Winning a seat at the ESG table

Received: 28th October, 2021

Jonny Frank
Partner, StoneTurn, USA

Jonny Frank is a Partner at global advisory firm StoneTurn. He serves as the Department of Justice (DOJ)-appointed Monitor to Deutsche Bank, DOJ voluntary monitor and remediation consultant to a northern European bank, forensic audit adviser to the SEC-appointed Independent Consultant of a Big Four public accounting firm, and US DOJ-appointed Independent Auditor to a top five automotive manufacturer. He previously served as the Executive Deputy Compliance Monitor of Volkswagen, NY Department of Financial Services Compliance Monitor of Ocwen Financial Corporation, a Big Four partner, Executive Assistant United States Attorney for the Eastern District of New York and on the faculties of the Yale School of Management, Fordham University Law School and Brooklyn Law School.

StoneTurn, 17 State Street, 2nd Floor, New York, NY 10004, USA
E-mail: jfrank@stoneturn.com

Jim Barolak
Partner, StoneTurn, USA

Jim Barolak is a Partner at global advisory firm StoneTurn. He views risk management and compliance through the lens of sustainability with a focus on corporate social responsibility and environmental, social and governance reporting (ESG) reporting. He is a subject matter expert (SME) on risk assessments and internal controls, and served as SME for the DOJ-appointed independent compliance and business ethics monitor to one of the world's largest investment banks and also supported the monitorship team of a large US mortgage servicer. He brings nearly 40 years of experience as a trusted adviser, results-driven project lead and engineer.

StoneTurn, 17 State Street, 2nd Floor, New York, NY 10004, USA
E-mail: jbarolak@stoneturn.com

Germari Pieterse
Managing Director, StoneTurn, USA

Germari Pieterse is a Managing Director at global advisory firm StoneTurn. She is a Charter Accountant in South Africa. A former COO and CFO, Germari leverages her significant C-suite expertise to help clients identify and implement pragmatic approaches to governance, management and analysis, as well as ESG reporting, corporate social responsibility and impact investment. She advises clients on the design of effective financial infrastructures, enhancement of governance and compliance programs and also conducts internal audits and assessments.

StoneTurn, 244 Jean Avenue, Norma Jean Square, Unit 5 Centurion, Gauteng 0046, South Africa
E-mail: gpieterse@stoneturn.com

Abstract Financial Institutions (FIs) struggle to identify, assess and develop appropriate responses that proactively address potential events for more traditional known risks let alone new, emerging and imprecise risks in the often difficult-to-quantify Environmental, Social & Governance (ESG) space. ESG-related risks present even greater challenges to established risk management frameworks such as COSO because ESG risks are generally not well known to the business and include 'black swans' or other unforeseen events that can challenge the entities' short-term or long-term performance or even survival; tend to be longer term in nature than the timeline with which strategy is set or risks have been considered historically; and beyond the scope of any one entity. The good news is that FIs' existing — and often highly sophisticated risk, compliance and legal functions (Risk Team) — are well equipped to integrate and mitigate these significant

ESG-related risks into the FI's risk management framework. The authors, drawing upon first-hand experience as government-appointed monitors for large, global financial institutions, provide a practical roadmap for defining and mapping ESG-related risks. They also explain why Chief Risk Officers, Chief Compliance Officers and Chief Legal Officers must seize this unique opportunity to not only avoid the financial, legal, regulatory, and reputational losses that will inevitably follow without an ESG risk management programme — but also enhance the value the Risk Team delivers as ESG priorities become pervasive across FIs worldwide. Acknowledging that sustainability and/or ESG professionals are uniquely qualified to provide critical guidance defining and communicating the FI's objectives, the authors provide a proven framework and methodology for compliance and risk practitioners to leverage as they reach across the aisle to their counterparts in Sustainability or Corporate Social Responsibility to elevate the ESG risk conversation and their own visibility.

Keywords: *ESG/environmental social & governance, ESG risks, greenwashing, sustainability, ESG integration, CSR*

INTRODUCTION

Prompted by ever-growing awareness and market interest in Environmental, Social & Corporate Governance (ESG) criteria, Financial Institutions (FIs) worldwide rushed to appoint Chief Social Impact & Sustainability Officers, Chief Corporate Responsibility Officers, Chief Social Responsibility Officers, Global Heads of Sustainability, Global Heads of Sustainable Finances, Head of Sustainable and Impact Investment Strategy, Chief ESG Officers or related functions (collectively, Chief Sustainability Officers or 'CSOs'). These appointments serve as a critical first step toward creating and communicating FI commitment to an ESG agenda.

But how do FIs establish ESG strategic objectives that balance societal, customer and business interests? How do the ESG objectives impact compliance, conduct, credit, market and operational risk? Who supports the CSO to identify and develop a response to ESG-related risks? Why must the Chief Risk Officer (CRO), Chief Compliance Officer (CCO) and Chief Legal Officer (CLO) sit at the ESG table?

In the ESG spotlight

ESG is neither new nor a fad. Sixty years ago, Rachel Carson wrote 'Silent Spring', raising public awareness and concern about the environment and linking pollution and public health. Fifty years ago, the US marked its first Earth Day, followed twenty years later as a global UN initiative.[1] Twenty-four years ago, work began on the Kyoto Protocol, with 191 countries pledging to reduce greenhouse gas emissions.[2] Twenty years ago, United National Global Compact issued 'a call to companies to align strategies and operations with universal principles on human rights, labor, environment, and anti-corruption, and take action to advance those goals'.[3] Ten years ago, the Sustainability Accounting Standards Board (SASB) launched standardised sustainability accounting and measurements across 77 industries.[4] Earlier this year, US President Joseph Biden appointed domestic and international 'climate czars' and, on his first day in office, signed an executive order re-joining the Paris Agreement.[5]

Now, ESG has taken the limelight in financial services as customers, investors and regulators demand FIs leverage their role as financial intermediaries to influence ethical and sustainable behaviour. Bloomberg reports, by 2025 ESG assets under management should reach $53tn, more than a third of the expected $140.5tn global total.[6]

CROs, CCOs and CLOs essential to successful ESG program

FIs espoused ESG commitments and appointed CSOs to establish and drive newly minted ESG programs,[7] often without first identifying and understanding practical implications. It is a 'no-brainer' to oppose human slavery and embrace diversity and inclusion. But does that require the FI

to conduct 'know your customer' (KYC) reviews to assess its clients, customers' and counterparties' human slavery and diversity and inclusion policies? How should a FI manage customer, investor, employee and NGO expectations following the appointment of a CSO? What risks must the CSO overcome to achieve the FI's ESG objectives? Must the CSO and the FI adjust objectives based on the identified risks?

For the ESG program to succeed, ESG risk culture and awareness must be woven up, down and across the fabric of the organisation. CROs, CCOs and CLOs (collectively, the 'Risk Team') know the ins and outs and participate in virtually every FI business unit and function. They oversee programs that overlap with ESG principles (eg, ethics and compliance, conduct risk). The Risk Team must support CSOs as clients, in the same way it supports revenue-generating businesses to identify, assess, prioritise and respond to ESG-related risks. Resource constrained and with a limited presence, CSOs can leverage the, by comparison, huge Risk Team to champion and market the ESG program.

But don't wait for an invitation

The surest way for Risk Teams to secure a seat at the ESG table is to co-host, with the CSO, workshops among key internal (and possibly external) stakeholders (eg, business unit leaders, Communications, Human Resources, Investor Relations, and Internal Audit) to discuss the implications and 'knock-on' effects of adopting an ESG agenda. Workshop participants will quickly realise the need to fold-in the ESG program into existing risk and compliance frameworks.

ESG risks manifest across the FI's own operations, its various business units and its customers, borrowers and clients. ESG issues crop up in known risks, lurk undetected as hidden risks and grow over time as emerging risks.

The good news is FIs, more so than most organisations, understand the benefits of effective risk management and potential disastrous consequences of poor risk management. The Risk Team can help CSOs identify and assess key ESG risks as part of this disciplined, pre-existing approach.

COSO provides a starting point

ESG risks should be integrated with the FI's existing risk management processes. For most FIs, it will be COSO,[8] the most widely used framework to manage strategic, operational, compliance and reporting risk. The COSO ERM framework, if thoughtfully designed and carefully implemented, provides a well-documented and integrated approach for integrating strategic objectives and effective risk management.

But don't be fooled by COSO's seeming simplicity. Experienced risk and compliance professionals know COSO requires several annual cycles to implement as organisations plough through setting objectives, defining and identifying risks, linking key control activities, assessing inherent and residual risk, developing and implementing a risk response and monitoring the program.

ESG-related risks are particularly challenging because they are often (1) new or emerging and may unexpectedly threaten an organisation's ability to achieve its strategy and business objectives; (2) not well known to the business and include 'black swans' or other unforeseen events that can challenge the entity's short-term or long-term performance or even survival; (3) longer term in nature, going beyond the timeline with which strategy is set or risks have been considered historically; (4) generally difficult to quantify and communicate in the context of business language and objectives; and/or (5) beyond the scope of one entity and therefore require response at industry or government levels.[9]

ESG OBJECTIVES

COSO begins with objectives and defines 'risk' as events that impede an organisation's ability to achieve strategic, operational, compliance and objectives. 'Opportunities' are events that enhance the likelihood of the organisation achieving objectives. This definition links objectives with risks.

To mitigate ESG risks, organisations must develop ESG objectives to determine the types of risks it will encounter in pursuit of achieving its ESG objectives. Conversely, the FI's capacity to handle certain risks will (or at least should) influence its decisions when deciding ESG objectives.

Ideally, the FI's ESG objectives should be rooted in a genuine desire to do what's right for a broad base of stakeholders. That differentiates ESG risk from other risk types that are regulatory or financially driven, and it elevates ESG as an important potential conduct, ethical leadership, and reputational risk.

As ESG/sustainability experts, CSOs play a vital role advising the Board and C-suite in defining and communicating the FI's ESG/sustainability objectives and agenda. However, the Risk Team, with its strong understanding and extensive operational experience with COSO, is best positioned to operationalise much of the FI's ESG strategic agenda. We specifically suggest the Risk Team take a lead role to help the FI: (1) develop and embed ESG culture and risk awareness; (2) identify and assess ESG risks; (3) develop and implement risk responses; and (4) create a process to investigate and remediate ESG 'incidents.'

ESG CULTURE AND RISK AWARENESS

ESG culture and risk awareness are as fundamental to an effective ESG program as a culture of integrity is essential to an effective compliance program.

FIs are better off not to mention ESG unless they plan affirmative steps to embed ESG into the corporate culture. Sooner or later — likely sooner — employees, NGOs, customers, investors, the media or regulators will attack the FI's commitment if ESG is a 'bolt-on' program, or worse, a hollow greenwashing initiative.

CCOs, because they already coordinate efforts to instil a culture of compliance and integrity, are well positioned to organise activities to embed the FI's ESG agenda into corporate culture. The principal difference is 'culture of integrity' focuses on what's best for the customer; ESG culture centres on what's best for society.

Define and measure ESG values and principles

Begin with the FI's official values and principles. Consider if and how the FI should revise them to incorporate the ESG agenda. Take particular care to understand the revenue and cost implications on individual business segments. At global banks, for example, the ESG agenda will vary among retail banking, corporate lending and asset management. It is one thing for asset management to consider the sustainability program of investment candidates. It's quite another for the retail and corporate bank units to force customers to adopt the FI's ESG agenda as a condition of obtaining a loan or some other bank service or product.

Next, assess whether the FI's corporate culture matches the revised values and principles. Do not rely exclusively on unreliable employee surveys.[10] We recommend using employee focus groups and interviews.

Ask employees to state the FI's official values and principles. (Prepare senior management to receive feedback that most employees do not know values and principles the FI spent many hours and money drafting and publicising.) The exercise will help shape the ESG culture and objectives and inform adjustments the FI must make to instil its desired ESG culture and risk awareness.

Leverage ongoing efforts to instil an ESG culture

FIs have programs to instil a culture of compliance and integrity, although maturity levels vary from bare mission and vision statements to comprehensive companywide culture programs. FIs with immature programs can leverage ESG to help bring the ethics and compliance program within regulatory and industry standards.

Key features for the Risk Team to consider and Chief Audit Executive to audit include: (1) a strong and consistent ESG tone from the top; (2) middle management reinforcement; (3) speak up; and (4) the employment lifecycle.

Develop Strong and Consistent ESG Tone from the Top

It is neither difficult, time consuming nor expensive for senior management to demonstrate it regards ESG as crucial to business success. Frequent and effective messaging and engagement about the importance of ESG is key.

Strategic appointments and changes to the institution's structures to reflect focus on ESG send a powerful message. The appointment of a CSO to serve on the senior leadership team is an important step in reinforcing this message. But, to avoid the appointment becoming an empty gesture, FIs must include the CSO as an active member of the senior leadership team no differently than CRO, CCO and CLO involvement in significant decision-making.

Middle Management Reinforcement

ESG risk management spreads across business and infrastructure functions. FIs vary on whether the CSO sits with the CEO, Risk & Compliance or other functions.[11] Besides organisational charts, the FI must ensure that ESG, as core to institutional culture, is embedded and promoted throughout all aspects of business operations.

Middle management serves as an essential catalyst of companywide implementation. Employees often take their cues as to what is important and unimportant from their immediate supervisor, not CEO platitudes.

FIs should consider managers' roles in instiling ESG culture from an integrated, but practical approach, to ensure no 'gaps'. Middle management should incorporate ESG into existing management practices including (1) engaging teams in regular discussions about ESG-related matters; (2) developing ESG-linked metrics and KPIs to assess success of efforts to instil an ESG culture in their business units; and (3) addressing issues indicated by the metrics and KPIs and/or identified as ESG risks. And FIs' Learning and Education functions should provide trainings and tools to help middle managers support raising ESG awareness and drive behavioural change.

Speak-up

Speak-up without fear of retaliation is fundamental to a healthy corporate culture. FIs should apply the same practices to ESG as they do other aspects of speak-up (eg, encouraging employees to raise ESG concerns without fear of negative consequences, recognising employees who speak-up, training managers to listen-up, and assessing the effectiveness of the speak-up program).[12]

Employment Lifecycle

The employee lifecycle offers additional opportunities to instil and demonstrate FIs' commitment to its ESG values and beliefs. Pay particular attention to the recruitment and onboarding processes to emphasise the FI's ESG culture and conduct expectations. Consider integrating the ESG agenda into mandatory training for new employees and ask them to self-certify they will align and comply with the institution's ESG values and policies. Performance and reward structures similarly provide an opportunity to make ESG real and demonstrate the FI's committment. Most important, FIs must ensure leadership, staffing and budget support the ESG program.

ESG RISK IDENTIFICATION AND ASSESSMENT

The Risk Team likely will need first to orient the CSO to risk management basics. COSO's *Applying Enterprise Risk Management to Environmental, Social and Governance-Related Risks* is an excellent primer.[9]

Start with the basics

Articulate ESG Objectives

ESG risk assessment begins by defining ESG objectives, which, among FIs, varies extensively. US-headquartered FIs tend to focus on the 'E' ESG pillar. European FIs tend to include all three pillars, and some even include financial crime and conduct risk in their ESG agenda.

Create Uniform Risk Description Format

The next step is to design a format to describe ESG risks to avoid miscommunication and misunderstanding during risk identification and assessment. Again, apply the same format the FI uses to describe other nonfinancial risks. We suggest describing risks in three parts: (1) the cause, (2) the risk and (3) effect.

Illustration: Greenwashing might be described: *'To impress shareholders* (**cause**), *the FI incorrectly reports gas emissions as decreasing when, in fact, they are increasing* (**risk**), *which negatively impacts brand value and*

L2 Risk Type	L3 Risk Type	L4 Risk Type	Example Scenarios
Environmental	Climate Change	Inadequate Diligence & Monitoring of Investments	Because the FI's asset management business conducted inadequate diligence (cause), the FI inadvertently mis-marketed FI mutual funds as environmentally friendly (risk), which resulted in potential civil and regulatory liability and loss of brand value (effect).
Social	Human Capital	Poor Diversity, Equity & Inclusion (DEI) Results	Because the FI failed to demonstrate the appropriate 'Tone from the Top' (cause), the FI did not meet its DE&I goals (risk), which resulted in staff resigning to join FIs more successful in DE&I recruiting and promotion (effect).
Governance	Corporate Behaviour	Poor Business Ethics	Because the FI did not consider ethics during recruitment or require ethical decision making in the on boarding curriculum (cause), the FI hired an employee, who, after previously being fired for sexual harassment, sexually harassed co-workers, who filed a lawsuit and expressed concerns on social media (risk), which led to civil liability and challenges to the FI's recruitment efforts (effect).

Figure 1: ESG risk taxonomy with definitions and scenarios

Note: Excerpt for illustrative purposes only.

undermines stakeholder confidence in the FI's commitment to ESG' (**effect**).

Treat ESG Risks as BOTH Standalone and Cross-Taxonomy Risks

FIs commonly organise risk taxonomies into two to four levels, depending on their risk and compliance frameworks. FIs might add ESG, for example, as a new Level 1 risk type alongside regulatory compliance, financial crime, technical, and other Level 1 risk types. Level 2 ESG risks could then derive from the three ESG pillars (ie, environmental, social and governance), with Levels 3 and Level 4 added for more granular risks at each ensuing level.

Best practices include sample scenarios for each risk type described in three parts (ie, cause, risk and effect) to illustrate how the risks can affect the FI's own operations and its customers, borrowers and clients (See Figure 1).

ESG risks can manifest across all risk types and must be assessed in an integrated manner across the FI's entire operations. Treat ESG risks *both* as standalone and cross-taxonomy risks. For example, the increased likelihood and impact of severe weather from global warming (the cause) manifests as an operational (ie, nonfinancial) risk if FI call centre employees cannot get to work (the risk), which disrupts customer service operations and slows response time (the effect). This same weather-induced risk manifests as a credit (ie, financial) risk if it disrupts a borrower's supply chains, production schedule, sales and revenues, which causes the borrower to default on its loan.

Establish ESG Risk Likelihood and Impact Categories

Successful FIs align their strategies and business objectives to achieve their missions, visions, and core values. A disciplined approach to understanding the likelihood and potential impact of risks is foundational to quantifying risk and setting risk appetite and risk tolerance levels. FIs use a two-dimensional risk rating matrix that measures likelihood and impact if the risk occurs. Some FIs measure likelihood as a percentage (eg, 20% chance the risk of occurring). Other FIs prefer to express likelihood in terms of the event occurring over a set time period (eg, once in every five years).

Impact involves more than the balance sheet or income statement. Besides financial implications, FIs should factor reputation, employee retention, investor and customer marketing and regulatory and legal consequences when measuring impact.

FIs can use the same two-dimensional risk rating to quantify current ESG risks with two caveats, First, the evolving ESG regulatory landscape is

likely to increase both likelihood of occurrence and potential impact. Secondly, even absent stricter regulations, the likelihood and impact of reputational risks may increase as societal awareness and demands for corporate responsibility continue to accelerate.

Identify ESG risks

Differentiate Among Known, Hidden and Emerging ESG Risks

Known risks on a FI's risk taxonomy commonly include: (1) compliance risks related to all laws and regulations within all jurisdictions in which the FI and its customers/clients operate; (2) risks identified from internal investigations; and (3) risks identified by internal audit findings.

Hidden risks are events and scenarios not included on the risk taxonomy. Many ESG risks fall into this category, at least until the FI conducts a proper ESG risk assessment. Revenue generators, especially mid-career employees, tend to be the best source to identify hidden risks. FIs can unlock the information through workshops and interviews.

Emerging risks are those arising from internal or external triggers (eg, changing ESG regulations, increased societal awareness, demand for corporate responsibility). To identify emerging ESG risks, FIs should systematically monitor news headlines, regulatory developments, and stakeholder opinions.

Collect information from Internal and External Sources

FIs stand on centre stage with customers, investors and regulators demanding FIs leverage their role as financial intermediary to influence ethical and sustainable behaviour. To identify ESG risks, FIs must collect information from an array of internal and external stakeholders. Failing to consider information from internal and external sources leaves FIs exposed to undetected known, hidden and emerging risks.

Key internal and external sources of direct and contextual risk information include: (1) the FI's law and regulations library; (2) prior risk assessments; (3) self-identified business issues; (4) results of internal investigations; (5) regulatory findings; (6) internal and external audit findings; (7) control testing results; (8) external events; and (9) industry knowledge.

Facilitate Cross-Functional Workshops

Cross-functional workshops endorsed (and, better yet, attended) by Board and C-Suite executives are essential to identify potential ESG risks. Gather key internal stakeholders, including representatives from Legal, Compliance, Risk, Audit and, most important, revenue-generating business units. Workshops with external stakeholders would also be valuable, although, as a practical matter, too much to include in the initial ESG risk assessment.

Engage workshop participants in creative 'out of the box' thinking to uncover possible events and scenarios that would impede achieving the ESG agenda and objectives. Consider ice breakers, role-playing and/or competitive exercises (eg, angels versus demons, red team versus blue team, 'the perfect crime' scenarios) to brainstorm reasonably likely scenarios to identify undetected known, hidden, or emerging ESG risks. Avoid optimism bias (eg, '…that could never happen here').

Identify ESG control activities

Identify and Link ESG Risks to Key Control Activities

Not all control activities are created equal. Focus the CSO Team on identifying key control activities — those that reduce the likelihood and mitigate the impacts of the most material risks. Some control activities are manual, others automated. Some are preventive, others detective. Deterrent control activities identify and remove causal and enabling factors. Directive control activities achieve desired risk outcomes through policies, processes and controls.

Identifying key control activities and potential controls gaps includes: (1) process mapping, (2) walkthroughs; and (3) risk and control owner(s) interviews. Process mapping involves documenting key business processes and mapping key controls through each step of the process. Use walkthroughs to validate the process mapping by tracing a specific activity from start to finish and identifying key controls (or control gaps) throughout the process. As a final validation, interview risk owners to

L4 Risk Type	Control Name	Control Description	Control Owner	Control Type (Preventive versus Detective)	Control Frequency	Automatic/ Manual
Inadequate Diligence & Monitoring of Investments	Diligence	Evaluate asset management investment candidates under a globally accepted ESG rating framework and scorecard.	1st Line of Defence (LoD) (eg, Asset Management)	Preventive	Ad Hoc	Manual
Poor DEI Results	Diversity Recruiting & Promotion	Consider a minority candidate when recruiting or promoting to a Level IV or above position.	1st LoD (eg, Business Unit Risk & Controls); 2nd LoD (eg, HR)	Preventive	Daily	Manual
Poor Business Ethics	Ethics Training	Include ethical decision-making framework training in onboarding curriculum.	1st LoD (eg, Business Unit Risk & Controls); 2nd LoD (eg, HR)	Preventive	Quarterly	Manual & Automated

Figure 2: ESG control inventory

Note: Excerpt for illustrative purposes only.

provide input on elements of the process that worked well, could be improved, and did not work effectively due to inadequately designed or implemented control activities.

Create and Populate Key ESG Control Activities Inventory

A control activities inventory links key control activities to the risks they mitigate. For each key control activity, the inventory provides information about WHO owns and performs the control; WHAT the control achieves; WHERE within the FI's business process the control is applied, WHEN the control is performed, WHY it is important and HOW it is performed (See Figure 2).

Assess ESG risks

Assess Inherent ESG Risk, ESG Control Activities Suite and Residual ESG Risk

Quantify inherent risk using the two-dimensional risk rating matrix that considers likelihood and impact. COSO defines inherent risk as 'the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact'.[13] Consider your risks with no control activities in place.

After quantifying inherent risk, assess control suite effectiveness. Some organisations do not consider control activities if inherent risk is within risk appetite. This approach saves time, but the FI forfeits the opportunity to eliminate unnecessary control activities.

Assess the design and test operating effectiveness of key control activities linked to ESG risks. Evaluate whether the control activities mitigate risk, not if they meet control objectives. Evaluate control activities as a suite of control activities, not individual control activities. Consider whether the FI tested key ESG control activities including reviewing documents, conducting individual and group interviews, performing walkthroughs, observing control activities, transaction testing of judgmental or random samples and re-performance testing of key controls. When testing operating effectiveness, assess the competency and authority of personnel performing processes and controls.

Next, assess residual risks; that is, '[t]he risk to the achievement of objectives that remains after management's response has been designed and implemented'.[14] Residual risks equal inherent risks less the risk reduction from control effectiveness.

There are at least two advantages to assessing inherent risks separately from residual risks. First, the FI is more likely to identify potentially hidden risks after stripping away the presumption there are no risks because mitigating controls are in place. Secondly, the FI can directly compare unmitigated inherent risks with mitigated residual risks, which clearly frames the effectiveness (or lack of effectiveness) of key controls.

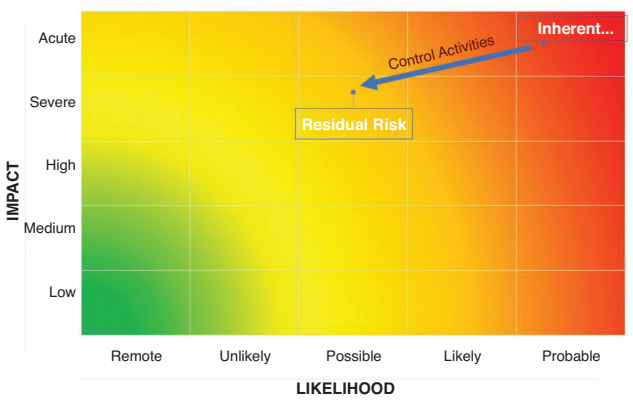

Figure 3: ESG risk heat map

Note: Excerpt for illustrative purposes only.

Populate Inherent and Residual ESG Risk Heat Maps

After completing the risk assessment, plot inherent and residual ESG risks on the FI's risk grid to depict visually the effectiveness of key ESG controls and most significant risks (See Figure 3).

RISK RESPONSE

An ESG risk heat map makes it easier to visualise and communicate ESG risks and controls for FIs to: (1) prioritise out-of-risk appetite/tolerance ESG risks, (2) select an ESG response; (3) create an ESG remediation plan; and (4) manage remediation through the ESG glide path.

Prioritise out-Of-risk appetite/tolerance ESG risks

Material ESG risks that approach or exceed risk appetite require a risk response. But, as a practical matter, the FI must prioritise which risks to address first. Factors to consider include:

- *Adaptability* — Consider the FI's capacity to respond. If a FI can easily adapt to an emerging ESG risk (eg, employee diversity), it makes sense to prioritise remediation for a quick win.
- *Complexity* — Some risks are highly complex and interdependent; others stand alone and can be easily remediated. Prioritising less complicated risks before remediating complex, interdependent risks typically return faster success. Prioritising less complicated risks also builds positive momentum and can untangle interdependencies with other risks, enhancing the success of future remediation efforts.
- *Velocity* — Some risks have an immediate impact, while others may require longer to manifest. Although FIs should not ignore slow-developing ESG risks (eg, rising sea levels), they likely will want to focus on more immediate issues (eg, DEI).
- *Persistence* — A persistent risk that manifests in multiple occurrences will likely take priority over a 'one and done' risk, provided the 'one and done' risk is not so severe that it threatens a FI's operations as a going concern.
- *Recovery* — This is the capacity of a FI to return to risk tolerance after a risk event (eg, continuing to function after a flood or other ESG weather-induced risk). Recovery excludes the time taken to return to tolerance, which is considered part of persistence, not recovery.

Select an ESG risk response

Classic risk responses include:

- Accept — A FI may accept a risk and continue business as usual. As a practical matter, risk acceptance may be appropriate for the near-term, but the growing public awareness and developing regulatory landscape will continue to push FIs to evaluate alternative ESG risk responses to meet their strategic objectives.
- Avoid — This option is expensive because it may require discontinuing certain business lines, declining to expand to a new geographical market or selling a division. FIs are already confronting tough decisions and are adjusting their financial offerings to carbon-based industries, as public sentiment and regulatory pressures continue to mount against those industries.
- Pursue — A FI may pursue (increase) a risk within tolerance to achieve improved business performance by adopting aggressive growth strategies, expanding operations or developing new products or services. Financing renewable energy, biodegradable packing materials, pollution

reduction technology and other Greentech are examples of ESG opportunities where FIs may pursue greater risks to achieve strategic objectives.
- Share — Insurance is a classic example of sharing risk. The risk of severe weather due to global warming, for example, may be covered by weather insurance, financial hedging and other risk sharing strategies.
- Reduce — Risk reduction is the most practical risk response to ESG risks. It involves mitigation strategies such as enhanced control activities to align residual risks to target risk appetite.

Create an ESG risk remediation plan

Start with a clear understanding of why residual risk exceeds appetite: is it because of inherently high likelihood or impact, missing or ineffective control activities or both? The rationale behind the residual risk rating informs effective ESG remediation design and implementation.

Engage the risk and control owners on how to reduce the risk. Develop meaningful metrics, including key risk indicators to monitor progress. Consider both preventive and detective controls activities and, if practical, automated control activities built on data science and analytics. Best practice includes enhancing the design and implementation of existing and new controls to reduce potential incentives/pressures, opportunities and rationalisations to circumvent control activities.[15] Formalise ESG risk remediation with a written plan that specifies target residual likelihood and impact, details design and implementation steps and clearly states key milestone and target dates.

Manage remediation through residual ESG risk glidepath

Track remediation progress from the original residual risk to target residual risk (See Figure 4). Plot starting, current and target residual risks on the ESG heat map for a clear visual depiction of remediation progress.

ESG INCIDENT REMEDIATION

FIs inevitably experience ESG 'incidents' (eg, inadequate ESG diligence, misreporting sustainability efforts). Because these incidents are more likely to occur during the early stages of the FI's ESG journey, it is important the Risk Team develops a framework to understand causes and prevent recurrence, which will facilitate continuous improvement as the ESG program matures.

Conduct root cause analysis

Remediation begins with root cause analysis that pays specific attention to the role of incentives/pressure, opportunities and rationalisations within the operating environment.[15] For ESG issues, root cause analysis often requires comprehensive assessment of the control environment, not just operational issues.

Once the root cause analysis is complete, shift focus to consider whether the FI could/should detect the issue earlier (eg, past risk assessments, audit reports, investigations of similar issues, external market trends).

Risk	Residual Risk Glidepath			Remediation Status	Commentary
	H1 2021	H2 2021	Target H2 2022	July 2021	
Human Rights/KYC Insufficient data on land use and the impact on indigenous people	**Critical** (Acute / Likely)	Significant (High / Likely)	Important (Medium / Possible)	On Track	Details on remediation action points.

Figure 4: ESG remediation through residual ESG risk glidepath

Note: Excerpt for illustrative purposes only.

Perform a 'read across'

Read across analyses enable the FI to early detect other ESG incidents. Say the FI unintentionally misreported sustainability metrics. Understanding why and how the misreporting occurred allows the FI to conduct risk-based procedures to search for similar incidents.

Develop and implement corrective measures

Once weaknesses are identified and analysed, develop and implement corrective measures. In today's environment, take particular care to leverage data by (1) identifying risk factors and indicators, and (2) considering whether and how forensic and scientific data science and analytics might serve as an earlier detection tool.

Report trends and issues to the C-suite and Board of Directors

In line with the envisioned 'speak-up' culture, there should be a formal and regular reporting process. The C-Suite and Board should be informed promptly of significant investigative matters, control weaknesses, remediation status, significant trends in misconduct and disciplinary measures.

Improve risk assessments, audit planning and control testing design

Last, the FI should see the learnings from the incident as an opportunity to improve the robustness of its risk assessments, audit and control design. With natural ESG events, it should pay particular attention to how the risk response process can be enhanced to minimise impact.

CONCLUSION

Besides being the right thing to do, creating an ESG agenda and appointing a CSO or an equivalent senior executive creates new business opportunities and enhances brand value. But ESG agendas also pose significant business and legal risks that will continue to grow as ESG expands.

CROs, CCOs and CLOs are in the business of managing risk. Not only must they sit at the ESG table for FIs to meet their ESG agenda, but they must also be deeply entrenched in efforts to avoid financial, legal, regulatory and reputational losses that will inevitably follow without an ESG risk management program. The good news is that partnering with a CSO provides compliance and risk professionals with a unique opportunity to deliver additional value to their organisations in a highly visible way. Savvy practitioners will reach across the aisle to their counterparts in Sustainability or Corporate Social Responsibility to elevate the ESG risk conversation as these priorities become pervasive across FIs. The Risk Team can and should play a pivotal role in transforming the business from the 'inside out' for the 'new outside in' world in which FIs now operate.

References

1 'Earth Day', available at https://www.earthday.org/history/ (accessed 11th August, 2021).
2 'United Nations Climate Change', available at https://unfccc.int/process/the-kyoto-protocol/status-of-ratification (accessed 11th August, 2021).
3 'United Nations', available at https://www.un.org/en/un-chronicle/un-global-compact-finding-solutions-global-challenges (accessed 11th August, 2021).
4 'SASB', available at https://www.sasb.org/about/ (accessed 11th August, 2021).
5 'The White House', available at https://www.whitehouse.gov/briefing-room/statements-releases/2021/01/27/fact-sheet-president-biden-takes-executive-actions-to-tackle-the-climate-crisis-at-home-and-abroad-create-jobs-and-restore-scientific-integrity-across-federal-government/ (accessed 13th August, 2021).
6 'Bloomberg, available at https://www.bloomberg.com/professional/blog/esg-assets-may-hit-53-trillion-by-2025-a-third-of-global-aum/ (accessed 11th August, 2021).
7 'Deloitte', available at https://www2.deloitte.com/global/en/pages/financial-services/articles/

the-future-of-the-chief-sustainability-officer.html (accessed 16th August, 2021).
8 COSO refers to the Committee of Sponsoring Organizations of the Treadway Commission, a private-sector initiative funded by the American Accounting Association (AAA), American Institute of CPAs (AICPA), Financial Executives International (FEI), The Institute of Management Accountants (IMA) and The Institute of Internal Auditors (IIA). 'COSO', available at https://www.coso.org/pages/aboutus.aspx (accessed 16th August, 2021).
9 'COSO', available at https://www.coso.org/Documents/COSO-WBCSD-ESGERM-Guidance-Full.pdf (accessed 16th August, 2021).
10 'Harvard Business Review', available at https://hbr.org/2020/01/the-new-analytics-of-culture (accessed 11th August, 2021).
11 'Deloitte', available at https://www2.deloitte.com/global/en/pages/financial-services/articles/the-future-of-the-chief-sustainability-officer.html (accessed 16th August, 2021).
12 'Corporate Compliance Insights', available at https://www.corporatecomplianceinsights.com/silence-not-golden-scorecard-speak-up/ (accessed 11th August, 2021).
13 'COSO', available at https://www.coso.org/Documents/COSO-ERM%20Risk%20Assessment%20in%20Practice%20Thought%20Paper%20October%202012.pdf (accessed 12th August, 2021).
14 'UN Sustainable Development Group', available at https://unsdg.un.org/sites/default/files/UNDG-Programme-Risk-Management-for-Pooled-Funding-Solutions-in-Conflict-and-Transition-Countries_Final.pdf (accessed 16th August, 2021).
15 Cressey, D. R., (1953), 'Other People's Money; A Study in the Social Psychology of Embezzlement', Free Press, New York (Cressy). 'AGA', available at https://www.agacgfm.org/Intergov/Fraud-Prevention/Fraud-Awareness-Mitigation/Fraud-Triangle.aspx (accessed 16th August, 2021).