



The View of ERM from Global Risk Management Frameworks

Dr Edwin Orero

Global Risk Management Frameworks



Contents

- Introduction to Global Risk Management Frameworks
- NIST Framework and it's View on ERM
- The CAS Framework and it's View on ERM
- The COBIT Framework and it's View on ERM
- The RIMS Risk Maturity Model Framework

Introduction to Global Risk Management



- COSO ERM Framework and ISO 31000 (2018) Frameworks widely adopted and cited. Both Frameworks have been discussed on Day 1.
- There are other Global Risk Management Frameworks too.

Factors influencing the use of different Global Risk Management Frameworks:

- Specific nature of certain risks, such as risks within Insurance.
- Industry based Frameworks, such as in Education, Manufacturing/ Supply Chains, Healthcare, Financial Services, Environmental Protection, etc
- Complexity of a Framework
- Business goals
- Technology Infrastructure
- Budget.
- Future growth of the organization.

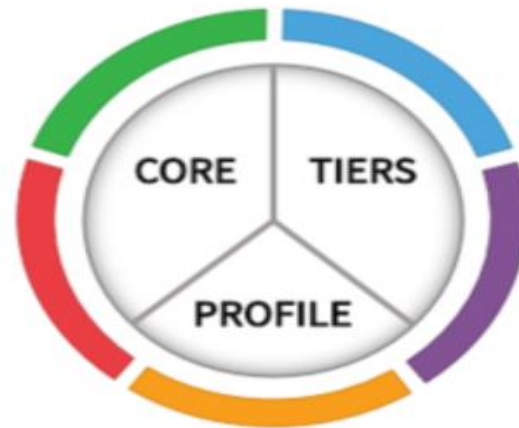
Vision: A world class Professional Accountancy Institute.

NIST Framework and it's view on ERM



- Developed by The National Institute of Standards and Technology (NIST), a U.S. Federal Government Agency.
- A Cybersecurity Framework used by private enterprises carrying of business with the US Federal Government.

Representation of the NIST Framework



Vision: A world class Professional Accountancy Institute.

NIST Framework and it's view on ERM



- Globally recognised for providing Cybersecurity Guidelines to organizations with Critical Infrastructure to safeguard and protect.

Views on Enterprise Cybersecurity Risk Management

Component	Description
Framework Core	<p>The Framework Core provides 5 Cybersecurity activities and outcomes using easy to understand language.</p> <p>These are: Identify, Protect, Detect, Respond, Recover.</p>
Framework Implementation Tiers	<p>These help provide context on how an organization views cybersecurity risk management.</p> <p>Organizations can consider the level of rigor for their cybersecurity program, including risk appetite, mission priority, and budget.</p>
Framework Profile	<p>This aligns the organization's objectives, risk appetite, and resources against the desired outcomes of the Framework Core.</p>

Vision: A world class Professional Accountancy Institute.

The CAS Framework and it's view on ERM



- The Casualty Actuarial Society (CAS) is a leading international organization for credentialing and professional education.
- The CAS is the world's only actuarial organization focused exclusively on property and casualty risks. Members are experts in property and casualty insurance, reinsurance, finance, risk management, and ERM.

Four Categories of Risks Identified by CAS:

Hazard - includes liability suits, property damage, natural disasters, crime, work-related injuries, and business interruption

Financial - including price risk, liquidity risk, credit risk, inflation risk, and hedging risk.

Vision: A world class Professional Accountancy Institute.

The CAS Framework and it's view on ERM



Strategic - includes competition, customer risk, demographic and cultural risk, innovation risk, capital availability, regulation, and political risk

Operational - including operational risk, empowerment risk, IT risk, integrity risk, and business reporting risk.

The CAS Risk Management Framework identifies 7 steps to be followed.

1. Establish the Context.
2. Identify Risks.
3. Analyze Risks.
4. Integrate Risks.
5. Prioritize Risks.
6. Exploit Risks.
7. Monitor Risks.

Vision: A world class Professional Accountancy Institute.

The COBIT Framework and it's view on ERM



- Control Objectives for Integrated and Related Technologies (COBIT) was developed by Information Systems Audit and Controls Association (ISACA).
- COBIT targets the improvement of IT Governance and Management.
- COBIT helps align the IT goals to the Business goals.

There are 3 Core Principles:

COBIT Principle	Description
Conceptual	Critical components should be identified and their relationships noted to for consistency and automation.
Agile	Openness and flexibility to new content, while addressing new issues with agility, integrity, and consistency.
Aligned	Align with different standards, other frameworks, and regulatory requirements.

Vision: A world class Professional Accountancy Institute.

The COBIT Framework and it's view on ERM



Six core requirements for an enterprise IT governance system:

Valuable: The Board, Leadership team and management should be able to see it's value.

Holistic: There should be a complete approach to risk management and governance, taking into consideration various components.

Dynamic: React to changes to the ERM program's design factors.

Distinct: Clear distinction between management and governance activities.

Customized: Should be customized to optimize risk mgnt and governance.

Comprehensive: Provide end-to-end ERM coverage for IT functions and processes.

Vision: A world class Professional Accountancy Institute.

The RIMS Risk Maturity Model Framework on ERM



- The Risk Maturity Model has been developed by the Risk Management Society (RIMS).
- Consists of 68 readiness indicators that describe 25 competency drivers for 7 critical ERM attributes.

7 attributes:

1. ERM-Based Approach: Focus is on the enterprise risk culture.
2. ERM Process Management: Culture of the organization and integration across business processes.
3. Risk Appetite Management: Decision making process on Risk Appetite.
4. Root Cause Discipline: Identify root causes of each risk.
5. Uncovering Risks: Performing Risk Assessment and documenting.
6. Performance Management: Quantitative and qualitative KPIs.
7. Business Resiliency and Sustainability: Scenarios Testing.

Vision: A world class Professional Accountancy Institute.

Global Risk Management Views on ERM



Q

Vision: A world class Professional Accountancy Institute.

Global Risk Management Views on ERM



Dr Edwin Orero holds a PhD in Management from Royal Holloway, University of London and is also a CPA (K). His thesis looked at the role that International Financial Institutions play in the promotion of Public Private Partnerships. Dr. Orero has been a career External Auditor, Internal Auditor and Risk Management Consultant in various organizations both in Kenya and in the UK.

Vision: A world class Professional Accountancy Institute.