Zuber's Healthcare Enterprise Risk Management Framework and Proposed Standards for Healthcare Governance

Zuber Mujeeb Shaikh
Corporate Executive Director of Quality, Patient Safety, Risk, Accreditations & Compliance
Dr. Sulaiman Al Habib Medical Services Group Company, Riyadh, Saudi Arabia.
ORCID ID: 0000-0002-1491-8379; Email: drzuber5@yahoo.co.in

Area/Section: Management.
Type of Paper: Conceptual Research.
Number of Peer Reviews: Two.
Type of Review: Peer Reviewed as pe |C|O|P|E| guidance.
Indexed in: OpenAIRE.
DOI: https://doi.org/10.5281/zenodo.23646773
Google Scholar Citation: PIJMESS

How to Cite this Paper:
Zuber Mujeeb Shaikh (2026). Zuber's Healthcare Enterprise Risk Management Framework and Proposed Standards for Healthcare Governance. *Poornaprajna International Journal of Management, Education & Social Science (PIJMESS), 3*(2), 589-604. DOI: https://doi.org/10.5281/zenodo.23646773

Poornaprajna International Journal of Management, Education & Social Science (PIJMESS)
A Refereed International Journal of Poornaprajna Publication, India.
ISSN: 3107-4626

Crossref DOI: https://doi.org/10.64818/PIJMESS.3107.4626.0078

Received on: 16/09/2026
Published on: 26/10/2026

© With Authors.

This work is licensed under a Creative Commons Attribution-Non-Commercial 4.0 International License, subject to proper citation to the publication source of the work.
Disclaimer: The scholarly papers as reviewed and published by Poornaprajna Publication (P.P.), India, are the views and opinions of their respective authors and are not the views or opinions of the PP. The PP disclaims of any harm or loss caused due to the published content to any party.

Zuber's Healthcare Enterprise Risk Management Framework and Proposed Standards for Healthcare Governance

Zuber Mujeeb Shaikh
Corporate Executive Director of Quality, Patient Safety, Risk, Accreditations & Compliance
Dr. Sulaiman Al Habib Medical Services Group Company, Riyadh, Saudi Arabia.
ORCID ID: 0000-0002-1491-8379; Email: drzuber5@yahoo.co.in

ABSTRACT

Purpose: *To develop Zuber's Healthcare Enterprise Risk Management (ZHERM) Framework as a healthcare governance architecture that connects enterprise risk oversight with clinical services, operational controls, patient experience, digital systems, and organizational continuity.*
Methodology: *Narrative synthesis and interpretive mapping were used to integrate published enterprise risk management, quality, patient safety, resilience, and governance sources. Sixteen operational domains were mapped to ASHRM's eight risk categories. The resulting architecture specifies governance responsibilities, evidence requirements, and priorities for prospective validation.*
Results/Analysis: *The framework comprises sixteen operational domains, a provisional ASHRM crosswalk, shared risk and assurance records, and a feedback process connecting assessment, controls, monitoring, and escalation. Comparison with established frameworks clarifies their complementary roles. The outputs are conceptual specifications; organizational effects and measurement properties remain to be evaluated.*
Originality/Value: *The proposed contribution is an operational decomposition of healthcare enterprise governance into explicit domain responsibilities and evidence requirements while retaining established ERM principles. Its feasibility, reliability, implementation burden, and effects require prospective evaluation.*
Type of Paper: *Conceptual framework-development paper with a proposed validation protocol.*
Keywords: Healthcare enterprise risk management; ZHERM; healthcare governance; patient safety; organizational resilience; digital governance; business continuity; risk assurance.

1. INTRODUCTION :

Healthcare organizations must coordinate risks arising from clinical care, workforce capacity, financing, information systems, infrastructure, regulation, and service continuity. A failure can propagate across these functions: an information-system outage, for example, may affect medication administration, diagnostic reporting, billing, and patient communication. Enterprise risk management provides a structure for discussing such dependencies, assigning responsibility, and reviewing exposures against organizational objectives [1, 2, 8, 13, 21].
Patient safety literature complements ERM by examining systems failures, organizational defenses, incident learning, and the conditions that support safe care [12, 18, 27, 39]. However, the existence of separate quality, compliance, finance, and technology programs does not establish that their information is coordinated effectively. The practical problem addressed here is how to organize their responsibilities and shared evidence within a common governance architecture.
ISO 31000 and COSO provide transferable risk-management principles, while ASHRM supplies a healthcare-specific ERM taxonomy [1, 2, 8, 13]. ZHERM translates these contributions into sixteen operational domains intended to clarify responsibilities and interfaces. The domains are organizational subdivisions rather than statistically independent risk constructs.
The term "standards" denotes the author's proposed governance requirements. These requirements are not accreditation standards, statutory obligations, or evidence of endorsement by ASHRM, ISO, COSO,

WHO, or accreditation bodies. Implementation must use the applicable laws, accreditation editions, professional guidance, and manufacturer instructions. Potential improvements in safety, resilience, or efficiency remain hypotheses to be tested.

2. OBJECTIVES :

(1) Synthesize selected literature on healthcare ERM, patient safety, quality, resilience, and governance.
(2) Define sixteen operational governance domains and make their relationships to ASHRM's eight categories explicit.
(3) Specify responsibility, control, evidence, monitoring, and escalation requirements for the proposed domains.
(4) Clarify how digital governance, patient involvement, organizational learning, and continuity operate across domain boundaries.
(5) Develop a prospective evaluation agenda for content relevance, reproducibility, feasibility, and organizational outcomes.

3. REVIEW OF LITERATURE AND CONCEPTUAL FOUNDATIONS :

3.1 Enterprise risk oversight and organizational accountability:

ISO 31000 describes a risk-management process linked to organizational context and objectives. COSO integrates ERM with strategy and performance. ASHRM adapts enterprise risk oversight to healthcare through operational, clinical/patient safety, strategic, financial, human capital, legal/regulatory, technology, and hazard categories [1, 2, 8, 13]. Their scopes overlap, but their purposes differ: a generic risk process, a strategic governance framework, and a healthcare risk taxonomy are complementary tools rather than competing measurement instruments.

Kaplan and Mikes emphasize risk dialogue and management judgment, supporting the use of quantitative information within accountable governance decisions [16]. Literature on board oversight and management responsibilities informs escalation, assurance, and resource allocation [6, 9, 21]. These principles provide the basis for ZHERM's proposed accountability arrangements.

3.2 Quality, systems safety, and high reliability:

Donabedian's quality-assurance synthesis distinguishes structure, process, and outcome measures [10]. In ZHERM, this distinction prevents a documented policy or completed training program from being presented as evidence that patient harm has decreased. The Institute of Medicine report, Reason's systems model, clinical risk-management studies, and Leveson's systems approach inform attention to interacting organizational conditions and controls [4, 12, 19, 27, 39, 41].

Safety-I examines failures and defenses, while Safety-II examines how work succeeds through adaptation. High-reliability literature emphasizes attention to failure, operational awareness, careful interpretation, resilience, and expertise [7, 11, 40]. ZHERM uses these perspectives as design principles. A domain checklist or governance score cannot establish that an organization is a high-reliability organization.

3.3 Workforce culture, patient partnership, and value:

Workforce capability, reporting culture, teamwork, and leadership are relevant to the operation of safety controls [14, 26, 28, 29]. Safety-culture questionnaires require appropriate interpretation and cannot alone demonstrate safe clinical performance. Patient partnership and integrated people-centred services inform consent, communication, equity, and participation in governance [3, 20, 23, 42]. Value-based care and quality strategy connect organizational performance with outcomes and resource use [5, 25].

3.4 Digital governance and continuity:

Cybersecurity governance addresses organizational responsibilities and technology-related exposures; it is not limited to purchasing technical security tools [22]. AI-enabled functions additionally require a defined intended use, evaluation of model performance, human oversight, monitoring, and a response to failure or drift [51]. A predictive dashboard must estimate a defined future event over a stated horizon; a current compliance score is not itself a validated prediction.

The pandemic-related literature provides context for service coordination and adaptive capacity [24]. Continuity planning requires defined critical activities, recovery requirements, dependencies, exercises, and follow-up [52]. Accreditation resources establish applicable institutional expectations [15, 38]; their existence does not demonstrate compliance or authorize an unverified standard-by-standard crosswalk.

3.5 Author-developed contributions and source boundaries:

The author's prior work contributes contextual examples of person-centred clinical governance, patient experience, pandemic preparedness, and the proposed Safety-III predictive-safety extension [34, 35, 36, 37]. Safety-III is used here in the sense defined in that publication, not as an internationally standardized replacement for Safety-I or Safety-II. These publications inform conceptual design and do not independently validate ZHERM.

The endoscopy FMEA and hand-hygiene studies provide examples of procedural risk and implementation context; electricity consumption and accreditation-related patient experience provide examples of resource use and patient-facing evaluation [30, 31, 32, 33]. Khan's literature review is relevant to accreditation and satisfaction, but those outcomes should not be equated with reduced harm [17].

The cost-of-quality, balanced-scorecard, and post-accreditation frameworks provide related approaches to performance oversight, strategy, and sustained compliance [44, 45, 46]. Earlier laboratory, blood-bank, demographic, economic, and health-resource studies illustrate indicator-based comparison [47, 48, 49, 50]. These studies provide measurement and implementation examples; their findings do not establish the performance of the proposed ZHERM architecture.

Table 1: Conceptual source roles and limits of inference

Source group	Role in ZHERM	Limit
ERM guidance [1, 2, 8, 13]	Risk process, taxonomy, strategic oversight	Does not establish ZHERM validity or endorsement.
Quality and systems safety [10, 12, 19, 27]	Separate structures, processes, outcomes and controls	Source validity is not inherited by a new framework.
High reliability and resilience [7, 11, 40]	Attention to operations, adaptation and learning	Checklist completion does not certify reliability.
Culture and partnership [20, 26, 28, 42]	Workforce participation and patient involvement	Requires appropriate instruments and local evaluation.
Digital and continuity guidance [22, 51, 52]	Cybersecurity, model oversight and recovery	Operational compliance and predictive validity are distinct.
Author-developed models [34, 36, 37, 44, 45, 46]	Healthcare-specific design precedents	Self-citations provide context, not independent validation.

4. MATERIALS AND METHODS :

4.1 Study design and evidentiary status:

This is a conceptual framework-development study using narrative synthesis and interpretive mapping. The outputs are domain definitions, proposed governance requirements, a comparison of intended framework roles, and a prospective validation plan. No hospital sample, assessor dataset, patient-level observations, or statistical results are analyzed in this paper. The proposed requirements are therefore design specifications rather than empirically demonstrated standards.

4.2 Source selection and review boundaries:

The source corpus comprises selected peer-reviewed publications, books, professional frameworks, institutional reports, and authoritative guidance on healthcare risk, quality, safety, governance, resilience, and digital systems. It includes publications from 1995–2026 and relevant foundational works. Sources were selected for conceptual relevance rather than through a reproducible systematic search. The synthesis therefore provides an interpretive basis for framework development, without claiming exhaustive coverage or pooled estimates of effectiveness.

Relevant English-language sources were considered for their contribution to organizational governance, risk processes, clinical safety, workforce capability, patient partnership, technology, or continuity. Non-healthcare sources were included where principles were transferable. Duplicate publications were

consolidated. Source quality and applicability require separate judgment: an institutional standard, an empirical study, and an author-developed conceptual model do not provide equivalent evidence for effectiveness.

4.3 Framework-development logic:

The development logic consists of eight linked steps: defining the coordination problem; identifying relevant sources; assessing their relevance; organizing governance concepts; mapping concepts to established risk categories; specifying sixteen operational domains; defining shared responsibility and evidence requirements; and identifying validation priorities. This author-led process uses interpretive synthesis; independent coding and formal consensus procedures were not part of the reported conceptual analysis.

Concepts were organized by their primary governance function. Related activities were grouped without assuming that the resulting domains are statistically independent. For example, infection control and medication safety have distinct operational owners but share clinical/patient safety exposures. Digital systems, environmental sustainability, and resilience can affect several domains and are treated as cross-domain responsibilities rather than additional numbered domains.

4.4 Domain mapping and boundaries:

The canonical sixteen-domain list is presented in Table 2. Medical insurance has a distinct operational scope; crisis management and business continuity are combined because preparedness, response and recovery share core dependencies. The ASHRM crosswalk is an author-proposed operational mapping, not an ASHRM-approved modification of its taxonomy. Each risk record receives one primary domain and may have secondary links. A shared event must not be counted repeatedly in an enterprise event total.

4.5 Proposed requirements and evidence:

Each domain should identify its purpose, accountable owner, relevant hazards, controls, verification evidence, monitoring measures, and escalation route. A requirement is considered implemented only when evidence demonstrates its operation over a defined review period. Document availability, control execution, and control effectiveness should be distinguished. Locally applicable statutes and professional requirements take precedence over generic proposals.

Specific reporting intervals, thresholds, samples, and risk criteria should be approved before assessment. Quarterly board reporting is proposed as a routine cadence, supplemented by urgent escalation outside that cycle. It is not presented as a universal legal requirement. A digital platform may enforce required fields, but this does not establish completeness of case ascertainment or accuracy of submitted data.

4.6 Measurement and analysis boundaries:

Governance assessment concerns evidence of controls and responsibilities. Residual risk concerns the remaining exposure after treatment. Clinical performance concerns observed outcomes under specified definitions. These quantities should be reported separately. This paper does not propose a validated composite score, statistically estimated weights, maturity cutoffs, or organizational ranking scheme for ZHERM.

If a likelihood–consequence matrix is used, definitions and escalation criteria should be established locally. Matrix products are ordinal prioritization aids rather than probabilities or expected financial losses; they should not be averaged across unrelated hazards as though they were interval measurements. Critical safety or statutory exceptions require escalation regardless of favorable scores elsewhere.

4.7 Prospective validation strategy:

A prospective protocol should assess content relevance, domain boundaries, assessor reproducibility, implementation burden, and relationships with independently measured organizational outcomes. Expert participants should include clinical, nursing, quality, risk, finance, workforce, technology, facilities, ethics, and patient representatives. Panel selection, conflicts of interest, rating instructions,

consensus thresholds, and stopping rules should be prespecified. Any Delphi consensus percentage is a protocol decision, not an observed result in this paper.

Pilot assessment should use trained assessors independently reviewing the same evidence before adjudication. Nominal domain assignments require a suitable unweighted agreement coefficient; ordinal ratings may use weighted kappa with prespecified weights. If continuous scores are subsequently defined, the intraclass correlation model should specify the assessor design, absolute agreement or consistency, and single-rating or average-rating interpretation [53]. Report estimates with 95% confidence intervals, raw agreement, category frequencies, and assessment conditions; reliability and agreement reporting should follow GRRAS [54]. Internal consistency should not be treated as a default validation criterion for a formative set of distinct governance responsibilities.

Evaluation should establish feasibility and reproducibility across organizations before examining outcome associations. Repeated observations may be nested within departments and hospitals; analyses should address clustering, exposure, case mix, and secular change. The protocol should distinguish missing, invalid, not-applicable, and zero-denominator observations, report their frequency and reasons, and prohibit coding unavailable observations as successful performance. Imputation, if justified, should follow prespecified assumptions and sensitivity analyses. Table 5 summarizes the proposed evaluation agenda.

4.8 Ethical and organizational permissions:

This conceptual paper presents published sources and proposed requirements without reporting identifiable participants or organizational datasets. Future expert assessment or implementation research requires an appropriate ethics determination and organizational permission before recruitment or data use, where applicable. Anonymizing an organization does not replace ethics review, an exemption decision, data-access authorization, or privacy safeguards. Approval or exemption identifiers should be reported only when documented.

4.9 Methodological limitations:

The narrative source selection is vulnerable to selection and interpretation bias. Search reproducibility, independent extraction, and formal evidence grading are not established. Domain construction is author-led, and self-cited examples require independent evaluation. Some governance activities overlap, national requirements differ, and digital risks evolve. The framework's feasibility, measurement properties, incremental value, and effects therefore remain uncertain.

5. RESULTS AND DISCUSSION :

5.1 Design output and the sixteen-domain architecture:

The design output connects leadership decisions with domain-level control implementation and shared evidence. Leadership defines objectives, risk appetite, accountability, and escalation criteria; domain teams implement and verify controls; shared records link risks, incidents, indicators, and actions; governance review directs treatment and follow-up. Figure 1 depicts this feedback process. Table 2 presents the sixteen domains and their provisional ASHRM mappings.

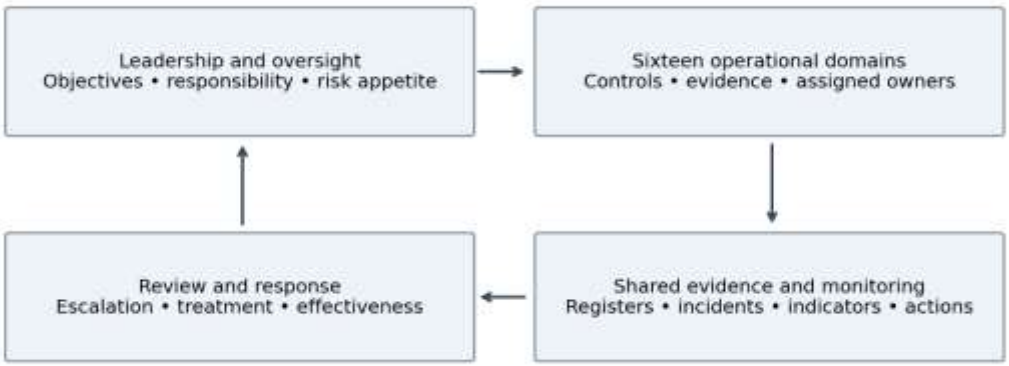


Fig. 1: Proposed ZHERM governance and evidence feedback architecture

Table 2: Canonical ZHERM domains and proposed ASHRM crosswalk

No. and ZHERM domain	Primary ASHRM category	Secondary interfaces
1. Strategic risks	Strategic	Operational; legal/regulatory
2. Legal, regulatory and compliance risks	Legal/regulatory	Strategic; clinical/patient safety
3. Operational risks	Operational	Human capital; technology; hazard
4. Financial risks	Financial	Strategic; operational
5. Supply chain management risks	Operational	Financial; clinical/patient safety
6. Information technology and communication risks	Technology	Legal/regulatory; operational
7. Medical insurance risks	Financial	Legal/regulatory; operational
8. Human capital, education and training risks	Human capital	Clinical/patient safety; operational
9. Safe environment and clinical engineering risks	Hazard	Technology; operational
10. Person-centred care and patient experience risks	Clinical/patient safety	Strategic; legal/regulatory
11. Infection prevention and control risks	Clinical/patient safety	Hazard; operational
12. Patient and medication safety risks	Clinical/patient safety	Operational; technology
13. Clinical research and ethical risks	Legal/regulatory	Clinical/patient safety; strategic
14. Quality, performance improvement and risk management risks	Operational	Clinical/patient safety; strategic
15. Marketing management and reputation risks	Strategic	Legal/regulatory; operational
16. Crisis and business continuity management risks	Operational	Hazard; technology; human capital

Table 2 assigns a primary category for record organization; it does not restrict a risk's consequences to one category. Sustainability is addressed through strategy, finance, procurement, facilities and continuity. Resilience and learning span all domains. Cybersecurity and AI governance are operationalized within Domain 6, with clinical and legal interfaces. These cross-cutting functions do not change the sixteen-domain count.

5.2 Proposed domain requirements:

The requirements below are operational specifications for local adaptation. The accountable roles are proposed functions rather than mandatory job titles. A single organization may assign one function to several people or combine functions, provided decision authority, competence and independent assurance remain clear. Domain oversight includes control ownership, evidence review, and escalation. ASHRM interfaces are listed in Table 2.

5.2.1 Strategic risks:

Accountability: Board and executive leadership.

Proposed requirements: Align objectives, risk appetite, service scope, resource allocation and delegated authority. Review ethics, conflicts of interest, competitive and regulatory changes, population needs, organizational structure, communication routes, policy control and committee accountability. Departmental plans should connect to enterprise priorities; clinical pathways, transport and out-of-hours services require operational owners rather than duplicate strategic risk records.

Assessment evidence: Approved strategy, delegated authorities, committee terms of reference, board risk decisions and follow-up records. Review unresolved enterprise actions and changes in strategic assumptions.

5.2.2 Legal, regulatory and compliance risks:

Accountability: Legal counsel and compliance leadership.
Proposed requirements: Maintain an obligations register with applicable law, regulator, accreditation edition, owner and evidence requirement. Assess changes, permissions, litigation exposures, confidentiality and contractual obligations. Verify corrective-action closure and distinguish accreditation readiness from demonstrated compliance.
Assessment evidence: Current obligations register, approvals, legal reviews, policy versions and verified closure evidence. Monitor overdue regulatory actions and material exceptions.

5.2.3 Operational risks:

Accountability: Operations leadership and service managers.
Proposed requirements: Coordinate patient flow, capacity, bed management, referral and consultation, transport, internal and external transfers, and service handovers. Address emergency codes, staffing disruption, technology failure, and approved downtime procedures. Maintain clear handover and escalation arrangements during out-of-hours service delivery and authorized patient leave.
Assessment evidence: Service plans, flow records, handover and transfer audits, downtime tests and disruption logs. Monitor delays and service interruptions using defined populations and exposure.

5.2.4 Financial risks:

Accountability: Finance leadership.
Proposed requirements: Review capital and operating budgets, cash flow, reimbursement changes, revenue-cycle integrity, alternative payment arrangements, utilization and resource decisions. Assess value using outcomes and costs together. Cost-of-quality and balanced-scorecard models may support oversight, but their scores are separate from residual risk [25, 44, 45].
Assessment evidence: Budget and variance reviews, revenue controls, contract analyses and resource-use evidence. Monitor financial exposures without interpreting a lower cost as proof of better care.

5.2.5 Supply chain management risks:

Accountability: Procurement, pharmacy and supply-chain leadership.
Proposed requirements: Manage pharmaceutical, equipment and consumable availability; supplier and third-party dependencies; cold-chain conditions; traceability; recalls; damaged stock; and expired products. Use shortage contingencies and verify supplier performance. Clinical engineering owns equipment performance, while the supply-chain owner retains procurement and availability controls.
Assessment evidence: Supplier assessments, temperature records, inventory and expiry controls, recall traceability and shortage plans. Monitor stockouts, wastage and cold-chain excursions with corrective-action verification.

5.2.6 Information technology and communication risks:

Accountability: Information technology, information security and information-governance leadership.
Proposed requirements: Protect information confidentiality, integrity and availability; access and release controls; retention; backups; recovery; and electronic or scanned records. Maintain data definitions and permitted abbreviations. Test planned and unplanned downtime, interoperability, communication routes and staff training. Digital and AI functions require intended-use approval, performance evaluation, human oversight and change control [22, 51].
Assessment evidence: Access reviews, security assessments, restoration tests, downtime records, data-quality checks and model-monitoring records. Monitor availability, privacy events and control exceptions; distinguish prediction accuracy from dashboard use.

5.2.7 Medical insurance risks:

Accountability: Insurance, revenue-cycle and legal leadership.
Proposed requirements: Assess professional liability and cybersecurity coverage, exclusions, limits, renewal and claims arrangements. Also review payer authorization, reimbursement disputes, fraud and abuse where relevant. Insurance transfers specified financial consequences; it does not remove the obligation to prevent harm or maintain effective controls.

Assessment evidence: Coverage and renewal reviews, claim records, payer contracts, authorization checks and fraud controls. Monitor uncovered exposures and disputed claims with legal and finance review.

5.2.8 Human capital, education and training risks:

Accountability: Human resources, medical and nursing leadership.
Proposed requirements: Maintain staffing plans, personnel records, orientation, role assignment, credentialing, clinical privileges and competency assessment. Use ongoing and focused professional practice evaluation where applicable. Coordinate education needs, continuing professional development, appraisals, retention, staff engagement and support, rights, complaints, employee health, burnout and workplace-violence prevention. Plan workforce contingencies for disasters and epidemics.
Assessment evidence: Staffing and credential records, competency observations, privilege decisions, training evaluations and workforce surveys. Attendance alone is not evidence of competence; recreational and recognition programs are supportive measures, not substitutes for safe staffing.

5.2.9 Safe environment and clinical engineering risks:

Accountability: Facilities, safety and clinical-engineering leadership.
Proposed requirements: Coordinate facility access, building and fire safety, security, smoke-free environments, radiation and laser safety, hazardous materials, biological and general waste, medical gases, utilities and equipment. Address construction, renovation and demolition; heating, ventilation and air conditioning; potable water; sewage; electrical systems and emergency power. Use environmental rounds, service testing and internal/external disaster interfaces.
Assessment evidence: Facility assessments, maintenance and equipment records, environmental and utility tests, safety-round findings and corrective actions. Assess resource conservation without compromising ventilation, sterilization, cold-chain or other critical requirements.

5.2.10 Person-centred care and patient experience risks:

Accountability: Patient-experience and clinical leadership.
Proposed requirements: Support patient and family rights, accessible communication, engagement, education, shared decisions and appropriate disclosure. Distinguish general consent, informed consent, research consent and authorization to release information. Review complaints and departures against medical advice, leaving without being seen and transitions of care. Use suitable experience instruments and responsible publication of aggregate data [20, 34, 36, 42].
Assessment evidence: Consent and disclosure audits, patient-partnership records, complaints and instrument documentation. Monitor communication failures and experience measures separately from clinical harm outcomes.

5.2.11 Infection prevention and control risks:

Accountability: Infection prevention and control leadership.
Proposed requirements: Maintain infection surveillance, isolation, personal protective equipment, environmental cleaning and validated decontamination or sterilization processes. Assess construction-related infection risk and preparedness for transmissible disease surges. Address antimicrobial resistance and local antibiograms with stewardship teams. Reprocessing or reuse of single-use items is not presumed permissible: applicable law, authorization, manufacturer instructions and validated safety requirements govern decisions [33, 35].
Assessment evidence: Surveillance definitions, reprocessing records, environmental audits, isolation assessments and surge plans. Monitor infection outcomes with exposure denominators and evaluate changes in ascertainment before attributing improvement.

5.2.12 Patient and medication safety risks:

Accountability: Clinical, nursing and pharmacy leadership.
Proposed requirements: Address identification, diagnostic processes, clinical guidelines, procedural safety, alarms, infusion devices, and tubing connections. Control high-alert, look-alike/sound-alike, hazardous, emergency, and controlled medicines; shortages; refrigerated and frozen storage; nutrition products; recalls; sterile compounding; stability; and compatibility. Coordinate antimicrobial

stewardship, clinical audit, test-result follow-up, and safe transitions. Incident investigation should examine system conditions and human factors, with fair and proportionate accountability rather than automatic attribution to individual error [18, 27, 32].

Assessment evidence: Clinical and medication audits, storage and compounding records, recalls, incident investigations and follow-up evidence. Monitor harm with validated definitions; more reported near misses may reflect improved reporting rather than increased harm.

5.2.13 Clinical research and ethical risks:

Accountability: Research governance and clinical-ethics leadership.

Proposed requirements: Maintain independent research review, informed consent, participant protection, data integrity and safeguards for vulnerable populations. Provide clinical ethics consultation for end-of-life decisions, transplantation and competing values or beliefs. Patient education and respect for cultural or religious preferences operate within applicable law and professional responsibilities.

Assessment evidence: Ethics decisions, consent records, protocol and data checks, participant-safety reports and documented clinical-ethics consultations. Clinical consent does not replace research authorization.

5.2.14 Quality, performance improvement and risk management risks:

Accountability: Quality and risk-management leadership.

Proposed requirements: Coordinate quality, safety and risk plans; indicator definitions; sampling; data validation; incident learning; safety-culture assessment; patient participation; and governance reporting. Maintain clear links to workforce safety and domain owners. Distinguish an incident report, a verified event and an exposure-adjusted outcome. Use clinical investigation and improvement methods appropriate to the problem [10, 26, 28, 43].

Assessment evidence: Indicator dictionaries, validation and sampling records, risk registers, incident analyses and improvement-effectiveness reviews. Monitor action closure and verified control function, not documentation completion alone.

5.2.15 Marketing management and reputation risks:

Accountability: Communications and marketing leadership.

Proposed requirements: Ensure truthful service descriptions, responsible claims, consent for identifiable patient information, and compliance with advertising requirements. Coordinate reputation monitoring, public communication, health-promotion activities and crisis messaging. Patient-experience teams own individual complaint resolution; communications teams manage enterprise reputational consequences and public responses.

Assessment evidence: Approved communication material, consent and review records, complaint escalation and reputation-response logs. Public visibility or positive publicity does not establish clinical quality.

5.2.16 Crisis and business continuity management risks:

Accountability: Emergency preparedness and continuity leadership.

Proposed requirements: Integrate hazard assessment, incident command, critical-service priorities, recovery arrangements and tested communications. Address disasters, outbreaks, cyber incidents, supply-chain resilience, surge capacity, workforce contingencies and restoration of information systems and utilities. Exercises should test coordination and recovery, identify deficiencies, and verify subsequent corrections [24, 52].

Assessment evidence: Business-impact analyses, response and recovery plans, exercise reports, recovery tests, and verified follow-up actions. Review restoration against defined recovery objectives and unresolved dependencies affecting critical services.

5.3 Comparison with established frameworks:

Table 3 compares the intended roles of established frameworks and ZHERM. This interpretive comparison concerns governance scope and operational specification rather than comparative effectiveness. ISO 31000 and COSO are applicable to clinical, digital, and sustainability risks, while

ASHRM includes technology and hazard categories. ZHERM's proposed contribution is to specify operational responsibilities and coordinate evidence across these established categories.

Table 3: Framework roles and proposed ZHERM contribution

Framework	Established or proposed role	Interpretation boundary
ISO 31000 [13]	General principles, framework and process for managing risk	Healthcare operational detail must be specified locally; broad applicability is not a deficiency.
COSO ERM [8]	Governance, strategy, performance and risk oversight	Does not prescribe a healthcare-specific checklist; remains applicable to healthcare strategy.
ASHRM ERM [1, 2]	Healthcare-specific taxonomy and implementation guidance	Includes eight risk domains; the sixteen-domain crosswalk is the author's subdivision.
ZHERM	Proposed operational domains, responsibility interfaces and shared evidence requirements	Implementation feasibility, incremental benefit and outcome effects have not been established.

5.4 Risk records, indicators and escalation:

A shared register should describe the risk as a cause, event and consequence, rather than as a department name or a generic topic. Records should link to existing incident, audit, continuity and improvement systems. Assigning a unique identifier, primary domain and owner supports traceability across those systems without creating duplicate events.

Table 4: Minimum proposed risk and assurance record

Field	Required specification
Identity and scope	Unique risk ID, service, location, assessment date, primary domain and secondary links.
Risk statement	Cause or source, potential event, consequence, affected population and relevant dependencies.
Ownership	Accountable decision-maker, control owner, reviewer and escalation authority.
Context and obligations	Objectives, risk criteria, applicable regulation and exact accreditation requirement where used.
Assessment	Likelihood and consequence definitions, time horizon, exposure, uncertainty and inherent/residual status.
Controls	Existing preventive, detective and recovery controls; design and operating-effectiveness evidence.
Monitoring measure	KPI or KRI definition, direction, unit, inclusion/exclusion, numerator/denominator if relevant, frequency and collection source.
Targets and thresholds	Approved target, escalation trigger, effective date and benchmark source; separate internal targets from external benchmarks.
Data quality	Validation method, completeness checks, missing/invalid/not-applicable flags and zero-denominator handling.
Treatment	Selected response, action, owner, resources, due date, expected control change and approval.
Review	Current exposure, overdue actions, critical exceptions, verified effectiveness and next review date.
Closure and retention	Closure authority, evidence, unresolved dependencies, reassessment decision and record version.

A KPI measures defined performance, whereas a key risk indicator (KRI) signals exposure or a control weakness; the same metric may serve both purposes only when its interpretation is explicit. Rates require an eligible exposure denominator. A zero denominator is not a zero event rate or successful

performance. Benchmarking requires comparable definitions, populations, case mix, exposure and ascertainment.

Escalation should follow consequence, urgency, statutory duties and control failure, with a named decision-maker. Routine domain review may feed quarterly enterprise reporting, but critical patient-safety conditions and major service disruptions need immediate action. Closure requires verification that the intended control change occurred and a reassessment of residual exposure, not merely an uploaded action plan.

5.5 Implementation and assurance:

Implementation should begin with a baseline inventory of existing committees, registers, policies and indicators. Organizations should identify shared records and assign primary owners before creating additional forms. A limited pilot can evaluate whether the architecture reduces unresolved ownership and improves decision traceability without increasing documentation burden.

Governance reporting should retain domain profiles and critical exceptions. Service managers own operational controls; specialist functions support interpretation and challenge; an appropriately independent assurance function tests whether controls operate as intended. Reporting to leadership does not replace frontline competence or local response. Patient and staff participation should be built into review of relevant policies, experiences and risks.

A digital platform can support record linkage, version control, due-date tracking, access permissions and dashboards. The platform is an implementation mechanism, not evidence that the framework is valid. Predictive functions require independent evaluation of calibration, discrimination, false alerts, subgroup performance and practical response usefulness before clinical or organizational benefit is claimed [51].

5.6 Scientific contribution and testable propositions:

The proposed contribution is a healthcare operational taxonomy connected to a shared governance process. The sixteen domains make responsibilities visible, while secondary interfaces acknowledge interdependence. This organization can be evaluated against existing local governance arrangements instead of assuming that broader coverage necessarily produces safer care.

Testable propositions include improved agreement on risk ownership, reduced duplicate records, more timely escalation, better traceability of control evidence, and lower administrative burden after integration. Subsequent studies may examine independently measured safety or continuity outcomes, while accounting for implementation fidelity and contextual changes. Such propositions do not imply causal effects from the present conceptual analysis.

5.7 Prospective evaluation and research priorities:

Table 5: Proposed validation questions and methods

Evaluation question	Suitable prospective approach	Required reporting
Content and boundaries	Independent multidisciplinary review; modified Delphi if justified.	Panel composition, conflicts, rounds, consensus rules and changes.
Domain assignment	Independent mapping of shared risks and scenarios.	Agreement, ambiguous cases, primary/secondary assignment and adjudication.
Assessment reproducibility	Independent review of the same evidence; nominal or ordinal agreement methods as appropriate [54].	Model choice, confidence intervals, agreement thresholds and assessor training.
Continuous scores, if later developed	Prespecified scoring study with an intraclass correlation model matched to the assessor design [53].	Score definitions, variance components, uncertainty and missingness rules.
Implementation feasibility	Pilot in different services and organizations.	Time, cost, usability, completeness, fidelity and unintended workload.

Evaluation question	Suitable prospective approach	Required reporting
Incremental governance benefit	Compare baseline and implementation periods using an appropriate design.	Ownership disputes, duplicate records, escalation delay and verified control closure.
Organizational outcomes	Exposure-adjusted longitudinal or comparative evaluation.	Case mix, clustering, secular trends, effect estimates and confidence intervals.
Predictive functions	Separate development and independent temporal/external evaluation.	Intended event and horizon, calibration, discrimination, alerts and response usefulness.

Table 5 outlines an evaluation sequence from content review to independent outcome assessment. Sample size should be justified by the primary endpoint, desired precision, and clustering. Protocols should prespecify estimands, analysis populations, handling of missing observations, and sensitivity analyses. Where hypothesis testing is appropriate, report effect estimates and confidence intervals alongside exact p-values. Practical relevance and potential harms should inform interpretation.

5.8 Limitations and applicability:

ZHERM is a conceptual governance framework whose feasibility and measurement properties require evaluation. Its domain boundaries need independent assessment, and an extensive checklist may increase workload when it duplicates existing systems. Application in hospitals, ambulatory services, and other settings will require adaptation to service scope, staffing, and available evidence. National law and accreditation requirements further constrain transferability.

The narrative synthesis is susceptible to source-selection and interpretation bias. The framework has not been compared prospectively with existing governance arrangements, so its incremental value and effects remain uncertain. Author-developed sources provide context but warrant independent scrutiny. Future studies should assess resource requirements, unintended consequences, and implementation failures alongside anticipated benefits.

6. CONCLUSION :

Zuber's Healthcare Enterprise Risk Management Framework proposes sixteen operational domains connected through accountable ownership, shared risk records, control evidence, monitoring and escalation. The architecture retains ASHRM's eight-domain taxonomy as a crosswalk and draws on established ERM, quality, patient-safety and resilience principles. Its contribution is an explicit governance specification for local adaptation and prospective evaluation.

The proposed requirements provide a basis for local adaptation, structured assessment, and prospective research. Evaluation should first establish clear domain boundaries, reproducible assessment, and feasible implementation, then examine changes in governance performance and independently measured organizational outcomes. Claims of improved safety or reliability will depend on the results of that evaluation.

REFERENCES :

[1] American Society for Health Care Risk Management. (2014). Enterprise risk management: A framework for success. https://www.ashrm.org/system/files/media/file/2019/06/ERM-White-Paper-8-29-14-FINAL.pdf

[2] American Society for Health Care Risk Management. (2020). Health care enterprise risk management playbook (2nd ed.). https://www.ashrm.org/enterprise-risk-management-playbook-second-edition

[3] Berwick, D. M. (2016). Era 3 for medicine and health care. JAMA, 315(13), 1329–1330. https://doi.org/10.1001/jama.2016.1509

[4] Briner, M., Manser, T., & Kessler, O. (2013). Clinical risk management in hospitals: Strategy, central coordination and dialogue as key enablers. Journal of Evaluation in Clinical Practice, 19(2), 363–369. https://doi.org/10.1111/j.1365-2753.2012.01836.x

[5] Centers for Medicare & Medicaid Services. (2023). CMS National Quality Strategy. https://www.cms.gov/files/document/cms-national-quality-strategy-handout.pdf

[6] Chambers, N. (2012). Healthcare board governance. Journal of Health Organization and Management, 26(1), 6–14. https://doi.org/10.1108/14777261211211133

[7] Chassin, M. R., & Loeb, J. M. (2013). High-reliability health care: Getting there from here. The Milbank Quarterly, 91(3), 459–490. https://doi.org/10.1111/1468-0009.12023

[8] Committee of Sponsoring Organizations of the Treadway Commission. (2017). Enterprise risk management: Integrating with strategy and performance. COSO.

[9] Darr, K. (2011). Introduction to management and leadership concepts, principles, and practices. In R. E. Burke & L. H. Friedman (Eds.), Essentials of management and leadership in public health (pp. 7–24). Jones & Bartlett Learning.

[10] Donabedian, A. (2003). An introduction to quality assurance in health care. Oxford University Press.

[11] Hollnagel, E. (2014). Safety-I and Safety-II: The past and future of safety management. Ashgate Publishing.

[12] Institute of Medicine. (2000). To err is human: Building a safer health system. National Academies Press. https://doi.org/10.17226/9728

[13] International Organization for Standardization. (2018). ISO 31000:2018 risk management—Guidelines. ISO.

[14] Johnstone, M. J., & Kanitsaki, O. (2006). Processes influencing the development of graduate nurse capabilities in clinical risk management: An Australian study. Quality Management in Health Care, 15(4), 268–277. https://doi.org/10.1097/00019514-200610000-00009

[15] Joint Commission International. (2024). Joint Commission International accreditation standards for hospitals, including standards for academic medical center hospitals (8th ed.; effective 1 January 2025). Joint Commission Resources.

[16] Kaplan, R. S., & Mikes, A. (2016). Risk management—the revealing hand. Journal of Applied Corporate Finance, 28(1), 8–18. https://doi.org/10.1111/jacf.12155

[17] Khan, G. (2020). The impact of healthcare accreditation on patients' satisfaction: A literature review. International Journal of Health Sciences and Pharmacy (IJHSP), 4(1), 49–56. https://doi.org/10.5281/zenodo.3862791

[18] Leape, L. L. (2009). Errors in medicine. Clinical Chimica Acta, 404(1), 2–5. https://doi.org/10.1016/j.cca.2009.03.020

[19] Leveson, N. (2011). Engineering a safer world: Systems thinking applied to safety. MIT Press.

[20] Lucian Leape Institute. (2014). Safety is personal: Partnering with patients and families for the safest care. National Patient Safety Foundation. https://www.ihi.org/library/publications/safety-personal-partnering-patients-and-families-safest-care

[21] Martin, N. (2020). Enabling effective oversight: Enterprise risk management and board governance in healthcare. Healthcare Management Forum, 33(4), 182–185. https://doi.org/10.1177/0840470420907260

[22] National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0. NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

[23] National Patient Safety Foundation. (2015). Free from harm: Accelerating patient safety improvement fifteen years after To Err Is Human. NPSF.

[24] Organisation for Economic Co-operation and Development. (2020). Strengthening the frontline: How primary health care helps health systems adapt during the COVID-19 pandemic. OECD Publishing.

[25] Porter, M. E., & Teisberg, E. O. (2006). Redefining health care: Creating value-based competition on results. Harvard Business School Press.

[26] Pronovost, P., & Sexton, B. (2005). Assessing safety culture: Guidelines and recommendations. Quality and Safety in Health Care, 14(4), 231–233. https://doi.org/10.1136/qshc.2005.015180

[27] Reason, J. (2000). Human error: Models and management. BMJ, 320(7237), 768–770. https://doi.org/10.1136/bmj.320.7237.768

[28] Sammer, C. E., Lykens, K., Singh, K. P., Mains, D. A., & Lackan, N. A. (2010). What is patient safety culture? A review of the literature. Journal of Nursing Scholarship, 42(2), 156–165. https://doi.org/10.1111/j.1547-5069.2009.01330.x

[29] Schein, E. H., & Schein, P. A. (2017). Organizational culture and leadership (5th ed.). Wiley.

[30] Shaikh, Z. M. (2019a). A case study on electricity consumption and value engineering in a tertiary care hospital. International Journal of Health Sciences and Pharmacy (IJHSP), 3(2), 11–15. https://doi.org/10.5281/zenodo.3411846

[31] Shaikh, Z. M. (2019b). The impact of hospital accreditation on the patients' experience of hemodialysis department: A case study. International Journal of Health Sciences and Pharmacy (IJHSP), 3(1), 31–39. https://doi.org/10.5281/zenodo.3237425

[32] Shaikh, Z. M. (2020a). A case study on recall of used scopes in the endoscopy department by using a Failure Mode & Effect Analysis (FMEA) proactive risk management. International Journal of Health Sciences and Pharmacy (IJHSP), 4(1), 13–24. https://doi.org/10.5281/zenodo.3766843

[33] Shaikh, Z. M. (2020b). Religious and cultural aspects of hand hygiene in healthcare accreditations: A review of literature. International Journal of Health Sciences and Pharmacy (IJHSP), 4(1), 40–48. https://doi.org/10.5281/zenodo.3773876

[34] Shaikh, Z. M. (2021a). Zuber's ten principles of patient-centric patient experience and a framework. International Journal of Health Sciences and Pharmacy (IJHSP), 5(1), 1–10. https://doi.org/10.5281/zenodo.4517634

[35] Shaikh, Z. M. (2021b). Zuber's coronavirus disease (COVID-19) standards for hospitals. International Journal of Health Sciences and Pharmacy (IJHSP), 5(1), 103–116. https://doi.org/10.5281/zenodo.4757071

[36] Shaikh, Z. M. (2021c). Zuber's person-centered care clinical governance standards for hospitals. International Journal of Health Sciences and Pharmacy (IJHSP), 5(1), 117–129. https://doi.org/10.5281/zenodo.4772988

[37] Shaikh, Z. M. (2025). Zuber's Safety-III: Advancing AI-driven predictive analytics for patient safety and high-reliability healthcare systems. International Journal of Health Sciences and Pharmacy (IJHSP), 9(1), 37–49. https://doi.org/10.5281/zenodo.15244941

[38] The Joint Commission. (2024). Comprehensive accreditation manual for hospitals. Joint Commission Resources.

[39] Vincent, C. (2001). Clinical risk management: Enhancing patient safety (2nd ed.). BMJ Books.

[40] Weick, K. E., & Sutcliffe, K. M. (2015). Managing the unexpected: Sustained performance in a complex world (3rd ed.). Wiley.

[41] World Health Organization (WHO). (2021). Global patient safety action plan 2021–2030: Towards eliminating avoidable harm in health care. WHO.

[42] World Health Organization. (2016). Framework on integrated people-centred health services. World Health Organization. https://www.who.int/health-topics/integrated-people-centered-care

[43] World Health Organization. (2020). Patient safety incident reporting and learning systems: Technical report and guidance. https://www.who.int/publications/i/item/9789240010338

[44] Shaikh, Z. M. (2026). Zuber's Cost of Quality Intelligence Framework (ZCoQ-IF): A Validated Model for Healthcare Quality Intelligence. Poornaprajna International Journal of Management, Education & Social Science (PIJMESS), 3(2), 334–345. https://doi.org/10.5281/zenodo.22756025

[45] Shaikh, Z. M. (2026). Zuber's Balanced Scorecard Intelligence Framework (ZBSC-IF): An Integrated Model for Strategic Performance Intelligence in Healthcare. Poornaprajna International Journal of Management, Education & Social Science (PIJMESS), 3(2), 346–358. https://doi.org/10.5281/zenodo.22756087

[46] Shaikh, Z. M. (2026). Zuber's Post-Accreditation Continuous Compliance Framework (ZPA-CCF): Addressing the Sustainability Gap in Healthcare Accreditation. Poornaprajna International Journal of Teaching & Research Case Studies (PIJTRCS), 3(2), 496–511. https://doi.org/10.5281/zenodo.22755817

[47] Shaikh, Z. M. (2018). A Comparative Study on Laboratory and Blood Bank Performance by Using the Quality Indicators. KY Publications. https://doi.org/10.13140/RG.2.2.12850.30403

[48] Shaikh, Z. (2018). A comparative study on the Demographic Indicators of the Kingdom of Saudi Arabia, Ministry of Health. RESEARCH REVIEW International Journal of Multidisciplinary, 3(6), 167–171. https://doi.org/10.5281/zenodo.1285883

[49] Shaikh, Z. M. (2011). A comparative study on the Economic Indicators of Ministry of Health, Kingdom of Saudi Arabia. Economic Indicators, 2006. https://doi.org/10.5281/zenodo.1285887

[50] Shaikh, Z. M. (2018). A comparative study on the Health Resources Indicators of the Ministry of Health, Kingdom of Saudi Arabia. RESEARCH REVIEW International Journal of Multidisciplinary, 3(6), 185–188. https://doi.org/10.5281/zenodo.1285900

[51] National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0). NIST AI 100-1. https://doi.org/10.6028/NIST.AI.100-1

[52] International Organization for Standardization. (2019). ISO 22301:2019 security and resilience—Business continuity management systems—Requirements. https://www.iso.org/standard/75106.html

[53] Koo, T. K., & Li, M. Y. (2016). A guideline of selecting and reporting intraclass correlation coefficients for reliability research. Journal of Chiropractic Medicine, 15(2), 155–163. https://doi.org/10.1016/j.jcm.2016.02.012

[54] Kottner, J., Audigé, L., Brorson, S., Donner, A., Gajewski, B. J., Hróbjartsson, A., Roberts, C., Shoukri, M., & Streiner, D. L. (2011). Guidelines for Reporting Reliability and Agreement Studies (GRRAS) were proposed. Journal of Clinical Epidemiology, 64(1), 96–106. https://doi.org/10.1016/j.jclinepi.2010.03.002

****