VeriSustain Article | VS-ERM05 - Integrating ESG Risk into ISO 31000: A Practical Guide

Executive Summary

ESG risks have evolved from being viewed primarily as sustainability or corporate responsibility issues into **core business risks** that can affect enterprise value, operational resilience, regulatory compliance, access to capital and stakeholder confidence.

Climate change can disrupt physical assets and supply chains. Rising energy and carbon costs can affect margins. Labour and workplace issues can create operational and reputational consequences. Supply-chain human rights concerns can expose organisations to customer, regulatory and market pressures. Governance failures can result in financial losses, regulatory action and significant damage to corporate reputation.

The challenge is therefore no longer simply whether organisations identify ESG risks.

The more important question is:

Are ESG risks being managed with the same discipline as strategic, operational, financial and other enterprise risks?

ISO 31000 provides a practical framework for answering that question. Rather than creating a completely separate ESG risk management system, organisations can integrate material ESG risks into their existing Enterprise Risk Management (ERM) processes.

This approach also creates a stronger foundation for sustainability reporting and climate-related disclosures under frameworks such as IFRS S1 and IFRS S2.

Why ESG Risk Matters

Organisations are increasingly exposed to risks arising from environmental, social and governance factors.

Climate-related events may disrupt facilities, logistics networks, utilities and production. Changes in energy prices and future carbon policies may increase operating costs. Supply-chain disruptions may affect availability of critical materials. Labour challenges may affect productivity, employee retention and business continuity.

Governance failures can be equally significant.

Weak oversight, inadequate internal controls, corruption, poor escalation mechanisms or ineffective accountability can create consequences extending well beyond the sustainability function.

These risks should therefore not be treated as isolated ESG issues.

They should be considered as part of the organisation's overall risk profile.

Effective ESG risk management enables management and the Board to understand:

- Which ESG risks could materially affect the organisation;
- Where those risks originate within the value chain;
- Who owns and manages each risk;
- What controls currently exist;
- What additional treatment actions are required; and
- Which indicators should be monitored as early warning signals.

The objective is not to create more documentation. The objective is to improve **decision-making and organisational resilience**.

Understanding ISO 31000

ISO 31000 provides principles and guidelines for managing risk across an organisation.

Its strength is that it is not limited to a particular risk category. ESG risks can therefore be incorporated alongside strategic, operational, financial, compliance, technology and other enterprise risks.

Key concepts within the ISO 31000 approach include **value creation and protection, integration, inclusiveness, structured and comprehensive processes, continual improvement, and consideration of the best available information**.

For ESG management, this is particularly important.

Many organisations already have ESG-related controls operating within different parts of the business.

For example:

- Environmental teams monitor energy, emissions and environmental compliance.
- Human resources manages labour and employee-related matters.
- Health and safety teams manage workplace risks.
- Procurement manages suppliers and due diligence.
- Compliance and legal teams monitor regulatory requirements.
- Finance monitors financial exposures and controls.
- Sustainability teams coordinate reporting and stakeholder expectations.

The problem is often not the absence of controls. **The missing link is integration.**

VeriSustain Insight: Integration Is the Missing Link

One of the most practical ways to improve ESG risk management is to avoid building a completely separate ESG risk system.

Instead, organisations should identify where existing ESG-related risks already sit within their enterprise risk architecture and then strengthen the connection between them.

For example, a company's climate risk should not remain solely within a sustainability report.

A physical climate risk affecting a manufacturing facility may also represent:

Climate hazard → operational disruption → production loss → revenue impact → liquidity pressure → financial risk.

Similarly:

Carbon pricing → higher production costs → margin compression → competitiveness risk → strategic risk.

And:

Supplier human rights issue → customer concern → contract risk → reputational damage → revenue risk.

This cause-and-effect thinking allows ESG risks to move from abstract sustainability concepts into management-level business risks.

A Practical ESG Integration Framework

Organisations can integrate ESG risks into their ISO 31000 process through a structured sequence.

1. Establish Context

Start by understanding the organisation's business model, strategy, operating environment and value chain.

Consider:

- Key operations and assets;
- Critical suppliers;
- Geographic exposure;

- Regulatory environment;
- Customer expectations;
- Strategic objectives; and
- Material sustainability issues.

The context provides the basis for determining which ESG risks are relevant to the organisation.

2. Identify ESG Risks

Translate material ESG issues into specific risk statements.

For example, instead of simply recording **“Climate Change”**, identify the underlying business risk:

> “Increasing frequency of extreme rainfall may disrupt production at flood-prone facilities and result in operational downtime and repair costs.”

This makes the risk more actionable.

3. Analyse Likelihood and Impact

Assess each risk using the organisation’s existing risk assessment methodology.

Where appropriate, consider:

- Likelihood;
- Financial impact;
- Operational impact;
- Legal or regulatory impact;
- Reputational impact;
- Time horizon; and
- Existing control effectiveness.

The same risk-rating methodology used for other enterprise risks should, where practical, be applied to material ESG risks.

4. Evaluate Significance

Determine whether the risk falls within the organisation’s risk appetite or tolerance.

This step is important because not every ESG issue requires the same level of management attention.

Material risks should receive appropriate escalation and resources.

5. Implement Treatment Actions

Risk treatment should move beyond general commitments.

A useful ESG risk register should identify:

Risk → Impact → Likelihood → Existing Control → Treatment → Risk Owner → Target Date → KPI/KRI.

For example:

ESG Risk	Impact	Likelihood	Existing Control	Treatment
Carbon Cost Exposure	High	Medium	Energy Monitoring	Decarbonisation Plan
Workplace Injury	High	Low	Safety System	Enhanced Training
Supply Chain Human Rights	Medium	Medium	Supplier Audit	Due Diligence

The objective is to convert identified risks into measurable management actions.

6. Monitor and Review

ESG risk management should not be a once-a-year exercise conducted before sustainability reporting. Risk indicators should be monitored throughout the year.

Depending on the organisation, these may include:

- Energy intensity;
- GHG emissions;
- Carbon exposure;
- Workplace incident rates;
- Supplier assessment results;
- Water consumption;
- Climate-related disruptions; and
- ESG-related regulatory developments.

These indicators can provide early warning signals before risks become significant business events.

Malaysian Case Example

Consider a Penang electronics manufacturer responding to increasing customer requests for climate and sustainability information.

Rather than treating the requests purely as a reporting exercise, management integrates climate-related risks into its existing ISO 31000 risk management process.

The exercise improves visibility of several exposures, including:

- Energy-cost exposure;
- Potential future carbon policies;
- Supply-chain vulnerabilities; and
- Customer sustainability requirements.

The immediate benefit is not simply a better sustainability report. Management gains a clearer understanding of how climate and ESG factors could affect the company's operating model and future competitiveness.

At the same time, the organisation becomes better prepared to respond to sustainability reporting requirements. This illustrates an important principle:

ESG reporting becomes stronger when it is supported by an underlying risk management process.

Connecting ESG Risk Management with IFRS S1 and IFRS S2

The integration of ESG risks into ERM also supports the organisation's sustainability reporting readiness. IFRS S1 and IFRS S2 place significant emphasis on governance, strategy, risk management, and metrics and targets relating to sustainability-related and climate-related risks and opportunities.

An organisation with an established ESG risk management process is therefore better positioned to demonstrate how risks are:

- Identified;
- Assessed;
- Prioritised;
- Managed;
- Monitored; and
- Reported.

For climate-related matters, this becomes particularly relevant when organisations assess physical and transition risks and their potential implications for business strategy and financial performance.

The risk register should therefore not exist independently from sustainability reporting.

Ideally, there should be a traceable connection:

Material ESG Issue → Risk → Risk Assessment → Treatment → KPI/KRI → Management Monitoring → Sustainability Disclosure.

This creates a more defensible reporting process.

Bursa Malaysia Perspective

For Malaysian listed companies, effective ESG risk governance can strengthen the quality of materiality assessments, sustainability statements and climate-related disclosures.

The key consideration is not simply whether ESG information appears in the sustainability statement. The more important question is whether the disclosed information reflects actual governance and management processes within the organisation.

A mature approach should allow management to demonstrate that material ESG risks have been considered within the broader corporate risk framework rather than being managed exclusively by a small sustainability team.

This also helps create clearer accountability between the Board, senior management, risk owners, sustainability functions, finance and other business functions.

What Boards Should Be Asking

Boards do not necessarily need to become technical ESG specialists. However, they should be asking the right governance questions:

What are our most significant ESG risks?

Who owns these risks?

How are they being monitored?

What controls are currently in place?

What indicators provide early warning signals?

Are ESG risks integrated into Enterprise Risk Management?

How do these risks potentially affect strategy, financial performance and enterprise value?

If management cannot confidently answer these questions, the organisation may have strong reporting capabilities but relatively weak ESG risk governance.

My View

The future of ESG management will increasingly depend on whether organisations can move beyond the **report-first mentality**. Sustainability reporting remains important. However, reporting should communicate the outcomes of governance, strategy and risk management processes.

It should not substitute for them.

ISO 31000 provides a practical foundation because it allows organisations to integrate ESG risks into an established enterprise risk architecture rather than creating a parallel system.

The most effective approach is therefore not:

ESG Reporting → ESG Risk Management

It is:

ESG Risk Identification → ERM Integration → Risk Treatment → Monitoring → Management Decision-Making → Sustainability Reporting.

That sequence produces a much stronger connection between what an organisation says and what it actually manages.

Final Thoughts

A sustainability report can tell stakeholders **what happened**.

An effective ESG risk management framework helps management understand **what could happen next**.

In an increasingly uncertain operating environment, organisations need both.

But if management is deciding where to begin, the starting point should be **governance, risk identification, assessment and treatment**. When ESG risks are properly integrated into ISO 31000 and Enterprise Risk Management, sustainability reporting becomes more than a disclosure exercise.

It becomes evidence of how the organisation understands, governs and manages the risks that may affect its future. **Reporting then has a stronger story to tell — because the story is supported by the organisation's risk management system.**
