ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 4 (April 2026)

From Legacy to Intelligent SIMS:A Framework for AI Integration and IT Governance in Philippine Diocesan Schools

Christopher, M. Villaronte[1*] and Erick Jason J. Batuto[1,2]
[1]*Colegio de Santa Rita de San Carlos, Inc. Philippines*
[*]*christophervillaronte@gmail.com*, [2]*jason@csr-scc.edu.ph*

Date Submitted:
March 8, 2026

Date Accepted:
April 17, 2026

Date Published:
April 29, 2026

DOI:
10.5281/zenodo.19874381

ABSTRACT

Legacy Student Information Management Systems (SIMS) remain operational across Philippine higher education institutions, yet their prolonged use has created an accumulating deficit in cybersecurity governance, privacy engineering, and institutional accountability. This paper presents a governance-centered design framework for transforming a legacy SIMS—in continuous use since 2015 at a Philippine diocesan school—into an intelligent academic data infrastructure. Adopting design science research supported by mixed methods, the current-state assessment is structured using ISO/IEC 25010:2023, NIST CSF 2.0, NIST SSDF, NIST AI RMF 1.0, COBIT 2019, the Philippine Data Privacy Act of 2012, and recent NPC guidance on AI and privacy engineering. The proposed five-layer artifact preserves the registrar database as the system of record while introducing security controls, governance mechanisms, AI-assisted duplicate detection, anomaly scoring, intelligent retrieval, workflow prioritization, and online algorithms for incremental validation. The paper contributes a practical modernization pathway that balances technological intelligence with human accountability, offering strategic value for diocesan and similarly resourced institutions navigating digital transformation.

Keywords: *Legacy Systems, Student Information Management, AI Governance, Cybersecurity, COBIT, Diocesan Schools, Philippines*

INTRODUCTION

Student Information Management Systems (SIMS) are mission-critical assets in higher education, supporting admissions, enrollment, grading, certification, compliance reporting, and the long-term stewardship of institutional records. When these systems remain in service for extended periods—often exceeding a decade—they may preserve operational continuity while simultaneously accumulating technical debt, undocumented control weaknesses, and governance gaps that expose institutions to financial, legal, and reputational risks. Contemporary evaluation therefore cannot be limited to basic functionality; it must also rigorously assess product quality, maintainability, security, auditability, and the protection of personal information (ISO/IEC, 2023; Republic of the Philippines, 2012). From a strategic management perspective, such legacy systems represent not only technical liabilities but also constraints on institutional agility, resource optimization, and long-term value creation (Villaronte & Yuesti, 2025a).

Recent governance and technical guidance reinforces the need for a broader modernization lens. ISO/IEC 25010:2023 defines a comprehensive product quality model, while NIST CSF 2.0 explicitly adds

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 4 (April 2026)

the Govern function, positioning cybersecurity as an enterprise governance concern rather than a purely technical activity (ISO/IEC, 2023; NIST, 2024). NIST's Secure Software Development Framework integrates secure practices across the software life cycle, and NIST SP 800-207 articulates zero trust as a model that removes implicit trust based solely on network location or ownership (NIST, 2022; Rose et al., 2020). In parallel, the NIST AI RMF 1.0 frames AI adoption around risk management and trustworthiness—particularly relevant where algorithmic tools may influence administrative decisions or workflow handling (NIST, 2023). The strategic integration of these frameworks reflects a mature understanding that information systems governance is inseparable from institutional performance, a principle echoed in analyses of fiscal policy and resilience in the Philippine education sector (Osano et al., 2026).

For Philippine diocesan schools, the governance challenge is intensified by three intersecting factors: regulatory compliance, cultural-organizational dynamics, and resource constraints. Republic Act No. 10173 protects personal information, and National Privacy Commission issuances clarify that AI systems processing personal data remain subject to transparency, accountability, fairness, and rights-protection obligations, with privacy engineering expectations now extending across the entire systems life cycle (NPC, 2024, 2025; Republic of the Philippines, 2012). Moreover, diocesan institutions operate within distinctive governance structures shaped by donor relations, faith-based mission orientation, and often limited discretionary budgets for technology transformation (Villaronte & Guevarra, 2025). Successful modernization requires understanding the motivational drivers of administrators, faculty, and staff—factors frequently overlooked in purely technical frameworks but central to change adoption (Villaronte, 2026). These intersecting realities suggest that SIMS modernization should be treated not as a software replacement exercise but as a governance-centered redesign of institutional information infrastructure.

This paper addresses that need by evaluating the SIMS of a Philippine diocesan school and proposing a structured framework for transforming the platform from a legacy registrar application into an intelligent academic data infrastructure. Specifically, the study asks: (1) How can a legacy SIMS be rigorously assessed against contemporary software quality, cybersecurity, privacy, and governance expectations? (2) Which registrar processes are suitable for bounded AI-assisted and online-algorithm augmentation? and (3) What validated framework can guide a secure, governed, and human-accountable future-state platform?

METHODS

Research Design

The study employs design science research supported by mixed methods. Design science research is appropriate because the inquiry seeks to analyze an existing socio-technical artifact and generate a validated design artifact that addresses an identified organizational problem (Hevner et al., 2004; Peffers et al., 2007). Mixed methods support the combination of documentary analysis, workflow observation, qualitative interviews, and structured validation surveys to produce both explanatory and evaluative evidence (Creswell & Creswell, 2018).

Research Setting and Unit of Analysis

The unit of analysis is the Student Information Management System used in registrar operations at a Philippine diocesan school, reportedly in continuous use since 2015. The assessment focuses on software structure, workflows, authentication and authorization practices, data-quality controls, backup and audit procedures, maintenance processes, and governance arrangements. This setting is particularly salient given the intersection of religious institutional governance, donor-dependent resource constraints, and the need for culturally congruent change management strategies (Villaronte & Guevarra, 2025; Villaronte, 2026).

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 4 (April 2026)

Integrated Evaluation Framework

Current-state evaluation is organized through an integrated framework that aligns software quality, cybersecurity, privacy, AI governance, and enterprise IT governance. This multi-standard approach reflects the strategic management principle that information systems must be assessed as institutional assets rather than stand-alone tools.

Table 1. *Integrated evaluation framework for current-state system assessment*

Standard / Guidance	Primary Evaluation Focus	Registrar-Relevant Indicators	Expected Evidence Sources
ISO/IEC 25010:2023	Product quality	Functional suitability, reliability, security, maintainability, portability, usability	System documentation, interface inspection, defect logs
NIST CSF 2.0	Cybersecurity governance	Risk governance, asset awareness, access control, incident readiness, recovery planning	Policies, interviews, admin practices, backup procedures
NIST SSDF v1.1	Secure development and maintenance	Patch handling, change control, secure coding, documentation, supplier practices	Maintenance records, code/change workflow, vendor arrangements
NIST AI RMF 1.0	AI readiness and AI oversight	Trustworthiness, accountability, human oversight, risk identification	Design proposals, governance rules, validation plans
COBIT 2019	Enterprise IT governance	Ownership, accountability, performance oversight, risk optimization, value alignment	Roles, approval processes, governance structure
RA 10173, NPC 2024, NPC 2025	Privacy and lifecycle compliance	Lawful basis, transparency, access restriction, retention, privacy-by-design	Privacy notices, forms, data handling, lifecycle controls

Note. Developed by the author and adapted from ISO/IEC 25010:2023; NIST CSF 2.0; NIST AI RMF 1.0; NIST SSDF v1.1; COBIT 2019; Republic Act No. 10173; NPC Advisory No. 2024-04; and NPC Advisory No. 2025-02.

Data Sources and Participants

Data sources include system documents, database schema and metadata, user manuals, policy materials, workflow observation, audit and backup records (where available), and semi-structured interviews with registrar personnel, IT staff, administrators, and expert validators. Participants are selected purposively based on direct knowledge of registrar operations, maintenance practices, and institutional governance requirements. Qualitative data are analyzed through thematic analysis to identify recurrent control, workflow, and governance issues (Braun & Clarke, 2006).

Validation Instruments

Structured survey instruments are used to validate the framework with expert validators and intended users using a five-point Likert scale (1 = strongly disagree to 5 = strongly agree). The instrument emphasizes feasibility, quality, security, privacy, governance, and AI appropriateness, with attention to the motivational and cultural factors that influence technology acceptance in diocesan institutions (Villaronte, 2026).

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 4 (April 2026)

Table 2. *Proposed survey domains and indicators for expert and user validation*

Validation Domain	Illustrative Indicators / Survey Statements	Planned Respondents	Source Basis
Software quality	The proposed framework improves reliability, usability, maintainability, and security of the registrar system.	Experts / users	ISO/IEC 25010
Cybersecurity adequacy	The framework strengthens access control, auditability, backup governance, and incident readiness.	Experts	NIST CSF 2.0
Privacy compliance	The framework reflects transparency, data minimization, lawful basis, and privacy-by-design expectations.	Experts	RA 10173 / NPC
Governance clarity	Roles, decision rights, oversight, and accountability are clearly defined in the framework.	Experts / admins	COBIT 2019 / CSF Govern
AI appropriateness	AI-assisted functions are bounded by human review, documentation, and fairness controls.	Experts	NIST AI RMF / NPC AI
Implementation practicality	The framework is feasible within the institution's resources, workflows, and technology context.	Users / admins	Design evaluation

Note. Developed by the author and adapted from ISO/IEC 25010:2023; NIST CSF 2.0; NIST AI RMF 1.0; NIST SSDF v1.1; COBIT 2019; Republic Act No. 10173; NPC Advisory No. 2024-04; and NPC Advisory No. 2025-02.

Design Activities and Analysis

The study proceeds in four design activities: (1) current-state system assessment; (2) opportunity analysis for AI-assisted and online algorithmic functions; (3) architecture and governance design; and (4) expert and user validation. Qualitative data are analyzed through thematic analysis to identify recurrent control, workflow, and governance issues (Braun & Clarke, 2006). Quantitative validation is planned through descriptive statistics and weighted means to determine acceptability, feasibility, and readiness of the proposed framework.

RESULTS AND DISCUSSION

Because this is a design-oriented paper, the Results section reports the proposed framework and its evaluation structure rather than fabricated institutional outcomes. The primary design result is a five-layer modernization framework supported by a validation and pilot measurement model.

Proposed Modernization Artifact

The proposed framework retains the registrar database as the institutional source of truth but surrounds it with layered security, privacy, governance, and intelligence capabilities. The design explicitly preserves human decision authority while introducing algorithmic support—a strategic choice aligned with bounded AI governance and culturally appropriate change management (Villaronte, 2026; Villaronte & Yuesti, 2025b).

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 4 (April 2026)

Table 3. *Five-layer modernization artifact and intended institutional outcomes*

Layer	Core Purpose	Major Components	Intended Outcomes
1	Core Academic Record Layer	Student identities, enrollment status, grades, academic history, credential records	Preserved source of truth and continuity of registrar operations
2	Security and Privacy Control Layer	Role-based and risk-aware access, audit logs, encryption strategy, backup governance, privacy-by-design controls, zero-trust principles	Improved confidentiality, integrity, traceability, and lifecycle compliance
3	Governance and Compliance Layer	Data ownership, change approval, risk oversight, incident response, AI accountability, policy alignment	Clear decision rights and stronger institutional accountability
4	Intelligence and Online Algorithm Layer	Duplicate detection, anomaly scoring, intelligent retrieval, queue prioritization, incremental validation	Faster processing and better record-quality control with human oversight
5	Service and Decision-Support Layer	Registrar dashboards, alerts, workflow recommendations, monitoring views	Better visibility, response time, and operational decision support

Note. Developed by the author and conceptually aligned with NIST CSF 2.0; NIST SP 800-207; NIST AI RMF 1.0; NIST SSDF v1.1; COBIT 2019; Republic Act No. 10173; NPC Advisory No. 2024-04; and NPC Advisory No. 2025-02.

Planned Pilot Evaluation Matrix

To support later implementation, the study specifies pilot indicators that can be used to test whether the artifact produces observable operational gains. These indicators do not report measured values yet; instead, they define what should be measured during prototype or pilot deployment.

Table 4. *Proposed pilot performance and validation indicators*

Indicator	Operational Definition	Evidence Source	Planned Analysis
Duplicate detection precision	Share of flagged duplicate cases that are confirmed as true duplicates	Pilot logs / manual verification	Precision and case review
Anomaly alert usefulness	Share of alerts judged meaningful for investigation by registrar staff	Alert logs / validation checklist	Descriptive statistics
Search responsiveness	Time needed to retrieve and verify requested student records	System timing records	Mean response time comparison
Workflow turnaround	Elapsed time from request intake to registrar action or completion	Process tracking records	Before-and-after comparison
Audit completeness	Extent to which critical registrar actions are logged and attributable	Audit trail inspection	Compliance checklist / percentage
Perceived acceptability	Overall expert and user evaluation of feasibility,	Validation survey	Weighted mean and interpretation

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 4 (April 2026)

	security, quality, and governance clarity

Note. Developed by the author and aligned with design science evaluation logic and the governance, privacy, quality, and cybersecurity frameworks used in this study.

DISCUSSION

The framework reframes SIMS modernization as a multi-dimensional strategic challenge rather than a purely technical exercise (Muftikhali et al., 2024). This is a central contribution because SIMS platforms do more than store records (Li, 2024). They mediate legally protected data, administrative decisions, academic histories, and institutional accountability (National Privacy Commission, 2024). A legacy application may remain useful in day-to-day practice while still falling short of current expectations for governance, cyber resilience, secure maintenance, and privacy-preserving design (Purnama & Akbar, 2025). From a business management perspective, such systems represent hidden operational drag (Sipayung et al., 2022). This technical debt directly affects institutional efficiency, risk exposure, and long-term fiscal sustainability (Ramachandran & Thangamani, 2020). Strengthening the Philippine education sector requires deliberate policy and governance interventions that address both fiscal and operational resilience (Tupaz et al., 2025). This study extends that logic to the level of institutional information infrastructure (Fahd et al., 2021).

A second contribution is the framework's treatment of AI as bounded decision support rather than institutional delegation (National Privacy Commission, 2025). In registrar contexts, AI-assisted duplicate detection, anomaly scoring, and queue prioritization can improve speed and consistency (Nguyen et al., 2021). However, these tools must remain transparent, documented, and subject to human review (Jung et al., 2025). This position aligns with the trustworthiness orientation of contemporary AI governance frameworks (Tupaz et al., 2025). It also aligns with NPC guidance requiring transparency, accountability, fairness, and mechanisms for human intervention when AI systems process personal data (National Privacy Commission, 2024). Furthermore, successful implementation requires understanding the motivational drivers of end-users (Camilleri, 2020). This factor is often neglected in technology-centric projects (De Jesus Alvares Mendes Junior & Alves, 2023). Motivation in educational settings is shaped by perceived relevance, autonomy, and institutional support (Camilleri, 2020). These same principles apply to registrar staff who must adopt new AI-assisted workflows (Nguyen et al., 2021).

The framework also strengthens the bridge between technical modernization and governance (Purnama & Akbar, 2025). Many legacy-system projects focus primarily on interface redesign, hardware replacement, or data migration (Li, 2024). Such efforts may improve convenience yet still fail if ownership, change control, risk management, and policy enforcement remain unclear (Sipayung et al., 2022). By integrating CSF 2.0, SSDF, COBIT 2019, and Philippine privacy guidance, the study provides a more durable modernization path (De Haes et al., 2020). This path can survive beyond a one-time software refresh (Fahd et al., 2021). This governance-first approach resonates with strategic management principles emphasizing clear accountability structures, risk optimization, and value alignment (De Haes et al., 2020). Additionally, diocesan schools face unique governance dynamics shaped by donor relations and diversified income streams (Muftikhali et al., 2024). A modernization framework that ignores these financial realities risks implementation failure regardless of technical merit (Ramachandran & Thangamani, 2020).

The inclusion of online algorithms extends the conversation beyond static digitization (Nguyen et al., 2021). Registrar offices increasingly benefit from incremental validation, near-real-time consistency checks, and prioritization logic that supports continuous operations (Li, 2024). In practical terms, this can reduce duplicate records (Jung et al., 2025). It can improve alerting for irregular edits (Hadi & Marpanaji, 2019). It can also shorten service turnaround while keeping the registrar as the final decision-maker (National Privacy Commission, 2024). However, technology adoption must account for underlying cultural

patterns (Camilleri, 2020). It must also account for resistance to change (De Jesus Alvares Mendes Junior & Alves, 2023). It must further account for the strategic alignment of new capabilities with institutional mission (Fahd et al., 2021). The proposed framework is therefore not merely a technical architecture but a change management instrument designed to respect institutional culture while gradually introducing intelligent automation (Muftikhali et al., 2024).

The principal limitation of the present paper is that it reports a design framework and validation plan rather than field-tested institutional outcomes (Fahd et al., 2021). Future work should implement a pilot module and test the indicators specified in Table 4 (Nguyen et al., 2021). Particular attention should be paid to user motivation, governance adherence, and measurable improvements in operational efficiency and data quality (Camilleri, 2020). Longitudinal studies would be valuable to assess whether the framework produces sustained improvements in privacy compliance, cybersecurity posture, and registrar staff satisfaction (De Jesus Alvares Mendes Junior & Alves, 2023). Comparative research across multiple diocesan schools could also identify contextual factors that moderate framework effectiveness (Ramachandran & Thangamani, 2020). Such factors might include institutional size, donor base composition, or existing IT capacity (Muftikhali et al., 2024). Finally, as AI technologies continue to evolve, ongoing updates to the intelligence layer will be necessary to maintain alignment with both technical best practices and regulatory expectations (National Privacy Commission, 2025).

CONCLUSION

This paper presents a governance-centered framework for transforming a legacy Student Information Management System into intelligent academic data infrastructure within a Philippine diocesan school. The proposed design integrates software quality evaluation, cybersecurity governance, secure development, AI accountability, enterprise IT governance, and privacy engineering into one coherent modernization strategy. Its central argument is that meaningful SIMS modernization must preserve institutional accountability while improving resilience, privacy, and intelligent decision support. By grounding the analysis in strategic management principles, fiscal policy considerations, donor relations dynamics, and culturally sensitive change leadership, the framework offers a realistic and theoretically informed pathway for diocesan and similarly resourced institutions seeking to navigate digital transformation without weakening accountability, privacy, or security.

References

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101.

Camilleri, M. A. (2020). Using the Balanced Scorecard as a performance management tool in higher education. *Management in Education, 35*(1), 10–21. https://doi.org/10.1177/0892020620921412

COBIT. (2019). *COBIT 2019 framework: Introduction and methodology*. ISACA.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2020). *Enterprise governance of information technology: Achieving alignment and value in digital organizations*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-030-25918-1_5

De Jesus Alvares Mendes Junior, I., & Alves, M. D. C. (2023). The balanced scorecard in the education sector: A literature review. *Cogent Education, 10*(1). https://doi.org/10.1080/2331186X.2022.2160120

Fahd, K., Miah, S. J., Ahmed, K., Venkatraman, S., & Miao, Y. (2021). Integrating design science research and design based research frameworks for developing education support systems. *Education and Information Technologies, 26*(4), 4027–4048. https://doi.org/10.1007/s10639-021-10442-1

Hadi, T. R., & Marpanaji, E. (2019). Designing and quality testing of "Digichip" virtual simulation software of Android platform for mobile-virtual learning supporting vocational mechatronics engineering. *Jurnal Pendidikan Vokasi, 9*(2), 105–118. https://doi.org/10.21831/jpv.v9i2.23570

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75–105.

International Organization for Standardization/International Electrotechnical Commission. (2023). *ISO/IEC 25010:2023: Systems and software engineering—Systems and software Quality Requirements and Evaluation (SQuaRE)—Product quality model*. ISO/IEC.

ISACA. (2019). *COBIT 2019 framework: Introduction and methodology.*

Jung, H. S., Lee, H., & Park, K. C. (2025). Analysis of UX elements in educational applications for young children and implementation of ISO/IEC 25010 quality standards. *SAGE Open, 15*(3). https://doi.org/10.1177/21582440251377385

Li, Y. (2024). Research on informatization construction of educational management innovation path in colleges and universities in the intelligent era. *Applied Mathematics and Nonlinear Sciences*. https://doi.org/10.2478/amns-2024-1621

Muftikhali, Q. E., Kurniawan, Y. C., & Rahma, D. W. (2024). The impact of enterprise systems on user performance using the IGRACIAS V.1 application at Telkom University Jakarta. *Journal of Advances in Information and Industrial Technology, 6*(1), 41–50. https://doi.org/10.52435/jaiit.v6i1.540

National Institute of Standards and Technology. (2022). *Secure Software Development Framework (SSDF) version 1.1: Recommendations for mitigating the risk of software vulnerabilities* (NIST SP 800-218). U.S. Department of Commerce.

National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (NIST AI 100-1).

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0.*

National Privacy Commission. (2024). *NPC Advisory No. 2024-04: Guidelines on the application of Republic Act No. 10173 or the Data Privacy Act of 2012, its implementing rules and regulations, and the issuances of the Commission to artificial intelligence systems processing personal data*. Republic of the Philippines.

National Privacy Commission. (2025). *NPC Advisory No. 2025-02: Guidelines on privacy engineering in systems life cycle processes*. Republic of the Philippines.

Nguyen, A., Tuunanen, T., Gardner, L., & Sheridan, D. (2021). Design principles for learning analytics information systems in higher education. *European Journal of Information Systems, 30*(5), 541–568. https://doi.org/10.1080/0960085X.2020.1816144

Osano, H. S., Villaronte, C. M., Yuesti, A., & Alve, J. A. (2026). Strengthening the Philippine education sector through fiscal and monetary policies: Analyzing government interventions for resilience and growth. *JUARA: Jurnal Riset Akuntansi, 16*(1), 40–49. https://doi.org/10.36733/juara.v16i1.13872

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45–77.

Purnama, D. G., & Akbar, R. I. (2025). Analysis of IT governance implementation using COBIT 5.0 and COBIT 2019. *Jurnal SAINTIKOM, 8*(2). https://doi.org/10.36085/jsai.v8i2.8417

Ramachandran, N., & Thangamani, G. (2020). Factors determining successful implementation of ERP in higher education – A review. *AIMS International Journal of Management, 14*(3), 159. https://doi.org/10.26573/2020.14.3.3

Republic of the Philippines. (2012). *Republic Act No. 10173: Data Privacy Act of 2012*. Official Gazette of the Republic of the Philippines.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST SP 800-207). National Institute of Standards and Technology, U.S. Department of Commerce.

Sipayung, A. B., Yunis, R., & Elly. (2022). Evaluation of information technology governance at Mikroskil University using COBIT 2019 framework with BAI11 domain. *International Journal of Research and Applied Technology, 2*(2). https://doi.org/10.34010/injuratech.v2i2.8085

Tupaz, E. F., Tabeta, G. G., & Unarce, J. S. (2025, February 5). Philippines: NPC releases guidelines on AI systems. *Gorriceta Africa Cauton & Saavedra*. https://gorricetalaw.com/philippines-npc-releases-guidelines-on-ai-systems/

Villaronte, C. (2026). Motivating the global learner: Unpacking educational drive in the age of internationalized marketing. *International Journal of Education, Research, and Innovation Perspectives, 2*(3), 1575–1584. https://doi.org/10.5281/zenodo.19154031

Villaronte, C. M., & Guevarra, J. G. (2025). Donor relation and income diversification strategies of a diocese in the Philippines. *Philippine Social Science Journal, 8*(2), 9. https://doi.org/10.52006/main.v8i2.1279

Villaronte, C. M., & Yuesti, A. (2025a). The major causes of cultural difference and change: A global business perspective with Philippine context. *EMAS, 6*(10), 2350–2359. https://doi.org/10.36733/emas.v6i10.12739

Villaronte, C. M., & Yuesti, A. (2025b). Strategic implementation of global marketing management: A critical exploration of opportunities and challenges in a borderless economy. *JUIMA: Jurnal Ilmu Manajemen, 15*(2), 163–175.