ACHSM Asia-Pacific Journal of Health Management

ANALYSIS OF MANAGEMENT PRACTICE

EMBEDDING ENTERPRISE RISK MANAGEMENT IN AN ACADEMIC HEALTH SYSTEM: THE NATIONAL UNIVERSITY HEALTH SYSTEM CASE STUDY

Wong Soo Min[1], Daniel Tan Kuan Wei [2], Lawrence Cheng Sai Him[2], Soo Jie Yi [2]*

1. Corporate Finance Office, National University Health System, Singapore
2. Group Enterprise Risk Management, Corporate Finance Office, National University Health System, Singapore

*Correspondence: jie_yi_soo@nuhs.edu.sg

ABSTRACT

BACKGROUND:

Academic Health Systems (AHSs) operate in complex environments where clinical, academic, and research functions intersect, creating interdependent risks that conventional governance models cannot fully address. Enterprise Risk Management (ERM) provides a structured approach to navigating these risks, yet limited studies describe its implementation within AHSs.

APPROACH:

NUHS implemented the OneNUHS ERM Framework, built on two complementary pillars of system and culture. The system pillar focused on establishing governance structures, standardised risk assessment processes while the culture pillar emphasised cultivating a risk-awareness through leadership visibility, capability building, and sustained risk communication.

OUTCOMES:

NUHS maintained a stable enterprise risk profile alongside a steady improvement in audit outcomes, with increasing proportions of reports achieving "Satisfactory" and "Good" ratings. Engagement from the first line of defence strengthened over time, reflecting a shift from a "push" model of risk management to a "pull" mindset where operational teams actively sought risk insights. Insights generated through ERM activities also supported broader organisational improvements, including process optimisation.

IMPLICATIONS:

The NUHS experience demonstrates that effective and sustainable ERM requires deliberate alignment between systems and people. Health systems seeking to strengthen ERM should embed risk management as an organisational practice that supports both governance and enterprise value creation.

KEYWORDS

Enterprise risk management; academic health system; organisational culture; governance; risk awareness; health leadership

INTRODUCTION

Academic Health Systems (AHS) combine clinical service, education, and research within one organisational structure. This multi-mission structure advances healthcare quality and innovation but also exposes AHSs to diverse and unique risks beyond conventional hospital operations. Effective management of such complexity requires integrated governance that aligns risk awareness across clinical, academic, and administrative domains [1,2].

Enterprise risk management (ERM) has long been recognised as a cornerstone of organisational resilience. First conceptualised in the financial sector [3], its application to healthcare has grown steadily over the past two decades in managing cross-cutting risks such as patient safety, workforce sustainability, and cybersecurity [4–6]. Yet, few studies have demonstrated success in embedding risk awareness into everyday culture and decision-making.

In Singapore, the National University Health System (NUHS) functions as an integrated AHS with a network of tertiary and secondary care hospitals, national centers, polyclinics, community and home care services, and the National University of Singapore's health faculties [7]. In 2016, NUHS embarked on a journey to move beyond siloed, compliance-driven risk approaches to the OneNUHS ERM Framework, built on two reinforcing pillars: a robust governance system and a risk-aware culture.

This case study adds to the growing body of research on healthcare risk governance by illustrating how ERM can be operationalised within an Academic Health System. It offers practical insights into the interplay between system and culture, an area still underexplored in ERM literature.

THE CHALLENGE: MANAGING RISKS IN AN ACADEMIC HEALTH SYSTEM

As an AHS, NUHS operates in a complex risk landscape. Unlike a single-entity, service-centric hospital, an AHS must simultaneously balance patient safety, research productivity, and educational excellence. These missions' function under differing regulatory regimes, funding mechanisms, performance incentives, and professional cultures. Clinical services prioritise safety and operational continuity. Research entities accept a degree of uncertainty inherent in innovation. Academic faculties value intellectual autonomy and scholarly independence. The coexistence of these varied priorities introduces structural tension that requires deliberate alignment at the enterprise level.

In addition, risks within an AHS are highly interdependent. For example, a cybersecurity breach may compromise clinical operations and research data integrity. Research misconduct may erode public confidence in clinical programmes. Workforce burnout may undermine both patient care and academic teaching quality. Risks therefore do not remain confined within functional silos but can propagate rapidly across domains, amplifying reputational, operational, and regulatory consequences.

For NUHS, this complexity is further heightened by its role as a publicly funded healthcare cluster. As a steward of public resources, NUHS operates under ministerial oversight and public accountability. Decisions concerning resource allocation must balance innovation with fiscal prudence and equity of access. This public mandate elevates expectations of transparency, trust, and system-wide coherence.

Prior to 2016, NUHS institutions had developed their own risk processes tailored to local priorities. The absence of a formalised, cluster-wide framework limited visibility of enterprise-level risks and cross-institutional dependencies. Introducing a unified ERM approach therefore required careful navigation of institutional sovereignty.
Rather than replacing existing systems through a purely top-down directive, the OneNUHS ERM Framework was developed through a process of co-creation with the institutions. This approach enabled NUHS to establish a shared governance architecture, common risk language and risk culture aspirations, while respecting the operational realities of individual institutions.

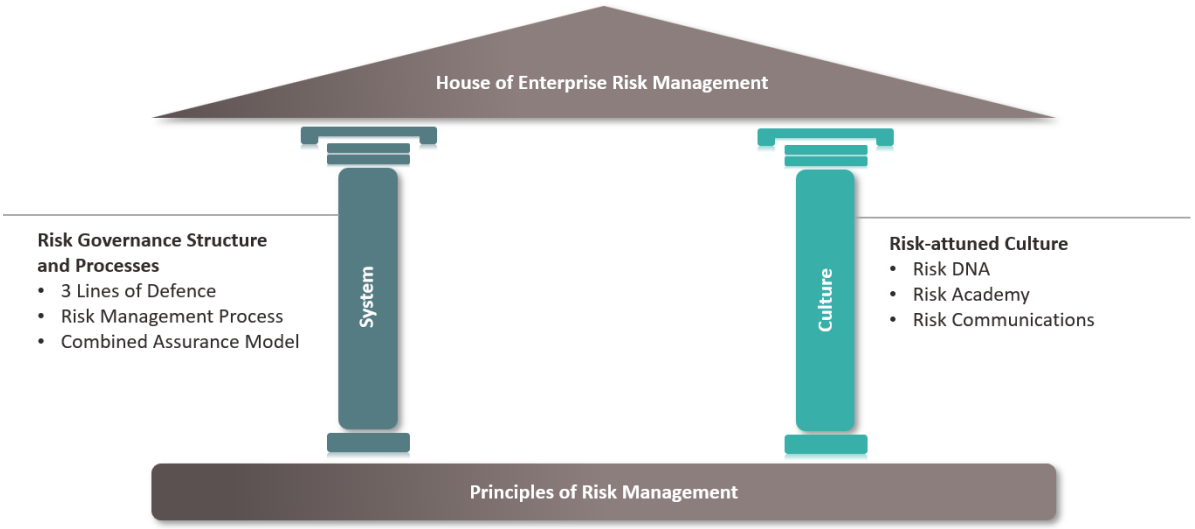
Importantly, while NUHS had established clinical risk governance structures including mechanisms for patient safety reporting and clinical quality oversight, they did not fully address enterprise-wide risks that extended beyond clinical domains, such as data protection and cybersecurity. Hence, the introduction of the OneNUHS ERM Framework served to complement existing risk management process at both institutional and cluster level, without the intention to overhaul or replace.

In this context, ERM was not merely a compliance exercise nor a mechanism for risk avoidance. It was conceived as a strategic enabler to protect value by strengthening internal controls, and to create value by optimising synergies across clinical, academic, and research domains. Embedding ERM within such a multifaceted and publicly accountable system required more than structural redesign. It demanded coordinated cultural and leadership transformation across the cluster.

BUILDING THE TWO PILLARS OF ERM

Effective risk management at NUHS rests on two interdependent pillars: System and Culture. The System represents the governance structures, processes, and accountabilities that form the organisation's risk management "hardware" [8]. In contrast, Culture embodies the shared norms and behaviours that determine how individuals recognise, discuss, and respond to risks [9]. This "heart-ware" element is essential for influencing attitudes and embedding risk management into everyday practice. Together, the 'hardware' and 'heartware' of risk management ensures alignment between processes and people.

FIGURE 1. THE NUHS HOUSE OF ERM COMPRISING TWO PILLARS: SYSTEM AND CULTURE



PILLAR 1: STRENGTHENING THE SYSTEM

Governance Structure

NUHS adopted the *Three Lines Model* [10] and adapted to NUHS' context to delineate clear roles and responsibilities across the organization at the various line of defence. The first line of defence (1LOD) comprises NUHS institutions and corporate office departments which are directly responsible for managing risks and controls within their respective operational areas.

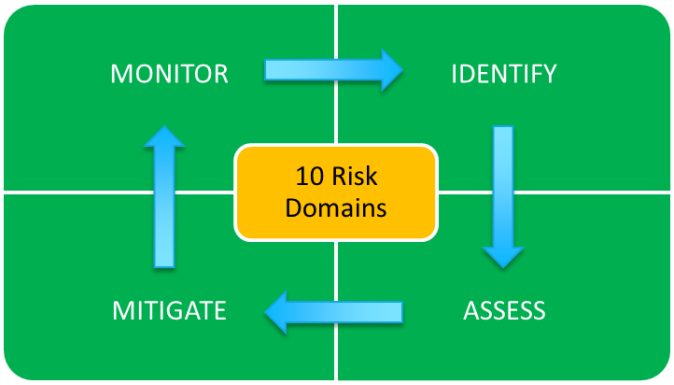
The second line of defence (2LOD) is fulfilled by the NUHS Group ERM Office which plays an advisory role to 1LOD. It provides analysis and reporting on the adequacy and effectiveness of risk management activities such as internal controls. The third line of defence (3LOD) consists of both internal and external auditors, providing objective assurance to the Board Audit and Risk Committee (ARC), which oversees governance, risk and audit matters independently.

Key to this structure is the Risk Management Steering Committee (RMSC), chaired by the NUHS Chief Executive. The RMSC ensures that risk issues raised across the cluster are escalated, discussed, and addressed at the highest level of leadership.

Risk Management Process

Aligned with ISO 31000:2018 – Risk Management: Guidelines [9], NUHS adopted a well-established and globally recognised framework that defines risk management as a structured, iterative process (Figure 2). As one of the most authoritative international standards, its adoption enabled NUHS to develop a shared language of risk, allowing risks to be surfaced and discussed systematically at RMSC.

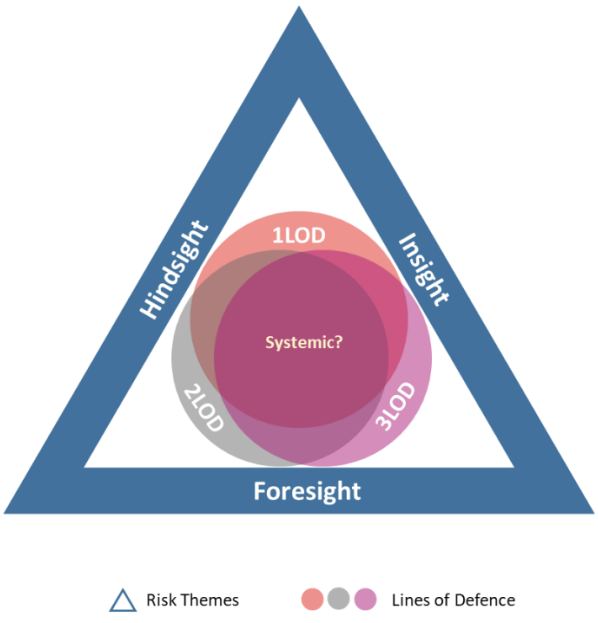
FIGURE 2. RISK MANAGEMENT PROCESS ALIGNED WITH ISO 31000:2018 – RISK MANAGEMENT: GUIDELINES.



Combined Assurance Model

NUHS also implemented a Combined Assurance Model to harmonize assurance activities across the Three Lines of Defence (Figure 3). Central to this is the use of Control Self-Assessments (CSAs), where managers and frontline staff collaboratively identify risks, evaluate the effectiveness of controls, and design processes to address any gaps. This participatory approach empowers staff, reinforces accountability, and heightens risk awareness at the operational level.

FIGURE 3. NUHS COMBINED ASSURANCE MODEL INTEGRATING THE THREE LINES OF DEFENCE



PILLAR 2: FOSTERING A CULTURE OF RISK AWARENESS

Recognising that systems alone do not guarantee effective governance, NUHS leadership deliberately positioned risk culture as a strategic priority. Visible leadership, particularly the Chief Executive's active chairing of the RMSC and direct risk communications by institution CEOs at various forums, signalled that risk transparency was expected and supported. Leadership messaging framed risk identification not as fault-finding, but as stewardship of patient trust and institutional integrity.

From this heart-ware perspective, risk management is more than a compliance exercise. It reflects collective attitude and everyday behaviors that guide decision [9]. To embed this mindset, NUHS introduced several initiatives designed to engage staff and foster a shared sense of responsibility for risk.

Risk DNA

NUHS launched the Risk DNA campaign, anchored by the tagline "See Something, Do Something." Introduced during a NUHS Chief Executive's Townhall session in April 2016, this simple and memorable phrase which encouraged employees to act when encountering risks.

Risk Academy

Risk Academy is a learning platform that offers training workshops that equip staff with foundational risk management knowledge and championed desired behaviors through real-life success stories.

Risk Communications

NUHS implemented ongoing risk communications to keep staff informed and vigilant. Relevant information, such as cybersecurity alerts, was regularly disseminated, reminding staff to report issues in line with the "See Something, Do Something" ethos.

RESULTS AND IMPACT

IMPROVED ENTERPRISE OVERSIGHT

The Key Risk Indicators (KRIs) developed through the standardised risk assessment process strengthened enterprise-level risk visibility and oversight across functional domains. With consistent monitoring and reporting to the RMSC, risk exposures could be tracked systematically at the cluster level rather than remaining confined within institutional silos. In recent reporting cycles, 80% of KRIs across domains in operations, human capital and legal recorded zero significant incidents, reflecting stable risk profiles and effective implementation of preventive controls.

Sustained improvements were also observed in assurance outcomes. Over a five-year period, the proportion of Audit Reports achieving a "Good" rating more than doubled compared to earlier years when reports were frequently assessed as "Need Strengthening".

CULTURAL MATURITY

Beyond governance processes, OneNUHS ERM also contributed to a visible strengthening of risk awareness across the organisation. Capability building was an important component of this effort. More than 120 managers participated in Control Self-Assessment (CSA) workshops and risk training programmes, establishing a common understanding of risk concepts and control evaluation.

Over a five-year period, 21 CSAs comprising more than 450 validated responses were conducted across functional domains. These participatory exercises strengthened cross-functional dialogue, improved the quality of risk information, and fostered shared accountability for control gaps across institutions.

Cultural maturity was also reflected in staff responsiveness to emerging digital risks. In a sector-wide simulated phishing email exercise, NUHS achieved a 95% passing rate, indicating strong awareness and vigilance among employees in identifying and responding to potential cybersecurity threats.

ENTERPRISE VALUE CREATION

As ERM processes matured, NUHS observed a shift in mindset from "push" to "pull" [13]. Rather than risk management being driven solely by the risk function, organisational stakeholders increasingly sought risk insights because they recognised their operational value. This shift represents one of the most significant outcomes of the OneNUHS ERM

implementation, reflecting a transition from focusing on the robustness of risk processes to recognising the broader value that risk management can create for the organisation.

This shift in mindset was demonstrated in the increasing engagement initiated by the first line of defence (1LOD), where operational teams proactively sought to strengthen internal controls and address emerging risks. As a result, the Compliance Review enabled by Data Analytics (CReDA), a process excellence initiative, emerged as a spin-off from risk management activities. CReDA developed automation tools to streamline previously manual and labour-intensive processes. These tools enabled the first line of defence to take greater ownership of operational risk management while improving process efficiency and control effectiveness.

CREDA solutions have since been applied across multiple operational areas, including facilities management, hospitality services, and portering functions across all three NUHS acute hospitals.

LESSONS LEARNT AND CONCLUSION

The NUHS experience offers several lessons for healthcare leaders seeking to embed enterprise risk management within complex health systems. First, it demonstrates that structured processes alone are insufficient unless supported by an enabling culture. Similarly, culture cannot flourish without clear systems to guide good behaviours.

Second, leadership visibility matters. The decision for the NUHS Chief Executive to personally chair the RMSC signalled that risk management was a strategic priority rather than an administrative exercise. This legitimised risk discussions and empowered frontline managers to surface issues without hesitation.

Thirdly, simplicity proved essential in driving adoption. The concise and memorable slogan "See Something, Do Something" resonated more deeply with staff than complex manuals or frameworks. Equally important was capability building, which ensured that staff possessed the competencies and confidence to participate meaningfully in risk activities.

Together, these lessons underscore the importance of aligning systems, people and purpose to embed risk management as a lived practice rather than a procedural requirement. More broadly, the NUHS experience illustrates how ERM can evolve from a compliance-oriented function into a strategic capability within an AHS. While NUHS operates within the distinctive environment of an AHS, the underlying principles demonstrated in this case may be relevant to any other healthcare organisation navigating similar complex operating environment.

As healthcare systems continue to face increasing technological disruption, regulatory complexity and evolving public expectations, effective ERM with the ability to identify and respond to emerging risks will remain essential to support resilient and adaptive healthcare organisations [13].

AUTHORSHIP

All authors have made substantial contributions to the conception, design, and execution of this work, including the analysis and interpretation of information presented in the manuscript. All listed authors have reviewed and approved the final version of the paper and agree to its submission to the Asia Pacific Journal of Health Management. Authorship criteria were applied in accordance with the guidelines of the International Committee of Medical Journal Editors (ICMJE).

ACKNOWLEDGEMENTS

The authors wish to thank colleagues from the National University Health System's Group Enterprise Risk Management Office for their support and insights during the development of this case study. The authors also acknowledge the leadership of the NUHS Chief Executive and members of the Risk Management Steering Committee for their continued commitment to fostering a risk-aware culture. No external funding was received for this work.

The authors used OpenAI's ChatGPT (GPT-5, 2025 version) to support language refinement and citation formatting during manuscript preparation. The authors reviewed and verified all generated content for accuracy, originality and adherence to the journal's guidelines. The final manuscript reflects the authors' own analysis and interpretation.

CONFLICTS OF INTEREST

The authors declare that there are no conflicts of interest that could have influenced the content or conclusions of this manuscript.

References

1. Gleißner W. Enterprise risk management: improving embedded risk management and risk governance. J Risk Financial Manag. 2024;17(3):156. doi:10.3390/jrfm17030156.
2. Martin N. Enabling effective oversight: enterprise risk management and board governance in healthcare. Healthc Manage Forum. 2020;33(4):182–185. doi:10.1177/0840470420907260.
3. Dionne G. Risk management: history, definition and critique. J Risk Financ Manag. 2013 Sep 6;6(3):218-298. doi:10.2139/ssrn.2231635
4. Sermhattakit H, Ekkawatpanit C, Siripipatthanakul S, Bunthamcharoen P. Key risks and mitigation strategies in enterprise risk management for private hospitals: a mixed-method study. SAGE Open Med. 2025;13:20503121251234. doi:10.1177/2050312125121234.
5. Sae-Lim P, Na Ayudhaya S. Beyond patient safety goal – towards hospital sustainable risk: a systematic review on the evolution of hospital risk management. Open Public Health J. 2024;17:e18749445284229. doi:10.2174/0118749445284229240313062944.
6. Ferdosi M, Rezayatmand R, Molavi Taleghani Y. Risk management in executive levels of healthcare organizations: insights from a scoping review. Risk Manag Healthc Policy. 2020;13:215–243. doi:10.2147/RMHP.S231712.
7. National University Health System. About NUHS [Internet]. Singapore: NUHS; 2025 [cited 2025 Oct 29]. Available from: https://www.nuhs.edu.sg
8. ISO. ISO 31000:2018 – Risk Management: Guidelines [Internet]. Geneva: International Organization for Standardization; 2018 [cited 2025 Oct 29]. Available from: https://www.iso.org/standard/65694.html
9. Association of Chartered Certified Accountants (ACCA). Risk cultures in healthcare: the role of accountancy. London: ACCA; 2024.
10. The Institute of Internal Auditors (IIA). The IIA's Three Lines Model: An Update of the Three Lines of Defense. Altamonte Springs (FL): The Institute of Internal Auditors; 2024.
11. McKinsey & Company. McKinsey on Risk, Number 10: The State of Risk Culture – Why Good Frameworks Are Not Enough. New York: McKinsey & Company; 2021 [cited 2025 Oct 29]. Available from: https://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/mckinsey%20on%20risk%20number%2010%20winter%202021/mckinsey-on-risk-number-10.pdf
12. Counts T, Himmel B, Millsaps S. Creating a Pull vs. Push Mindset. ERM Initiative, NC State University Poole College of Management [Internet]. 2026 Feb 4 [cited 2026 Mar 9]; Available from: https://erm.ncsu.edu/resource-center/creating-a-pull-vs-push-mindset-about-erm/
13. Di Palma G, Scendoni R, Tambone V, Alloni R, De Micco F. Integrating enterprise risk management to address AI-related risks in healthcare: Strategies for effective risk mitigation and implementation. J Healthc Risk Manag. 2025;44(1):25-33. doi:10.1002/jhrm.70000