Artificial Intelligence and Institutional Accountability

Applying Existing Legal and Governance Frameworks to AI-Influenced Decision-Making.

The governance challenge posed by artificial intelligence is institutional, not technological. The critical question is not what AI does, but who decided to use it.

RT Consulting Ltd

Prepared for policymakers, senior leadership, regulatory authorities, and institutional decision-makers.

RT CONSULTING
By Experts, For Executives

About The Author:

Dr Róis Ní Thuama is a Doctor of Law and a governance & cyber-risk specialist who advises boards and senior leaders across the UK, EU and USA on aligning security practice with legal and fiduciary duties. She has briefed the U.S. Department of Defense, the UK Parliament and major corporates, and serves as a contributing editor with PC Pro.

Acknowledgements:

The author is grateful to those who contributed to the roundtable discussion Combatting the AI Firehose – Prioritising Assets, Strengthening Defences, held at the Cavalry and Guards Club in London in September 2025. The roundtable was convened by Dr Rois Ní Thuama with the support of the Worshipful Company of Information Technologists (WCIT) and chaired by Col. James Greaves, whose leadership and insights helped shape the discussion and informed the thinking presented in this paper.

Participants included Andy Bates, Jon Brewer, Steve Hill, Kathleen Moriarty, Sharon Morris, Jim Mulheron Ian Thornton-Trump, Arthur Virgo, Terry Wilson and others who contributed to the discussion.

The author also thanks Dr Dinos Kerrigan-Kyrou and Ian Dyson QPM DL for thoughtful conversations on the intersection of technology, governance and the law.

Responsibility for the views expressed in this paper rests solely with the author.

RT CONSULTING
By Experts, For Executives

About RT Consulting Ltd:

RT Consulting Ltd helps boards and senior leaders convert digital and operational risk into clear, defensible decisions.

Our flagship framework, RAPID-T™, aligns governance with NIS2, DORA, directors' duties and key EU/UK obligations, creating observable evidence leaders can stand over. We provide board education, executive workshops and implementation support across the UK, EU and US for corporates, financial services, critical-infrastructure and public-sector clients.

Executive Summary

Artificial intelligence (AI) is increasingly used across government, business, and defence. Public debate often frames AI as an existential threat, raising concerns that autonomous systems may undermine traditional structures of responsibility.

This paper argues that the governance challenge posed by artificial intelligence is not primarily technological but institutional.

Legal systems already contain well-established doctrines for assigning responsibility when harm arises from complex chains of action involving multiple actors.

The real risk lies not in a disappearance of responsibility, but in failures of organisational governance. Where responsibility appears unclear, it is often because institutions have not clearly allocated ownership, oversight, or accountability for the deployment of AI systems.

Effective AI governance therefore requires institutions to ensure that responsibility for decisions influenced by artificial intelligence remains clearly defined, documented, and subject to appropriate oversight.

Artificial intelligence may influence decisions, but it does not change who remains responsible for them.

Key Findings

- AI does not remove human responsibility for decisions. Legal responsibility continues to rest with identifiable actors and institutions.
- Existing legal doctrines - including negligence, corporate liability, product liability and duty of care - are capable of addressing harms involving AI systems.
- The idea of a "responsibility gap" is often overstated. Apparent gaps usually arise from unclear governance structures rather than a lack of legal accountability.
- The real challenge for organisations is governance: ensuring that responsibility for the deployment and supervision of AI systems is clearly allocated and documented.
- Effective AI governance therefore requires institutional accountability rather than entirely new legal frameworks.
- Effective governance must focus on decision accountability rather than technology control.

1. Introduction

In September 2025, we convened a roundtable at the Cavalry and Guards Club in London to discuss artificial intelligence, responsibility, defence, and strategy. Participants included representatives with expertise in law, technology, defence, business, engineering, and the civil service. The discussion brought together practitioners and policymakers concerned with how rapidly advancing technologies are being deployed within institutions without corresponding governance and oversight.

Artificial intelligence (AI) may influence decisions, but it does not change who remains responsible for them.

A central theme of the discussion was the growing volume of public commentary suggesting that AI represents an existential threat to humanity. Media coverage frequently frames AI in dramatic terms, often emphasising catastrophic scenarios in which machines operate beyond human control.

Whether these narratives arise from misunderstanding, editorial incentives, or broader information dynamics, they have contributed to considerable public confusion about the nature of the risks involved. Organisations and policymakers increasingly face complex questions about AI without clear frameworks for responding to them.

This paper proceeds from a simple premise: before designing new regulatory responses, it is necessary to understand the problem clearly. Artificial intelligence does not remove human responsibility for decisions. The real governance challenge lies in ensuring that institutions deploying AI retain clear structures of accountability.

The purpose of this paper is therefore to clarify where responsibility lies when AI is deployed within intstitutions.

Safeguarding businesses, institutions and ultimately the wider economy is a matter of national security and requires coordinated effort. Responsibility for technological governance does not reside within a single organisational function. For many years practitioners and policymakers have emphasised the need for a holistic approach. AI governance does not belong solely to compliance, legal, IT or operations; rather, it sits at the intersection of these functions and requires coordinated oversight.

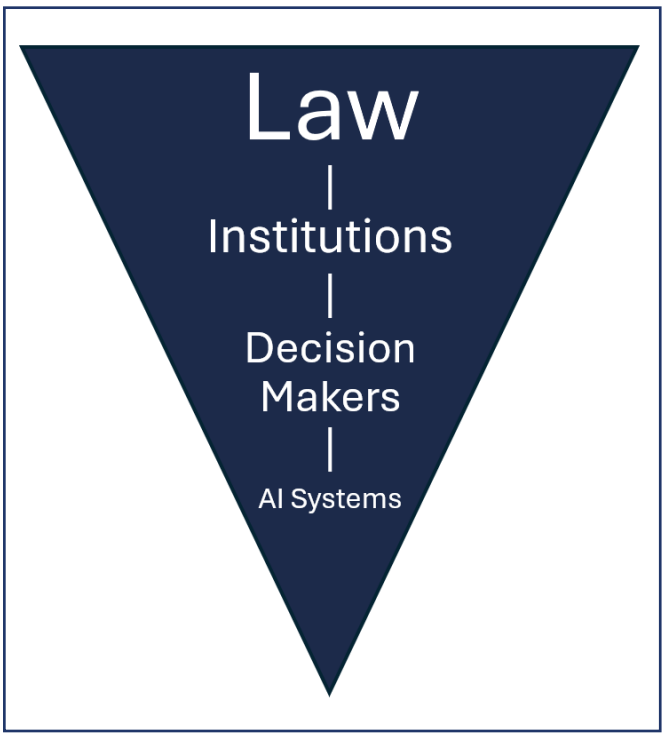

Figure 1. Institutional accountability in AI deployment

Artificial intelligence systems operate within organisational decision structures governed by law. Responsibility therefore flows through institutions and human decision-makers rather than residing within technological systems themselves.

Artificial intelligence may influence decisions, but it does not change who remains responsible for them.

2. The AI Governance Challenge

The prevailing debate on artificial intelligence often assumes that AI creates unprecedented governance problems requiring entirely new regulatory systems. This paper takes a different view. The core challenge is not technological but institutional: as organisations deploy increasingly powerful tools, legal responsibility for outcomes remains with human actors.

AI is now embedded across commercial, governmental, and public-sector contexts[1]. It supports functions such as fraud detection, operational monitoring, customer interaction, credit assessment, research, and strategic analysis. This diffusion has rightly attracted regulatory attention[1,2]. Yet focusing primarily on the technical properties of AI - such as model transparency, training data provenance, bias, or safety - risks obscuring a more fundamental point: organisations using AI continue to operate within established legal and regulatory frameworks.

Crucially, AI does not alter the structure of accountability in law. Directors, executives, and corporate entities remain responsible for decisions and outcomes produced within their institutions, regardless of the tools employed. What changes is not who is accountable, but how accountability must be evidenced and exercised. AI introduces complexity into decision-making processes, heightens the need for documented oversight, and requires clarity about roles, authorities, and controls.

Accordingly, the governance challenge is institutional rather than technological. Legal systems already regulate fraud, negligence, corporate responsibility, and decision-making authority. The introduction of AI does not remove these obligations. Instead, it raises practical questions about how organisations demonstrate responsibility in environments where decisions are supported - or influenced - by algorithmic systems. Effective AI governance should therefore prioritise:

Clear lines of responsibility: unambiguous allocation of oversight and decision rights when AI is used.

Process transparency: traceable workflows, documentation of model use, and explainability commensurate with risk.

Control and assurance: appropriate testing, monitoring, and escalation mechanisms integrated into existing risk and compliance frameworks.

Evidence of accountability: records that show how human judgment was applied, what controls operated, and how issues were managed.

In short, AI is an operational tool[3] whose deployment must be governed through institutional design and practice. Rather than constructing entirely new regulatory architectures for AI as a technology, policymakers and organisations should ensure that existing accountability frameworks are applied rigorously and adapted to the specific complexities AI introduces. This approach maintains continuity in the law while strengthening the practical mechanisms that uphold responsibility, oversight, and trust.

This raises a central governance question: How should institutions govern the use of AI when legal responsibility for outcomes remains with human actors?

The answer is institutional rather than technological.

The governance challenge posed by AI lies not in the technical properties of the systems themselves but in the structures through which organisations manage risk, allocate responsibility, and demonstrate accountability.

Institutions have always been required to govern complex tools. AI represents a powerful new category of tool, but it does not alter the fundamental legal structure through which responsibility is assigned.

3. The Governance Challenge is Institutional, Not Technological

Much of the current policy debate treats AI as a novel technological phenomenon that requires entirely new regulatory structures. While AI systems undoubtedly introduce new capabilities, the fundamental

1: UK Government, National AI Strategy (Department for Digital, Culture, Media and Sport 2021).
2: European Commission, Regulation (EU) 2024/1689Artificial Intelligence Act (2024).
3: OECD (2019), Artificial Intelligence in Society, OECD Publishing, Paris, https://doi.org/10.1787/eedfee77-en.

governance question they raise is an old one: how institutions remain accountable for the consequences of decisions taken within them.

Artificial intelligence does not remove responsibility from organisations or their leaders. Companies continue to operate within legal systems that assign duties, obligations, and liability to identifiable actors: directors, executives, employees, and corporate entities themselves.

The deployment of AI therefore does not alter the underlying structure of accountability. Instead, it complicates it.

Where AI is deployed organisations must still be able to demonstrate:

- who authorised the use of the system;
- what risks were considered before deployment;
- how outputs were interpreted and verified;
- who remained responsible for the resulting decision.

The governance problem is therefore not the existence of AI itself. It is ensuring that institutional accountability remains visible and enforceable[4].

For this reason, effective AI governance should begin not with the technical characteristics of AI systems, but with the institutional responsibilities that already exist within law and corporate governance.

4. The Law is Largely Technology-Neutral

Legal systems have historically been designed to regulate harmful conduct rather than specific technologies. As new tools emerge, the law typically applies established principles to new circumstances instead of creating entirely new legal regimes. The rise of the internet, for example, did not require the invention of new categories of fraud, theft, negligence, or breach of duty. Existing legal doctrines were extended to conduct occurring through digital channels: fraud committed electronically remained fraud, and negligence facilitated by software remained negligence.

Artificial intelligence follows the same pattern. Although AI may alter how decisions are made, how information is processed, and the speed at which actions occur, it does not change the underlying allocation of legal responsibility. Directors remain bound by duties under company law; individuals remain liable for fraudulent acts; and organisations remain accountable for negligent behaviour within their operations, irrespective of whether AI tools were involved.

This technology neutral character of the law has two significant implications for AI governance.

First, many harms associated with AI - such as fraud, misrepresentation, discrimination, breach of fiduciary duty, and negligent decision making - already fall within existing legal frameworks. The primary challenge for organisations is therefore not the absence of applicable law, but ensuring that established responsibilities are effectively upheld as AI systems are incorporated into decision making processes.

Second, governance frameworks should focus less on regulating the technology itself and more on ensuring that responsibility for decisions remains clear and demonstrable when AI systems are involved. The central task is not to construct an entirely new regulatory architecture, but to ensure that existing structures of accountability continue to function in environments where automated systems inform, shape, or influence human judgment.

5. Corporate Governance Law Already Anticipates Technological Change

Corporate law has long recognised that communication technologies evolve over time. Rather than prescribing specific technical mechanisms, legislation often regulates what must occur legally, while allowing flexibility in how those actions are carried out electronically. The Companies Act 2006 provides a useful illustration of this approach.

4: RT Consulting Limited Whitepaper; Credit Ratings, Governance Duties, & the New Systemic Risk Perimeter; 2025.

The Act contains numerous provisions governing the use of electronic communications in corporate processes, including:

- electronic delivery of company documents to shareholders;
- electronic communication of notices and resolutions;
- the circulation of written resolutions;
- electronic filing of company documents;
- communication between companies and members through electronic means.

Importantly, these provisions generally do not mandate a specific technological system or platform. Instead, they establish legal requirements such as:

- consent of the recipient to electronic communication;
- the reliability and accessibility of the information communicated;
- the ability of recipients to access and retain the information;
- clear identification of the sender and the document being transmitted.

In other words, the law specifies the legal conditions that must be satisfied, rather than prescribing the particular technological tools used to satisfy them.

This approach reflects a long-standing principle of legislative design: law regulates legal responsibility and evidential standards, not the underlying technology through which actions occur. The same principle is relevant to the governance of AI.

The flexibility embedded within the Companies Act 2006 has been recognised previously in legal scholarship examining how electronic communications facilitate shareholder participation and diligence. Earlier research analysing the Act identified numerous provisions enabling companies to communicate electronically with shareholders and to publish key corporate information through digital channels[5].

This statutory framework illustrates that corporate governance law has already adapted to earlier waves of technological change by regulating legal obligations and evidential standards rather than specific technologies.

Artificial intelligence represents another technological development whose deployment must be governed by organisations. However, its existence does not alter the underlying legal expectations placed upon corporate actors. Directors remain responsible for the decisions taken within the organisations they oversee, regardless of whether those decisions are informed by human analysis, software systems, or AI.

The challenge for AI governance is therefore not to construct entirely new legal frameworks, but to ensure that existing corporate governance obligations remain capable of being fulfilled and evidenced when AI tools are deployed.

6. From Technology Governance to Decision Governance

Much of the current discourse around AI focuses on the governance of technology itself. Discussions frequently centre on model architecture, training data, algorithmic bias, transparency, and system explainability.

While these issues are important from a technical perspective, they do not fully resolve the governance question faced by organisations deploying AI systems. Institutions are not ultimately judged by the internal mechanics of their technologies. They are judged by the decisions taken within them and the consequences of those decisions.

Courts, regulators, and investigators rarely ask how a model was trained or which architecture it used. Instead, they ask questions such as:

- Who authorised the use of the system?
- What risks were considered before it was deployed?
- What safeguards existed to detect error or misuse?

5: Rois Ni Thuama, Rediscovering Shareholder Activism: A Critique of Public Company Conduct in Relation to Facilitating Shareholder Diligence (PhD thesis, Bangor University Law School 2015).

- How were outputs interpreted by decision-makers?
- Who remained responsible for the final decision?

These are questions of decision governance rather than technology governance. AI therefore exposes a structural tension within many organisations. Sophisticated technical systems are often introduced into environments where decision accountability mechanisms have not evolved at the same pace. The result can be a widening gap between the complexity of the tools being used and the clarity of responsibility for the outcomes those tools influence.

Effective AI governance must therefore focus not only on the design and behaviour of technological systems, but also on the institutional processes through which AI-related decisions are authorised, challenged, documented, and reviewed.

This shift in focus, from the governance of technology to the governance of decisions, provides a more practical foundation for organisations seeking to deploy AI responsibly while remaining compliant with existing legal and regulatory obligations.

7. Identifying the Harms AI Governance Should Address

If AI governance is to be effective, it must begin by identifying the harms organisations are seeking to prevent or mitigate. Attempts to regulate AI (as a single category) risk obscuring the wide range of risks that different AI systems may present in practice.

A more practical approach is to examine how the use of AI may intersect with existing areas of legal liability and organisational risk. Many of the harms associated with AI are not novel in themselves; rather, AI can amplify or accelerate forms of misconduct or error that legal systems have long recognised. Several broad categories of harm are particularly relevant in the corporate context.

7.1 Fraud and Economic Crime

AI systems may be used to facilitate or scale fraudulent activity. Generative tools can be used to create convincing phishing communications, impersonate individuals through synthetic voice or video, or automate aspects of social engineering attacks.

In such cases the underlying harm remains fraud or deception, conduct already addressed under legislation such as the Fraud Act 2006 and related criminal offences. AI does not create a new category of wrongdoing it does significantly increase the speed, scale, and sophistication with which such offences can occur.

7.2 Misrepresentation and Commercial Harm

AI-generated content may also expose organisations to risks of misrepresentation. Where businesses rely on automated systems to generate communications, marketing materials, research outputs, or advisory content, inaccuracies or fabricated information may be disseminated unintentionally. If such information is relied upon by customers, counterparties, or investors, the resulting harm may fall within existing legal frameworks governing negligent misstatement, misrepresentation, or breach of contract.

7.3 Operational and Decision-Making Risk

Another area of concern arises where AI systems influence operational or strategic decisions. Decision-support systems may generate analyses, forecasts, or recommendations that are relied upon by employees or executives.

Where such outputs are flawed, incomplete, or misunderstood, organisations may make decisions that result in financial loss, regulatory breaches, or operational failure. The legal consequences may arise through negligence, breach of duty, or regulatory enforcement.

7.4 Discrimination and Rights-Based Harm

Certain AI systems may also introduce risks relating to discrimination or unfair treatment. Automated decision systems used in areas such as recruitment, lending, or service provision may unintentionally replicate or amplify biases present in training data.

Such outcomes may engage legal obligations under equality and anti-discrimination law, as well as broader regulatory frameworks concerned with fairness and consumer protection.

In employment contexts this issue is particularly acute. Organisations increasingly use automated systems to assist with recruitment screening, performance assessment, and workforce management. Where such systems influence employment decisions, employers remain responsible under existing employment and equality law for ensuring that those decisions are lawful and non-discriminatory. The use of automated tools does not displace these obligations. Instead, it increases the importance of governance structures capable of demonstrating how automated outputs were interpreted, validated, and incorporated into human decision-making.

7.5 Governance and Accountability Failures

Finally, a less visible but significant category of harm arises from governance failures themselves. Organisations may deploy AI tools informally, without clear ownership, risk assessment, or oversight. Decisions may become increasingly influenced by automated outputs without corresponding documentation of how those outputs were interpreted or validated.

In these circumstances the harm lies not solely in the behaviour of the technology, but in the absence of governance structures capable of ensuring accountability for AI-influenced decisions. The identification of these harms highlights an important point: the legal system already provides frameworks for addressing many of the risks associated with AI.

The central question for organisations is therefore not whether AI requires entirely new legal obligations, but how existing corporate governance duties apply when decisions are influenced by automated systems. The next section examines these duties in more detail.

8. Corporate Governance Duties in an AI Environment

The deployment of AI within organisations does not occur in a legal vacuum. Corporate decision-making remains governed by long-established principles of company law that assign responsibility to identifiable individuals, particularly directors and senior management.

In the United Kingdom, these duties are primarily set out in the Companies Act 2006, which establishes the legal framework within which directors must exercise their functions. Several duties are particularly relevant when organisations deploy AI.

8.1 Duty to Exercise Reasonable Care, Skill and Diligence (Section 174)

Section 174 of the Companies Act 2006 requires directors to exercise reasonable care, skill and diligence in the performance of their duties.

This duty incorporates both:

- an objective standard, reflecting the general knowledge, skill, and experience reasonably expected of a director, and;
- a subjective standard, reflecting the actual knowledge and experience possessed by the particular director.

In the context of AI, this duty raises important governance questions. Directors are not expected to become technical experts in machine learning systems. However, they are expected to exercise reasonable judgement when authorising the deployment of technologies regardless of its purpose..

This may require directors to ensure that:

- appropriate risk assessments are conducted before AI systems are deployed;
- relevant expertise is consulted when evaluating technical systems;
- governance mechanisms exist to monitor the ongoing performance of AI tools;
- potential errors or limitations in AI outputs are properly understood.

Failure to consider such issues could expose directors to allegations that reasonable care and diligence were not exercised.

8.2 Duty to Exercise Independent Judgement (Section 173)

Section 173 requires directors to exercise independent judgement when making decisions.

The rapid adoption of AI and the procurement of increasingly sophisticated analytical tools raise important questions about how this duty should be interpreted in practice. While such systems may assist directors and executives by processing large volumes of information, reliance on automated outputs does not relieve decision-makers of the obligation to apply their own judgement.

In practice, this requires directors to understand the function and limitations of the tools they authorise for use within the organisation. Without appropriate governance structures that enable meaningful scrutiny of such systems, it may become difficult to demonstrate that independent judgement has been exercised.

8.3 Duty to Promote the Success of the Company (Section 172)

Section 172 requires directors to act in a way they consider most likely to promote the success of the company for the benefit of its members, while having regard to a range of broader considerations including employees, customers, suppliers, and the long-term consequences of decisions.

The deployment of AI tools must therefore align with the long-term interests of the company and its stakeholders. Cases in which automated systems have produced harmful outcomes[6] - for example, where algorithmic assessment tools have led to unfair employment decisions and subsequent legal challenge[7] - illustrate how the use of AI can expose organisations to liability.

Directors must therefore evaluate whether the benefits of automation are appropriately balanced against potential risks, including operational failure, reputational damage, employee harm, or regulatory scrutiny.

9. Governance Implications

Taken together, these duties highlight an important point: the legal responsibility for decisions taken within a company continues to rest with human actors, even where those decisions are influenced by automated systems. AI systems may assist in generating analysis, predictions, or recommendations. However, they do not possess legal personality and cannot assume legal responsibility.

The role of corporate governance is therefore to ensure that organisations retain clear lines of accountability when AI systems influence decision-making.

This requires governance structures capable of demonstrating:

- who authorised the deployment of the system;
- what risks were considered prior to deployment;
- how outputs are interpreted and validated;
- who remains responsible for the resulting decisions.

Without such structures, organisations may find it difficult to demonstrate that directors have fulfilled their legal duties.

9.1 Responsibility, "Autonomy," and the So-Called Gap

The literature on artificial intelligence frequently invokes a "responsibility gap," often linked to claims about "autonomous" systems. Following Matthias[8], the concern is that as systems become capable of performing complex tasks with minimal human intervention, responsibility for harmful outcomes appears to diffuse across numerous actors—designers, deployers, operators—and, ostensibly, the system itself.

6: Bartz v. Anthropic PBC, No. 3:24-cv-05417-WHA https://www.anthropiccopyrightsettlement.com/
7: Payout for Estée Lauder women 'sacked by algorithm' https://www.thetimes.com/business/technology/article/payout-for-estee-lauder-women-sacked-by-algorithm-wnq0ffzt3
8: Andreas Matthias, 'The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata' (2004) 6 Ethics and Information Technology 175.

This paper uses the term *autonomous* only as a descriptive label adopted in the literature to denote systems capable of executing tasks without continuous human input. It does not accept that such systems possess agency. Tools described as "autonomous" remain tools: they operate within the parameters of their design, training, programming, and configuration, under objectives and constraints defined by humans. This is not autonomy in the sense of independent agency; it is automated execution within human-defined rules and environments.

Recognising this distinction dissolves much of the supposed responsibility gap. Legal responsibility does not migrate into a machine simply because the machine performs steps without real-time human oversight. Responsibility attaches to the human and institutional decisions that specify objectives, architect systems, select and process data, set thresholds, authorise deployment, monitor performance, and respond to alerts and failures[9]. Advanced automation does not displace these responsibilities; it heightens the need to allocate, document, and evidence them.

Accordingly, what is often framed as a "responsibility gap" is better understood as a governance failure: the absence of clearly defined decision rights, escalation paths, controls, and records showing how human judgement was exercised around a system's design, deployment, and use. Addressing this is an institutional task, not a metaphysical one. It requires:

- **Defined accountability:** explicit assignment of roles for model design, validation, deployment, monitoring, and incident response.
- **Control integration:** embedding testing, change management, and performance monitoring within existing risk, audit, and compliance frameworks.
- **Traceability:** maintaining artefacts that demonstrate the basis for decisions (requirements, data lineage, testing results, approvals, thresholds, overrides).
- **Operational supervision:** mechanisms to detect, triage, and remediate errors or harms, supported by clear escalation paths and documented outcomes.

In short, so-called "autonomous" systems neither possess agency nor create a legal vacuum. They are automated tools operating within boundaries set by people. Effective governance ensures that those people—and the institutions within which they act—remain visibly and demonstrably accountable[10].

9.2 The Real Problem Is Governance, Not Responsibility

From this perspective, responsibility does not disappear. Rather, organisations may fail to design governance structures that clearly allocate and evidence responsibility.

When responsibility appears unclear, it is often because:

- systems were deployed without clearly identified ownership;
- oversight mechanisms were weak or ineffective;
- decision-making processes were poorly documented;
- multiple actors assumed that responsibility lay elsewhere.

In such circumstances, what appears to be a responsibility gap is more accurately understood as a governance failure. AI therefore does not create a new category of responsibility; it exposes weaknesses in existing governance arrangements.

10. Conclusion

Artificial intelligence is often framed as a technological revolution that requires entirely new legal frameworks. This paper takes a different view. The deployment of AI systems does not remove responsibility from institutions or their leaders. Existing legal doctrines remain capable of assigning responsibility when harm arises from complex chains of action involving multiple actors.

9: Joanna J Bryson, 'Robots Should Be Slaves' in Yorick Wilks (ed), Close Engagements with Artificial Companions (John Benjamins 2010).
10: Rois Ní Thuama, "Fear is a business model. It captures your attention and opens your wallet" PC Pro (2024), Issue 376, 116–117.

The real governance challenge therefore lies not in regulating artificial intelligence as a technology, but in ensuring that institutions deploying AI systems retain clear structures of accountability. Organisations must be able to demonstrate who authorised the use of AI tools, what risks were considered before deployment, how outputs were interpreted, and who remained responsible for the resulting decisions.

Artificial intelligence may influence decisions, but it does not change who remains responsible for them.

11. References

[1]UK Government, National AI Strategy (Department for Digital, Culture, Media and Sport 2021).

[2]European Commission, Regulation (EU) 2024/1689Artificial Intelligence Act (2024).

[3]OECD (2019), Artificial Intelligence in Society, OECD Publishing, Paris, https://doi.org/10.1787/eedfee77-en.

[4]RT Consulting Limited Whitepaper; Credit Ratings, Governance Duties, & the New Systemic Risk Perimeter; 2025.

[5]Rois Ní Thuama, Rediscovering Shareholder Activism: A Critique of Public Company Conduct in Relation to Facilitating Shareholder Diligence (PhD thesis, Bangor University Law School 2015).

[6]Bartz v. Anthropic PBC, No. 3:24-cv-05417-WHA https://www.anthropiccopyrightsettlement.com/

[7]Payout for Estée Lauder women 'sacked by algorithm' https://www.thetimes.com/business/technology/article/payout-for-estee-lauder-women-sacked-by-algorithm-wnq0ffzt3

[8]Andreas Matthias, 'The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata' (2004) 6 Ethics and Information Technology 175.

[9]Joanna J Bryson, 'Robots Should Be Slaves' in Yorick Wilks (ed), Close Engagements with Artificial Companions (John Benjamins 2010).

[10]Rois Ní Thuama, "Fear is a business model. It captures your attention and opens your wallet" PC Pro (2024), Issue 376, 116–117.

RT CONSULTING
By Experts, For Executives

About Us:

RT Consulting Ltd (Company Number 10539548) helps boards make faster, better, and more legally defensible decisions.

RT CONSULTING
By Experts, For Executives

We created RAPID-T™, a governance framework that aligns leadership behaviour with NIS2, DORA, and directors' duties.

Contact: info@rtconsulting.ltd | www.rtconsulting.co.uk | www.rapid-t.com.

Registered Office: 82a James Carter Road, Mildenhall, Suffolk, IP28 7DE.