

Enterprise Risk Management

Enterprise risk management (ERM) in health care promotes a comprehensive framework for making risk management decisions which maximize value protection and creation by managing risk and uncertainty and their connections to total value.



Source: ©2017, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission.

ERM Guiding Principles

The following guiding principles based on the framework adopted by the Council of Sponsoring Organizations of the Treadway Commission (COSO, 2017), in concert with ASHRM's mission and vision have been developed as basic building blocks supporting the framework for ERM in health care:

- Advance safe and trusted health care
- Empower health care risk managers to mitigate risk and maximize value
- Promote ethical and transparent decision-making
- Improve patient safety through execution of ERM principles
- Improve strategic decision making

ERM Practices:

- Are continuous
- Require a paradigm shift in how an organization identifies and manages risks and opportunities
- Are "not a stop on the road, but a journey"

ERM Domains

Operational



Clinical/Patient Safety



Strategic



Financial



Human Capital



Legal/ Regulatory











Technology



Hazard



ERM Risk Domains

Domain	Description/Example
Operational 	<p>The business of health care is the delivery of care that is safe, timely, effective, efficient, and patient-centered within diverse populations. Operational risks relate to those risks resulting from inadequate or failed internal processes, or systems that affect business operations. Examples include risks related to: adverse event management, credentialing and staffing, documentation, chain of command, lack of internal controls, supply chain and identification of existing opportunities within management oversight.</p>
Clinical/Patient Safety 	<p>Risks associated with the delivery of care to patients, residents and other health care customers. Clinical risks include: failure to follow evidence based practice, medication errors, hospital acquired conditions (HAC), serious safety events (SSE), health care equity, opportunities to improve safety within the care environments, and others.</p>
Strategic 	<p>Risks associated with the focus and direction of the organization. Because the rapid pace of change can create unpredictability, risks included within the strategic domain are associated with brand, reputation, competition or failure to adapt to changing times (such as health reform or shifting customer priorities). Managed care relationships/partnerships, conflict of interest, marketing and sales, media relations, mergers, acquisitions, divestitures, joint ventures, affiliations and other business arrangements, contract administration, and advertising are other areas generally considered as potential strategic risks.</p>
Financial 	<p>Decisions that affect the financial sustainability of the organization, access to capital or external financial ratings through business relationships or the timing and recognition of revenue and expenses make up this domain. Risks might include: capital structure, credit and interest rate fluctuations, foreign exchange, growth in programs and facilities, capital equipment, regulatory fines and penalties, budgetary performance, accounts receivable, days of cash on hand, capitation contracts, reimbursement rates, managed care contracts, revenue cycle/billing and collection.</p>
Human Capital 	<p>This domain refers to the organization's workforce. Included are risks associated with employee selection, retention, turnover, staffing, absenteeism, on-the-job work-related injuries (workers' compensation), work schedules and fatigue, productivity, compensation, succession planning and labor unionization activity. Human capital associated risks may cover recruitment, diversity, retention, and termination of members of the medical and allied health staff.</p>
Legal/Regulatory 	<p>Risk within this domain incorporates the failure to identify, manage and monitor legal, regulatory, and statutory mandates on a local, state and federal level. Such risks are generally associated with fraud and abuse, licensure, accreditation, product liability, management liability, Centers for Medicare and Medicaid Services (CMS) Conditions of Participation (CoPs) and Conditions for Coverage (CfC), as well as issues related to intellectual property.</p>
Technology 	<p>This domain covers machines, hardware, equipment, devices, wearable technologies and tools, but can also include techniques, systems and methods of organization. Health care has seen an escalation in the use of technology for clinical diagnosis and treatment, training and education, information storage and retrieval, and asset preservation. Examples also include Electronic Health Records (EHR) and Meaningful Use, financial and billing systems, social media and cyber security; cyber risks can be significant.</p>
Hazard 	<p>This ERM domain covers assets and their value. Traditionally, insurable hazard risk has related to natural exposure and business interruption. Specific risks can also include risk related to: logistics/supply chain, facility management, plant age, parking (lighting, location, and security), valuables, construction/renovation, earthquakes, windstorms, tornadoes, floods, fires and pandemics.</p>