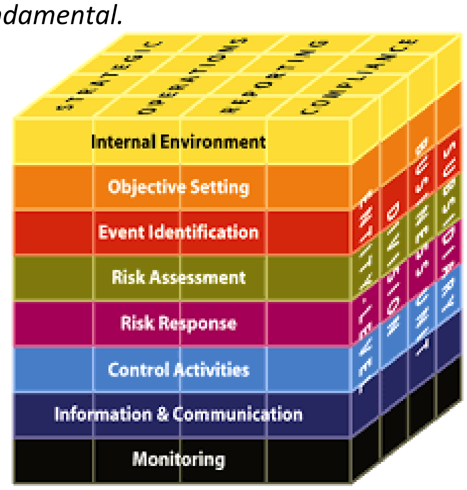
NEXTLEVELSOLUTIONS RISK AND REGULATORY INSIGHTS

2022-RRI-06

ENTERPRISE RISK MANAGEMENT – A STRATEGIC FOCUS

Everyday organizations have to take or respond to risks in the process of pursuing business objectives. Risk management, if present, is often treated as an attendant function to this process, primed and ready to manage and protect the entity from the downside of the risks involved. Risk management is often positioned as firefighters rather than part of strategic planning. Risk management for some becomes an administrative, routine and mundane function. This is largely because there is opacity in the line of sight as to how it connects to and interacts with strategy.

According to Enterprise Risk Management Integrating with Strategy and Performance *[COSO (2018)], "when risk is considered in the formulation of an organization's strategy and business objectives, enterprise risk management helps to optimize outcomes". There is greater value to be created when your organizations elevate risk management to a strategic level in strategic and operational planning. Risk management is a critical bridge between the strategic and operational management of the organization. Therefore, being properly integrated in strategic planning and appropriately structured to respond to the exposures created by the pursuit of the agreed business objective is fundamental.*



ERM SHOULD TAKE A FULLY INTEGRATED AND PROACTIVE APPROACH TAKING COMPLETE COGNISANCE OF THE STRATEGIC OBJECTIVES OF THE ENTITY - NEXTLEVELSOLUTIONS

"COSO Enterprise Risk Management - Integrated Framework enables organizations to effectively and efficiently develop systems of internal control that adapt to changing business and operating environments, mitigate risks to acceptable levels, and support sound decision making and governance of the organization"

"A direct relationship exist between objectives [strategic, operations, reporting, compliance] which are what an entity strives to achieve, [the eight] components and the organizational structure".

When we consider authoritative material on enterprise risk management (ERM), we find important clues as to where risk management is expected to fundamentally "reside". COSO defines Enterprise Risk Management (ERM) as a process, effected by an entity's board of directors, management and other personnel enterprise wide at strategic level, designed to identify potential events that may affect the entity, and mange risks to remain within its risk appetite, and to provide reasonable assurance regarding the achievement of entity objectives. To achieve effective and sound implementation *of ERM, management must focus on ensuring there is a sound governance framework in place.*

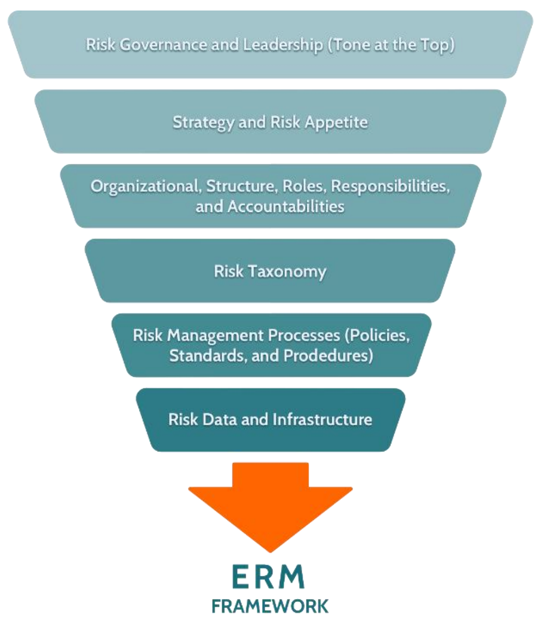
A careful deconstruction of the definition highlights a number of important issues including: ERM is a process and not an event or a serious of reactionary actions. If your organization finds itself managing risk in a reactive manner then it is highly likely that and effective and well-structured "process" is non-existent. It points to risk management taking on strategic nature. This becomes easily understood when we understand that ERM is the responsibility of the board where business objectives are set, who is ultimately responsible for execution and where critical governance factors such as risk appetite, risk tolerance and philosophy is determined and crystalized.

According to Compliancecore.com an ERM framework refers to *"an organization's structure and approach to managing risk across the organization. The objective of an ERM Framework is to ensure that the organization has the structure, governance, roles, and responsibilities as well as the culture, skills, expertise, data and technology infrastructure, and tools to manage risk".*

ERM OBJECTIVES

Risk management is not simply about organizing a series of manual (policies and procedures) and routinely following a set of checklist and completing reports for boards. Full realization of the value occurs when an entity, for example, effectively leverages its risk management function and positions itself to be able to exploit greater opportunities (within the confines of its risk appetite); to expand its capacity and competency and ability to more effectively manage more complex risks and therefore better enhance shareholders value; create confidence for extending risk appetite. Consider this depiction of an ERM framework as noted by Compliancecore.com:

- *Aggregate and assess risk across the organization.*
- Protect and enhance an organization's reputation.
- Facilitate an organization's mission by integrating risk considerations into strategic and operational planning decisions, and *by managing risk to the organization's earning*, capital, operational strength, and reputation in a manner that promotes prudent, effective decision-making, optimizes risk-reward, and instills accountability for risk in fulfilling the organization's strategy and mission.
- *Promote a strong risk culture that includes a thorough understanding of risk appetite* along with clear roles, responsibilities, and accountabilities for the ownership and management of risks.
- *Ensure that a strong risk infrastructure supports the effective management of risks* and consistency in the management of risks.
- *Maintain a risk governance structure at the board and management level* that ensures identification, measurement, analysis, management, monitoring, and reporting of all material risks along with effective risk response strategies and escalation protocols.
- *Ensure effective, proactive management for each of the organization's risk categories along with anticipation and management of material risk interdependencies.*



SOURCE: COMPLIANCE.COM

The above provides a useful depiction of the general structure that should be evident in an organization's risk management function. Risk governance emanates from the board and drives strategy and risk appetite. There must be clearly defined roles, responsibilities and accountabilities. Within the entity, there should be a clear and common classification (taxonomy) with processes and practices appropriately managed by a well-defined set of risk management processes. Where appropriate based ion size and complexity appropriate data and technology infrastructure should be available to facilitate the management of risk on a more quantitative basis.

SELF-ASSESSMENT QUESTIONAIRE

Risk management is often treated as an esoteric matter with only a few persons capable of understanding it. The truth is that while knowledge will vary and capacity, based on exposure and experience, will differ, risk management falls within the mandate of every single employee and therefore demands the attention and focus of each employee within your organization.

*At **NextLevelSolutions**, we find it useful to reduce risk issues to simple commonsense questions. An answer may be known with confidence (yes or no) or there might be uncertainty. Whatever the case the outcome will provide valuable insight. Being uncertain about what you ought to know is as critical an issue in risk management as being certain of what you do know.*

The table below lays out a series of questions that should help to enhance appreciation of the preceding material. The questionnaire essentially follows the flow of the diagram above moving from the highest level of governance, to making enquiries about operational readiness and potential remediation.

In any instance where there are terms appearing to be technical nature we encourage brief research which will aid in helping to cement and broaden understanding.

RISK GOVERNANCE COMPONENT	SELF-ASSESSMENT QUESTIONS	YES	NO
Risk Governance, Appetite, Tolerance and Philosophy	1. Has your board of directors set out and approved clearly defined risk appetite statements for your organization?		
	2. Has your board of directors set out clear, quantifiable and appropriate risk tolerance levels?		
	3. Is your board of directors fully cognizant of, and appreciate the importance of setting risk tolerance levels for your organization?		
	4. Is strategic decision making by executive and the board respectful of your organization's risk governance structure and consistently takes into account the risk philosophy of your organization?		
	5. Is the board and executive management fully aware of the desired risk culture and objectively assessed are the main drivers, setting the appropriate tone by example?		
	6. Does the board and executive management understand the risk capacity of your organization?		
	7. Is your organization's risk appetite defined for climate, cyber and environmental risk, contemplates catastrophic occurrences such as pandemics?		
Risk Management	8. Has your organization undertake a comprehensive risk assessment to identify the key risk and impediments to achieving its objectives?		
	9. Do you have in place a structured process that takes you beyond risk identification and ongoing assessment of changes in risk profile?		

	10. Does your organization have models and the scenario analysis in place to measure and quantify these risks? 11. Have your board and executive management allocated appropriate ‘risk budget’ for managing the key risk to your business lines or products? 12. Are there clear delineation of key risk indictors for each category of risk identified? Are you able to determine whether these are leading or lagging indicators? 13. Does your organization have customized risk policies and procedures implemented to assess, report on and mitigate risks, where possible, and are the necessary controls in place and effective? 14. Is your organization managing applying risk treatment to residual risk?		
Incentives, Training and Capacity	15. Does your staff, as well as your board members, have the skills and expertise to grasp the risks your organization faces? 16. Does your organization have an organizational structure in place to support enterprise-wide risk management? 17. Does your organization have an effective process for reliable reporting on risks and risk-management performance? 18. Does your organization have in place a structures system to provide assurances on the proper functioning of risk controls? 19. Has your organization incorporated performance metrics for the risk types identified in the incentive structures of management and staff? 20. Does your organization undertake routine training for and evaluation of its board of directors? 21. Where the answers to any of the above are in the negative, is there a clear roadmap in place to address and remediate the challenges?		

We will be delighted to respond to any questions or queries you may have on this or any issue of Risk and Regulatory Insights. Past issues are available on our website at www.nlsolutionsbahamas.com under Risk and Regulatory Forum.

****