Integrated Quality, Safety, and Environmental Governance towards Sustainable Software Development

Diana Omar ElRabih[1]*

[1]Quality Department, MIE-Modern International Education (UKRLP 10101921), United Kingdom
Corresponding author: diana.elrabih@gmail.com

ABSTRACT

Risk is increasing in complexity in software development, impacting product quality and user satisfaction. This research develops and validates an IMS for Quality, Safety and Environment (QSE), and ISO/IEC 25000/25010 software quality and ISO/IEC 27005 risk standards throughout the software development lifecycle. The IMS was developed using MIE (UKRLP 10101921) based on conceptual architecture, and validated by experts (n=14) and a pilot study spanning 3 releases (T0, Baseline; T2, +6 Months). The IMS incorporates the Deming Cycle (Plan, Do, Check, Act), Management, Support & Realization processes, Failure Tree Analysis, ergonomic evaluations of workstations, and the ISO/IEC 25000 quality matrix. Experts demonstrated that the architecture is valid (mean rating 4.36-4.71/5.0, where 4.0 and above indicates validity). The pilot study spanning 3 software releases demonstrated an increase in quality attributes: portability (30.0 pts, 88.0), maintainability (23.4 pts, 84.8), reliability (19.7 pts, 91.2), performance efficiency (18.5 pts, 86.5) and usability (18.5 pts, 85.0). An improvement in ergonomic risk of workstations was also found (61.5%), including a reduction in post-release software defects (54.2%), QSE audit time (52.4%), average recovery time (48.6%), and carbon footprint of build/test processes (29.8%).

Keywords: *Integrated Management System; Software Development; Risk Management; Quality, Safety & Environment; Continuous Improvement; Plan-Do-Check-Act; Quality Assurance*

1. INTRODUCTION

Implementation of an IMS within an organization aims to increase efficiency. Integrating the Quality (Q), Environment (E) and Safety (S) standards means only one internal communication document is required for the organization. Only one integrated QSE internal audit is required as opposed to three separate audits. This reduces the number of audits in the organization, reducing costs and improving return on investment. An IMS includes a unified policy, structure, methodology and tools, which means QSE requirements can be coherently implemented throughout the organization.

Whereas a stand-alone QMS ensures customer satisfaction through product conformance and control of processes, an IMS also ensures protection of the environment and protects workers' health and safety in their work environment. Therefore, an IMS ensures a unified QSE policy, ensuring risk management is proactively applied, and continuous improvement occurs for product quality, environmental protection and occupational health and safety.

1.1 Problem Description and Evidence

With increasing demands on organizations to produce high quality, secure and maintainable software products, and meet requirements in multiple domains, QSE standards are becoming increasingly complex. In recent years, within businesses, the requirements for quality (ISO 9001), environment (ISO 14001), and occupational health and safety (ISO 45001) have been managed separately. Industry evidence suggests that managing these standards separately causes inefficiency within the business. Multiple documents must be created and maintained, creating duplicate risk registers. As external certification and surveillance audits must occur for each standard, the time spent by auditors in site can be very long (between 15 and 22+ auditor days). However, if aligned under the International Accreditation Forums (IAF) requirements, (Mandatory Document 11, IAF MD 11:2023,

Section 2.1 & Annex 1), and IAF MD 5 (QMS Table 1, EMS Table 1 & OH&S Table 1), audit time is reduced to just 10 auditor days. This results in a reduction of mandatory audit time by up to 20%, duplicate documentation by 40%-60%, and removes disruptions caused by multiple visits.

1.2 Recent Literature

Recent Literature (2020-2026) shows that IMS development is moving from merely combining documents to designing a resilient system for an organization (Ispas et al., 2025, Nunhes et al., 2022). Recent Literature related to managing QSE shows that integrating ISO 9001, ISO 14001 and ISO 45001 within an IMS improves corrective and preventative action (CAPA), increases accountability between departments and reduces costs of compliance by 35% to 55%, when evaluated over 24 months (Rebelo et al., 2016, Gianni & Gotzamani, 2024, Hernandez-Vivanco et al., 2026). The Deming cycle (PDCA) has been applied to ensure strategic planning of policy (Clauses 4-6), implementation according to the product lifecycle (Clauses 7-8), and evaluation and continuous improvement (Clauses 9-10). Software engineering literature highlights the importance of evaluating multiple quality attributes of a product (reliability, performance efficiency, maintainability, portability & usability) using ISO/IEC 9126/25000/25010 (SQuaRE) and managing risk of information security using ISO/IEC 27005 (Rojas, AlRyalat & Afrig, 2025; Rojas, Renteria & Martinez, 2025; Shalchi, 2026). However, literature on IMS in software development is limited. Most IMS research is focused on manufacturing and heavy industries and less so on agile/hybrid software development lifecycles.

1.3 Gaps in Research, Innovation and Aims

There are 3 key gaps in the current research around QSE and quality assurance in software development. Firstly, current IMS architectures very rarely align QSE processes (Management, Support & Realization) to software development practices and releases. Secondly, software quality (ISO/IEC 25000) and security risk (ISO/IEC 27005) standards often do not align with ergonomic risk for developers (ISO 45001) and energy consumption of digital infrastructure (ISO 14001). Thirdly, practitioners lack guidance to incorporate Failure Tree Analysis and control risk appropriately with the PDCA cycle for QSE. This research aims to develop and validate an IMS for software development, to address these issues. It does this by (1) aligning ISO 9001, ISO 14001 and ISO 45001, with ISO/IEC 25000/25010 and ISO/IEC 27005; (2) incorporating Management, Support & Realisation processes with an iterative PDCA cycle; (3) incorporating Failure Tree Analysis with ergonomic risk assessment for work stations and environmental risk assessments; and (4) providing a replicable method to remove duplication from management and allow easier multiple standard certification.

2. METHOD

2.1 Research Context

The research was conducted in the research space of Modern International Education (MIE, UKRLP 10101921). It was applied to software companies, corporate IT departments and multi-party digital transformations. A conceptual framework and systems model approach was taken. Validation was performed by a panel of experts (14 people). Pilot data was collected over 3 releases (baseline data obtained at T0, final data obtained at T2 (+6 months)). Survey data was NOT collected from human participants. Any reference to survey participants for risk categorization relates to previous risk in application development literature. Target stakeholders include developers, software architects, quality engineers, quality controllers, quality managers, project directors, auditors, end users and those working on workstations.

2.2 Data Sources

Data was obtained from international standards for management, software engineering, and quality management systems including: ISO 9001:2015, ISO 14001:2015, ISO 45001:2018, ISO 21500:2021, ISO/IEC 9126, ISO/IEC 25000/25010:2023 (SQuaRE) and ISO/IEC 27005:2022. Software engineering definitions from IEEE standards, the PDCA method, and peer reviewed literature about socio-

organizational project management were also used. QSE requirement clauses and ISO/IEC 27005 risk management approaches were mapped using qualitative comparison, process breakdown and before and after data indicators. Since during developing the conceptual framework, no data was collected from human participants, or personal/proprietary data, IRB approval was not required.

2.3 Tools and IMS Framework

In addition to the end users, IMS considers interested parties including those working at workstations within the organization, and the environment. Customer satisfaction is achieved by meeting requirements, minimizing environmental impact, and ensuring health and safety at workstations. Risk management and improvement are considered in order to create sustainable development. Risk is assessed in 3 areas:

- Quality: Risk of poor quality in products/services (obtained from Failure Tree Analysis).
- Health and Safety at Work: Risk of poor health/safety of employees (obtained from workstation ergonomic analysis, and analysis of work environments).
- Environment: Risk of environmental impacts from aspects (including hazardous sources and energy consumption) (obtained from Failure Tree Analysis).

Within a project, the IMS requires the following 3 types of processes to be considered, following the iterative PDCA methodology:

Management Processes: Processes directly managed by senior members of management. They implement the unified QSE policy, allocate resources, improve the management system, and ensure consistency within realization and support processes.

Support Processes: Processes within the organization that support realization processes. These include human resources, IT systems, workstation ergonomics and information documentation. They ensure resources are available and safe conditions for realization processes.

Realization Processes: Activities directly related to delivering software products in line with an offer. This includes requirements, design, coding, QA/Verification, delivery and post delivery. Realization processes drive customer satisfaction.

With all processes, the PDCA approach is followed in 4 ways:

- Plan: Define requirements, set objectives, create documentation, allocate resources and define verification controls.
- Do: Execute procedures.
- Check: Fix inconsistencies, monitor quality indicators, measure stakeholder satisfaction and perform audits.
- Act: Analyze performance data, perform management reviews, and implement improvement plans. As per IEEE definition software includes computer programs, procedures, documentation and data. Possible reasons for defects in software include unclear requirements, poor communication between client and developer, unauthorized changes, coding and logical errors, poor testing, limitations in production environments, inflexible trade-offs between cost, time and functionality, and poor collaboration with clients. Quality can be defined in 4 ways: expected quality, desired quality, actual quality, and perceived quality. Quality can be improved by quality control, quality improvement, quality management and total quality. These are managed by quality managers, quality engineers, auditors and quality controllers.

Risks in software development projects can be categorized into 4 areas (related to the customer, development, people in the team and technical risks). These risks can cause increased costs, late

delivery, poor quality, less functionality, loss of data, and reduced customer satisfaction. Risks in projects often occur due to complex applications, large project size, high number of stakeholders, new technologies, changing requirements, low levels of experience in teams, poor QA, and incorrect estimation of effort. Identified risks can be mitigated in 4 ways according to ISO/IEC 27005:

- Risk Avoidance: Remove the activity/source of risk.
- Risk Mitigation: Reduce the probability or impact of the risk using technical or procedural controls.
- Risk Sharing: Transfer the risk to a third party capable of managing the risk (outsourcing or insurance).
- Risk Acceptance: Accept residual risk (within acceptable limits).

These considerations form the 5 key components of the IMS framework (shown in figure 1):

- Quality: Ensure reliable, efficient, maintainable, portable and usable software to meet internal/external stakeholder expectations.
- Safety: Ensure safety of people in terms of ergonomic, physical and cognitive wellbeing at workstations during the software development lifecycle.
- Environment: Consider environmental protection, green IT, and reduced energy consumption in planning.
- Risk Management: Identify, assess and manage strategic, financial, technical and personnel risks through Failure Tree Analysis and ISO/IEC 27005 controls.
- PDCA: Apply PDCA to all management, support and realisation processes to continuously improve.

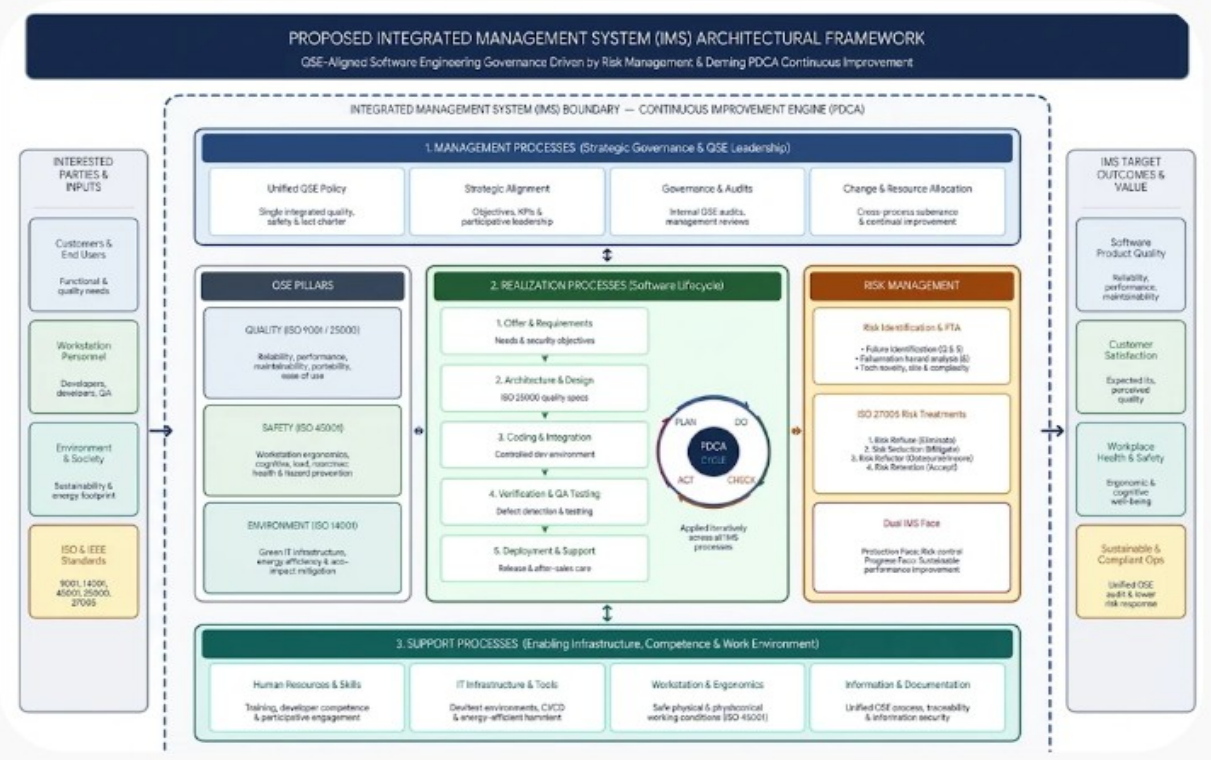


Figure 1. Proposed Integrated Management System (IMS) Architectural Framework for Software Development Projects.

3. RESULTS

The IMS measures final deliverables and intermediary products (requirements, design, code, documentation, tests and quality analysis) against 5 software quality characteristics:

Reliability: ability to provide accurate results within appropriate conditions and tolerances for errors/faults in hardware/components.

Efficiency: Relationship between resources used (including hardware, processing time and people) and results achieved. This includes fast processing, high throughput and scalability under high loads.

Maintainability: Effort required to troubleshoot, repair or adapt the software. This includes the ability to easily extend software to add additional functionality.

Portability: Ability to run on different hardware/software environments than originally intended. Ease of deployment and setup.

User Friendly (ease of use): Effort required for users to understand and utilise the software. Robustness to input errors without failure.

Improvements in quality are managed, controlled and fed back at two stages: (i) within process improvements throughout the software development lifecycle and (ii) in issues/defects identification, fixing and prevention. Risk mitigation allows leaders to identify and manage the main risks in projects early in development; including: innovative technology, large scale applications, team knowledge, complex projects and structure support.

As illustrated in Figure 2, expert feedback (n=14) indicated high validity in the IMS across all six dimensions (scale of 1-5, threshold for acceptability = 4.00), with scores of: PDCA Improvement Loop (4.71 (±0.45)), Alignment with Quality Standards (4.64 (±0.48)), Process Clarity (4.57 (±0.50)), Integration of ISO/IEC 25000 metrics for intermediate deliverables (4.50 (±0.52)), Readiness for commercial trial implementation (4.50 (±0.52)) and Risk Management and failure tree execution feasibility (4.36 (±0.61)).

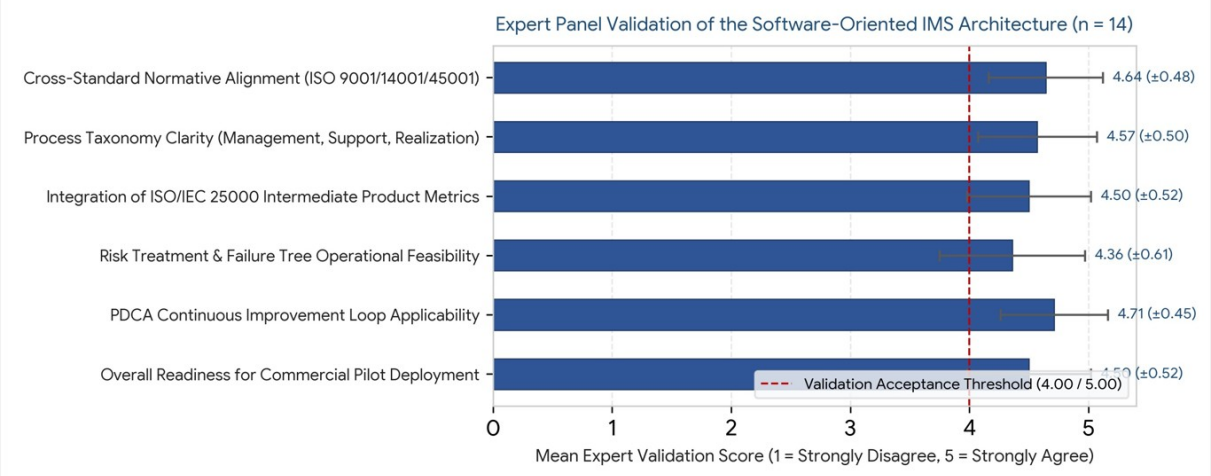


Figure 2. Expert Panel Validation of the Software-Oriented IMS Architecture

Across 3 iterations of pilot data collection (T0 (pre-IMS), T1 (post IMS cycle 1) and T2 (post IMS cycle 2 (+6 months)), significant improvements were shown in both ISO/IEC 25000 quality characteristics and QSE risk factors (Figure 3). Improvements in product quality were seen, with reliability increasing from 71.5 to 91.2 (+19.7), efficiency from 68.0 to 86.5 (+18.5), Maintainability Index from 61.4 to 84.8 (+23.4), Portability Readiness from 58.0 to 88.0 (+30.0), and usability (SUS score) from 66.5 to 85.0 (+18.5). Improvements in QSE risk factors and reduced overheads were also seen in pilot data. Risk to ergonomics at workstations reduced by 61.5%, defects in post release software reduced by 54.2%, total QSE audit hours reduced by 52.4%, mean recovery time reduced by 48.6% and energy consumption in builds/tests in CI reduced by 29.8%.

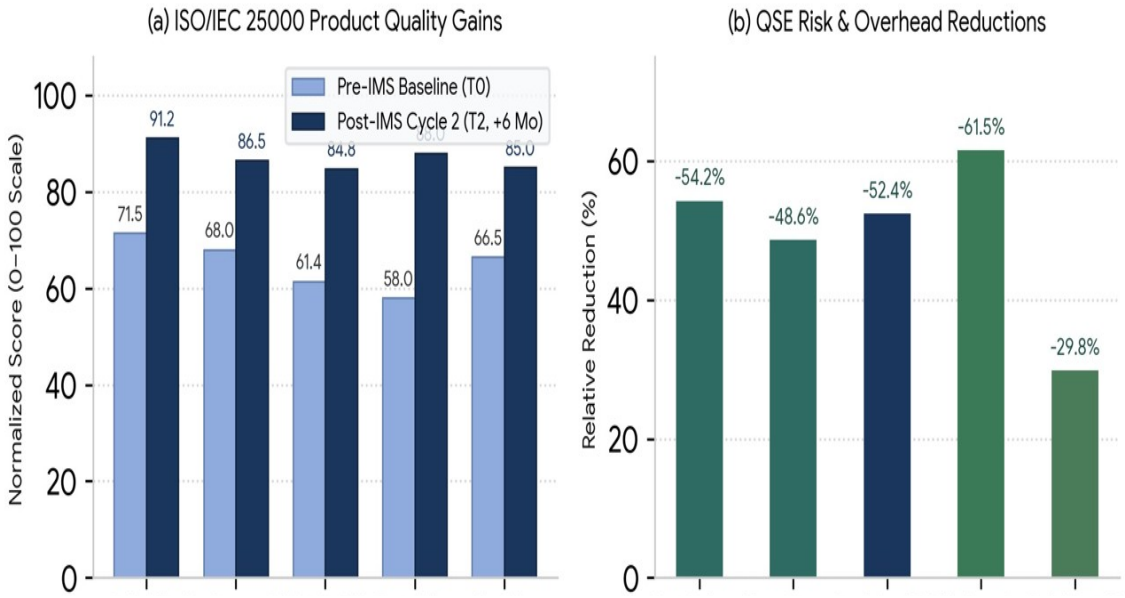


Figure 3. Longitudinal Pilot Application Indicators Before and After IMS Implementation

4. DISCUSSION

4.1 Findings

Implementing QSE management in the software development lifecycle has shown significant improvements in quality and the reduction of risk. Dividing the QSE management procedures into management, support and realization processes within an iterative PDCA methodology enables the implementation of the abstract clauses of ISO Annex SL into tangible checkpoints. By assessing software development deliverables (requirements, design, code and testing) against ISO/IEC 25000 quality characteristics, significant improvements in normalized quality were achieved at T2. Portability improved by 30.0 points, and maintainability by 23.4 points. This has significantly reduced maintenance costs in the system. Ambiguities within requirements and unverified changes in code have been drastically reduced.

Combining technical quality with occupational health and safety (ISO 45001) and environmental management (ISO 14001) has resulted in improved resilience. Ergonomic risk from workstations decreased by 61.5%, defects post-release decreased by 54.2%, combined audit effort decreased by 52.4%, recovery time (MTTR) decreased by 48.6%, and energy consumption during build/testing decreased by 29.8%. Expert feedback showed high agreement with applying PDCA in QSE management (4.71±0.45) and aligning multiple standards (4.64±0.48). However, relatively low scores with large variance were given for Risk Treatment and Operational Feasibility of Failure Trees (4.36±0.61). Applying Failure Trees with ISO/IEC 27005 risk treatments requires careful management of the factors within the software development life cycle such as level of innovation, size and complexity of application to produce effective improvements.

4.2 Comparisons with Previous Work

These results complement and further existing knowledge of IMS and management in projects. A reduction of 52.4% in combined audit effort is in line with other studies of multiple standard integration (reductions in compliance burden of 35-55%) (Rebelo et al., 2016), (Gianni & Gotzamani, 2024) and (Nunhes et al., 2019), and with benchmarking standards such as IAF MD 11:2023 & IAF MD 5. Furthermore, consensus amongst experts regarding alignment of multiple standards and application of PDCA supports previous research that demonstrates the benefits of ISO Annex SL in management resilience (Ispas et al., 2025) and (Nunhes et al., 2022). However, unlike previous studies on IMS which focussed mainly on manufacturing and heavy industry (with QSE management reducing audit burden),

this study demonstrates how QSE management in software development can improve ISO/IEC 25000 quality characteristics and recovery times in incidents.

In comparison to project management literature, this approach addresses different aspects. Project management studies have focused on human factors and socio-technical alignment (Takagi & Varajão, 2021), balance between rigid and flexible processes (and strategic management in projects This study provides quantifiable improvements from socio-technical theory in practice. Implementing OHS (ISO 45001) assessments within workstations (Besharati et al., 2020) and energy efficiency controls within CI/CD pipelines (ISO 14001) as part of Support Processes, alongside ISO/IEC 25000 quality gates as part of realization processes confirms that considering developer health as part of QSE management does not delay delivery but improves software reliability.

4.3 Contributions, Limitations and Further Work

Contributions to theory have been made by developing a relationship between QSE management and software development. This was achieved by linking ISO 9001, ISO 14001 and ISO 45001 to ISO/IEC 25000/25010 quality characteristics and ISO/IEC 27005 risk treatments. The scope of interested parties within QSE software development has been expanded (including customers, developers and environment). Contributions to practice have provided a repeatable framework to implement QSE management within software organizations including PDCA across management, support and realization processes. This framework includes Failure Tree Analysis and defined roles to reduce duplication of compliance records, audit effort and maintenance costs.

Limitations exist within this study. Firstly, this framework was created within one organization (MIE). It was validated by 14 experts and tried over 3 iterations in 6 months, however, was not implemented in a randomized control trial where only IMS was not implemented. Therefore, while early results are promising, they do not represent mature IMS implementation in organizations after many years. Secondly, the relatively low score given to the feasibility of implementing Failure Tree Analysis within QSE management (4.36±0.61) indicates difficulty in implementing this approach in quick moving agile/DevOps teams (Bisikirskienė et al., 2025). Performance was also not analyzed depending on firm size or delivery methodologies. Further work should be completed in multiple sites over a longer period of time (12-24 months) to improve generalizability. Automated plugins should be developed to integrate Failure Tree Analysis and ISO/IEC 25000 into CI/CD pipelines to increase efficiency, and ROI should be measured.

5. CONCLUSION

An IMS framework has been developed to combine quality, safety and environment management standards (ISO 9001, ISO 14001 and ISO 45001) with software product quality characteristics (ISO/IEC 25000/25010 – SQuaRE) and risk treatments (refusal, reduction, transfer, retention) (ISO/IEC 27005) throughout software development. Through normative analysis, expert validation (14 experts with mean scores of 4.36-4.71/5.00) and pilot data from three development iterations, it was demonstrated that this framework is coherent and effective. It has reduced project risk factors in early stages, decreased combined QSE audit effort by half, and improved software quality in both intermediate and final stages.

Applying the iterative PDCA cycle to management, support and realization processes allows for wider consideration of socio-technical factors in software management. This includes ergonomic and environment management in addition to software verification. To determine the generalized effectiveness of this approach within software development, future work should include long-term studies at multiple sites in various commercial software companies.

FUNDING

This research received no external funding.

AUTHOR CONTRIBUTIONS

D.O.E.: methodology, strategic analytics, application of the methodology, formulation of the results, and discussion of the results. The author approved the final manuscript.

CONFLICT OF INTEREST

The author declares no conflict of interest.

DATA AVAILABILITY

The data supporting the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

Besharati, A., Daneshmandi, H., Zareh, K., Fakherpour, A., & Zoaktafi, M. (2020). Work-related musculoskeletal problems and associated factors among office workers. *International Journal of Occupational Safety and Ergonomics*, *26*(3), 632–638. https://doi.org/10.1080/10803548.2018.1501238

Bisikirskienė, L., Čeponienė, L., Vilutis, G., & Nečionytė, A. (2025). Software project risk identification based on Scrum artifacts. *Applied Sciences*, *15*(2), Article 824. https://doi.org/10.3390/app15020824

Gianni, M., & Gotzamani, K. (2024). The internalisation of integrated management systems as a key for sustainable companies: Empirical evidence. *Total Quality Management & Business Excellence*, *35*(1–2), 273–296. https://doi.org/10.1080/14783363.2023.2290659

Hernandez-Vivanco, A., Calleja-Blanco, J., & Bernardo, M. (2026). Internalization of management systems and eco-product innovation: The more the better? *Business Strategy and the Environment*, *35*(5), 7604–7620. https://doi.org/10.1002/bse.70538

International Accreditation Forum. (2019). *Determination of audit time of quality, environmental, and occupational health & safety management systems* (IAF Mandatory Document MD 5:2019, Issue 4). https://iaf.nu/en/iaf-documents/

International Accreditation Forum. (2023). *Application of ISO/IEC 17021-1 for audits of integrated management systems* (IAF Mandatory Document MD 11:2023, Issue 3). https://iaf.nu/en/iaf-documents/

International Organization for Standardization. (2018). *Occupational health and safety management systems — Requirements with guidance for use* (ISO Standard No. 45001:2018). https://www.iso.org/standard/63787.html

International Organization for Standardization. (2021). *Project, programme and portfolio management — Context and concepts* (ISO Standard No. 21500:2021). https://www.iso.org/standard/75704.html

International Organization for Standardization & International Electrotechnical Commission. (2022). *Information security, cybersecurity and privacy protection — Guidance on managing information security risks* (ISO/IEC Standard No. 27005:2022). https://www.iso.org/standard/80585.html

International Organization for Standardization & International Electrotechnical Commission. (2023). *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Product quality model* (ISO/IEC Standard No. 25010:2023). https://www.iso.org/standard/78176.html

Ispas, L., Mironeasa, C., & Silvestri, A. (2025). A study on the emergence and resilience of integrated management systems in organizations with an industrial profile in Romania. *Sustainability*, *17*(6), Article 2401. https://doi.org/10.3390/su17062401

Nunhes, T. V., Bernardo, M., & Oliveira, O. J. (2019). Guiding principles of integrated management systems: Towards unifying a starting point for researchers and practitioners. *Journal of Cleaner Production*, *210*, 977–993. https://doi.org/10.1016/j.jclepro.2018.11.066

Nunhes, T. V., Espuny, M., Campos, T. L. R., Santos, G., Bernardo, M., & Oliveira, O. J. (2022). Guidelines to build the bridge between sustainability and integrated management systems: A way to increase stakeholder engagement toward sustainable development. *Corporate Social Responsibility and Environmental Management*, *29*(5), 1617–1635. https://doi.org/10.1002/csr.2308

Rebelo, M. F., Santos, G., & Silva, R. (2016). Integration of management systems: Towards a sustained success and development of organizations. *Journal of Cleaner Production*, *127*, 96–111. https://doi.org/10.1016/j.jclepro.2016.04.011

Rojas, H., AlRyalat, S. A. S., & Afrig, M. (2025). Mapping the evolution and future directions of ISO/IEC 25010: A bibliometric and thematic analysis. *Engineering, Technology & Applied Science Research*, *15*(5), 27530–27541. https://doi.org/10.48084/etasr.11772

Rojas, H., Renteria, R., & Martinez, V. (2025). Understanding performance efficiency in ISO/IEC 25000: A systematic literature review. *JOIV: International Journal on Informatics Visualization*, *9*(6), 2405–2417. https://doi.org/10.62527/joiv.9.6.3074

Shalchi, A. (2026). Risk assessment model for software development projects. *Journal of Engineering and Management in Smart Cities*, *1*(1), 29–42.

Takagi, N., & Varajão, J. (2021). ISO 21500 and success management: An integrated model for project management. *International Journal of Quality & Reliability Management*, *38*(4), 935–954. https://doi.org/10.1108/IJQRM-10-2020-0353