COSO ERM COMPONENTS

Internal Environment

Risk Management Philosophy – Risk Culture – Board of Directors – Integrity and Ethical Values – Commitment to Competence – Management's Philosophy and Operating Style – Risk Appetite - Organizational Structure – Assignment of Authority and Responsibility – HR Policies and Practices

Objective Setting

Strategic Objectives – Related Objectives – Selected Objectives – Risk Appetite – Risk Tolerance

Event Identification

Events – Factors Influencing Strategy and Objectives – Methodologies and Techniques – Event Interdependencies – Event Categories – Risk and Opportunities

Risk Assessment

Inherent and Residual Risk – Likelihood and Impact – Methodologies and Techniques - Correlation

Risk Response

Identify Risk Responses – Evaluate Possible Risk Responses – Select Responses – Portfolio View

Control Activities

Integration with Risk Response – Types of Control Activities – General Controls – Application Controls – Entity Specific

Information and Communication

Information – Strategic and Integrated Systems - Communication

Monitoring

Separate Evaluations – Ongoing Evaluations

Source: COSO Enterprise Risk Management – Integrated Framework - September 2004. *www.coso.org*

Example of Use of COSO ERM Framework for Environment and Social Work

THE COSO ERM FRAMEWORK CAN BE USED FOR BOTH ASSURANCE AND ADVISORY WORK.

ASSURANCE WORK: *Audit of IFC's Environment and Social Review Process*

The audit **objective** was to determine whether the risk management, control and governance over IFC's environment and social review process provide reasonable assurance that:

- significant programs, plans and business objectives will be achieved;
- resources are acquired economically and used efficiently;
- significant financial, managerial and operating information is accurate, reliable and timely;
- actions of the organization are in compliance with policies, procedures, contracts and applicable laws and regulations; and
- assets are safeguarded.

The **scope** of the audit encompassed:

- reviewing and testing process-level key controls relating to internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring;
- reviewing and testing activity-level key controls relating to specific products / processes.

ADVISORY WORK : *Advisory Engagement Related to the Activities of the Carbon Finance Unit*

The **objective** of the assignment was to provide advice on the design of risk management and control processes related to the activities of the Bank's Carbon Finance Unit.

The **scope** of the assignment was to:

- Provide feedback on the control framework to manage carbon finance risks, including operational process design for the Regions (event identification, risk analysis, risk response; control activities);
- Review completeness of the CFU's risk assessments; control design for the creation of Emission Reduction Payment Agreements (ERPA); and *Control Activities* for: payments of ERs using Loan Disbursement facility (LOA); processing by the back office; recovering costs; defining pricing and advance payment policies; and Carbon Fund financial administration.

Example of Use of COSO ERM Framework for Environment and Social Work

1. Internal Environment – *The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.*

Ref	Risk/Implications	Expected Controls	Testing Outline
01	Risk management philosophy is not effective.	• Entity's risk management philosophy represents shared beliefs and attitudes characterizing how the entity considers risk in all activities. • Reflects the entity's values, influencing its culture and operating style. • Affects how ERM components are applied, including how events are identified, the kind of risk accepted, and how they are managed. • Is well developed, understood and embraced by the entity's personnel. • Is captured in policy statements, oral and written communications, and decision making. • Management reinforces the philosophy with everyday actions.	• Verify that posture towards E&S matters is clearly defined, is in line with development objectives and shared by management: obtain policies. • Verify how E&S policies address MDGs: compare MDGs with E&S policies and standards
02	Risk appetite is not effective	• Entity's risk appetite reflects its risk management philosophy and influences its culture and operating style. • Entity's risk appetite is considered in strategy setting, with strategy aligned with risk appetite.	• Review the E&S performance standards (PPS) and related guidance notes to ensure that they are implementable. • Verify how Management ensures consistency between PPS and Bank's environment and social policies
03	The functioning of the Board of Directors (or comparable body) is not effective	• Board is active and possesses an appropriate degree of management, technical, and other expertise, coupled with the mindset necessary to perform its oversight responsibilities. • Board is prepared to question and scrutinize management's activities, present alternative views, and act in the face of wrongdoing. • Board has a majority of independent outside directors. • Board provides oversight to ERM and is aware of and concurs with the entity's risk appetite.	• Verify what involvement the BOD has in E&S matters.
04	The integrity and ethical values are not effective	• Entity's standards of behaviour reflect integrity and ethical values. • Ethical values are communicated and accompanied by explicit guidance regarding what is right and wrong.	• Review the Performance Standards to identify issues related to ethical standards. • Review the role of the Compliance / Advisory Ombudsman.

Example of Use of COSO ERM Framework for Environment and Social Work

Ref	Risk/Implications	Expected Controls	Testing Outline
		• Integrity and ethical values are communicated in a formal code of conduct. • Upward communications channels exist where employees feel comfortable bringing relevant information. • Penalties are applied to employees who violate the code, mechanisms encourage employee reporting of suspected violations, and disciplinary actions are taken against employees who knowingly fail to report violations. • Integrity and ethical values are communicated through management actions and the examples they set.	
05	The commitment to competence is not effective	• Competence of the entity's people reflects the knowledge and skills needed to perform assigned tasks. • Management aligns competence and cost.	• For a sample of employees verify that job description against employee qualifications
06	The organizational structure is not effective	• Organizational structure defines key responsibility and accountability. • Establishes lines of reporting. • Is developed in consideration of the entity's size and nature of activities. • Enables effective ERM.	• Verify current and future organizational structure for the E&S process
07	The assignment of authority and responsibility is not effective	• Assignment of authority and responsibility establishes the degree to which individuals and teams are authorized and encouraged to use initiative to address issues and solve problems, and provide limits to authority. • Assignments establish reporting relationships and authorization protocols. • Policies describe appropriate business practices, knowledge and experience of key personnel, and associated resources. • Individuals know how their actions interrelate and contribute to the achievement of objectives.	• Verify current and future E&S process segregation of duties and delegated authority. • Verify that procedures clearly specify roles and responsibilities of parties involved. • Verify existence of TORs / job descriptions
08	The Human Resource Standards are not effective	• Standards address hiring, orientation, training, evaluating, counselling, promoting, compensation, and remedial actions, driving expected levels of integrity, ethical behaviour, and competence. • Disciplinary actions send the message that violations of expected behaviour will not be tolerated.	• Verify leave records, training taken by employees and that performance evaluations are conducted timely and in accordance to HR procedures.

Example of Use of COSO ERM Framework for Environment and Social Work

2. Objective Setting - *Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.*

Ref	Risk/Implications	Expected Controls	Testing Outline
01	The Strategic Objectives are Unsatisfactory	• Entity's strategic objectives establish high-level goals that align with and support its mission/vision. • They reflect management's strategic choices as to how the entity will seek to create value for its stakeholders. • Management identifies risks associated with strategy choices and considers their implications.	• Verify that strategic objectives for E&S process are clearly defined Review strategy and business plan
02	The Related Objectives are Unsatisfactory	• Related objectives (for operations, reporting, and compliance) support and are aligned with selected strategy, relative to all entity activities. • Each level of objectives is linked to more specific objectives that cascade through the organization. • The objectives are readily understood and measurable and align with risk appetite.	• Verify that departmental strategy aligns with corporate broader objectives and that budget is allocated to implement strategy.
03	The risk tolerances are Unsatisfactory	• Risk tolerances are measurable, preferably in the same units as the related objectives, and align with risk appetite.	• Verify that policies/ procedures/ strategy clarify the level of residual risk that the corporation is willing to assume and define tolerance for non compliance and performance measurements.

Example of Use of COSO ERM Framework for Environment and Social Work

3. Event Identification *Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channelled back to management's strategy or objective-setting processes.*

Ref	Risk/Implications	Expected Controls	Testing Outline
01	Event identification is Unsatisfactory	• Management identifies positive or negative potential events affecting strategy implementation or achievement of objectives • Even events with a relatively low possibility of occurrence are considered if the impact on achieving an important objective is great.	• Verify that events have been identified that could impact the successful implementation of the strategy. Review strategy
02	Event Identification Techniques are Unsatisfactory	• Techniques used, look to both the past and future; Management selects techniques that fit its risk management philosophy, and ensures the entity develops needed event identification capabilities. • Event identification is robust, forming a basis for risk assessment and risk response components.	• Verify that the department has a methodology to monitor strategy implementation and analyze causes and effects. Review strategy

4. Risk Assessment - Risks *are analyzed, considering likelihood and impact, as a basis to determine how they should be managed. Risks are assessed on an inherent and a residual basis*

Ref	Risk/Implications	Expected Controls	Testing Outline
01	Assessment of Inherent and Residual risk is Unsatisfactory	• Management assesses inherent risks. • Once risk responses have been developed, management considers residual risk.	• Verify that key risks inherent in the E&S review process have been identified by management and that residual risk is being accepted in line with the defined risk tolerance.
02	Assessment Techniques are Unsatisfactory	• Management uses a combination of qualitative and quantitative techniques. • The techniques support development of a composite assessment of risk.	• Verify what methodology is used by management identify and measure risk.

5. Risk Response - *Management selects risk responses – avoiding, accepting, reducing, or sharing risk – develop a set of actions to align risks with the entity's risk tolerances and appetite.*

Ref	Risk/Implications	Expected Controls	Testing Outline
01	Risk response not well designed or operating effectively	• In responding to risk, management considers among risk avoidance, reduction, sharing and acceptance.	• Identify what key controls have been put in place to manage risks.

6. Control Activities - Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.

Ref	Risk/Implications	Expected Controls	Testing Outline
01	Integration with risk response is Unsatisfactory	• Management identifies control activities needed to ensure that risk responses are carried out properly and in a timely manner. • Selection or review of control activities includes consideration of their relevance and appropriateness to the risk response and related objective. • In selecting control activities, management considers how control activities interrelate.	• Verify that procedures exist and describe key risks and controls, and that key controls mitigate risks.
02	Policies and Procedures are Unsatisfactory	• Policies are implemented thoughtfully, conscientiously, and consistently. • Procedures are carried out with sharp, continuing focus on conditions to which the policy is directed. • Conditions identified as a result of the procedure are investigated and appropriate corrective actions are taken	• Test compliance with procedures for a sample of …...
03	Controls over Information Systems are Unsatisfactory	• Application controls are built into computer programs and supporting manual procedures, and are designed to provide completeness and accuracy of critical information. • General computer controls are broad and include access control, change and incident management, systems development and deployment, data backup and recovery, third party vendor management, and physical security controls critical to the integrity of the underlying process. • End-user computing processes, including spreadsheets and other user-developed programs are documented, secured, backed-up, and reviewed for process integrity.	• Identify all applications that are used for E&S review process. • Carry out test of IT system

7. Information and Communication - *Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.*

Ref	Risk/Implications	Expected Controls	Testing Outline

01	Identification and capture of Information is Unsatisfactory	• Relevant information is obtained from internal and external sources; the entity captures and uses historical and present data as needed to support effective ERM.
		• The entity's information infrastructure converts raw data into relevant information that assists personnel in carrying out their ERM and other responsibilities.
		• Information is provided at a depth and in a form and timeframe that are actionable, readily usable, and linked to defined accountabilities – including the need to identify, assess, and respond to risk.
		• Source data and information are reliable, and provided on time at the right place to enable effective decision making. Timeliness of information flow is consistent with the rate of change in the entity's internal and external environments.
		• Information systems change as needed to support new objectives.
			• Verify that key information for the E&S review process is obtain reliably and timely:
			  • information from clients
			  • information from internal departments

02	Communication of Information is Unsatisfactory	• Management provides specific and directed communication addressing behavioural expectations and responsibilities of personnel, including a clear statement of the entity's risk management philosophy and approach and clear delegation of authority.
		• Communication about processes and procedures align with, and underpin the desired culture. All personnel receive a clear message from top management that ERM must be taken seriously. Personnel know how their activities relate to the work of others, enabling them to recognize problems, determine cause, and take corrective action. Personnel know what is deemed acceptable and unacceptable behaviour.
		• There are open channels of communication and a willingness to listen, and personnel believe their superiors truly want to know about problems and will deal with them effectively.
		• Communications channels outside normal reporting lines exist and personnel understand there will be no reprisals for reporting relevant
			• Review the communication structure of the unit under audit to ensure clarity of objectives:
			  • with senior management and the Board
			  • with other parts of the organization
			  • within the department
			  • with the public and clients
			• Interview a number of employees to validate that the communication is transparent and effective

Ref	Risk/Implications	Expected Controls	Testing Outline
		information. • An open communications channel exists between top management and the board of directors, with appropriate information communicated on a timely basis. • Open external communications channels exist, where customers and suppliers can provide significant input. • The entity communicates relevant information to regulators, financial analysts, and other external parties.	

Example of Use of COSO ERM Framework for Environment and Social Work

8. Monitoring - The entirety of ERM is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

Ref	Risk/Implications	Expected Controls	Testing Outline
01	Monitoring of ERM is Unsatisfactory	• Management determines, through ongoing monitoring activities or separate evaluations, or a combination, whether the functioning of ERM continues to be effective.	• Verify how E&S rating are monitored vis-à-vis financial and operational risks in a project
02	Ongoing Monitoring of activities is Unsatisfactory	• Monitoring activities are built into the entity's normal, recurring operations, performed in the ordinary course of running the business. • They are performed on a real-time basis and they react dynamically to changing conditions.	• Verify how the department monitors compliance with policies and standards by personnel and clients; quality and consistency of work performed by employees at every stage of the project; and time charged on projects
03	Separate Evaluation process is Unsatisfactory	• Separate evaluations focus directly on enterprise risk disclosure effectiveness and provide an opportunity to consider the continued effectiveness of the ongoing monitoring activities. • The evaluator understands each of the entity's activities and each ERM component being addressed. • The evaluator analyzes ERM design and the results of tests performed, against the backdrop of management's established standards, determining whether ERM provides reasonable assurance with respect to the stated objectives.	• Verify what type of review is carried out by other oversight units

04	Reporting of deficiencies is Unsatisfactory	• Deficiencies are reported from both internal and external sources carefully considered for their implications for ERM, and corrective actions are taken
		• All identified deficiencies that affect the entity's ability to develop and implement its strategy and to achieve its established objective are reported to those positioned to take necessary action.
		• Reported transactions or events are investigated and corrected, and potentially faulty underlying procedures are also re-evaluated.
		• Protocols are established to identify what information is needed at a particular level for effective decision making.
			• Verify what reports are available for:
			  • Board and Senior Management
			  • operational management
			  • oversight bodies
			  • the public