A Comprehensive Risk Management Framework for Energy Performance Contracting: Integrating Governance, Process, and Energy Management Systems

Md. Nazri Othman[1]*, Zamri Zakaria[2], Hidayat Zainuddin[1], Mohd Anuar Adip[1]

[1]Faculty of Electrical Technology and Engineering, Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia

[2]Department of Electrical Engineering, Politeknik Port Dickson, Negeri Sembilan, Malaysia

***Corresponding Author**

DOI: https://doi.org/10.47772/IJRISS.2026.100900404

Received: 24 September 2026; Accepted: 29 September 2026; Published: 13 October 2026

ABSTRACT

Energy Performance Contracting (EPC) is a widely adopted mechanism for delivering guaranteed energy savings without upfront capital outlay from building owners, yet its adoption in emerging markets remains constrained by fragmented and poorly integrated risk governance. While prior studies have proposed risk taxonomies or stage-specific risk models for EPC, few have combined governance structures, the EPC project process, a formal risk management system, and an Energy Management System (EnMS) into a single, empirically grounded and practitioner-validated framework. This study addresses that gap by developing and validating a comprehensive risk management framework for EPC projects in Malaysian. Using a mixed-methods design, twenty-four purposively sampled stakeholders (industry experts, energy managers, and Energy Service Company (ESCO) representatives) were engaged through semi-structured interviews, an embedded case study, and focus group discussions; reflexive thematic analysis (assisted by ATLAS.ti) classified risk evidence into six categories and twenty-two risk factors, each scored on a 5×5 probability-impact matrix aligned with ISO 31000:2018. These empirical inputs were synthesised into an integrated framework comprising four interlocking components — governance, EPC project process, an ISO 31000-aligned risk management system, and an EnMS built on the Plan-Do-Check-Act cycle — and validated through a focus group of five senior practitioners and academics. Results show behavioural and operational risks (mean risk level = 19.0 of 25) as the dominant threat to EPC delivery, substantially ahead of technological (14.0), measurement and verification (10.0), contractual (7.0), regulatory (6.8), and financial risks (6.0). The focus group unanimously endorsed the framework's comprehensiveness and its applicability to both public and private sector projects, while recommending dedicated energy management committees and expanded risk treatment provisions. The framework contributes a governance-anchored, standards-aligned model that links qualitative risk evidence to a living, auditable control system, offering ESCOs, building owners, and policymakers an actionable tool for prioritising risk mitigation investment in EPC delivery.

Keywords: Energy Performance Contracting; Risk Management Framework; ISO 31000; Energy Management System; Governance; Mixed-Methods Research; Malaysia

INTRODUCTION

Energy Performance Contracting (EPC) has become one of the most widely promoted mechanisms for delivering energy efficiency and emission reduction at scale, allowing Energy Service Companies (ESCOs) to design, finance, install, and guarantee energy-saving measures on behalf of building owners without requiring upfront capital investment (Hashempour et al., 2020; Economidou et al., 2020). Despite its appeal, EPC uptake continues to be constrained by uncertainty: financial exposure, regulatory ambiguity, technological unfamiliarity, and disputed measurement and verification (M&V) outcomes routinely undermine the predictability of contracted

savings (Alam et al., 2019; Piccinini et al., 2021; Wu & Zhou, 2019). In Malaysia, where fossil fuels still supply the overwhelming majority of primary energy demand, EPC is positioned as a central instrument of the National Energy Transition Roadmap, yet its expansion into public-sector assets such as polytechnics and other educational institutions is slowed by the absence of a standardised, end-to-end risk governance model (Ghazali et al., 2023; Ludin et al., 2022).

A substantial body of literature has proposed risk taxonomies and stage-specific risk models for EPC. Berghorn and Syal (2016, 2019a) developed a comprehensive risk assessment framework for correctional-facility retrofits structured around identification, assessment, and management stages; Garbuzova-Schlifter and Madlener (2017) applied an Analytic Hierarchy Process to construct a risk hierarchy for EPC projects in the Russian public sector; and Hansen (2006) proposed a tripartite financing-technical-procedural risk classification still widely referenced in guaranteed-savings EPC models. Wang et al. (2019) ranked EPC risk factors using a best-worst network method, while Frangou et al. (2018) and Kamenders et al. (2018) examined contractual standardisation and quality management as risk-mitigating mechanisms. More recently, Wan et al. (2023) re-examined EPC risk allocation for Chinese commercial buildings through an incomplete-contract lens, Tang et al. (2025) applied a DEMATEL-ISM model to map the influence pathways among EPC risk factors, Guo et al. (2025) constructed a cloud-matter-element risk early-warning model for ESCOs undertaking retrofit projects, and Yang et al. (2025) synthesised seven categories of EPC adoption barriers and twenty-eight critical success factors in a critical review spanning political, economic, organisational, relational, and technical dimensions. This most recent wave of scholarship confirms that EPC risk research remains active and methodologically diversifying, yet it also confirms the pattern identified by the earlier literature: these 2023-2025 studies continue to model risk classification, contractual allocation, or early-warning analytics as separate exercises rather than embedding them within a single governance-anchored framework. Collectively, these studies treat risk identification, technical M&V improvement, and organisational governance as largely separate problems. Few frameworks integrate governance structures, the operational EPC process, a formal ISO 31000-aligned risk management system, and an Energy Management System (EnMS) into a single model, and fewer still have been empirically validated by practitioners against the specific institutional conditions of an emerging, guaranteed-savings-only EPC market such as Malaysia's.

This gap matters because EPC risk in practice is rarely confined to one domain. A behavioural lapse in operations and maintenance can invalidate a technically sound M&V design; a governance vacuum at the top-management level can leave a well-designed risk register unimplemented; and an EnMS that is not wired into the risk management system produces energy data without producing risk-relevant intelligence. Addressing EPC risk therefore requires a framework that is simultaneously structural (who is accountable), procedural (what happens at each project stage), methodological (how risk is scored and treated), and operational (how energy performance is continuously monitored and fed back into governance decisions).

This study responds to that need. Its objective is to develop and empirically validate a comprehensive risk management framework for EPC projects that integrates governance, the EPC project process, an ISO 31000:2018-aligned risk management system, and an Energy Management System, using evidence drawn from Malaysian polytechnic EPC implementation. The framework is constructed from thematic analysis of interview and focus group data and an embedded case study and is validated through an independent focus group discussion with senior industry and academic experts. The paper makes three contributions. First, it operationalises risk identification into a quantified, ISO 31000-aligned risk matrix covering six categories and twenty-two factors, giving practitioners a decision-ready prioritisation tool rather than a descriptive taxonomy. Second, it proposes an integrated four-component framework — governance, process, risk management system, and EnMS — with an explicit analytics-to-governance feedback loop, addressing the fragmentation identified in prior literature. Third, it reports expert-panel validation evidence, adding practitioner-endorsed credibility that is largely absent from earlier EPC risk models.

The remainder of the paper is organised as follows. Section 2 reviews the literature on EPC risk frameworks, ISO 31000, and EnMS integration, and situates the research gap. Section 3 describes the mixed-methods design, sampling, and framework-development procedure. Section 4 presents the results: the governance structure, the EPC process, the risk identification and risk matrix findings, the EnMS component, the integrated framework,

and the focus group validation. Section 5 discusses the findings against the literature and their practical implications, and Section 6 concludes with contributions, limitations, and directions for future research.

LITERATURE REVIEW

Risk in Energy Performance Contracting

EPC risk has been studied predominantly as a classification problem. Hansen (2006) proposed a tripartite structure of financing, technical, and procedural risk applicable to the vendor-financing, shared-savings, and guaranteed-savings EPC models, the last of which remains the only model currently in use in Malaysia. Berghorn and Syal (2016) extended this into a more granular technical risk framework spanning energy audit quality, ECM selection and installation, commissioning, operation and maintenance, and M&V, arguing that risk exposure is distributed across the entire EPC lifecycle rather than concentrated at contract signing. Garbuzova-Schlifter and Madlener (2017) used an Analytic Hierarchy Process to build a three-level risk hierarchy for the Russian public sector, decomposing eight top-level risk factors into granular root causes — an approach that demonstrated the value of structured, traceable risk decomposition but stopped short of proposing an implementation-ready governance model.

More recent studies have emphasised that a comprehensive risk framework must draw on the perspectives of all key stakeholders — project developers, building owners, contractors, and ESCOs — because each group is exposed to different risk profiles and holds different risk-relevant information (Berghorn & Syal, 2019a). Empirical validation of these frameworks, however, remains scarce; Ruan, Gao and Mao (2018) explicitly call for more empirical assessment of risk management strategy effectiveness in real EPC projects, a call this study answers directly through focus-group validation. Building on this research programme's own systematic review of EPC risk evidence (Zakaria et al., 2024a), which synthesised risk categories reported across the global EPC literature, and its companion systematic review of M&V-specific risk (Zakaria et al., 2024b), the present study moves from cataloguing reported risks to developing and empirically validating an integrated, governance-anchored framework grounded in primary Malaysian stakeholder evidence — addressing the gap between descriptive risk review and field-ready governance tooling that both reviews identified.

ISO 31000:2018 as a Risk Governance Standard

ISO 31000:2018 provides a structured, internationally recognised approach to risk management built around eight guiding principles and a cyclical process of establishing context, risk identification, risk analysis and evaluation, risk treatment, and continual monitoring, review, communication, and consultation (ISO, 2018a, 2018b). Its generic, sector-agnostic design makes it well suited to EPC, where risk spans financial, technical, regulatory, and behavioural domains simultaneously. Several EPC studies reference ISO 31000 principles in passing (Anton & Nucu, 2020; Ow, 2023), but few operationalise the standard's full cycle — including risk scoring matrices and defined escalation thresholds — into a project-specific EPC risk management system.

Energy Management Systems and EPC Risk Mitigation

An Energy Management System (EnMS), typically implemented under ISO 50001, provides the organisational discipline needed to convert continuous energy data into decision-relevant intelligence: energy policy, planning, operational control, and performance evaluation organised around a Plan-Do-Check-Act (PDCA) cycle. In EPC contexts, EnMS is argued to reduce the central risk of underperformance against guaranteed savings by enabling continuous tracking of key performance indicators, early detection of equipment or behavioural drift, and standardisation of energy performance reporting (Guo & Zhang, 2020; Kamenders et al., 2018). Yet the literature typically discusses EnMS and risk management systems as parallel rather than integrated mechanisms. Where M&V-focused studies have proposed simulation-based methods — including Monte Carlo simulation — to better quantify energy-saving uncertainty (Agenis-Nevers et al., 2021; Castillo et al., 2022; Feng et al., 2022), these advances have rarely been connected explicitly back to a governance-level risk matrix, leaving a disconnect between technical M&V improvement and the organisational decisions it should inform. This paper's own preceding systematic review of M&V-specific EPC risk (Zakaria et al., 2024b) similarly found that M&V risk

mitigation is typically reported as a stand-alone technical concern rather than as an input to organisational governance — a gap this study closes through the analytics-to-governance feedback loop described in Section 4.5. Sector-specific applications continue to appear in the most recent literature: Zong and Liu (2026), for instance, use a Work Breakdown Structure and Delphi analysis to identify financial management, technology, financing capability, talent, and decision-making as the dominant EPC risk factors in hotel-building retrofits under the Energy Management Contracting mode, again without embedding these findings in a governance or EnMS architecture.

Research Gap

Three gaps in the literature motivate this study. First, existing EPC risk frameworks are typically partial: they classify risk (Berghorn & Syal, 2016; Wang et al., 2019), model financial/technical risk quantitatively (Agenis-Nevers et al., 2021; Castillo et al., 2022), or, in the most recent 2023-2026 literature, analyse contractual risk allocation and early-warning analytics in isolation (Wan et al., 2023; Tang et al., 2025; Guo et al., 2025; Zong & Liu, 2026), but rarely combine governance, process, risk management, and energy management into one integrated model. That this fragmentation persists in studies published as recently as 2025-2026 indicates the gap is not merely historical but a continuing feature of the field. Second, risk assessment models are seldom adapted to the legal, institutional, and market conditions of emerging EPC markets; most published frameworks, including the most recent ones, originate from mature EPC markets in North America, Europe, or China, limiting direct transferability to a nascent, guaranteed-savings-only market such as Malaysia's — a gap Yang et al.'s (2025) otherwise comprehensive critical review of EPC barriers and success factors likewise does not address for Southeast Asian markets specifically. Third, empirical validation of proposed frameworks by independent practitioner panels is rare, leaving a credibility gap between conceptual frameworks and field-ready governance tools. This study addresses all three gaps by developing an integrated governance-process-risk management system-EnMS framework, grounded in Malaysian polytechnic EPC evidence, and validated by an independent expert focus group.

METHODOLOGY

Research Design

This study adopted a mixed-methods design combining qualitative evidence elicitation with quantitative risk scoring to develop and validate an integrated EPC risk management framework. The qualitative strand used semi-structured interviews, an embedded case study, and focus group discussions to identify and classify risk factors and to co-construct and validate the proposed framework; the quantitative strand converted qualitative frequency and severity evidence into a structured probability-impact risk matrix aligned with ISO 31000:2018. This exploratory-confirmatory architecture allowed qualitative elicitation to initialise the set of risk variables, with structured scoring subsequently transforming that evidence into a ranked, decision-relevant risk register (Kiger & Varpio, 2020; Woolf & Silver, 2017b).

Study Context and Sampling

The empirical setting is Malaysian public polytechnic institutions implementing EPC under the guaranteed-savings model, the only model currently active in the Malaysian market. Polytechnics were selected because they combine high energy intensity with significant efficiency potential and sit within the core scope of national energy-transition policy. Data were collected from Energy Service Companies (ESCO project leads), client-side energy managers, facility engineers, M&V consultants, and policymakers through purposive, criterion-based sampling supplemented by snowball referral. Twenty-four stakeholders were engaged in total: ten industry experts, eleven practitioners, and three ESCO representatives, each required to hold a recognised energy-management credential (Certified Energy Manager, Registered Energy Manager, Certified Professional M&V, or Certified Energy Auditor) or more than ten years of EPC-relevant experience. An embedded case study of one operating polytechnic EPC project supplied site-level artefacts — commissioning logs, M&V plans, and contractual schedules — that triangulated stakeholder accounts against documentary evidence.

Framework Development Procedure

Framework development proceeded in four stages. First, semi-structured interview and case-study data were analysed using reflexive thematic analysis, assisted by ATLAS.ti, to identify recurring risk factors and their categorical structure. Second, each identified risk factor was scored on two 5-point scales — a Probability Index (likelihood of occurrence, calibrated against the frequency of coded qualitative references and industry benchmarks) and an Impact Parameter (severity of consequence, calibrated against whether the risk required no intervention, operational-level correction, or escalation to top management and/or the ESCO) — and combined multiplicatively into a Risk Level (Probability × Impact) mapped onto a 5×5 risk matrix consistent with ISO 31000:2018 practice. Third, the scored risk register was synthesised, together with evidence on stakeholder roles, the EPC project process, and EnMS practice, into an integrated four-component framework: governance, EPC project process, risk management system, and EnMS. Fourth, the draft framework and its four components were presented to an independent focus group of five senior practitioners and academics — spanning sustainable energy management, energy efficiency policy, engineering/commissioning, governance, and academic risk management — for structured validation and refinement (Table 1).

Analytical Techniques

Qualitative data (interview transcripts, case-study documents, and focus group recordings) were coded and thematically analysed in ATLAS.ti following reflexive thematic analysis procedures (Kiger & Varpio, 2020), with member-checking used to strengthen credibility. Risk scoring followed the calibration logic described above: for example, a risk factor coded 30–49 times across the qualitative corpus was assigned Probability Index 4 (60–79% likelihood), while impact severity requiring senior management and ESCO intervention was scored as Impact Parameter 5 (catastrophic). This scoring approach is used descriptively in Section 4 to prioritise the twenty-two risk factors, and its outputs are, in the companion strand of this research programme, further cross-validated against regression-based baseline energy modelling and Monte Carlo simulation of savings uncertainty — an analytics-to-governance linkage summarised conceptually in Figure 1 but not re-estimated in this paper, which focuses on framework structure and expert validation.

Table 1. Focus group discussion participants.

ID	Field / Scope	Current Position	Experience
E01	Energy Efficiency / EPC Projects	Manager, Sustainable Energy	Above 25 years
E02	Energy Efficiency / EPC Projects	Assistant Director, Energy Efficiency & Conservation Unit	Above 20 years
E03	Energy Efficiency / EPC Projects	General Manager, Engineering, Consultation & Commissioning	Above 25 years
E04	Energy Efficiency / EPC Projects	Deputy Director, Governance and Excellence Division	Above 20 years
E05	Risk Management Systems	Senior Lecturer	Above 10 years

RESULTS

Governance Structure

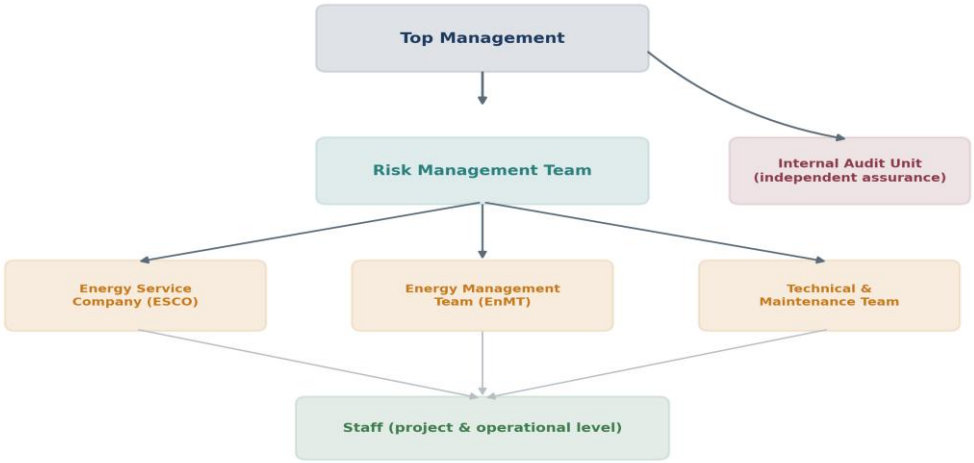
The proposed governance structure (Figure 2) anchors accountability for EPC risk management at top management, who hold ultimate responsibility for establishing and resourcing the risk management framework, approving risk registers, and cultivating a risk-aware culture among stakeholders. Operational execution is delegated to a Risk Management Team, which coordinates three functional sub-teams — the ESCO, the Energy Management Team (EnMT), and the Technical and Maintenance Team — each responsible for collecting and analysing risk data within its domain and escalating findings to top management. An Internal Audit Unit provides

independent assurance that the framework is implemented as designed, while project-level staff are positioned as the first line of risk detection and response. Table 2 summarises the roles and responsibilities attached to each governance tier.

Table 2. Roles and responsibilities within the governance structure (condensed).

Structure	Key Responsibilities
Top Management	Establish and resource the risk management framework; approve risk registers and treatment plans; ensure integration of risk management into the EPC process; ensure staff training.
Risk Management Team	Develop, implement, and continuously improve the framework; monitor emerging risks; report framework effectiveness periodically to top management; build risk-management culture.
ESCO / EnMT / Technical & Maintenance Team	Drive risk management at their respective operational levels across all EPC process stages; collect and analyse risk data; assist in determining risk levels.
Internal Audit Unit	Conduct independent audits of framework adherence; report audit findings to the Risk Management Team.
Staff	Acknowledge, communicate, and respond to emerging or changing risks; contribute to risk profiling; implement risk treatment within their area of responsibility.

Figure 2. Governance structure of the proposed EPC risk management framework, showing accountability from top management through to project-level staff.



EPC Project Process

The EPC project process component situates risk management within the operational sequence familiar to Malaysian EPC practice: energy audit (walk-through followed by investment-grade audit), EPC contract negotiation, implementation (installation and commissioning), operation and M&V, and payment reconciled against verified savings. Each stage carries distinct risk exposure — for example, an inadequately scoped walk-through audit inflates savings estimates that later strain contract feasibility, while unclear M&V provisions at the contracting stage are a recurrent source of owner-ESCO dispute. Embedding the risk management system

across these stages, rather than applying it only at the point of contract signing, was strongly endorsed by focus-group participants as a precondition for effective risk control.

Risk Management System: Identification, Scoring, and Treatment

Thematic analysis of interview, case-study, and focus-group evidence identified six risk categories comprising twenty-two distinct risk factors (Table 3): Behavioural and Operational, Measurement and Verification (M&V), Technological, Contract, Regulatory and Policy, and Financial and Investment risk.

Table 3. Risk categories and risk factors identified in Malaysian EPC projects.

Risk Category	Risk Factors
Behavioural & Operational	Difficult staff management/ineffective staff; inadequate O&M; lack of involvement in EnMS; lack of qualified professionals; organisational and occupant behaviour
Measurement & Verification (M&V)	High cost of energy/M&V audit; improper M&V design; lack of competence in M&V and savings evaluation; poor data quality
Technological	Lack of competence in new technology; poor equipment performance; unavailable technology
Contract	Contract duration; contract parameters; no building-owner participation in contract development
Regulatory & Policy	Difficulty of procurement and finance process; insufficient incentive policies; lack of standardisation and guidelines; weak legislation
Financial & Investment	Financing difficulties; insufficient investment; lack of financial resources; lack of skills/expertise in financing

Following ISO 31000:2018-aligned scoring (Section 3.3), each factor was rated on a Probability Index (1–5) and Impact Parameter (1–5) and located on a 5×5 risk matrix (Figure 3, Figure 4). Risk level was calculated as Probability × Impact, giving a maximum theoretical score of 25. Figure 4 plots all twenty-two identified risk factors on the matrix; Figure 5 aggregates these into mean risk level by category.

Figure 3. ISO 31000:2018-aligned risk management process applied to the EPC risk management system, with recording and reporting embedded at every stage.

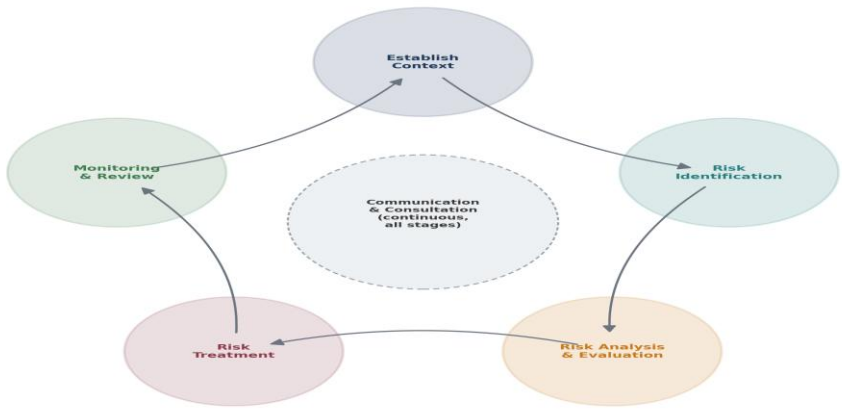
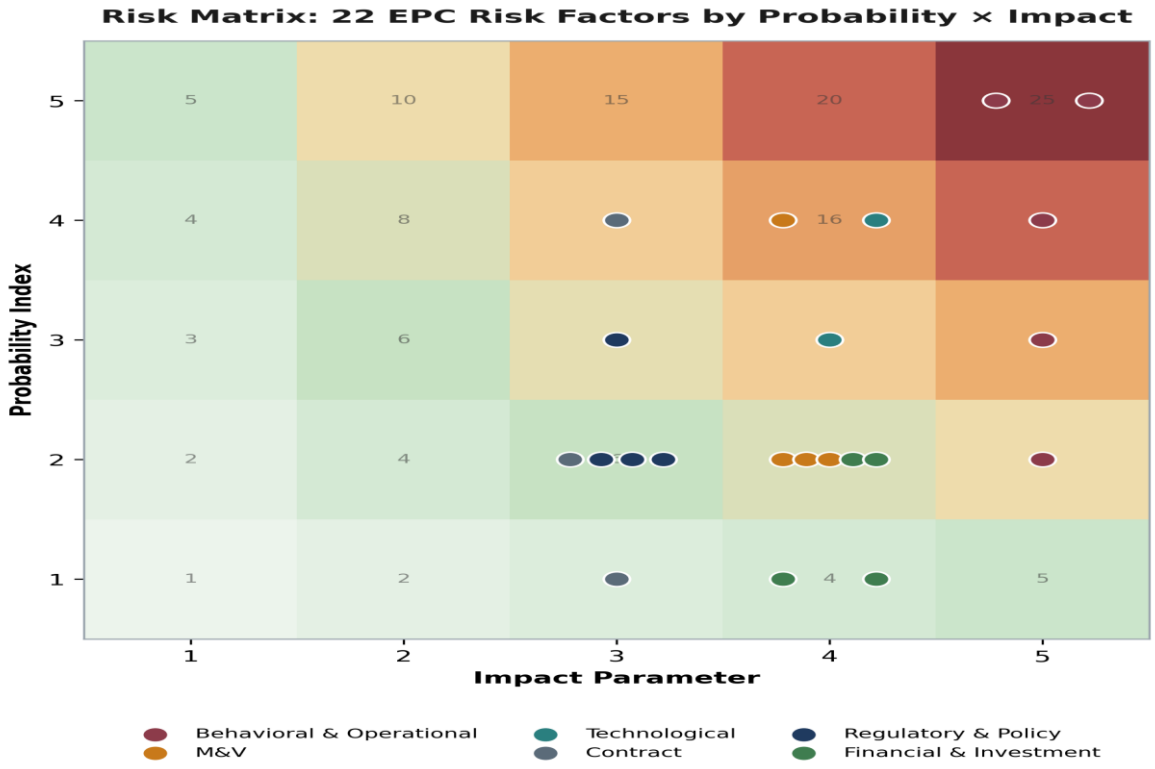
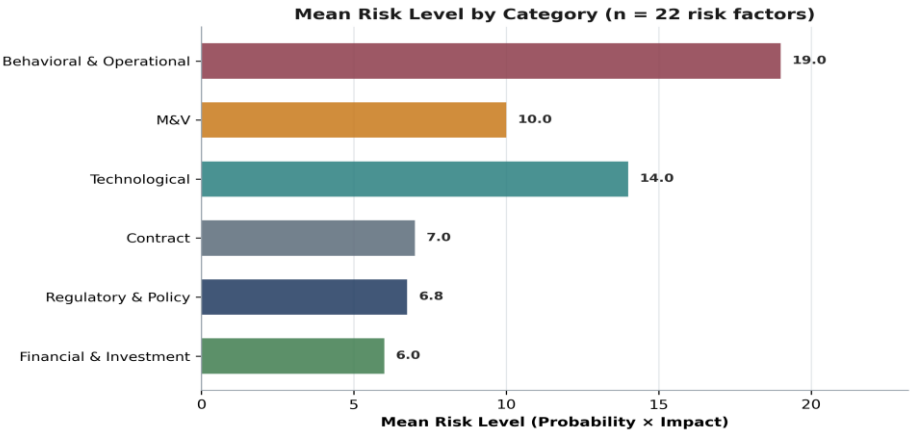


Figure 4. Risk matrix mapping the 22 identified risk factors to probability and impact scores (Risk Level = Probability Index × Impact Parameter).



Behavioural and operational risk emerged as the dominant threat category, with a mean risk level of 19.0 out of 25 — driven by "inadequate operation and maintenance" and "lack of qualified professionals," both scoring the maximum 25 (Probability 5 × Impact 5). Technological risk followed at 14.0, led by "poor equipment performance" (Probability 4 × Impact 4 = 16). M&V risk averaged 10.0, with "lack of competence in M&V and savings evaluation" scoring highest within the category (Probability 4 × Impact 4 = 16). Contract, regulatory/policy, and financial/investment risks scored consistently lower on average (7.0, 6.8, and 6.0 respectively), suggesting that, in the Malaysian polytechnic context, procedural and people-centred risks pose a materially greater threat to EPC delivery than financing or regulatory friction.

Figure 5. Mean risk level by category (n = 22 risk factors). Behavioural and operational risks carry the highest average risk level; financial and regulatory risks score lower on average.



Risk treatment strategies were derived directly from expert and practitioner interviews and mapped to each risk factor (Table 4, condensed). For the highest-scoring behavioural and operational risks, recommended treatments include appointing a full-time Energy Manager, formalising ESCO-owner cooperation, and establishing an effective EnMS and technical team. For M&V risk, recommended treatments centre on strengthening energy

monitoring systems, improving M&V competency, referencing recognised M&V standards (IPMVP), and applying simulation-based methods such as Monte Carlo simulation to make savings uncertainty auditable rather than a source of dispute.

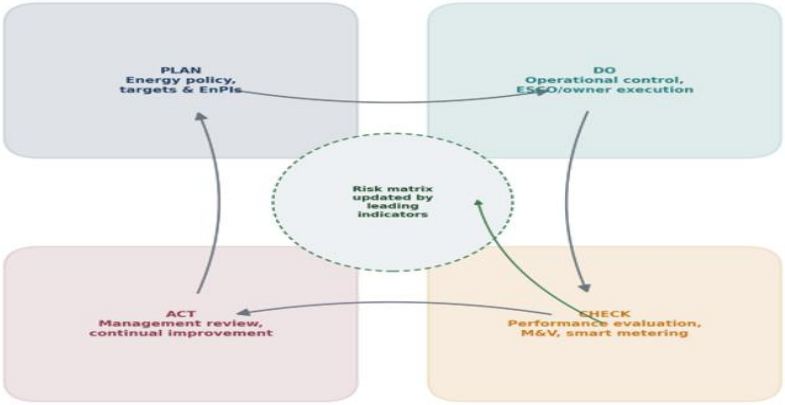
Table 4. Representative risk treatment strategies by category (condensed from full risk register).

Risk Category	Representative Mitigation Strategies
Behavioural & Operational	Assign full-time Energy Manager; strengthen ESCO–owner cooperation; establish effective EnMS and technical team; staff training and competitions to build engagement
M&V	Effective energy monitoring system; strengthen M&V competency; reference recognised M&V standards (IPMVP); apply Monte Carlo simulation for savings uncertainty
Technological	Factory Acceptance Testing; mutual ESCO–owner agreement on technology selection; authority recognition of new-technology designs
Contract	Clear contract terms on savings, M&V, and risk-sharing; legal/ministry briefings; standardised contract templates; owner participation in contract development
Regulatory & Policy	Government-certified ESCO competence; clear procurement guidance; ministry-level coordination committee; performance-based incentives
Financial & Investment	Energy Audit Conditional Grant (EACG); alternative financing (e.g., Malaysian Debt Venture); structured budget-application support

Energy Management System (EnMS)

The EnMS component operationalises continuous energy performance oversight through a Plan-Do-Check-Act cycle (Figure 6): energy policy, targets and Energy Performance Indicators (Plan); operational control and ESCO/owner execution (Do); performance evaluation via M&V and smart metering (Check); and management review driving continual improvement (Act). Within the integrated framework, the EnMS functions as the leading-indicator engine for the risk management system: anomalies detected during the Check stage — in load shape, plant efficiency, or equipment runtime — feed back into the governance-level risk matrix, allowing risk levels to be updated proactively rather than only after a savings shortfall is reported. Focus-group participants confirmed that EnMS had already been integrated into prior EPC projects and endorsed its inclusion as a formal framework component.

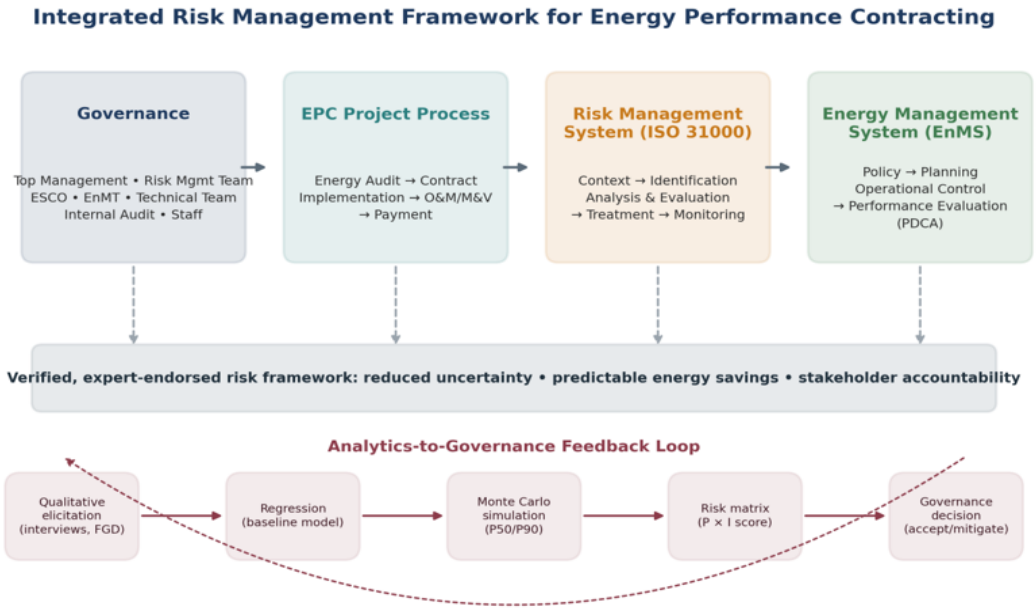
Figure 6. EnMS Plan-Do-Check-Act (PDCA) cycle integrated with EPC risk monitoring: anomalies from the Check stage feed as leading indicators into the governance risk matrix (Figure 4), enabling proactive rather than reactive risk response.



Integrated Framework

Figure 1 synthesises the four components into a single integrated risk management framework. Governance supplies accountability and decision rights; the EPC project process supplies the operational sequence within which risk materialises; the ISO 31000-aligned risk management system supplies a structured method for identifying, scoring, and treating risk; and the EnMS supplies continuous, auditable performance data that keeps the risk matrix current. The analytics-to-governance feedback loop — qualitative elicitation informing regression-based baseline modelling, which in turn informs Monte Carlo-based uncertainty quantification, which in turn updates the probability side of the risk matrix — closes the framework into what focus-group participants described as a practically usable, "living" control system rather than a static compliance document.

Figure 1. Integrated risk management framework linking governance, the EPC project process, an ISO 31000-aligned risk management system, and the Energy Management System (EnMS).



Expert Verification: Focus Group Discussion

The draft framework was presented to the five-member focus group described in Table 1 for structured validation. Participants unanimously agreed that the overall framework was comprehensive, with E02 recommending its extension across both government and private-sector EPC projects, and E03 noting the importance of accounting for building type in application. All four components — governance, EPC project process, risk management system, and EnMS — were judged "appropriate to be included in the framework." Governance and the EPC project process were confirmed as already present, in some form, in prior EPC projects, with E04 recommending the establishment of a dedicated energy management committee for each project. The risk management system attracted the most substantive feedback: E01 and E02 noted that risk management was only partially implemented in past EPC projects and recommended policy revisions and additional risk treatments, while E05 supported the identification of risk factors and categories from the expert interviews and suggested further expansion of the treatment library. The EnMS component was confirmed as consistent with prior practice and endorsed for formal inclusion. This convergence of independent expert judgement with the empirically derived framework structure constitutes the study's validation evidence.

DISCUSSION

Interpreting the Dominance of Behavioural and Operational Risk

The finding that behavioural and operational risk carries the highest mean risk level (19.0/25) — nearly double that of the next-ranked technological category (14.0) — reframes how EPC risk should be prioritised in the

Malaysian context. Much of the international literature foregrounds financial and technical risk as the primary barriers to EPC adoption (Alam et al., 2019; Piccinini et al., 2021); this study's evidence suggests that, once a guaranteed-savings project is underway in the Malaysian public education sector, the more consequential threat to delivery is organisational — staff capability, operations and maintenance discipline, and stakeholder engagement — rather than external financing or regulatory conditions. This is consistent with Razali (2017) and prior EPC human-capital findings (Berghorn & Syal, 2019a) but sharpens the point by quantifying the gap: financial and investment risk scored barely a third of the behavioural and operational average (6.0 versus 19.0). The practical implication is that ESCOs and building owners investing primarily in financial risk-sharing instruments while under-investing in energy-manager capability and O&M discipline are likely mis-targeting their risk mitigation budget.

Contribution Relative to Existing Frameworks

Compared with Berghorn and Syal's (2016) technical risk framework and Garbuzova-Schlifter and Madlener's (2017) AHP-based risk hierarchy, the framework developed here differs in scope rather than in method: where prior frameworks classify and rank risk, this framework embeds that classification within a four-component governance architecture — governance, process, risk management system, and EnMS — and closes the loop with an explicit analytics-to-governance feedback mechanism. This addresses Ruan, Gao and Mao's (2018) call for empirically validated risk frameworks: rather than a conceptual proposal, the framework reported here reflects the convergent judgement of practitioners directly involved in Malaysian EPC delivery, strengthening its claim to field readiness. The same limitation persists in the most current literature: Wan et al.'s (2023) incomplete-contract risk-allocation model, Tang et al.'s (2025) DEMATEL-ISM influence-path analysis, and Guo et al.'s (2025) cloud-matter-element ESCO early-warning model each advance a single analytical layer of EPC risk management with genuine methodological sophistication, but, like their predecessors, none embeds its output within a governance architecture that assigns organisational accountability and closes an analytics-to-decision loop. The integration of EnMS as a leading-indicator source for the risk matrix, rather than a parallel compliance activity, is, to the authors' knowledge, not explicitly modelled in prior EPC risk literature — including this most recent wave of studies — and represents this study's principal conceptual contribution.

Practical and Policy Implications

For ESCOs and building owners, the risk matrix (Figure 4, Figure 5) offers a prioritisation tool: behavioural and operational risk factors scoring 20 or above (difficult staff management, inadequate O&M, lack of qualified professionals) warrant immediate treatment planning and top-management escalation under the framework's own risk-level thresholds, ahead of lower-scoring financial or regulatory concerns. For policymakers, the focus group's recommendation to institutionalise a dedicated energy management committee per EPC project, together with the framework's governance layer, offers a template for the standardised risk-governance guidance that Ghazali et al. (2023) and Ludin et al. (2022) identify as currently lacking in Malaysian EPC regulation. More broadly, the framework's alignment with both ISO 31000 (risk management) and the ISO 50001/EnMS tradition positions it as compatible with existing international management-system certification pathways, potentially easing adoption by organisations already pursuing ISO certification.

Limitations

This study's evidence base is drawn from a single national market and a specific building typology — Malaysian public polytechnics under the guaranteed-savings EPC model — which constrains direct transferability to other EPC models (shared-savings, vendor financing) or building sectors without contextual adaptation. Risk probability and impact scores, while calibrated against coded qualitative frequency and documented severity, ultimately rest on expert and practitioner judgement rather than longitudinal loss data, and the cross-sectional design captures a snapshot of risk exposure rather than its evolution across the EPC contract lifecycle. The focus group that validated the framework, while professionally senior and diverse in scope, comprised five participants; a larger, multi-round Delphi-style validation would strengthen confidence in the framework's generalisability across project types and sectors.

Future Research

Future work should extend framework validation to shared-savings and vendor-financed EPC models and to non-educational building sectors, test the framework's analytics-to-governance loop with live regression and Monte Carlo simulation data over multiple contract years, and explore digital implementation — for example, a dashboard that operationalises Figure 1's feedback loop in real time using smart-metering data. Comparative cross-country validation would also help establish which elements of the framework are context-specific to Malaysia and which generalise to other emerging EPC markets.

CONCLUSION

This study developed and validated a comprehensive risk management framework for Energy Performance Contracting projects that integrates governance, the EPC project process, an ISO 31000:2018-aligned risk management system, and an Energy Management System. Using mixed-methods evidence from twenty-four Malaysian EPC stakeholders and an embedded polytechnic case study, the study identified six risk categories and twenty-two risk factors, quantified their relative severity through a probability-impact risk matrix, and found behavioural and operational risk to be the dominant threat to EPC delivery — well ahead of technological, M&V, contractual, regulatory, and financial risk. An independent focus group of five senior practitioners and academics validated the framework's comprehensiveness and all four of its components, while recommending dedicated project-level energy management committees and an expanded risk-treatment library. By closing the loop between qualitative risk evidence, quantitative risk scoring, and continuous EnMS-based monitoring, the framework offers ESCOs, building owners, and policymakers a practically validated, standards-aligned tool for prioritising risk mitigation investment and strengthening the governance foundations needed to scale EPC adoption in Malaysia and comparable emerging markets.

REFERENCES

1. Agenis-Nevers, M., Wang, Y., Dugachard, M., Salvazet, R., Becker, G., & Chenu, D. (2021). Measurement and Verification for multiple buildings: An innovative baseline model selection framework applied to real energy performance contracts. Energy and Buildings, 249, 111183.
2. Alam, M., Zou, P. X., Stewart, R. A., Bertone, E., Sahin, O., Buntine, C., & Marshall, C. (2019). Government championed strategies to overcome the barriers to public building energy efficiency retrofit projects. Sustainable Cities and Society, 44, 56–69.
3. Anton, S. G., & Nucu, A. E. A. (2020). Enterprise risk management: A literature review and agenda for future research. Journal of Risk and Financial Management, 13(11), 1–22.
4. Berghorn, G. H., & Syal, M. G. (2016). Risk framework for energy performance contracting building retrofits. Journal of Green Building, 11(2), 93–115.
5. Berghorn, G. H., & Syal, M. (2019a). Risk model for energy performance contracting in correctional facilities. Journal of Green Building, 14(2), 61–82.
6. Castillo, J. N., Resabala, V. F., Freire, L. O., & Corrales, B. P. (2022). Modeling and sensitivity analysis of the building energy consumption using the Monte Carlo method. Energy Reports, 8, 518–524.
7. Economidou, M., Todeschi, V., Bertoldi, P., D'Agostino, D., Zangheri, P., & Castellazzi, L. (2020). Review of 50 years of EU energy efficiency policies for buildings. Energy and Buildings, 225, 110322.
8. Feng, Z., Wu, X., Chen, H., Qin, Y., Zhang, L., & Skibniewski, M. J. (2022). An energy performance contracting parameter optimization method based on the response surface method: A case study of a metro in China. Energy, 248, 123612.
9. Frangou, M., Aryblia, M., Tournaki, S., & Tsoutsos, T. (2018). Renewable energy performance contracting in the tertiary sector: Standardization to overcome barriers in Greece. Renewable Energy, 125, 829–839.
10. Garbuzova-Schlifter, M., & Madlener, R. (2017). Risk analysis of energy performance contracting projects in Russia: An Analytic Hierarchy Process approach. Operations Research Proceedings 2015, 683–690.

11. Ghazali, F., Wan Zahari, W. M. Z., & Karim, R. (2023). Energy efficiency management towards sustainable development: The need for an energy efficiency legal framework. IIUM Law Journal, 31(2), 179–206.
12. Guo, H., Jia, S., Wang, M., & Zhang, Y. (2025). Construction and empirical analysis of ESCO risk early warning model for energy-saving retrofit project of existing buildings based on cloud matter element theory in China. Energies, 18(6), 1390.
13. Guo, K., & Zhang, L. (2020). Guarantee optimization in energy performance contracting with real option analysis. Journal of Cleaner Production, 258.
14. Hansen, S. J. (2006). Performance contracting: Expanding horizons.
15. Hashempour, N., Taherkhani, R., & Mahdikhani, M. (2020). Energy performance optimization of existing buildings: A literature review. Sustainable Cities and Society, 54, 101967.
16. International Organization for Standardization. (2018a). ISO 31000 risk management. https://www.iso.org/iso-31000-risk-management.html
17. International Organization for Standardization. (2018b). ISO 31000:2018 risk management — Principles and guidelines. ISO.
18. Kamenders, A., Kass, K., Biseniece, E., Lupkina, L., & Bazbauers, J. (2018). Quality management in energy performance contracting projects. Energy Procedia, 147, 636–640.
19. Kiger, M. E., & Varpio, L. (2020). Thematic analysis of qualitative data: AMEE Guide No. 131. Medical Teacher, 42(8), 846–854.
20. Ludin, N. A., Phoumin, H., Chachuli, F. S. M., & Hamid, N. H. (2022). Sustainable energy policy reform in Malaysia. In Revisiting electricity market reforms: Lessons for ASEAN and East Asia (pp. 251–281). Springer Nature Singapore.
21. Ow, P. (2023). ISO 31000 risk management process — Practical risk training. https://practicalrisktraining.com/iso31000
22. Piccinini, A., Hajdukiewicz, M., & Keane, M. M. (2021). A novel reduced order model technology framework to support the estimation of the energy savings in building retrofits. Energy and Buildings, 244, 110896.
23. Razali, N. S. (2017). Visual basic GUI for an improved M&V framework considering risk assessment. International Journal on Advanced Science, Engineering and Information Technology, 7(6), 2018–2026.
24. Ruan, H., Gao, X., & Mao, C. (2018). Empirical study on annual energy-saving performance of energy performance contracting in China. Sustainability, 10(5).
25. Tang, C., Yang, C., He, D., Xu, Y., Xiang, Y., & Hou, L. (2025). Analysis of risk factors and an influence path study of existing building energy performance contracting project based on the DEMATEL-ISM model. Environment, Development and Sustainability. Advance online publication. https://doi.org/10.1007/s10668-025-06478-9
26. Wan, S., Liu, Y., Ding, G., Runeson, G., & Er, M. (2023). Risk allocation for energy performance contract from the perspective of incomplete contract: A study of commercial buildings in China. International Journal of Climate Change Strategies and Management, 15(4), 457–478.
27. Wang, Z., Xu, G., Lin, R., Wang, H., & Ren, J. (2019). Energy performance contracting, risk factors, and policy implications: Identification and analysis of risks based on the best-worst network method. Energy, 170, 1–13.
28. Woolf, N. H., & Silver, C. (2017b). Qualitative analysis using NVivo. Routledge.
29. Wu, Y., & Zhou, J. (2019). Risk assessment of urban rooftop distributed PV in energy performance contracting (EPC) projects: An extended HFLTS-DEMATEL fuzzy synthetic evaluation analysis. Sustainable Cities and Society, 47.
30. Yang, E., Chen, C., Li, K., Guo, K., Hua, Y., & Zhang, L. (2025). Challenges and strategies for energy performance contracting: A critical review. Journal of Building Design and Environment, 3(1), 202510.
31. Zakaria, Z., Othman, M. N., Zainuddin, H., Rosdi, M. J., & Khallawi, A. R. (2024a). Systematic review of risks in Energy Performance Contracting (EPC) projects. Journal of Advanced Research in Applied Sciences and Engineering Technology, 48(2), 235–250.
32. Zakaria, Z., Othman, M. N., Zainuddin, H., Rosdi, M. J., Khallawi, A. R., & Adip, M. A. (2024b). Risks in Measurement and Verification (M&V) in Energy Performance Contracting (EPC) projects: A

systematic review. Journal of Advanced Research in Applied Sciences and Engineering Technology. Online first.

33. Zong, Q., & Liu, A. (2026). Research on risk assessment of energy saving renovation projects in hotel buildings under EMC mode. In Knowledge and Systems Sciences (KSS 2025), Communications in Computer and Information Science (Vol. 2731, pp. 250–267). Springer, Singapore.