Rudy Shoushany, 2026, 14:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Technology as the Fourth Pillar

Rudy Shoushany
Digital Transformation, Artificial Intelligence, ICT Governance and Cybersecurity DX Talks and BCC Management, Beirut, Lebanon

Abstract- Environmental, Social and Governance (ESG) analysis has become the dominant grammar of corporate non-financial accountability, yet its tripartite architecture was conceived in 2004, before the smartphone, large scale cloud computing, platform data economies and generative artificial intelligence reshaped organisational risk. This paper advances a governance first theory of ESGT, in which technology is elevated to an explicit fourth pillar, denoted T, encompassing artificial intelligence governance, algorithmic accountability, data governance, digital ethics and responsible technology, and cybersecurity. The framework is organised around an auditable pillar principle, namely that a governance dimension earns recognition only if it can be measured and assured, and it therefore anchors the T pillar in a mature stack of standards, including ISO/IEC 42001, the European Union Artificial Intelligence Act, the NIST Artificial Intelligence Risk Management Framework, COBIT 2019 and ISO/IEC 27001. Particular weight is placed on COBIT 2019, whose explicit separation of governance from management, seven governance components and design factor tailoring supply the architectural template through which the T pillar is structured and made auditable. The contribution is threefold. First, the paper documents the technology gap across the major reporting standards, drawing on recent evidence that fewer than one in ten large European firms disclose artificial intelligence as a risk category. Second, it answers the central objection that technology governance is unmeasurable by mapping the T pillar to auditable instruments and by drawing on the scholarly construct of Corporate Digital Responsibility (Lobschat et al., 2021) for its normative content. Third, it engages the strongest counterarguments, namely dilution, framework proliferation, redundancy and rating divergence, and specifies the empirical conditions under which a separate pillar is justified rather than mere integration. The framing is global and standard agnostic, intended to inform standard setters, boards and investors.

Keywords: ESG; ESGT; technology governance; artificial intelligence governance; Corporate Digital Responsibility; double materiality; COBIT 2019; ISO/IEC 42001; EU AI Act; non-financial reporting.

I. INTRODUCTION

The proposition that companies should be assessed on more than financial performance is no longer contested. Over two decades, Environmental, Social and Governance analysis has moved from the margins of responsible investing into the centre of corporate disclosure, capital allocation and regulation. The vocabulary itself was coined in a single United Nations initiative in 2004, and the conceptual triad of environment, society and governance has proven durable precisely because it is intuitive and comprehensive enough to absorb a wide range of concerns (UN Global Compact, 2004; Pollman, 2024).

That durability is now also a liability. The ESG architecture was designed for an industrial and analogue economy, in which technology was an enabler of operations rather than a primary source of risk, harm and value in its own right. In the intervening period, digital platforms, ubiquitous data collection and, most recently, generative artificial intelligence have become defining features of corporate conduct. Algorithmic systems decide who is hired, who receives credit, who is flagged for fraud and what information billions of people encounter. The governance of these systems is not a narrow technical matter. It is a question of rights, accountability, environmental burden and institutional trust, which are the very concerns ESG was built to surface.

This paper argues that the established triad no longer offers an adequate home for technology, and that the time has come to recognise Technology as an explicit fourth pillar, producing the configuration ESGT. The argument is deliberately framed at the level of governance architecture rather than any single jurisdiction. It is global in scope because the underlying drivers, namely the diffusion of artificial intelligence, the materiality of cyber risk and the

extraterritorial reach of digital regulation, are themselves global. The central claim is not that existing frameworks ignore technology entirely, but that they scatter it across the other three letters in ways that obscure its materiality, fragment its measurement and leave it without a coherent disclosure logic.

The paper proceeds as follows. Section 2 revisits the origins and architecture of ESG. Section 3 documents the technology gap across the principal reporting standards and presents recent empirical evidence of underreporting. Section 4 sets out the conceptual foundations of the framework and surveys competing framings. Section 5 develops the theoretical grounding. Section 6 assembles the materiality evidence. Section 7 anchors the proposed pillar in a stack of auditable standards and develops COBIT 2019 as its architectural template. Section 8 proposes an operational disclosure architecture. Section 9 engages the strongest counterarguments and limitations. Section 10 discusses the conditions under which the framework holds and outlines a research agenda, and Section 11 concludes.

II. THE ORIGINS AND ARCHITECTURE OF ESG

The term ESG first appeared in the 2004 report Who Cares Wins, a United Nations initiative that brought together twenty financial institutions from nine countries, together representing more than six trillion United States dollars in assets under management (UN Global Compact, 2004). The report argued that integrating environmental, social and governance factors into capital markets would produce more resilient markets and better long term outcomes for both investors and society. A companion legal opinion commissioned through the United Nations Environment Programme Finance Initiative, widely known as the Freshfields report, argued in 2005 that the integration of such factors was consistent with, and arguably part of, the fiduciary duty owed by institutional investors (UNEP FI, 2005). The Principles for Responsible Investment followed in 2006 and gave the concept an institutional vehicle.

Legal scholarship has since observed that the term was coined without a precise definition, leaving a normative ambiguity that persists to this day (Pollman, 2024). This openness is part of why the triad has been able to expand to accommodate new concerns, from climate transition to human rights in supply chains. It is also why the framework can be stretched to the point of incoherence, a critique returned to in Section 9. For present purposes, the decisive observation is chronological. The entire 2004 to 2006 architecture predates the mass adoption of the smartphone, the maturation of cloud computing, the rise of data driven platform business models and, by roughly two decades, the public arrival of generative artificial intelligence. Technology governance was simply not a category the framers had reason to contemplate as a distinct pillar.

III. THE TECHNOLOGY GAP IN EXISTING FRAMEWORKS

If technology governance mattered to the architects of ESG, it would be visible in the standards that operationalise the concept. A review of the principal frameworks shows instead that technology, data and artificial intelligence are addressed only indirectly, as sub topics of the existing three letters, and that no widely adopted sustainability standard treats artificial intelligence as a dedicated disclosure category.

The Global Reporting Initiative, which uses an impact oriented notion of materiality, addresses technology mainly through data protection, privacy, non discrimination and labour topics (GRI, 2021). It contains no indicators for algorithmic bias, automated decision making or the environmental footprint of artificial intelligence. The Sustainability Accounting Standards Board, which uses a financial notion of materiality organised by industry, captures data security, customer privacy and systems reliability where these are financially material, but systemic or ethical harms that are not readily monetised fall outside its scope (SASB, 2018). The Task Force on Climate related Financial Disclosures is climate specific and does not address digital or artificial intelligence risk, although its four part

structure of governance, strategy, risk management and metrics was inherited by the International Sustainability Standards Board (TCFD, 2017).

The International Sustainability Standards Board issued its first two standards, IFRS S1 and IFRS S2, in June 2023, effective for reporting periods beginning on or after the first of January 2024 (ISSB, 2023). These are investor focused and grounded in financial materiality. Significantly, the Board has confirmed that its first thematic research after these standards concerns nature and human capital rather than artificial intelligence or digital matters, so there is no dedicated artificial intelligence standard on the immediate horizon (IFRS Foundation, 2024).

The European Union Corporate Sustainability Reporting Directive and its associated European Sustainability Reporting Standards represent the most comprehensive regime, employing the concept of double materiality. Even here, however, technology and artificial intelligence are captured only through existing entry points, namely governance and oversight, the double materiality assessment itself, and the standard addressing consumers and end users through data governance, privacy and non discrimination. There is no dedicated artificial intelligence standard (Primec, Belak and Cufar, 2026).

The most rigorous recent treatment combines doctrinal legal analysis with content analysis of the 2024 reports of twenty large European companies (Primec, Belak and Cufar, 2026). The authors find that artificial intelligence related risks are treated as technical or operational matters, separate from the core concept of sustainability, which leads firms to underestimate their materiality. In their sample, only two of twenty companies disclosed artificial intelligence as a risk category, roughly ten percent, while thirteen disclosed cybersecurity and nine disclosed data governance or privacy. They conclude that artificial intelligence is an emerging and structurally under embedded ESG risk dimension, more often framed by firms as an opportunity than as a risk. This empirical underreporting is the practical signature of a missing pillar.

IV. CONCEPTUAL FOUNDATIONS OF THE ESGT FRAMEWORK

A governance first theory of ESGT

This paper advances a governance first theory of ESGT in which technology is treated not as a loose collection of digital concerns but as a distinct governance discipline that can be defined, measured and assured. In this formulation the T pillar comprises five interlocking domains, namely artificial intelligence governance, algorithmic accountability, data governance, digital ethics and responsible technology, and cybersecurity. What distinguishes the framework is its organising premise, here termed the auditable pillar principle, which holds that a dimension earns a place in a disclosure framework only if it can be evidenced through assurable controls rather than asserted through narrative. The T pillar is therefore defined from the outset by reference to the established governance frameworks through which technology is already audited in practice, a connection developed in Section 7.

The broad intuition that ESG should be extended with a technology dimension has been raised before in practitioner literature (Bonime-Blanc, 2020). The contribution of this paper is to move that intuition from proposition to framework. It grounds the fourth pillar in stakeholder and agency theory, connects it to the scholarly construct of Corporate Digital Responsibility, demonstrates its materiality with documented evidence, and, above all, renders it auditable by deriving its architecture from an established enterprise governance framework. Where earlier commentary asserted that technology belongs in ESG, the framework set out here specifies how technology can be governed, measured and disclosed as a fourth pillar, and on that basis treats ESGT as a theory of technology governance rather than a slogan.

Corporate Digital Responsibility

The leading scholarly parallel is Corporate Digital Responsibility. In an influential definition, it denotes the set of shared values and norms that guide an organisation in its operations across the lifecycle of digital technology and data, spanning the creation of technology, its operation in decision making, the

inspection and assessment of its impact, and its refinement (Lobschat et al., 2021). A complementary strand maps this construct directly onto the environmental, social and governance framework and treats it as an extension of corporate social responsibility for the digital age (Mueller, 2022). Subsequent work has begun to operationalise its dimensions, including data privacy and protection, digital wellbeing, environmental sustainability, digital inclusion and accessibility, and the ethical use of technology, and to develop validated measurement scales from the perspective of both firms and consumers (Wirtz et al., 2023).

Corporate Digital Responsibility and the framework advanced here are complementary rather than competing. Corporate Digital Responsibility is a values and responsibility construct, rooted in business ethics and information systems scholarship, that supplies the normative content of what responsible technology means across the lifecycle and across stakeholders. ESGT as developed in this paper is a governance and disclosure construct, rooted in risk management and assurance, that supplies the structural home and the auditable form. The former answers what responsible technology requires, the latter answers how a board is to govern, evidence and disclose it.

Competing framings

At least four distinct ways of locating technology within or alongside ESG can be identified. Table 1 summarises them with their principal strengths and weaknesses.

Table 1. Competing ways of locating technology within or alongside ESG.

Framing	Core idea	Strength	Weakness
Standalone fourth pillar (ESGT)	Technology becomes an explicit pillar co equal with E, S and G	Forces board visibility and distinct disclosure of a cross cutting risk	Adds to framework proliferation and taxonomic complexity
Tech ethics and digital responsibility	Emphasis on values such as fairness, transparency and accountability	Rich normative content and stakeholder grounding	Weaker as a reporting and comparability mechanism
Folding AI into Governance	AI oversight treated as a corporate governance sub topic	Parsimonious and uses existing structures	Buries a material, cross cutting risk and underweights its social and environmental dimensions
Corporate Digital Responsibility	A parallel responsibility construct across the data and technology lifecycle	Strong academic foundation and emerging measurement scales	Not yet integrated into mainstream investor disclosure

V. THEORETICAL GROUNDING

A proposal to restructure a governance framework requires more than a list of incidents. It requires a theory of why technology behaves as a distinct dimension. Three established bodies of theory converge on this conclusion.

Stakeholder theory provides the first foundation. In its classic formulation, the firm must manage relationships with all constituencies affected by its operations, not only its shareholders (Freeman, 1984). Digital and algorithmic systems create new categories of affected parties, including data subjects whose information is processed, individuals subjected to automated decisions and even non users who are excluded or profiled without ever interacting with the firm.

The expansion of the stakeholder map by digital technology is precisely what justifies a dedicated governance lens, and it is notable that the Corporate Digital Responsibility construct is itself built on a multi stakeholder model (Lobschat et al., 2021).

Agency theory provides the second. The separation of ownership and control generates information asymmetries between managers and those to whom they are accountable (Jensen and Meckling, 1976). In the technology domain this asymmetry is acute, because boards frequently lack the expertise to interrogate the artificial intelligence systems their

organisations deploy. The documented tendency of firms to frame artificial intelligence as opportunity rather than risk, and to disclose it rarely, is consistent with a governance gap of exactly this kind (Primec, Belak and Cufar, 2026). A pillar that carries explicit board competence and oversight expectations is a direct response.

The third foundation links technology to sustainability itself. The literature on sustainable artificial intelligence distinguishes between artificial intelligence used to advance sustainability and the sustainability of artificial intelligence as an artefact with its own energy, water and carbon costs (van Wynsberghe, 2021). This distinction connects the proposed T pillar directly to the E of the existing triad and shows that technology is not a free standing silo but a dimension that interacts with environmental and social concerns. The same connective logic underlies the treatment of artificial intelligence within global ethics instruments that tie it explicitly to sustainable development (UNESCO, 2021).

These three foundations also explain why double materiality, the concept at the heart of the European reporting regime, is the natural bridge for the T pillar. Double materiality combines impact materiality, meaning the effect of the firm on people and the environment, with financial materiality, meaning the effect of external factors on the firm (Deloitte, 2024). Technology satisfies both lenses at once. The energy footprint and human rights consequences of artificial intelligence are matters of impact materiality, while breach costs, regulatory fines and business disruption are matters of financial materiality. A factor that is simultaneously material in both senses, and that cuts across environment, society and governance, behaves like a distinct dimension rather than a sub item of any one letter.

VI. THE MATERIALITY OF TECHNOLOGY RISK

The case for a pillar ultimately rests on materiality. The evidence that technology and artificial intelligence risks are financially and socially material is now substantial and spans data breaches, regulatory fines and documented algorithmic harms. On data breaches, the most widely cited industry benchmark places the global average cost of a breach at a record 4.88 million United States dollars in 2024, an increase of roughly ten percent on the prior year, with around seventy percent of the organisations studied reporting significant or moderate operational disruption (IBM, 2024). On privacy enforcement, a single decision by the Irish Data Protection Commission imposed a record fine of 1.2 billion euros on Meta in May 2023 for unlawful transfers of personal data, and that firm's cumulative penalties under the

General Data Protection Regulation exceed two billion euros (EDPB, 2023). These are board level, financially material events by any reasonable threshold.

The most instructive cases, however, are those in which algorithmic systems caused direct harm to people. Table 2 summarises a set of well documented incidents that illustrate the breadth of technology risk, from public administration to hiring.

Table 2. Selected documented incidents of algorithmic and digital harm.

Incident	Year	Nature of harm	Consequence
Dutch childcare benefits scandal	2019 to 2021	Risk classification algorithm used nationality as a fraud indicator, ruled discriminatory	Tens of thousands of families wrongly accused; national regulator fine; resignation of the cabinet
Clearview AI facial recognition	2021 to 2024	Unlawful scraping of facial images for a recognition database	Maximum level fines across several European regulators
Apple Card and Goldman Sachs	2019 to 2021	Allegations of gender bias in credit limit decisions	Regulatory investigation; no fair lending violation found but transparency criticised
EEOC v. iTutorGroup	2023	Recruiting software automatically rejected older applicants	First United States settlement on AI hiring discrimination; redress fund established

The Dutch childcare benefits scandal is the most vivid illustration. A self learning risk classification system used by the national tax administration treated nationality as an indicator of fraud risk, a practice later ruled discriminatory. The responsible agency has acknowledged at least tens of thousands of wrongly accused families, the national data protection authority imposed fines for unlawful and discriminatory processing, and the affair contributed to the resignation of the national government in January 2021 (Autoriteit Persoonsgegevens, 2021). The episode demonstrates that a failure of technology governance can escalate into a constitutional event. The settlement in the iTutorGroup matter, the first of its kind brought by the United States Equal Employment Opportunity Commission, shows the same dynamic in the private sector, where recruiting software automatically rejected qualified applicants on the basis of age (EEOC, 2023). Taken together, the breach data, the enforcement record and the harm cases establish that technology risk is not speculative but realised, recurring and expensive.

VII. ANCHORING THE T PILLAR IN AUDITABLE STANDARDS

The available stack

The most serious objection to a technology pillar is that technology governance cannot be measured with the rigour expected of a disclosure category. This objection was once persuasive. It is now increasingly answerable, because a mature stack of auditable instruments has emerged that can give the T pillar concrete and certifiable substance. Table 3 sets out the principal instruments.

Table 3. A stack of auditable instruments available to anchor a technology pillar.

Instrument	Issuer and year	Contribution to the T pillar
COBIT 2019	ISACA, 2018	Enterprise governance of information and technology; supplies the architectural template for the pillar, developed in Section 7.2
ISO/IEC 42001	ISO and IEC, 2023	First certifiable management system standard for artificial intelligence, covering policy, risk and impact assessment, lifecycle and supplier oversight
EU AI Act	European Union, 2024	First comprehensive AI law; risk based obligations on providers and deployers with extraterritorial reach
NIST AI RMF 1.0	NIST, 2023	Voluntary framework organised around Govern, Map, Measure and Manage, with a generative AI profile added in 2024
OECD AI Principles	OECD, 2019 and 2024	First intergovernmental AI standard; values based principles adopted by the G20
UNESCO Recommendation on AI Ethics	UNESCO, 2021	First global ethics instrument adopted by all member states, including impact assessment provisions
ISO/IEC 27001	ISO and IEC, 2022	Certifiable information security management system standard
NIST CSF 2.0	NIST, 2024	Adds Govern as a top level cybersecurity function alongside Identify, Protect, Detect, Respond and Recover

The significance of this stack is that it converts an abstract aspiration into something an auditor can examine. ISO/IEC 42001, issued in 2023, is the first management system standard dedicated to artificial intelligence and follows the same harmonised structure as the well established information security standard, which means it can be certified by accredited third parties (ISO, 2023). The European Union Artificial Intelligence Act, in force from August 2024 with its principal high risk obligations applying from August 2026, imposes a risk based set of duties including risk management, data governance, documentation, human oversight, transparency and robustness, and its extraterritorial reach makes it globally relevant to corporate governance (European Commission, 2024). The NIST frameworks supply a widely adopted vocabulary, and the information security standard supplies long established and certifiable controls. None of these instruments, however, tells a board how to structure the pillar itself. For that, the framework turns to COBIT 2019.

COBIT 2019 as the architectural template for the T pillar

COBIT 2019, issued by ISACA as the framework for the enterprise governance of information and technology, occupies a distinctive place in this framework. The other instruments in Table 3 are largely substantive, in that they prescribe what an organisation should do about artificial intelligence, information security or fundamental rights. COBIT is architectural, in that it prescribes how governance over technology should be structured, allocated and evidenced. It is therefore adopted here not as one control set among several but as the organising template of the T pillar.

Four features of the framework make it suitable for this role. The first and most important is its explicit separation of governance from management, which is one of its governance system principles and is expressed structurally in its core model. That model comprises forty governance and management objectives distributed across five domains. A single governance domain, Evaluate, Direct and Monitor, contains five objectives and is addressed to the governing body, while the remaining thirty five objectives sit in four management domains, namely Align, Plan and Organise, Build, Acquire and Implement, Deliver, Service and Support, and Monitor, Evaluate and Assess, which are addressed to management (ISACA, 2018). This distinction is precisely the one that non financial disclosure requires and frequently lacks. A disclosure framework should report what the board evaluated, directed and monitored, not merely what the technology function implemented.

The second feature is the framework's articulation of seven governance components, namely processes, organisational structures, principles, policies and procedures, information flows and items, culture, ethics and behaviour, people, skills and competencies, and services, infrastructure and applications. These components turn a governance objective into something that can be evidenced from several independent angles, which is the practical requirement of assurance. The third feature is design factor tailoring. The framework provides a set of design factors through which an enterprise determines which objectives are material to it and at what capability level, which directly answers the proportionality objection that a fourth pillar would burden smaller organisations. The fourth is interoperability. COBIT was explicitly constructed for compatibility with other standards, including those of the International Organization for Standardization and the National Institute of Standards and Technology, so adopting it as the architecture of the T pillar does not force an organisation to abandon the artificial intelligence, information security or cybersecurity standards it already operates.

Table 4 sets out the resulting mapping. Each of the five governance objectives in the Evaluate, Direct and Monitor domain is expressed as a corresponding governance question and disclosure expectation for the T pillar. The mapping is offered as the structural core of the framework proposed in this paper.

Table 4. Mapping the COBIT 2019 governance domain to the proposed T pillar.

COBIT 2019 governance objective (EDM domain)	Governance question for the T pillar	Corresponding T pillar disclosure
EDM01 Ensured governance framework setting and maintenance	Is there a board approved framework for governing artificial intelligence and digital technology, with a defined mandate and owner?	Existence, scope and ownership of the technology and artificial intelligence governance policy, and the board committee accountable for it
EDM02 Ensured benefits delivery	Are the purpose, value and justification of artificial intelligence deployments articulated and reviewed?	Statement of intended purpose and benefit for material artificial intelligence systems, with review cadence
EDM03 Ensured risk optimisation	Has the board set a risk appetite for artificial intelligence, data and cyber risk, and is it monitored?	Technology risk appetite, risk register entries, impact assessments and incident record for the reporting period

EDM04 Ensured resource optimisation	Does the organisation possess the skills, data quality and infrastructure that responsible deployment requires?	Board and workforce competence in artificial intelligence governance, data governance maturity and assurance capacity
EDM05 Ensured stakeholder engagement	Are affected stakeholders informed, consulted and able to seek redress?	Transparency measures, stakeholder and rights holder engagement, and mechanisms for contesting automated decisions

Two implications follow. First, the mapping demonstrates that the T pillar need not be invented from first principles, because a mature and widely taught governance vocabulary already exists and can be adapted with minimal translation. Second, and more consequentially for disclosure, the mapping produces reportable items that are governance items rather than technical ones. Each row of Table 4 describes something a board can be asked whether it did, and something an assurance provider can test. This is what the auditable pillar principle set out in Section 4.1 requires, and it is the respect in which the framework proposed here differs from a general appeal to include technology in ESG.

VIII. OPERATIONALISING THE T PILLAR

Drawing the preceding sections together, the T pillar can be expressed as a coherent disclosure architecture rather than a slogan. The following indicators are proposed as a starting set, each traceable to the governance architecture of Table 4, the instruments of Table 3 and the materiality evidence of Section 6.

1. Governance and oversight, including a board approved technology and artificial intelligence governance framework and a named accountable committee, following the Evaluate, Direct and Monitor domain of COBIT 2019 and the governance function of the NIST Cybersecurity Framework.
2. Management system maturity, including conformity with or certification to ISO/IEC 42001 for artificial intelligence and ISO/IEC 27001 for information security, reported at the capability level attained rather than as a binary claim.
3. Risk and impact assessment, including adoption of the NIST Artificial Intelligence Risk Management Framework and the conduct of algorithmic impact and fundamental rights assessments for higher risk systems.
4. Regulatory alignment, including classification and conformity status for systems within the scope of the European Union Artificial Intelligence Act and analogous regimes.
5. Incident and outcome metrics, including the number and severity of data breaches, privacy fines and material artificial intelligence incidents over the reporting period.
6. Environmental footprint of technology, including the energy and carbon intensity attributable to artificial intelligence and data operations, linking the T pillar to the E pillar.
7. Data governance and digital responsibility, including privacy protection, digital inclusion and accessibility, drawing on the dimensions of Corporate Digital Responsibility.

This architecture is intentionally modular and proportionate. Because the underlying framework tailors its objectives through design factors, an organisation discloses against those elements material to its size, sector and technology intensity rather than against all of them uniformly. An organisation that already reports against information security and cybersecurity standards can extend that reporting into artificial intelligence governance without abandoning its existing investments, and a standard setter could accommodate the pillar either as a new standard or as a clearly delineated cluster within an existing regime.

IX. COUNTERARGUMENTS AND LIMITATIONS

Intellectual honesty requires that the strongest objections be stated in their own terms rather than caricatured. Four deserve particular attention.

The first is dilution and incoherence. Critics argue that ESG is already an amorphous label that bundles unlike concerns, and that it should be disaggregated rather than expanded (Keeley, 2022). Adding a fourth letter, on this view, compounds the problem. The response is that technology is not an arbitrary addition but a dimension with its own theory, its own materiality and its own auditable architecture, which is more than can be said for some concerns already housed within the triad.

The second is framework proliferation and fatigue. There are already hundreds of ESG standards and ratings, the use of ESG terminology in corporate filings has begun to decline, and investors report a degree of fatigue with the entire enterprise (Harvard Law School Forum on Corporate Governance, 2026). A proposal to expand the framework runs against this tide. The response is twofold. The materiality evidence does not depend on the popularity of the ESG label, and the proposal deliberately reuses an established governance framework rather than inventing a new one, which limits the marginal burden it imposes.

The third is redundancy, the claim that technology is already covered within governance and social topics. The empirical record undercuts this claim. If technology were adequately covered, disclosure rates for artificial intelligence risk would not sit near ten percent among large and sophisticated firms (Primec, Belak and Cufar, 2026). Coverage in principle is not coverage in practice.

The fourth is rating divergence. ESG ratings already correlate poorly across providers. A widely cited study of several major raters found an average correlation of around 0.54, far below the near unanimity of credit ratings, with most of the divergence attributable to differences in measurement and scope (Berg, Kolbel and Rigobon, 2022). A new pillar could worsen this divergence if it is introduced without standardised metrics. This is a genuine risk and is the strongest reason to tie the T pillar to an established governance architecture and to certifiable standards rather than to leave it to the discretion of individual raters.

Several limitations of the present contribution should also be acknowledged. The paper advances a conceptual and normative argument rather than an empirical test, and the proposed mapping in Table 4 has not yet been validated in field conditions. Some of the supporting figures, particularly breach cost benchmarks, originate in industry rather than peer reviewed sources and should be read as benchmarks rather than settled findings.

The artificial intelligence governance standards on which the framework relies are themselves young and evolving, so any specific metric set will require periodic revision. A further limitation concerns the architectural choice itself. COBIT is an information technology governance framework by origin, and adapting it to a sustainability disclosure context imports assumptions about enterprise structure that may not hold for every organisation. Finally, the political backlash against ESG in some jurisdictions means that proposing to expand the framework carries a strategic risk, even though it does not undercut the substantive materiality argument.

X. DISCUSSION AND RESEARCH AGENDA

The framework advanced here is conditional rather than absolute, and it is useful to state the conditions under which it holds. If disclosure of artificial intelligence and digital risk rises substantially under existing reporting regimes, without the introduction of a dedicated pillar, then integration within the governance letter becomes a defensible alternative and the marginal value of a separate pillar declines. If, on the other hand, disclosure remains sparse despite the availability of entry points within current standards, the case for an explicit and separately governed pillar strengthens. The roughly ten percent disclosure rate observed in recent evidence is the empirical baseline against which this condition can be tested over time.

Four lines of research would advance the agenda. The first is empirical measurement, namely the development and validation of a technology governance disclosure index built on the mapping in Table 4 and on the emerging Corporate Digital

Responsibility scales. The second is field validation of that mapping through case studies in organisations that already operate the underlying governance framework, in order to test whether the governance objectives translate into disclosures that assurance providers can meaningfully test. The third is comparative institutional analysis, examining whether jurisdictions that have begun to require artificial intelligence and digital disclosures achieve materially better governance outcomes than those relying on voluntary integration. The fourth is the study of rating behaviour, testing whether anchoring a technology pillar to an established governance architecture reduces the inter rater divergence that afflicts ESG ratings more generally.

XI. CONCLUSION

Environmental, Social and Governance analysis was a conceptual achievement of its time, but its time was the early twenty first century, before artificial intelligence became a primary determinant of how organisations create value and impose risk. The triad now scatters technology across its three letters in a way that obscures materiality, fragments measurement and leaves the governance of the most consequential technologies of the age without a coherent disclosure logic.

This paper has argued that technology should be recognised as an explicit fourth pillar, that this pillar can be given measurable and auditable substance by deriving its architecture from an established framework for the enterprise governance of information and technology, and that the strongest objections, while real, are outweighed by the evidence of materiality and the documented gap in disclosure.

The proposal is offered in a global and standard agnostic spirit, as a contribution to the way boards, investors and standard setters might govern technology deliberately rather than by default. In an age in which organisations can no longer govern without technology, governance frameworks can no longer afford to treat technology as an afterthought.

ESGT FRAMEWORK DIAGRAM

REFERENCES

1. Autoriteit Persoonsgegevens. (2021). Decision imposing a fine on the Dutch Tax and Customs Administration for unlawful and discriminatory data processing. The Hague: Dutch Data Protection Authority.
2. Berg, F., Kolbel, J. F., and Rigobon, R. (2022). Aggregate confusion: the divergence of ESG ratings. Review of Finance, 26(6), 1315 to 1344.
3. Bonime-Blanc, A. (2020). Gloom to Boom: How Leaders Transform Risk into Resilience and Value. London: Routledge.
4. Deloitte. (2024). Unpacking the double materiality assessment under the EU Corporate Sustainability Reporting Directive. Deloitte Accounting Research Tool.
5. European Commission. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union.
6. European Data Protection Board. (2023). 1.2 billion euro fine for Facebook as a result of EDPB binding decision. Brussels: EDPB.
7. Freeman, R. E. (1984). Strategic Management: A Stakeholder Approach. Boston: Pitman.
8. Global Reporting Initiative. (2021). GRI Universal Standards. Amsterdam: Global Reporting Initiative.
9. Harvard Law School Forum on Corporate Governance. (2026). ESG shifting tides: an analysis of the changing narrative around sustainability and ESG investment contraction. Cambridge, Massachusetts.

10. IBM Security. (2024). Cost of a Data Breach Report 2024. Research conducted by the Ponemon Institute. Armonk, New York: IBM.
11. IFRS Foundation. (2024). ISSB to commence research projects about risks and opportunities related to nature and human capital. London: IFRS Foundation.
12. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection, information security management systems. Geneva: ISO.
13. International Organization for Standardization. (2023). ISO/IEC 42001:2023 Information technology, artificial intelligence, management system. Geneva: ISO.
14. International Sustainability Standards Board. (2023). IFRS S1 General Requirements for Disclosure of Sustainability related Financial Information and IFRS S2 Climate related Disclosures. London: IFRS Foundation.
15. ISACA. (2018). COBIT 2019 Framework: Introduction and Methodology. Schaumburg, Illinois: ISACA.
16. ISACA. (2018). COBIT 2019 Framework: Governance and Management Objectives.
17. Schaumburg, Illinois: ISACA.
18. ISACA. (2018). COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution. Schaumburg, Illinois: ISACA.
19. Jensen, M. C., and Meckling, W. H. (1976). Theory of the firm: managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3(4), 305 to 360.
20. Keeley, T. R. (2022). Sustainable: Moving Beyond ESG to Impact Investing. New York: Columbia Business School Publishing.
21. Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., and Wirtz,
22. J. (2021). Corporate digital responsibility. Journal of Business Research, 122, 875 to 888.
23. Mueller, B. (2022). Corporate digital responsibility: new corporate responsibilities in the digital age. Business and Information Systems Engineering.
24. National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework, AI RMF 1.0. Gaithersburg, Maryland: NIST.
25. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, Maryland: NIST.
26. Organisation for Economic Co-operation and Development. (2019, updated 2024).
27. Recommendation of the Council on Artificial Intelligence. Paris: OECD.
28. Pollman, E. (2024). The making and meaning of ESG. European Corporate Governance Institute Law Working Paper.
29. Primec, A., Belak, J., and Cufar, M. (2026). Artificial intelligence as an emerging risk dimension in corporate sustainability reporting: a legal and governance perspective. Sustainability, 18(5), article 2278.
30. Sustainability Accounting Standards Board. (2018). SASB Conceptual Framework. San Francisco: SASB, now part of the IFRS Foundation.
31. Task Force on Climate related Financial Disclosures. (2017). Recommendations of the Task Force on Climate related Financial Disclosures. Basel: Financial Stability Board.
32. UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO.
33. United Nations Environment Programme Finance Initiative. (2005). A legal framework for the integration of environmental, social and governance issues into institutional investment.
34. The Freshfields report. Geneva: UNEP FI.
United Nations Global Compact. (2004). Who Cares Wins: Connecting Financial Markets to a Changing World. New York: United Nations.
35. United States Equal Employment Opportunity Commission. (2023). EEOC v. iTutorGroup, settlement of the first AI hiring discrimination case. Washington, District of Columbia: EEOC.
36. van Wynsberghe, A. (2021). Sustainable AI: AI for sustainability and the sustainability of AI. AI and Ethics, 1, 213 to 218.
37. Wirtz, J., Kunz, W. H., Hartley, N., and Tarbit, J. (2023). Corporate digital responsibility in service firms and their ecosystems. Journal of Service Research.