibility compliance should be assessed against established standards such as WCAG (Web Content Accessibility Guidelines), and necessary modifications should be made to improve system usability for individuals with disabilities.

By implementing these recommendations, organizations can enhance the efficiency and effectiveness of their testing processes, leading to improved system reliability, security, and overall performance. However, it is important to acknowledge that these recommendations are general in nature, and specific actions will depend on the unique circumstances of each organization and testing team.

The field of complex testing methods in information systems is vast and constantly evolving. As technology continues to advance, new challenges will emerge, requiring ongoing research and innovation in testing methodologies. Future research should focus on the integration of artificial intelligence in automated testing, the impact of cloud-based testing solutions, and the role of blockchain technology in securing information systems. Additionally, further exploration of real-time adaptive testing frameworks and their application in large-scale enterprise environments would be beneficial in addressing modern testing challenges.

Ultimately, the success of information system testing depends on a proactive approach to addressing challenges, investing in continuous improvement, and leveraging emerging technologies to enhance testing methodologies. By fostering collaboration between testing professionals, developers, and stakeholders, organizations can create a more resilient and efficient testing ecosystem that aligns with evolving business needs and technological advancements. Ensuring robust testing frameworks will not only enhance software quality but also contribute to greater user satisfaction, operational efficiency, and overall business success.

References:

- 1) Lortkipanidze, N., & Otkhзорia, N. (2024). Navigating business excellence: The crucial role of information technology service management through best practice ITIL. *Georgian Scientists*, 6(1), 120–124. <https://doi.org/10.52340/g.s.2024.06.01.15>
- 2) Otkhзорia, N., Petriashvili, L., Kudukhashvili, A., & Nino, K. (2023). Comparative analysis of complex information system testing methods. *World Science*, 4(82), 5. https://doi.org/10.31435/rsglobal_ws/30122023/8076
- 3) Otkhзорia, N., Zhvania, T., Petriashvili, L., & Lortkipanidze, N. (2024). The critical role of information technology service management using ITIL best practices to improve business management. *Works of GTU*, 2(532), 6. <https://doi.org/10.36073/1512-0996-2024-2-171-176>
- 4) Rose, E. (2023). Usability testing plan template: A flexible tool for planning and teaching usability evaluation. Association for Computing Machinery. <https://doi.org/10.1145/3548658>
- 5) Masuda, S., Nishi, Y., & Suzuki, K. (2020). Complex software testing analysis using international standards. 2020 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), 241–246. <https://doi.org/10.1109/ICSTW50294.2020.00049>
- 6) Garousi, V., & Zhi, J. (2013). A survey of software testing practices in Canada. *Journal of Systems and Software*, 86(5), 1354–1376. <https://doi.org/10.1016/j.jss.2012.12.051>
- 7) Nass, M., Alégroth, E., & Feldt, R. (2021). Why many challenges with GUI test automation (will) remain. *Information and Software Technology*, 138, 106625. <https://doi.org/10.1016/j.infsof.2021.106625>
- 8) Sahin, C., Haan, J. D., & Neretina, E. (2020). Banking stress test effects on returns and risks. *Journal of Banking & Finance*, 117, 105843. <https://doi.org/10.1016/j.jbankfin.2020.105843>
- 9) Salas, M. I. P., & Martins, E. (2014). Security testing methodology for vulnerabilities detection of XSS in web services and WS-Security. *Electronic Notes in Theoretical Computer Science*, 302, 133–154. <https://doi.org/10.1016/j.entcs.2014.01.024>

- 10) Wang, Y., Mäntylä, M. V., Demeyer, S., Wiklund, K., Eldh, S., & Kairi, T. (2020). Software test automation maturity: A survey of the state of the practice. *Proceedings of the 15th International Conference on Software Technologies (ICSOFIT)*, 1, 27–38. <https://doi.org/10.5220/0009766800270038>
- 11) Zhong, H., Zhang, L., & Khurshid, S. (2019). TestSage: Regression test selection for large-scale web service testing. *2019 12th IEEE Conference on Software Testing, Validation and Verification (ICST)*, 430–440. <https://doi.org/10.1109/ICST.2019.00052>
- 12) Otkhozoria, N., Tsiklauri, N., & Otkhozoria, V. (2024). Selection of mathematical optimization methods for solving engineering practice problems. *Georgian Scientists*, 6(2), 286–293. <https://doi.org/10.52340/gi.2024.06.02.30>
- 13) Otkhozoria, N., Azmaiparashvili, Z., Petriashvili, L., Otkhozoria, V., & Akhlouri, E. (2023). LabVIEW in the research of fractal properties of the topology of networks and stochastic processes. *World Science*. https://doi.org/10.31435/rsglobal_ws/30092023/8020
- 14) Eisty, N. U., & Carver, J. C. (2022). Testing research software: A survey. *arXiv preprint arXiv:2205.15982*. <https://arxiv.org/abs/2205.15982>
- 15) Kanewala, U., & Bieman, J. M. (2018). Testing scientific software: A systematic literature review. *arXiv preprint arXiv:1804.01954*. <https://arxiv.org/abs/1804.01954>
- 16) Rehman, A. U., Nawaz, A., & Abbas, M. (2020). Agile methods: Testing challenges, solutions & tool support. *arXiv preprint arXiv:2008.13108*. <https://arxiv.org/abs/2008.13108>