Research Article

Reclaiming Control: Enterprise Architects on Winning with APM (Application Portfolio Management)

Kiran Kumar Chitrada*

Indian Institute of Management (Kozhikode), India.
* **Corresponding Author Email:** reach.kiranchitrada@gmail.com- **ORCID:** 0000-0002-5247-785X

Abstract:

Application Portfolio Management has emerged as a transformative discipline enabling enterprise architects to regain control over increasingly complex digital ecosystems. Modern organizations face unprecedented challenges managing heterogeneous application landscapes that span legacy systems, cloud-native platforms, and hybrid infrastructures. This technical review demonstrates how comprehensive APM implementation creates strategic value through integrated multi-portfolio governance encompassing applications, information assets, and technology platforms. The evolution from reactive IT management to proactive, data-driven portfolio optimization represents a fundamental paradigm shift that enables organizations to achieve substantial cost reductions while enhancing operational efficiency and regulatory compliance. Contemporary APM frameworks leverage sophisticated data models, automated governance processes, and advanced analytics capabilities to provide enterprise architects with comprehensive visibility into portfolio interdependencies and business impact relationships. The integration of compliance and risk management capabilities transforms APM platforms from operational tools into strategic enablers that address complex regulatory landscapes across financial services, healthcare, and government sectors. Organizations implementing mature APM practices realize significant business value through portfolio rationalization initiatives, strategic transformation enablement, and operational excellence achievement, ultimately transforming IT organizations from cost centers into value-generating capabilities that support competitive advantage and sustainable growth.

1. Introduction

In today's rapidly evolving digital landscape, enterprise architects face unprecedented challenges in managing complex, heterogeneous application ecosystems. The proliferation of legacy systems, cloud-native applications, and hybrid infrastructures has created a critical need for comprehensive Application Portfolio Management (APM) strategies [1]. This technical review examines how enterprise architects are leveraging APM as a strategic enabler to transform operational chaos into controlled, value-driven digital portfolios.

Modern enterprises operate in an environment where application portfolios have grown exponentially in both size and complexity. Organizations frequently struggle with application sprawl, where decentralized procurement and development practices have resulted in overlapping functionalities and redundant systems across different business units. The lack of centralized visibility into application landscapes creates significant challenges for decision-makers attempting to optimize their digital investments while maintaining operational efficiency.

The emergence of APM as a discipline represents a fundamental shift from reactive IT management to proactive, data-driven portfolio optimization. Contemporary APM approaches emphasize holistic portfolio assessment that encompasses not merely application inventory, but comprehensive evaluation of business value, technical health, and strategic alignment. This evolution has been particularly pronounced in highly regulated sectors such as financial services, healthcare, and government organizations where compliance requirements demand thorough documentation and control mechanisms.

Application portfolio complexity manifests through various dimensions including technological

heterogeneity, architectural inconsistencies, and integration dependencies. Legacy systems often represent substantial portions of enterprise portfolios, creating maintenance burdens while simultaneously serving as foundational elements for critical business processes. The challenge intensifies when considering cloud migration strategies, modernization initiatives, and digital transformation programs that must account for existing application interdependencies and business continuity requirements.

Effective APM implementation requires sophisticated analytical frameworks that can assess applications across multiple evaluation criteria including business criticality, technical condition, operational costs, and compliance adherence. Traditional approaches focused primarily on technical metrics have evolved to incorporate business impact assessments, user satisfaction measures, and strategic value propositions. This comprehensive evaluation methodology enables organizations to make informed decisions regarding application retirement, modernization, or continued investment [2].

The strategic importance of APM has been amplified by increasing regulatory pressures, cybersecurity concerns, and operational efficiency mandates. Organizations are recognizing that effective portfolio management extends beyond cost optimization to encompass risk mitigation, compliance assurance, and innovation enablement. The integration of APM with broader enterprise architecture practices creates opportunities for strategic alignment between technology investments and business objectives, ultimately transforming IT from a cost center into a value-generating capability that supports organizational growth and competitive advantage.

2. APM Implementation Framework and Methodology

2.1. APM Platform Selection and ServiceNow CSDM

Application Portfolio Management can be implemented through various enterprise architecture platforms and tools available in the market, each offering distinct capabilities and integration approaches for managing complex application landscapes. Leading APM solutions include specialized platforms from vendors such as LeanIX, Mega, Software AG Alfabet, and BiZZdesign, alongside enterprise platform-integrated solutions. Within the ServiceNow ecosystem, organizations have multiple options including the dedicated Enterprise Architecture application that provides

comprehensive APM capabilities, as well as the Application Portfolio Management module. The ServiceNow Enterprise Architecture application offers robust portfolio management features that leverage the platform's native capabilities for workflow, reporting, and integration [reference to ServiceNow APM documentation]. When implementing APM within the ServiceNow platform, the Common Service Data Model (CSDM) serves as the prescribed data model framework used to standardize information across various ServiceNow modules, including IT Service Management, IT Operations Management, and Enterprise Architecture applications. Implementing ServiceNow's Application Portfolio Management capabilities according to the CSDM framework represents a best-practice approach that provides enterprise architects with standardized data structures for portfolio management, enabling improved data consistency and enhanced reporting capabilities across the entire ServiceNow platform ecosystem.

The technical foundation of successful APM initiatives relies heavily on robust data models and platform capabilities that enable comprehensive enterprise data portfolio management [3]. Contemporary APM implementations require sophisticated integration architectures that can accommodate the diverse nature of modern enterprise environments while maintaining data consistency and accuracy across multiple organizational domains. Implementing ServiceNow's Application Portfolio Management (APM) module according to the Common Service Data Model (CSDM) framework represents a best-practice approach that provides enterprise architects with standardized data structures for portfolio management, enabling improved data consistency and enhanced reporting capabilities across the platform.

CSDM's hierarchical structure facilitates the establishment of consistent relationships between business services, applications, and underlying infrastructure components. This standardization becomes particularly critical when organizations must reconcile data from legacy systems, cloud-native platforms, and hybrid environments that often employ different naming conventions, data formats, and semantic models. The framework supports extensive configuration item types and relationship mappings, allowing organizations to achieve standardization across complex multi-vendor environments while preserving the contextual relationships that drive business value.

Data architecture and integration considerations form the cornerstone of effective APM implementations, requiring sophisticated technical

infrastructure capable of processing high-volume data streams from multiple enterprise sources. Modern implementations involve integration with numerous core enterprise systems, including Configuration Management Databases, IT Service Management platforms, security scanning tools, and business applications. The centralized inventory approach eliminates organizational data silos by creating unified repositories that aggregate information from diverse enterprise systems, establishing automated validation and reconciliation processes that maintain data integrity across the entire portfolio ecosystem.

Metadata enrichment strategies extend far beyond basic application cataloging to incorporate comprehensive contextual information that enables sophisticated analysis and decision-making capabilities. Advanced implementations capture extensive metadata attributes encompassing detailed cost attribution models, business ownership mapping, usage analytics, and performance characteristics. This comprehensive approach to data portfolio management enhances enterprise architecture by providing deeper insights into application utilization patterns, business impact relationships, and operational dependencies [4].

Portfolio visualization and analytics capabilities represent critical success factors for APM platform adoption and organizational effectiveness. Modern platforms must support simultaneous analysis of portfolio data across multiple dimensions, generating comprehensive visualizations that encompass large-scale application ecosystems and their complex interdependencies. Advanced analytics capabilities enable identification of optimization opportunities through automated similarity analysis and functional overlap detection, supporting strategic decision-making processes that drive organizational growth and operational efficiency.

The ability to visualize application dependencies, cost centers, and business impact relationships proves essential for effective portfolio governance, particularly in environments where applications maintain extensive dependencies across multiple system components and architectural layers.

Table 1. APM Implementation Framework Components and Technical Considerations [3, 4]

Implementation Component	Technical Considerations	Strategic Benefits
Data Architecture Integration	Sophisticated infrastructure for high-volume data streams, automated discovery mechanisms, API-based integrations across multiple enterprise systems	Eliminates organizational data silos, creates unified repositories, maintains data integrity across entire portfolio ecosystem
CSDM Framework Implementation	Hierarchical structure supporting extensive configuration item types, standardized relationship mappings, multi-vendor environment compatibility	Enables consistent relationships between business services and infrastructure, facilitates semantic model reconciliation across hybrid environments
Metadata Enrichment Strategy	Comprehensive contextual information capture, detailed cost attribution models, business ownership mapping, usage analytics integration	Provides deeper insights into application utilization patterns, supports sophisticated analysis and strategic decision-making capabilities
Portfolio Visualization Analytics	Multi-dimensional data analysis capabilities, automated similarity analysis, functional overlap detection, complex dependency mapping	Enables identification of optimization opportunities, supports strategic decision-making processes that drive organizational growth and operational efficiency
Enterprise System Integration	Integration with Configuration Management Databases, IT Service Management platforms, security tools, business applications	Maintains real-time portfolio visibility, supports automated validation and reconciliation processes, enables comprehensive enterprise governance

3. Multi-Portfolio Integration Strategy

3.1. Unified Application, Information, and Technology Portfolio Management

The evolution from traditional application portfolio management to integrated multi-portfolio governance represents a significant maturity leap in enterprise architecture practice. This approach recognizes the interconnected nature of modern digital ecosystems where applications, data assets,

and technology platforms must be managed as cohesive, interdependent portfolios. The integration of IT portfolio management with enterprise architecture management creates synergistic relationships that enhance organizational capability to respond to changing business requirements while maintaining operational stability [5].

Contemporary enterprise environments demonstrate increasing complexity through the proliferation of hybrid cloud architectures, microservices implementations, and distributed data management systems. Organizations implementing unified portfolio approaches report substantial improvements in strategic decision-making capabilities compared to those managing portfolios in isolation. The complexity demands sophisticated coordination mechanisms that can accommodate dynamic transformation initiatives while ensuring architectural consistency and governance compliance across multiple organizational domains. Information portfolio integration represents a critical dimension of comprehensive enterprise governance, involving systematic approaches to mapping data domains, privacy classifications, and regulatory requirements across the entire application landscape. This integration creates comprehensive visibility into information risk and compliance posture, enabling informed decision-making regarding data retention policies, privacy impact assessments, and regulatory compliance requirements. Modern implementations establish data lineage relationships that connect applications to underlying data assets, facilitating proactive identification of governance gaps and compliance vulnerabilities during assessment phases.

The integration process encompasses establishing governance frameworks that span multiple organizational domains, each presenting distinct stakeholder groups, compliance requirements, and operational characteristics. Organizations implementing comprehensive information portfolio integration experience significant reductions in compliance-related incidents and enhanced response capabilities to regulatory inquiries. The approach enables systematic evaluation of data governance effectiveness while supporting strategic initiatives related to data modernization and regulatory alignment.

Technology portfolio governance encompasses systematic tracking of platforms, frameworks, middleware, and infrastructure dependencies, providing enterprise architects with comprehensive visibility needed for strategic technology management. The governance framework facilitates identification of standardization opportunities and technology consolidation potential through automated analysis and dependency mapping techniques. This approach supports strategic technology roadmap planning while reducing complexity associated with maintaining diverse technology environments.

Portfolio optimization strategies demonstrate measurable performance improvements when applied systematically across enterprise environments [6]. Organizations implementing technology portfolio governance frameworks achieve substantial reductions in technology stack complexity and realize significant cost savings in licensing and maintenance expenses. The systematic approach enables strategic vendor management optimization and supports more favorable licensing arrangements based on comprehensive usage analytics and dependency analysis.

Cross-portfolio dependency mapping represents the cornerstone of integrated portfolio governance, enabling comprehensive understanding of relationships between applications, data assets, and supporting technology platforms. This capability facilitates sophisticated impact analysis and change management processes essential for effective risk assessment and strategic planning initiatives. Modern dependency mapping implementations utilize automated discovery tools and relationship analysis algorithms to maintain real-time visibility into portfolio interdependencies, enabling more accurate impact assessment and improved change success rates while reducing unplanned outages.

Table 2. Enterprise Architecture Multi-Portfolio Management: Integration Elements and Organizational Benefits [5, 6]

Integration Component	Key Capabilities and Features	Strategic Organizational Benefits
Unified Portfolio Management	Synergistic integration of IT portfolio management with enterprise architecture, coordination mechanisms for hybrid cloud architectures, microservices implementations, and distributed data management	Enhanced strategic decision-making capabilities, improved organizational response to changing business requirements, architectural consistency across multiple domains
Information Portfolio Integration	Systematic mapping of data domains and privacy classifications, comprehensive data lineage relationships, regulatory	Comprehensive visibility into information risk posture, informed decision-making for data retention policies, proactive compliance

	compliance frameworks, governance gap identification	vulnerability management, enhanced regulatory response capabilities
Technology Portfolio Governance	Systematic tracking of platforms and frameworks, middleware and infrastructure dependency management, automated analysis and dependency mapping, standardization opportunity identification	Strategic technology roadmap planning, reduced technology environment complexity, substantial cost savings in licensing and maintenance, optimized vendor management relationships
Cross-Portfolio Dependency Mapping	Automated discovery tools and relationship analysis algorithms, real-time portfolio interdependency visibility, sophisticated impact analysis capabilities, change management process enhancement	Comprehensive understanding of application-data-technology relationships, improved change success rates, reduced unplanned outages, enhanced risk assessment, and strategic planning
Portfolio Optimization Strategies	Performance measurement frameworks, systematic optimization across enterprise environments, strategic vendor partnership management, usage analytics, and dependency analysis integration	Measurable performance improvements in portfolio management, enhanced negotiation capabilities for licensing arrangements, strategic alignment between technology investments and business objectives

4. Compliance and Risk Management Integration

4.1. Regulatory Alignment and Governance Framework

In heavily regulated industries, APM implementation must incorporate comprehensive compliance and risk management capabilities that address the complex regulatory landscape facing modern enterprises. Organizations operating in financial services, healthcare, and government sectors face increasingly sophisticated compliance requirements across multiple regulatory frameworks simultaneously, with individual applications often subject to overlapping compliance mandates. The integration of data certifications, governance metadata, and regulatory alignment features transforms APM from an operational tool into a strategic compliance enabler [7].

Contemporary regulatory environments demand sophisticated tracking and monitoring capabilities that can accommodate the dynamic nature of modern compliance requirements. Organizations without integrated compliance management experience significantly longer resolution times for regulatory inquiries and face substantial penalties due to compliance failures. The complexity of regulatory alignment increases exponentially with organization size, requiring comprehensive compliance monitoring across extensive application portfolios and their associated data processing activities.

Modern APM solutions must support automated compliance monitoring and reporting for standards such as PCI DSS, HIPAA, GDPR, SOX, and industry-specific regulations, including FISMA, NERC CIP, and FDA validation requirements. This capability encompasses automated policy enforcement mechanisms that can process and evaluate compliance status across large application portfolios in real-time, monitoring multiple distinct compliance parameters per application. Organizations implementing automated compliance monitoring report substantial reductions in manual audit preparation time and significant improvements in regulatory response accuracy.

The automation framework includes compliance gap identification algorithms that continuously scan application portfolios for potential violations, with mature implementations capable of detecting the majority of compliance deviations before they result in regulatory violations. Remediation workflow management capabilities coordinate response activities across multiple organizational teams, with typical implementations involving numerous different stakeholder groups in compliance resolution processes. Organizations utilizing automated compliance workflows experience faster remediation cycles and substantial reductions in repeat compliance violations.

Risk assessment and mitigation capabilities represent critical components of comprehensive APM implementations, requiring integration of security scanning results, vulnerability assessments, and business impact analysis into unified risk scoring frameworks. Modern implementations aggregate risk data from multiple security tools and assessment platforms, processing extensive vulnerability information across application portfolios that may contain thousands of individual security findings at any given time [8]. The

integration enables comprehensive risk scoring and prioritization mechanisms that support risk-based decision-making processes.

Organizations implementing integrated risk management report substantial improvements in security incident response times and significant reductions in high-severity security vulnerabilities through focused remediation efforts. The approach enables organizations to concentrate resources on the highest-impact vulnerabilities, with implementations identifying that a minority of discovered vulnerabilities represent the majority of actual organizational risk exposure. Advanced risk scoring algorithms incorporate business impact analysis, threat intelligence, and environmental context to provide nuanced risk assessments.

Data governance integration creates unified views of data classification, lineage, and privacy requirements across entire application portfolios, enabling organizations to maintain comprehensive oversight of sensitive data processing activities. This integration proves essential for organizations managing sensitive data across complex regulatory environments, tracking extensive data governance requirements across their application landscapes. Organizations implementing comprehensive data governance integration experience faster privacy impact assessment completion and reduced data breach incident response times, while achieving improved regulatory audit outcomes and substantial reductions in privacy-related compliance violations.

Table 3. APM Compliance and Risk Management [7, 8]

Integration Component	Core Capabilities and Functions	Strategic Compliance Benefits
Regulatory Alignment Framework	Comprehensive compliance capability integration across multiple regulatory frameworks, data certifications, and governance metadata management, sophisticated tracking and monitoring mechanisms for dynamic compliance requirements	Transforms APM from operational tool to strategic compliance enabler, addresses complex regulatory landscape requirements, substantial reduction in compliance-related audit findings, and regulatory inquiry resolution times
Automated Compliance Monitoring	Real-time compliance status evaluation across large application portfolios, automated policy enforcement mechanisms for PCI DSS, HIPAA, GDPR, SOX standards, compliance gap identification algorithms with continuous portfolio scanning	Substantial reductions in manual audit preparation time, significant improvements in regulatory response accuracy, faster remediation cycles, and reduced repeat compliance violations
Risk Assessment and Mitigation	Integration of security scanning results and vulnerability assessments, unified risk scoring frameworks with business impact analysis, comprehensive risk prioritization mechanisms supporting risk-based decision making	Substantial improvements in security incident response times, significant reductions in high-severity vulnerabilities, enable resource concentration on highest-impact vulnerabilities with nuanced risk assessments
Data Governance Integration	Unified views of data classification and lineage requirements, comprehensive oversight of sensitive data processing activities, automated data lineage mapping across application boundaries	Faster privacy impact assessment completion, reduced data breach incident response times, improved regulatory audit outcomes, and substantial reductions in privacy-related compliance violations
Enterprise Compliance Orchestration	Coordinated response activities across multiple organizational stakeholder groups, remediation workflow management capabilities, privacy requirement enforcement mechanisms for sensitive data processing	Enhanced organizational compliance coordination, comprehensive regulatory framework coverage, strategic alignment between compliance requirements and business operations across complex regulatory environments

5. Business Value Realization and Strategic Outcomes

5.1. Quantified Benefits and Transformation Impact

The strategic value of comprehensive APM implementation extends far beyond operational efficiency gains, with organizations realizing substantial financial benefits while simultaneously improving their risk posture and strategic agility. Contemporary enterprise environments demonstrate that effective application portfolio management creates measurable business value through multiple interconnected value streams including direct cost reduction, risk mitigation, operational efficiency improvements, and strategic capability enhancement [9]. The financial benefits manifest through systematic optimization approaches that enable organizations to achieve significant returns on investment over implementation cycles while maintaining enhanced application availability metrics and reduced operational costs per application.

Leading organizations implementing mature APM frameworks report substantial annual cost savings through systematic portfolio optimization, with individual enterprises achieving varying levels of financial benefit depending on portfolio size, optimization maturity, and organizational commitment to strategic portfolio management disciplines. The return on investment demonstrates compelling business cases for APM implementation, particularly when organizations treat application portfolio management as a strategic discipline rather than tactical operational activity.

Portfolio rationalization results represent the most immediately quantifiable benefits of systematic APM implementation through application decommissioning, consolidation, and modernization initiatives. The systematic approach to application portfolio analysis and optimization typically yields significant cost savings, with organizations commonly identifying substantial portions of their application inventory as candidates for retirement or consolidation. Industry analysis indicates that enterprises discover considerable optimization opportunities during initial rationalization phases, generating substantial cost savings through eliminating licensing, maintenance, and infrastructure expenses.

Advanced organizations implementing comprehensive rationalization programs report extensive benefits per decommissioned application when including indirect advantages such as reduced security management overhead, simplified compliance monitoring, and decreased technical debt management. The tangible financial impact from data-driven portfolio management demonstrates conservative estimates of achievable savings, with organizations typically realizing substantial portions of projected rationalization benefits within initial implementation periods while achieving remaining benefits through longer-term modernization and consolidation initiatives.

Strategic transformation enablement represents perhaps the most significant long-term value proposition of effective APM implementation, fundamentally altering the operational paradigm of enterprise IT organizations [10]. This transformation enables enterprise architects to focus on innovation, digital transformation initiatives, and strategic technology adoption rather than reactive operational management. Organizations experience substantial reductions in time spent on firefighting activities and significant increases in strategic project capacity following APM maturation, enabling IT leadership to contribute more directly to business value creation.

The strategic transformation benefits extend beyond IT organizations to encompass broader business capability enhancement, with companies reporting improved business agility metrics following comprehensive APM implementation. Organizations with mature APM capabilities achieve higher success rates for digital transformation initiatives compared to those with traditional portfolio management approaches, while experiencing improved project success rates and reduced project delivery timelines through enhanced strategic focus and more effective resource allocation.

Operational excellence achievement through comprehensive portfolio visibility, automated governance processes, and data-driven decision-making capabilities creates sustainable foundations for long-term organizational success. Enhanced security posture manifests through reduced security vulnerabilities per application and faster security incident response times, while compliance management improvements result in fewer audit findings and accelerated regulatory response capabilities. Organizations implementing mature APM frameworks experience substantial reductions in unplanned system outages and significant improvements in application performance consistency, extending operational benefits to include reduced infrastructure costs through improved capacity planning and decreased licensing expenses through enhanced utilization visibility.

Table 4. Enterprise Application Portfolio Management: Value Creation Elements and Organizational Impact Assessment [9, 10]

Value Realization Component	Key Capabilities and Measurement Areas	Strategic Organizational Outcomes
Portfolio Rationalization Impact	Systematic application portfolio analysis and optimization, application decommissioning and consolidation initiatives, modernization program implementation, indirect benefit calculation including security and compliance overhead reduction	Substantial annual cost savings through systematic optimization, significant returns on investment over implementation cycles, elimination of licensing and maintenance expenses, reduced technical debt management burden
Strategic Transformation Enablement	Fundamental alteration of IT operational paradigm, enhanced focus on innovation and digital transformation initiatives, strategic technology adoption capabilities, reduced reactive operational management requirements	IT leadership contribution to direct business value creation, substantial reduction in firefighting activities, increased strategic project capacity, improved business agility metrics, and transformation success rates
Operational Excellence Achievement	Comprehensive portfolio visibility establishment, automated governance process implementation, data-driven decision-making capability development, enhanced change management processes	Sustainable foundations for long-term organizational success, reduced security vulnerabilities and faster incident response, improved compliance management with accelerated regulatory response, enhanced application performance consistency
Business Value Measurement Framework	Multiple interconnected value stream analysis, direct cost reduction quantification, risk mitigation assessment, operational efficiency improvement tracking, strategic capability enhancement evaluation	Measurable business value creation through systematic optimization approaches, substantial financial benefits while maintaining enhanced availability metrics, compelling business cases for strategic portfolio management disciplines
Scalability and Future-Proofing Capabilities	Clear governance process establishment, standardized data model implementation, automated management capability development, enhanced architectural consistency achievement, effective technology evolution support	Faster adaptation to changing business requirements, more efficient integration of emerging technologies, sustainable growth support with reduced complexity growth rates, improved application interoperability, and reduced integration complexity

Conclusion

The strategic implementation of Application Portfolio Management represents a critical capability for organizations seeking to navigate the complexities of modern digital transformation while maintaining operational stability and regulatory compliance. Enterprise architects leveraging comprehensive APM frameworks achieve significant competitive advantages through enhanced portfolio visibility, automated governance mechanisms, and data-driven decision-making capabilities that enable proactive management of application ecosystems. The integration of multi-portfolio governance strategies creates synergistic relationships between applications, information assets, and technology platforms, facilitating sophisticated impact assessments and strategic planning initiatives that support organizational agility and innovation enablement. Compliance and risk management integration proves essential for organizations operating in regulated industries,

transforming APM platforms into strategic compliance enablers that address complex regulatory landscapes while maintaining comprehensive oversight of sensitive data processing activities. The business value realization achieved through systematic portfolio optimization extends beyond immediate cost savings to encompass strategic transformation outcomes that fundamentally alter IT operational paradigms, enabling enterprise architects to focus on innovation and digital transformation rather than reactive operational management. Organizations committed to treating application portfolio management as a strategic discipline rather than tactical activity achieve sustainable competitive advantages through improved business agility, enhanced security posture, and accelerated regulatory response capabilities that position them for long-term success in rapidly evolving digital markets

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Pouya Aleatrati Khosroshahi, et al., (2016). What Drives Application Portfolio Complexity? An Empirical Analysis of Application Portfolio Cost Drivers at a Global Automotive Company, *IEEE Xplore.* [Online]. Available: https://ieeexplore.ieee.org/document/7780324

[2] SAP LeanIX, Application Portfolio Management. [Online]. Available: https://www.leanix.net/en/wiki/apm/application-portfolio-management

[3] The Modernization Engineering Company, Enterprise Data Profile. [Online]. Available: https://www.sonata-software.com/platformation-services/enterprise-data-portfolio

[4] Djurdjija Radojevic, How Data Portfolio Management Enhances Your Enterprise Architecture. [Online]. Available: https://www.boc-group.com/en/blog/ea/how-data-portfolio-management-enhances-your-enterprise-architecture-and-drives-growth

[5] Daniel Simon, et al., (2015). Integrating IT Portfolio Management with Enterprise Architecture Management, *ResearchGate*. [Online]. Available: https://www.researchgate.net/publication/309423317_Integrating_IT_Portfolio_Management_with_Enterprise_Architecture_Management

[6] Jason Narsoo, (2017). Performance Analysis of Portfolio Optimisation Strategies: Evidence from the Exchange Market, *ResearchGate*. [Online]. Available: https://www.researchgate.net/publication/31694 9978_Performance_Analysis_of_Portfolio_Opt imisation_Strategies_Evidence_from_the_Exch ange_Market

[7] PlanView, Application Portfolio Management (APM) Best Practices. [Online]. Available: https://www.planview.com/resources/articles/top-10-application-portfolio-management-best-practices/

[8] Tac Security, (2023). Risk-based Vulnerability Management Portfolio of ESOF by TAC Security. [Online]. Available: https://tacsecurity.com/risk-based-vulnerability-management-portfolio-of-esof-by-tac-security/

[9] Shanal Aggarwal, (2024). How to Measure the Business Value of Enterprise Application, *Techahead.* [Online]. Available: https://www.techaheadcorp.com/blog/how-to-measure-the-business-value-of-enterprise-applications/

[10] Alfabet, Strategic IT transformation: simply better business. [Online]. Available: https://www.alfabet.com/resources/guide/strategic-it-transformation-simply-better-business