ancoram™

ESG Controls Toolkit

A Comprehensive Framework for Sustainability Reporting

March 2025

Why ESG controls matter now

Reliable ESG data is the foundation of credible sustainability reporting, yet businesses face significant challenges in ensuring its accuracy, completeness and consistency across multiple frameworks and diverse data sources

Reliable sustainability data is no longer a nice-to-have. For companies in scope of the Corporate Sustainability Reporting Directive (CSRD), high-quality ESG information is now a legal requirement. But for forward-looking businesses, it is also a commercial advantage. The ability to trust, explain and stand behind your ESG numbers is critical to telling a credible sustainability story.

Yet many organisations remain unprepared. Sustainability data often lives outside finance systems, comes from loosely governed sources, and is collected by teams unfamiliar with control frameworks. Inconsistent definitions, manual inputs, third-party dependencies and evolving frameworks create fertile ground for misstatements. The risks are not only reputational and regulatory. They also undermine the confidence of internal stakeholders who need this information to make decisions.

This toolkit offers a practical route forward. It sets out how to build effective internal control over sustainability reporting (ICSR), drawing on the COSO *Internal Control – Integrated Framework* (2013) and the 2023 COSO guidance on applying that framework to ESG disclosures. It blends that structure with our practical experience of ESG data and assurance.

Our aim is simple: to help finance and sustainability leaders design and implement ESG controls that actually work.

Tim Dee-McCullough FCCA FRSA

Director, Ancoram Limited

tim@ancoram.com

What this toolkit covers

Effective ESG reporting starts long before year-end. It begins with the right culture, the right questions, and the courage to challenge what's taken for granted.

This toolkit is structured around the five components of the COSO framework:

1. Control environment
2. Risk assessment
3. Control activities
4. Information and communication
5. Monitoring activities

Each section unpacks the COSO principles, explains how they relate to ESG, and provides practical suggestions for designing and implementing controls. We also include real-world data examples, industry insights and common pitfalls to avoid.

Along the way, we challenge unhelpful assumptions. For example:

- That ESG data can be treated like financial data
- That controls are only needed at the reporting stage
- That audit readiness is a year-end exercise

We also provide tools to help you tailor controls to different sustainability topics – whether you're managing Scope 3 emissions, social impact data or governance disclosures.

Understanding the COSO components

Why a strategic approach to ESG controls will enhance your reporting

01 Control environment

The foundation of trustworthy reporting

You cannot bolt controls onto a broken culture. Effective internal control over sustainability reporting depends on having the right tone, structure and expectations in place from the outset.

The COSO framework identifies five principles under the control environment component:

- A commitment to integrity and ethical values
- Oversight by the board of directors
- Clear organisational structure, authority and responsibility
- A commitment to competence
- Accountability for performance

Let's take each in turn, and consider what it means for ESG reporting.

Control environment (continued)

Integrity and purpose

Sustainability reporting cannot succeed in a culture of box-ticking. A commitment to ethical values means more than publishing a purpose statement – it means ensuring that people throughout the organisation understand why accurate ESG reporting matters.

For example, a business that commits to net zero by 2040 but consistently underreports emissions undermines its own credibility. A control environment rooted in integrity will empower staff to raise concerns, challenge inconsistent data and treat ESG disclosures with the same seriousness as financial results.

Practical steps:

- Set expectations at executive level that ESG reporting is a matter of integrity
- Link ESG disclosures to the company's stated purpose and stakeholder expectations
- Reinforce the importance of ethical reporting through policies, leadership messaging and staff training

Board oversight

Boards must take responsibility for ESG data in the same way they do for financial data. This means establishing formal oversight of sustainability reporting, either through the audit committee or a dedicated sub-committee.

Practical steps:

- Assign ESG reporting oversight to a board-level committee
- Ensure the board is briefed on key reporting risks and controls
- Embed ESG data responsibilities into board agendas and risk discussions
- Provide case studies or examples of ethical dilemmas in ESG reporting during training

Control environment (continued)

Roles, authority and reporting lines

Sustainability reporting often suffers from unclear accountability. Is it the remit of finance, sustainability, risk or legal? Too often it sits between them.

Practical steps:

- Define clear ownership for ESG data collection, validation and disclosure
- Appoint named control owners across business units and functions
- Ensure ESG responsibilities are included in role descriptions and performance goals
- Develop internal ESG champions to advocate for control design across departments

Competence

Many organisations lack internal ESG expertise. And even when sustainability knowledge exists, teams may lack experience with control frameworks, audit requirements and regulatory expectations.

Practical steps:

- Provide training on ESG reporting requirements to finance and sustainability teams
- Build capacity around internal control design and control testing
- Support cross-functional collaboration between finance, risk, sustainability and operations
- Regularly review the skills and knowledge required for effective ESG control ownership
- Include ESG control topics in competency frameworks or appraisal discussions

Control environment (continued)

Accountability

Without clear consequences, controls can be viewed as optional. To build a culture of control, businesses should embed ESG reporting into governance, performance and escalation mechanisms.

Practical steps:

- Include ESG control performance in risk committee and management reviews
- Introduce escalation protocols for ESG reporting issues
- Ensure individuals responsible for key controls are held accountable for outcomes
- Track ESG control performance through a dashboard or similar tool
- Link ESG control outcomes to incentive structures where relevant

Control environment (continued)

At this point, it's worth considering the purpose of different controls. Robust ESG control frameworks incorporate mechanisms that work together to **detect**, **prevent**, and **correct** reporting errors. These controls must operate at multiple levels within an organisation to create a comprehensive safety net for sustainability data:

Detective controls

Detective controls identify issues after they occur, ensuring discrepancies are recognised and addressed promptly.

These controls are essential for continuous monitoring and improvement. They might include periodic reconciliations of energy usage data or analytical reviews that identify unusual patterns in emissions reporting.

Preventative controls

Preventive controls mitigate risks before errors occur through protocols, approvals, and validation checks.

By establishing guardrails at the outset, preventive controls help businesses avoid common pitfalls in sustainability reporting.

Examples include mandatory training for data input personnel or automated system validations that reject implausible values.

Corrective controls

Corrective controls rectify identified errors through data revision, system updates, and accountability measures.

These ensure that when issues are discovered, there are clear processes for addressing them and preventing recurrence.

Control environment (continued)

Controls also need to be strategically implemented across different business levels and company hierarchies:

Entity-level controls (ELCs)

ELCs establish the overall control environment and governance structures that influence all ESG reporting.

These foundational controls, such as clear accountability structures and organisational culture, set expectations for integrity throughout the business.

Typically we would expect an Internal Audit function to report to the Audit & Risk Committee on the implementation / effectiveness of ELCs, particularly for businesses in scope of the CSRD.

Reporting oversight controls

These controls focus on the aggregation, review, and finalisation of ESG disclosures.

These include approvals, trend analysis, and reconciliations that safeguard the reporting process itself.

We find that many businesses do not (yet) fully understand their sustainability data and the challenges associated with specific ESG data types and sources. Accordingly, effective oversight controls are critical to ensure disclosures are audit-ready.

Transaction-level controls

Transaction-level controls operate at the most granular level, ensuring accuracy of individual data points. These don't just apply to financial transactions but to each piece of sustainability data.

These controls include field validations, arithmetic checks, and limit verifications that maintain data integrity at its source.

In some businesses, the purpose and objective of collecting ESG data is not widely understood and so there may be less integrity in this process. Effective controls at the granular level can restore accuracy to the process and minimise costly corrections later on.

02 | Risk assessment

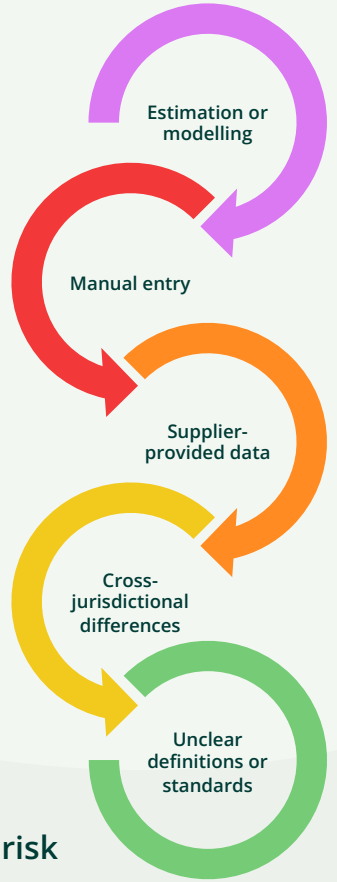
Understanding what could go wrong

Every effective control framework starts with a clear view of what might go wrong. In the context of sustainability reporting, this means recognising the specific risks that can compromise the quality, completeness or credibility of ESG disclosures.

The COSO framework sets out four key principles for risk assessment:

1. Specify suitable objectives
2. Identify and analyse risks
3. Assess fraud risk
4. Identify and analyse significant changes

These principles guide businesses through a structured approach to understanding ESG reporting risks and responding with appropriate controls.



Common sources of ESG data risk

Risk assessment (continued)

Specify suitable objectives

Controls only make sense when they are anchored in clearly defined objectives. For ESG reporting, this includes regulatory requirements (such as ESRS under CSRD), internal management needs, and voluntary commitments made to stakeholders.

Practical steps:

- Translate your sustainability commitments into measurable disclosure objectives
- Map each objective to corresponding datapoints (e.g. IG3 disclosures on health and safety, emissions, or diversity)
- Clarify which metrics are subject to limited or reasonable assurance, and what level of precision is required
- Align disclosure objectives with regulatory requirements and internal goals

Example objectives might include:

- *Report all work-related fatalities and lost-time injuries in line with ESRS S1*
- *Disclose Scope 1 and 2 emissions with at least limited assurance, using verified methodologies*
- *Provide a year-on-year comparison of gender representation in senior leadership roles*
- *Demonstrate progress against the company's stated net-zero target, including decarbonisation of operations*
- *Report on water consumption in high-stress regions using consistent location-based metrics*

Risk assessment (continued)

Identify and analyse risks

Once objectives are defined, you should identify the ESG data risks that threaten their achievement. These risks may vary by topic, data source or reporting process.

For example:

- Health and safety incident data is often reliant on manual incident reporting. This creates a completeness risk if near misses or non-critical injuries go unreported.
- Scope 3 emissions estimates may depend on third-party or modelled data, increasing the risk of input errors or methodological inconsistency.
- Social impact metrics may lack clear definitions, leading to inconsistent interpretation across regions.

Practical steps:

- Conduct ESG-specific risk assessments across all material topics
- Consider sources of estimation, external data reliance, and manual input
- Prioritise high-impact and high-judgement areas for additional control scrutiny
- Use scenario analysis to anticipate potential ESG data failures
- Revisit ESG risk registers annually or following major events

Risk assessment (continued)

Assess fraud risk

Greenwashing is no longer just a reputational issue – it is a regulatory risk. Businesses are under increasing pressure to substantiate claims and avoid misleading disclosures.

Practical steps:

- Consider incentives and pressures that might lead to manipulation of ESG data
- Include ESG metrics in fraud risk assessments typically focused on financial reporting
- Establish safeguards against intentional overstatement or selective omission of sustainability information

Monitor changes

ESG reporting is evolving rapidly. Standards change. Data sources mature. Stakeholder expectations shift. It's important to assess how these changes affect the risk profile and control environment.

Practical steps:

- Track regulatory developments (e.g. new ESRS standards, assurance mandates, or value chain requirements)
- Monitor changes in operations or systems that affect ESG data collection
- Establish periodic reviews of control design adequacy in response to change
- Incorporate stakeholder and investor feedback on ESG disclosures

03 Control activities

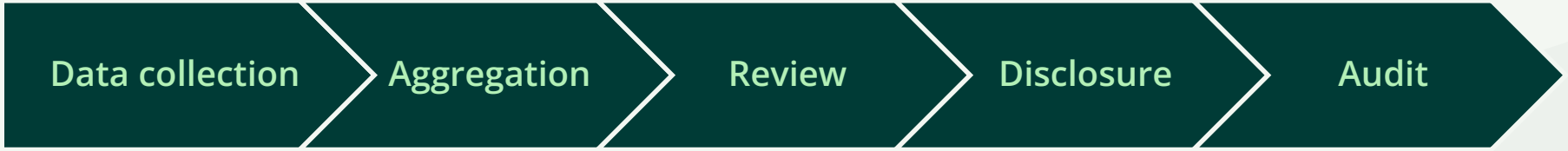
Putting ESG controls into action

Control activities are the mechanisms businesses use to prevent, detect or correct errors and misstatements in ESG reporting. This is where the theory meets execution. Without well-designed, clearly assigned and consistently operated control activities, even the most robust risk assessment will fall flat.

COSO outlines three principles within this component:

1. Select and develop control activities
2. Select and develop general controls over technology
3. Deploy controls through policies and procedures

For ESG reporting, control activities need to account for the unique challenges of non-financial data – from estimation and decentralised systems to supplier dependencies and narrative disclosures.



Control layering along the data lifecycle

Control activities (continued)

Select and develop control activities

Controls should be proportionate to the risks identified and tailored to the ESG topics in scope. While many businesses are familiar with financial controls, fewer have adapted their control mindset to the nature of sustainability data.

The table on the following pages provides illustrative examples of control risks and control activities for key ESRS topical standards. It is not an all-inclusive list, but a starting point to support tailored risk and control design based on material sustainability matters.

Practical steps:

- Identify control points throughout the data lifecycle – from collection and aggregation to review and disclosure
- Design controls that are simple, repeatable and auditable
- Ensure every control has a named owner with accountability for operation
- Layer detective, preventive and corrective controls where appropriate
- Test control design before deployment to confirm feasibility and usefulness

Control activities (continued)

ESG control activities by ESRS topic – Environmental

ESRS topic	Example data collected	Common control risks	Example control activities
E1 Climate change	• Scope 1, 2 and 3 emissions • Energy consumption • Net Zero targets	• Estimation errors • Inconsistent methodologies • Data duplication	• Automated meter data feeds • Scope 3 methodology validation checks
E2 Pollution	Emissions to air, water, soil	Incomplete or unverified external data from sites	• Site-specific pollution logs • Third-party lab result verification
E3 Water and marine resources	• Water withdrawal • Discharge • Consumption in high-stress areas	Misreporting due to inconsistent units or assumptions	• Water stress mapping • Data input templates with unit standardisation
E4 Biodiversity	• Impact on protected areas • Species risk assessments	• Subjectivity in impact scoring • Inconsistent spatial boundaries	• Use of Geographic Information System (GIS) controls • Peer review of assessments
E5 Resource use and circular economy	• Waste generation • Material inputs • Circularity metrics	Overstatement or data gaps in supply chain-derived metrics	• Supplier survey controls • Waste log reconciliation • Duplicate entry flags

Control activities (continued)

ESG control activities by ESRS topic – Social and Governance

ESRS topic	Example data collected	Common control risks	Example control activities
S1 Own workforce	• Headcount • Injury rates • Diversity, equality and inclusion (DEI) representation	• Underreporting • Inconsistent demographic classification	• HR systems cross-checks • Mandatory incident reporting workflows
S2 Workers in the value chain	• Labour practices • Working hours • Health and safety	Limited visibility into suppliers' and distributors' data	• Supplier data attestations • Audit sampling • Escalation procedures
S3 Affected communities	• Community engagement • Impact assessments	• Qualitative bias • Unverified claims	• Community feedback logs • Third-party verification of engagement records
S4 Consumers and end-users	• Product safety incidents • Accessibility metrics	• Gaps in incident logging • Regional inconsistency	• Product defect database reconciliation • Uniform group-wide definitions across markets
G1 Business conduct	• Anti-corruption • Lobbying • Board composition	Selective omission or data not tracked at all	• Annual declarations • Board register reviews • Conflict of interest checks

Control activities (continued)

Technology and data lineage

Many ESG metrics are generated outside financial systems and flow through spreadsheets, manual processes or third-party systems. This creates a high risk of breakpoints in data integrity.

Mapping your data flows and control points is critical to identify or evidence the strength of your reporting. The diagram opposite outlines common steps we encounter in ESG data flows.

Practical steps:

- Document data lineage for all key ESG metrics
- Apply system access controls and version control over ESG datasets
- Embed validations and logic checks in tools used for data processing
- Conduct regular data flow walkthroughs to check for hidden breakpoints

Control activities (continued)

Policies and procedures

Controls do not operate in a vacuum. To be effective, they need to be underpinned by clear policies, documented procedures and training that ensures consistency.

What a good ESG control policy includes

- ✓ A statement of purpose and scope
- ✓ Definitions of key terms and responsibilities
- ✓ Description of control activities and their intended frequency
- ✓ Documentation and evidence retention expectations
- ✓ Escalation and remediation pathways for control failures

Practical steps:

- Integrate ESG control documentation into your broader internal control framework
- Train control owners on policy expectations and what good evidence looks like
- Review and update policies annually, or sooner if ESG standards evolve
- Store ESG control policies in an accessible, version-controlled repository

04 Information and communication

Ensuring the right people see the right data at the right time

Even the best controls fail if they are not supported by clear, timely and purposeful information flows. For ESG reporting, this means ensuring that the right people can access, interpret and act on sustainability data – from data owners in operational teams to senior leaders signing off public disclosures.

COSO defines three principles within this component:

1. Use relevant, high-quality information
2. Communicate internally
3. Communicate externally

Each plays a vital role in creating a transparent and responsive ESG control environment.

Information and communication (continued)

Relevant, high-quality information

Information is only useful if it is accurate, timely and relevant to the task at hand. For ESG reporting, this includes both quantitative data (such as emissions or headcount) and qualitative disclosures (such as risk descriptions or governance practices).

The checklist opposite summarises the critical questions to ask around information quality.

Practical steps:

- Define the minimum quality criteria for ESG metrics used in internal and external reporting
- Assign data stewards to oversee critical ESG datasets
- Use dashboards or visual tools to support interpretation of ESG trends

Information and communication (continued)

Internal communication

Clear communication within the business ensures that ESG control responsibilities are understood, supported and acted upon. It also supports cross-functional collaboration – especially between finance, sustainability and operations teams.

Practical steps:

- Establish ESG reporting forums or working groups across departments
- Provide periodic control performance updates to management
- Use visual walkthroughs or flowcharts to explain ESG reporting processes
- Encourage open discussion of ESG control challenges and learnings

Case study: Aviva

The FTSE 100-listed insurance group recognised that its reporting strength was concentrated within its financial reporting team, who already knew its business inside-out and understood the importance of an effective control environment over corporate reporting.

Instead of recruiting external hires to run with its sustainability reporting, existing financial reporting specialists moved into sustainability reporting and took responsibility for CSRD implementation. Board committees oversee the implementation of ESG reporting, with direct reporting lines and clear communication.

As a result, Aviva's sustainability reporting is subject to similar and consistent controls and oversight as the group's financial reporting, demonstrating high readiness for the rigour of external assurance.

Information and communication (continued)

External communication

What a business discloses externally shapes stakeholder trust. Controls over external communication – from sustainability reports to investor decks – are essential to ensure accuracy and consistency across channels.

Practical steps:

- Reconcile narrative and numeric disclosures across sustainability and annual reports
- Use disclosure checklists for ESRS or other relevant frameworks
- Embed final review and approval steps into the ESG reporting calendar

05 Monitoring activities

How to know if your ESG controls actually work

Designing controls is only half the challenge. Without mechanisms to evaluate whether controls are operating as intended, businesses risk relying on a false sense of security. Monitoring activities provide the feedback loop that enables continuous improvement and builds readiness for external assurance.

COSO includes two core principles in this component:

1. Perform ongoing and/or separate evaluations
2. Evaluate and communicate control deficiencies

Together, these principles help businesses assess the effectiveness of their ESG control framework and respond proactively to weaknesses.

Monitoring activities (continued)

Perform evaluations

Monitoring can take many forms – from informal spot checks to structured internal audit programmes. The goal is not to create unnecessary bureaucracy, but to ensure controls are functioning and delivering value.

Options for ESG control monitoring:

- **Ongoing monitoring:** Performed by those executing the process (e.g. regular data quality checks by ESG analysts)
- **Separate evaluations:** Performed independently (e.g. internal audit reviews or walkthroughs of control design and operation)

Signs your ESG controls need a refresh:

- Control ownership is clear or has changed
- ESG data inconsistencies are identified post-disclosure
- Material changes in systems, regulations or organisational structure
- Repeated manual overrides of control outputs
- Delays in completing ESG reporting due to control bottlenecks
- Feedback from auditors or assurance providers highlights gaps

Practical steps:

- Include ESG controls within internal audit or second line assurance scope
- Use walkthroughs to test design and operating effectiveness
- Establish periodic control reviews aligned with reporting cycles

Monitoring activities (continued)

Evaluate and communicate deficiencies

Identifying weaknesses is not a failure – it is a sign the control framework is working. What matters is how the business responds.

Practical steps:

- Track control failures in a centralised issue log
- Define remediation plans with clear deadlines and responsibilities
- Ensure control deficiencies are escalated to appropriate governance bodies (e.g. audit committee)

What makes an effective ESG control walkthrough

- ✓ Explain the control and its purpose
- ✓ Show evidence of operation (screenshots, reports, timestamps)
- ✓ Identify dependencies (people, systems, timing)
- ✓ Clarify how the control mitigates the identified risk

Practical steps:

- Include ESG controls within internal audit or second line assurance scope
- Use walkthroughs to test design and operating effectiveness
- Establish periodic control reviews aligned with reporting cycles
- Conduct root cause analysis to prevent recurrence

Integrating double materiality into ESG controls

Why materiality mapping should shape your control framework

Integrating double materiality into ESG controls

Why double materiality changes the control conversation

Double materiality is central to CSRD and GRI – and increasingly, to stakeholder expectations more broadly. It requires businesses to consider not just how sustainability matters affect their own performance (financial materiality), but also how their activities impact people and the planet (impact materiality).

This expanded lens has significant implications for internal controls. It broadens the scope of what needs to be reported and heightens the need for controls over both qualitative and quantitative data.

Traditional control frameworks focus on financial reporting risks. But under double materiality, controls must also address:

- Narrative disclosures about sustainability risks, impacts and opportunities
- Forward-looking information, such as transition plans or decarbonisation roadmaps
- Data from across the value chain, often outside direct operational control

Without robust controls, this information can be vague, inconsistent or selectively framed – exposing businesses to accusations of greenwashing and regulatory non-compliance.

Practical steps:

- Build control activities around your double materiality assessment process
- Include impact materiality in risk and control matrices
- Test controls for qualitative data alongside numeric metrics (e.g. process for impact narratives, stakeholder input validation)

Integrating double materiality into ESG controls (continued)

Controls through the lens of stakeholder impact

Controls should reflect not only what matters to the business, but also what matters to people, communities and ecosystems. This requires broader input and broader testing.

Embedding impact thinking into control design

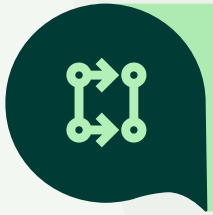
- ✓ Does the control reflect stakeholder concerns identified during materiality assessment?
- ✓ Has the control owner considered how impacts are measured and verified?
- ✓ Are assumptions, limitations and exclusions documented and challenged?
- ✓ Is there evidence that the control accounts for both short-term and long-term impacts?
- ✓ Has the control design been informed by direct stakeholder engagement or feedback?

Example controls over impact-related data

A business discloses a biodiversity impact narrative. Effective controls might include:

- Peer review of ecological assessments by qualified internal or external experts
- Clear sourcing of data used for impact measurement (e.g. satellite imagery, field studies)
- Documentation of scope boundaries and estimation techniques

Integrating double materiality into ESG controls (continued)



Aligning control maturity with materiality

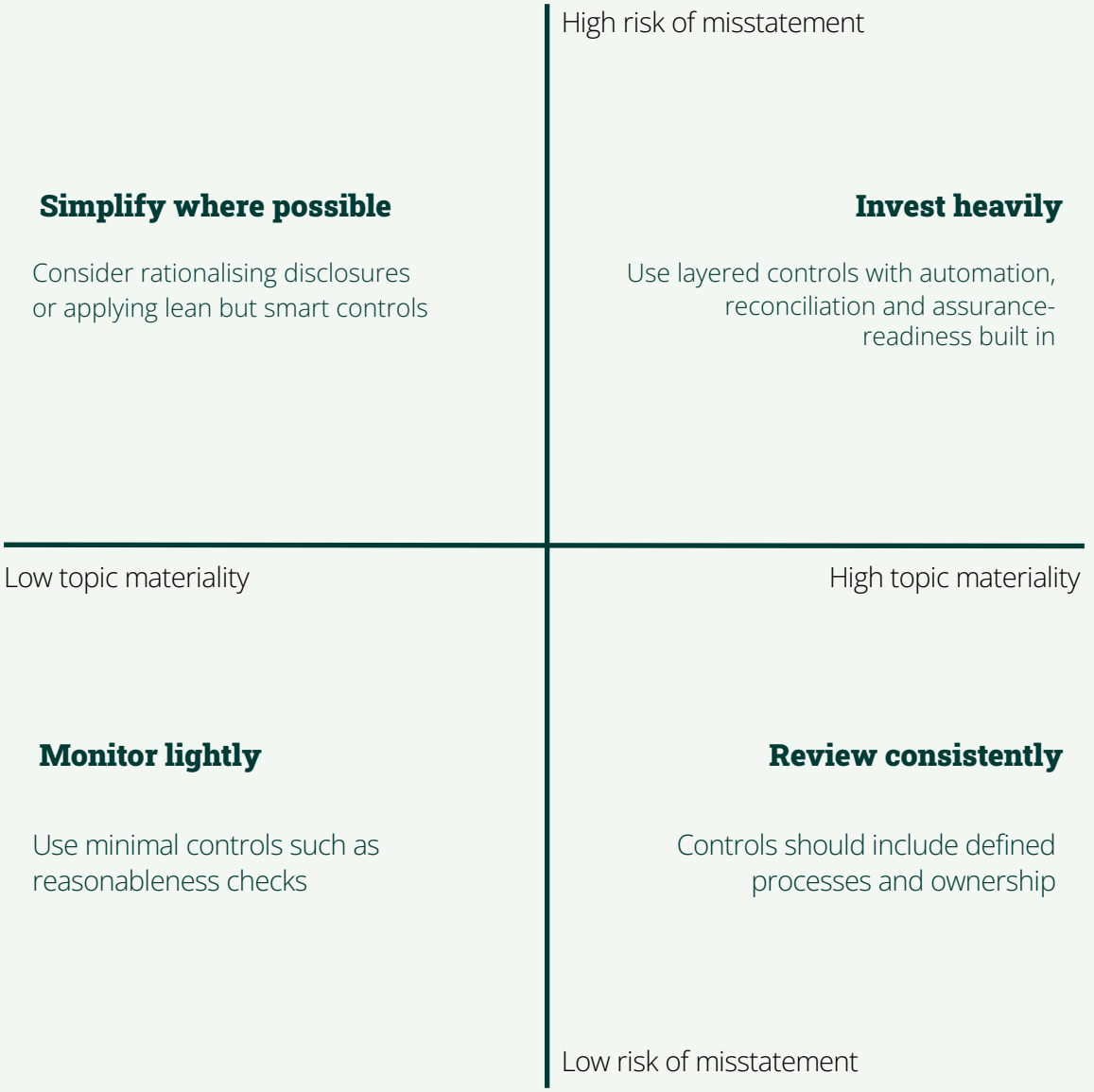
Not all ESG data points are equal. Businesses are advised to match the strength of their control environment to the materiality of the information being disclosed.

Practical steps:

- Prioritise control investment around material metrics and topics
- Use double materiality outcomes to justify where strong, formal controls are essential
- Align ESG control testing with the outcomes of your materiality reassessment each year
- Consider whether the frequency of control operation matches materiality level
- Adjust control ownership based on topic significance and complexity

ESG control design by materiality and risk

As ESG reporting becomes more complex, businesses need a practical way to decide how much time and resource to allocate to different control areas. Not every data point demands the same level of rigour.



Practical implementation

Where to start and how to know if you succeed

Getting started

Diagnose your current position

Begin by understanding what controls already exist – and where the biggest gaps or risks lie. Many businesses already have ad hoc controls in place, but they are undocumented, inconsistently applied or not clearly owned.

Focus on foundational controls

Some controls create a multiplier effect – making everything else easier to manage. These include data ownership, validation logic, approval sign-offs and version control.

Prioritise based on risk

Rather than spreading effort thinly across all disclosures, focus on the most material topics and highest-risk data. This is where the greatest value – and the greatest exposure – tends to lie.

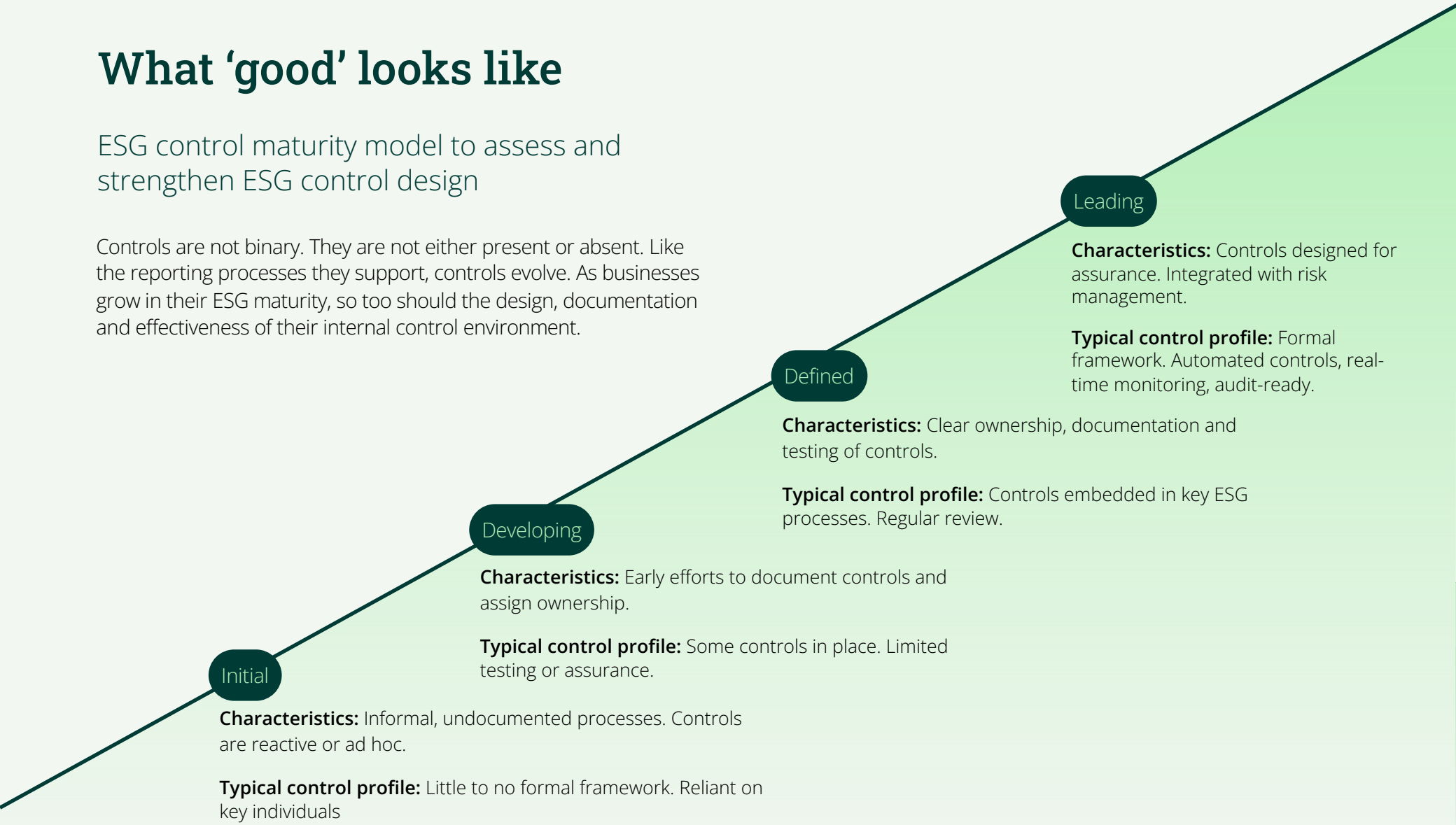
Build from the inside out

It is tempting to focus first on what goes into the sustainability report. But good ESG controls begin upstream – at the point of data entry or collection. The further upstream controls are embedded, the less rework and remediation is needed downstream.

What ‘good’ looks like

ESG control maturity model to assess and strengthen ESG control design

Controls are not binary. They are not either present or absent. Like the reporting processes they support, controls evolve. As businesses grow in their ESG maturity, so too should the design, documentation and effectiveness of their internal control environment.



Preparing for assurance

Designing controls with audit in mind

Assurance is becoming the new norm in ESG reporting. Under CSRD, limited assurance over sustainability information is required – and reasonable assurance may follow. This means auditors will evaluate whether reported ESG data is supported by effective internal controls.

Unlike traditional financial audits, ESG assurance requires scrutiny of data that may originate from outside core finance systems. The processes and controls used to generate that data need to be clear, consistent and auditable.

Practical steps:

- Identify ESG metrics that will be subject to assurance in the current or future reporting cycle
- Review whether control design and documentation would pass a basic walkthrough test
- Start building an audit trail for narrative as well as numeric disclosures

What auditors look for

While approaches may differ by firm or jurisdiction, there are common elements most assurance providers expect:

- **Governance and oversight:** Board or executive responsibility for sustainability disclosures
- **Control design:** Documented controls for material metrics and narratives
- **Control operation:** Evidence that controls are operating effectively throughout the reporting period
- **Documentation and traceability:** Clear records supporting ESG disclosures, including source data and calculations
- **Walkthroughs:** Step-by-step demonstrations of how data flows through the reporting process

Preparing for assurance (continued)

Building audit-ready controls

Controls do not need to be complex to be effective. But they do need to be demonstrable. This means auditors can see:

- What the control is intended to achieve
- Who owns it
- When and how it operates
- What evidence supports its operation

Features of audit-ready ESG controls

✓ Defined objective and link to ESG risk or disclosure requirement

✓ Documented steps or SOP for how the control works

✓ Timestamped and version-controlled evidence

✓ Record of control owner review or approval

Example walkthrough – GHG emissions control

A facilities manager uploads energy use data monthly into a central platform. The controller reviews for anomalies using a standard dashboard, flags any spikes, and signs off on the final value for reporting. Evidence includes the source file, dashboard screenshot, email sign-off and timestamped records.

Specific ESG controls and where to implement them

Entity-level controls

Control type	Description	Most relevant ESG data types
Accountability	Assigns clear responsibility for ESG data accuracy and integrity throughout the business	ESG reporting, sustainability impact statements
Access controls	Restricts data access to authorised personnel only, preventing unauthorised changes	HR diversity metrics, compliance data
Culture	Embeds sustainability responsibility within corporate values and daily operations	Ethical sourcing, social responsibility policies
Risk assessment and risk management	Systematically evaluates and manages ESG risks that could impact reporting quality and completeness	Governance disclosures, climate risk management
Segregation of duties	Ensures different personnel handle data collection, approval, and reporting to prevent manipulation of disclosures	Financial ESG data, carbon emissions tracking

Specific ESG controls (continued)

Reporting oversight controls

Control type	Description	Most relevant ESG data types
Approvals	Requires formal sign-off on ESG disclosures before publication	Sustainability performance targets, executive ESG reports
Backups	Ensures ESG data integrity by maintaining secure backups	Environmental impact data, supplier due diligence records
Matching controls	Ensures consistency between internal records and external ESG reports	Investor ESG disclosures
Reconciliations	Systematically matches data across different sources to identify and resolve discrepancies	Supply chain emissions, water and energy usage
Sequence checks	Ensures proper sequencing and timing of ESG reporting processes	Compliance deadlines, audit logs
Trend analysis and analytical review	Identifies anomalies in ESG data trends and unusual patterns requiring investigation	Carbon emissions, social impact metrics

Specific ESG controls (continued)

Transaction-level controls

Control type	Description	Most relevant ESG data types
Arithmetic checks	Verifies calculations and formulae within ESG reports for accuracy	Carbon footprint calculations, impact metrics
Data validation	Cross-checks data inputs against standard values and expected ranges	Waste reduction, ethical procurement
Field checks	Ensures valid and appropriate entries in all ESG data fields	Employee diversity data, energy consumption
Limit checks	Automatically flags values that exceed predetermined thresholds	Greenhouse gas emissions, water usage

Building better reporting

Next steps and key takeaways

Building better reporting

Strong ESG controls are not about bureaucracy. They are about confidence.

Confidence that the data you disclose is complete, consistent and credible.

Confidence that your teams know what they are responsible for.

Confidence that your business can meet the rising bar of investor and regulatory expectations.

This toolkit has walked through the five COSO components – from control environment to monitoring – and shown how they apply to ESG reporting. Along the way, we have offered practical guidance, real-world examples, and decision aids to help you design controls that are right-sized, risk-aware and ready for assurance.

If you are just beginning, start small. Focus on material ESG topics and high-risk data. Map what controls you already have. Identify gaps. Build out from there.

If you already have controls in place, pressure test them. Can you walk through them with an auditor? Is there clear ownership? Do you have evidence they are working?

If you are preparing for assurance, lean into it. Assurance is not just a regulatory requirement – it is a strategic opportunity to strengthen your ESG narrative and build trust with stakeholders.

Five takeaways to remember:

1. **Controls build trust.** ESG reporting needs the same rigour as financial reporting – and controls are the foundation.
2. **Materiality should guide your efforts.** Not all metrics matter equally. Prioritise controls where the risk and importance are highest.
3. **Controls can be simple.** What matters is that they are defined, assigned and evidenced – not that they are complex.
4. **Documentation matters.** If it's not documented, it didn't happen. Clarity supports audit readiness and team continuity.
5. **It is a journey.** Build iteratively. Strengthen over time. Bring your teams along with you.

How Ancoram helps businesses like yours

ESG reporting and compliance

A structured approach to ensuring accurate and compliant sustainability disclosures

Forensic ESG and due diligence

In-depth risk assessment processes to uncover and mitigate ESG risks – both in your business and its value chain

Fractional CSO

Expert sustainability leadership to drive growth and profitability, without the need for a fulltime Chief Sustainability Officer

Governance, risk and controls

Enhancing governance frameworks and reporting controls to improve your ESG disclosures and get audit-ready

Market positioning

ESG storytelling and stakeholder engagement to build trust and transparency

Materiality and value chain

Assessing sustainability impacts, risks and opportunities in your business, your supply chain, customers and other critical players

Biography

Tim Dee-McCullough

FCCA, FRSA, MIoD

Tim Dee-McCullough is a specialist in ESG reporting, assurance and value chain due diligence. With extensive experience in regulatory compliance, internal controls and sustainability disclosures, he has worked with international groups across multiple sectors to enhance governance and improve the integrity of ESG reporting.

Tim's expertise spans key reporting frameworks, including CSRD / ESRS, ISSB, SASB, GRI, TCFD and TNFD, as well as assurance standards such as ISAE 3000 (Revised) and ISSA 5000. He is also proficient in business French and German.

Tim has played a pivotal role in supporting ESG reporting programmes by developing methodologies that align with international standards. His work includes reviewing reporting frameworks, conducting materiality assessments and performing due diligence on the value chain. Tim has also contributed to thought leadership in ESG, producing insights on evolving regulations and best practice in sustainability reporting.

Tim's previous roles include:

- Sustainability & ESG Technical Director, MHA / Baker Tilly Ireland
- Regional Lead, Policy & Insights at ACCA – informing and influencing policy with the UK and Irish Governments, European Commission, EFRAG, EFAA, Accountancy Europe and SEC
- Social Innovation Fellow, Year Here
- Accounting policy leadership roles at National Grid, RSA Insurance Group, AIG, Deloitte Australia, HSBC

ancoram™

Our promises

We practice what we preach. We're not in the business of green- or blue-washing to keep shareholders or other stakeholders happy. That's why we're on our way to becoming a B Corp. This is just the beginning.

We start (so our clients can finish well). We pioneer, experiment, and bring people, policies and processes together to create epic outcomes.

We are grounded in the present. We know our limitations. We are aware of what is (and isn't) possible based on existing technology and resources, and commit to continually growing our capacity.

We are future-focused. We thrive on innovating, ensuring anything we build will outlive us and evolve with future generations.

Above all, we act with integrity. We say what we mean, and we do what we say. We own our mistakes, learn from them, fix them, and celebrate them.

Our offices

London

71-75 Shelton Street,
Covent Garden,
London WC2H 9JQ
United Kingdom

Thames Valley

Botanica Ditton Park,
Riding Court Road,
Datchet SL3 9LL
United Kingdom

ACCA

Carbon Accounting Alliance Member

1% FOR THE PLANET — MEMBER —

ancoram.com

Legal information – public report