How to Build an ESG Risk Register Using COSO ERM

If there is one question I hear repeatedly from boards, risk managers and sustainability teams, it is this: "Where do we start with ESG risk management?"

My answer is often straightforward. Start with an ESG Risk Register.

Many organizations have ESG policies, sustainability reports and ambitious commitments. However, far fewer have a structured mechanism for identifying, assessing, managing and monitoring ESG risks in a way that supports decision-making.

An ESG Risk Register serves as the bridge between sustainability aspirations and enterprise risk management. It translates ESG issues into business risks, assigns accountability and enables effective oversight by management and the board.

Why an ESG Risk Register Matters

A common mistake is treating ESG as a separate initiative from Enterprise Risk Management. Under the COSO ERM framework, ESG risks should be assessed using the same discipline applied to strategic, operational, financial and compliance risks.

An effective ESG Risk Register allows organizations to identify material ESG risks, evaluate potential impacts, prioritize resources, assign ownership and monitor performance through meaningful indicators.

Step 1: Identify ESG Risks

Begin by identifying environmental, social and governance risks that could affect business objectives.

Environmental risks may include climate transition, carbon pricing, water scarcity, waste management and biodiversity impacts.

Social risks may include labour practices, employee wellbeing, human rights concerns, talent retention and community relations.

Governance risks may include corruption, conflicts of interest, weak oversight, cybersecurity and regulatory non-compliance.

The objective is not to create a long list. The objective is to identify risks that could materially affect value creation and business performance.

Step 2: Develop Clear Risk Statements

Every risk should be expressed as a risk statement.

For example: Failure to reduce greenhouse gas emissions in line with stakeholder expectations may result in increased operating costs, loss of customers and reputational damage.

Strong risk statements help management understand both causes and consequences.

Step 3: Assess Likelihood and Impact

The next step is to evaluate the likelihood and impact of each ESG risk.

Organizations should consider financial, operational, regulatory, reputational and stakeholder impacts. Using a consistent risk matrix ensures ESG risks can be compared against other enterprise risks.

Step 4: Identify Existing Controls

An ESG Risk Register should document controls currently in place.

Examples include sustainability policies, supplier audits, anti-bribery programmes, cybersecurity controls, environmental management systems and board oversight mechanisms.

Understanding existing controls helps determine residual risk exposure.

Step 5: Assign Risk Ownership

Every ESG risk should have a clearly identified risk owner.

One of the biggest weaknesses I observe is that ESG risks are often assigned solely to sustainability teams. In reality, ownership should sit with the business functions responsible for managing the risk.

Step 6: Establish Risk Treatment Plans

For high-priority risks, organizations should develop specific mitigation actions.

These may include emission reduction initiatives, enhanced supplier due diligence, workforce development programmes, strengthening governance controls or improving data management processes.

Step 7: Define Key Risk Indicators (KRIs)

A risk register should not be a static document.

KRIs provide management with early warning signals and enable continuous monitoring.

Examples include carbon emissions, injury frequency rates, employee turnover, supplier audit findings, compliance breaches and cybersecurity incidents.

What a Good ESG Risk Register Looks Like

At a minimum, the register should include:
• Risk ID
• ESG Category
• Risk Statement
• Likelihood Rating
• Impact Rating
• Inherent Risk
• Existing Controls
• Residual Risk
• Risk Owner
• Treatment Actions
• Key Risk Indicators

My View

The value of an ESG Risk Register is not the document itself. The value lies in the conversations it creates.

A well-designed register helps boards and management move beyond sustainability reporting and focus on risk-informed decision-making.

Organizations that integrate ESG risks into COSO ERM frameworks are better positioned to improve resilience, strengthen governance and create long-term value.

Final Thoughts

An ESG Risk Register is often the first practical step in embedding ESG into Enterprise Risk Management.

The organizations that will lead in the coming years are not necessarily those producing the longest sustainability reports. They are the organizations that understand their ESG risks, assign accountability and take proactive action before those risks become business problems.

About the Author:

KC Teo is a National Quality Expert (Corporate Sustainability & ESG Frameworks) conferred by the Institute of Quality Malaysia (IQM). As Principal Consultant and Founder of VeriSustain MyESG PLT, he specializes in ESG advisory, IFRS S1/S2 readiness, GHG accounting, and sustainability assurance-readiness.

Website: https://verisustain.my | Email: consultant@verisustain.my | Mobile: +60 13-699 6033