

Enterprise Risk

Summer 2024 / www.enterpriseriskmag.com

The official magazine of the Institute of Risk Management

Securing biodiversity: Moves to halt the extinction of species and protect biodiversity are gathering momentum, and businesses are under pressure to take a lead



Smarter governance: integrating behavioural economics into governance / **IRM's Africa strategy:** historic conference in East Africa / **DNA of a controls lifecycle:** handling the UK's revised corporate governance code / **Regulatory overdrive:** digital regulations come of age across Europe and beyond / **Sick of work:** health and safety makes a surprising return as a top risk

Do you manage risk in your organisation?



Scan me!

Get risk ready with the IRM

There has never been a better time to increase your earning potential and career prospects by gaining an internationally recognised risk management qualification.

a.r.u. | Anglia Ruskin University

• EDINBURGH •
THE CITY OF EDINBURGH COUNCIL

Gateshead
Council

NHS

Norfolk
County Council

The Open
University

www.theirm.org | Tel: +44 (0)20 7709 9808 | Email: enquiries@theirm.org

irm

Editor
Arthur Piper

Produced by
Smith de Wint
Cobden Place, 5 Cobden Chambers
Pelham Street, Nottingham, NG1 2ED
Tel: +44 (0)115 958 2024
risk@sdw.co.uk
www.sdw.co.uk

**Sponsorship and
Advertising Sales Manager**
Redactive Media
IRMsales@redactive.co.uk
Tel: +44(0)20 7324 2753

Enterprise Risk is the official publication of
the Institute of Risk Management (IRM).

ISSN 2397-8848

About the IRM

The IRM is the leading professional
body for Enterprise Risk Management
(ERM). We drive excellence in managing
risk to ensure organisations are ready for
the opportunities and threats of the future.

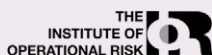
We do this by providing internationally
recognised qualifications and training,
publishing research and guidance, and
setting professional standards.

For over 30 years our qualifications have
been the global choice of qualification for
risk professionals and their employers.

We are a not-for-profit body,
with members working in all industries,
in all risk disciplines and in all sectors
around the world.

Institute of Risk Management
2nd Floor, Sackville House, 143-149
Fenchurch Street, London, EC3M 6BN
Tel: +44 (0)20 7709 9808
Fax: +44 (0)20 7709 0716
enquiries@theirm.org
www.theirm.org

Copyright © 2024 Institute of Risk
Management. All rights reserved.
Reproduction without written permission
is strictly forbidden. The views of outside
contributors are not necessarily the views
of IRM, its editor or its staff.



Rising regulation

There has been a huge increase in the number and scope of regulation in recent years. Much of this is coming from the European Union (EU) and, while the UK is no longer directly under its jurisdiction, those rules will apply to any organisations wishing to do business there.

Risk managers, compliance functions and internal auditors tend to be at the sharp end of making sure that these rules are properly understood and implemented. But the sheer volume of new and sometimes overlapping regulation (either recently enacted or in the pipeline) could make that task all-consuming.

Catching up

One reason for this sudden glut of paperwork is that law-makers in Europe have finally caught up with the implications of living in a digital economy (see *Regulatory overdrive*, pages 28-32). It takes time and experience to know what can go wrong and the kinds of controls that are needed to protect organisations and consumers from any downsides from technological systems.

And yet, there are areas such as AI where regulations are in place, but the details for key risk categories remain vague. That creates a dilemma for innovative businesses who want to create new products and services. Do they launch early and capture the market and risk being non-compliant – or do they wait?

Another reason is that global policymakers are demanding regulation in new areas. Nature and biodiversity is a key emerging risk where the political agenda is driving change (see *Securing biodiversity*).

Biodiversity

While there is little doubt that non-human species on the planet are diminishing in variety, precise data on the location of danger spots and rates of decline are still developing. The EU's Corporate Sustainability Reporting Directive – for which the first reports are being produced now for publication in 2025 – includes detailed disclosure requirements in those areas.

Many businesses have little experience of creating data on the impact of their activities on land, rivers and seas. Nor do they understand well the interdependencies between specific environments and the species that live there. And acquiring the talent to do so is expensive even when it is available. But they will need to report as well as they can and hope for the best.

Given the scale and complexity of that task, it is not surprising that one or two heads of risk have told me confidentially that they do not expect to meet the first filing deadline – with the potential reputation and capital funding impacts that may have.

It is highly likely that all organisations are going to be non-compliant with some rules and regulations over the coming two or three years. Let's hope they have processes in place to manage that if the worst happens.

Arthur Piper
Editor

**Increase your
earning
potential with
this OFQUAL
accredited
qualification**



International Certificate in Financial Services Risk Management

Stay on top of international regulatory developments such as Solvency II and Basel III risk requirements. Study with the IRM to ensure you remain compliant and gain an understanding of how risk management impacts strategy and performance.

www.theirm.org | Tel: +44 (0)20 7709 9808 | Email: enquiries@theirm.org

irm



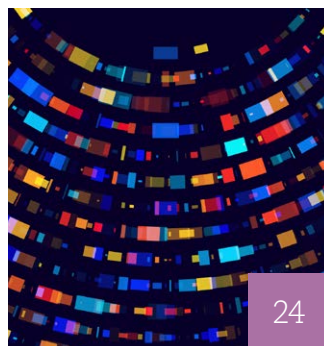
10



16



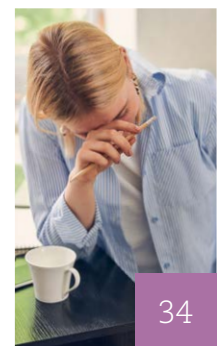
22



24



28



34

Features

10 Securing biodiversity
Moves to halt the extinction of species and protect biodiversity are gathering momentum, and businesses are under pressure to take a lead

16 Pathways to smarter governance
Principles from behavioural economics can be integrated into governance frameworks to address human biases, ethical challenges, and decision-making processes

22 IRM's strategy for the African continent
May 10th saw a historic in-person event with our East African, Nigerian, Zimbabwean and South African Groups for IRM's Strategy for the African continent combined with IRM's maiden board visit to Kenya

24 The DNA of a controls lifecycle
The UK's revised corporate governance code sets out stricter board responsibilities over the threats organisations face. Six critical steps create a controls lifecycle that underpins successful compliance

28 Regulatory overdrive
The EU has been creating a raft of digital regulations to help protect businesses and consumers against hackers. But that is likely to come with an unprecedented regulatory burden

34 Sick of work
With cyberattacks and AI often dominating headlines, social risks often rank poorly in surveys – which is why it was surprising to see health and safety making a strong showing in a recent poll

REGULARS

7 IRM Viewpoint
A change of office in London and new premises in Kenya should serve IRM's changing strategic and operational needs well

8 Trending
The stories and news affecting the wider business environment as interpreted by our infographics team

36 Directory
In need of insurance services, risk management software and solutions, or training? Look no further than our listings

38 Toffler
Human intelligence is inherently biased, which may prove essential when working with machines

**Supercharge
your career with
this OFQUAL
accreditation!**



Scan me!

International Certificate in Enterprise Risk Management

Risk is part of every business, from the pandemic-to cyber threats-to supply chain disruptions. Study with the IRM to improve your career and earning potential by gaining a solid foundation in the theory and practice of effective risk management.

www.theirm.org | Tel: +44 (0)20 7709 9808 | Email: enquiries@theirm.org

irm

Important office updates

A change of office in London and new premises in Kenya should serve IRM's changing strategic and operational needs well

We have some exciting news about important changes at the Institute of Risk

Management. Due to evolving business needs and a strategic shift towards a more flexible working environment, we will be relocating our London office to a new address on 1 July.

New office address:
Institute of Risk Management
2nd Floor, 80 Leadenhall Street
London EC3A 3DH

You can view our new location on [Google Maps](#).

Strategic goals

The decision to move was driven by several key factors that align with our long-term strategic goals:

Reduced office space requirements: As we transition to a more agile working model, the need for a large office space has diminished. Our new office will be better suited to our current and future needs.

Enhanced flexibility: The new office will support our initiatives for nimble staff working, allowing our team members to work more efficiently and collaboratively, whether in the office or remotely.

Cost savings: By moving to a more appropriately sized office, we can achieve significant



completed by early July, and we will strive to ensure that there is minimal disruption to our operations during this period.

At the same time, we are pleased to also announce the location of the first IRM Africa office, which will be legally registered in Kenya. The office address will be effective 1 July 2024:

IRM Africa: KOFISI
95, Keystone Park, Riverside Drive
3rd Floor, Block A
P.O. BOX 856 – 00606



The decision to move was driven by several key factors that align with our long-term strategic goals


savings, which can be reinvested into enhancing our services and support for our members and the risk community that we represent.

High quality

We are confident that this move will allow us to continue delivering high-quality service while adapting to the changing dynamics of our work environment. The transition to our new office will be

Nairobi, Kenya

You can view the location on [Google Maps](#). Please contact [Dorothy Maseke](#) with any enquiries.

Thank you for your continued support and understanding as we make these important transitions. 

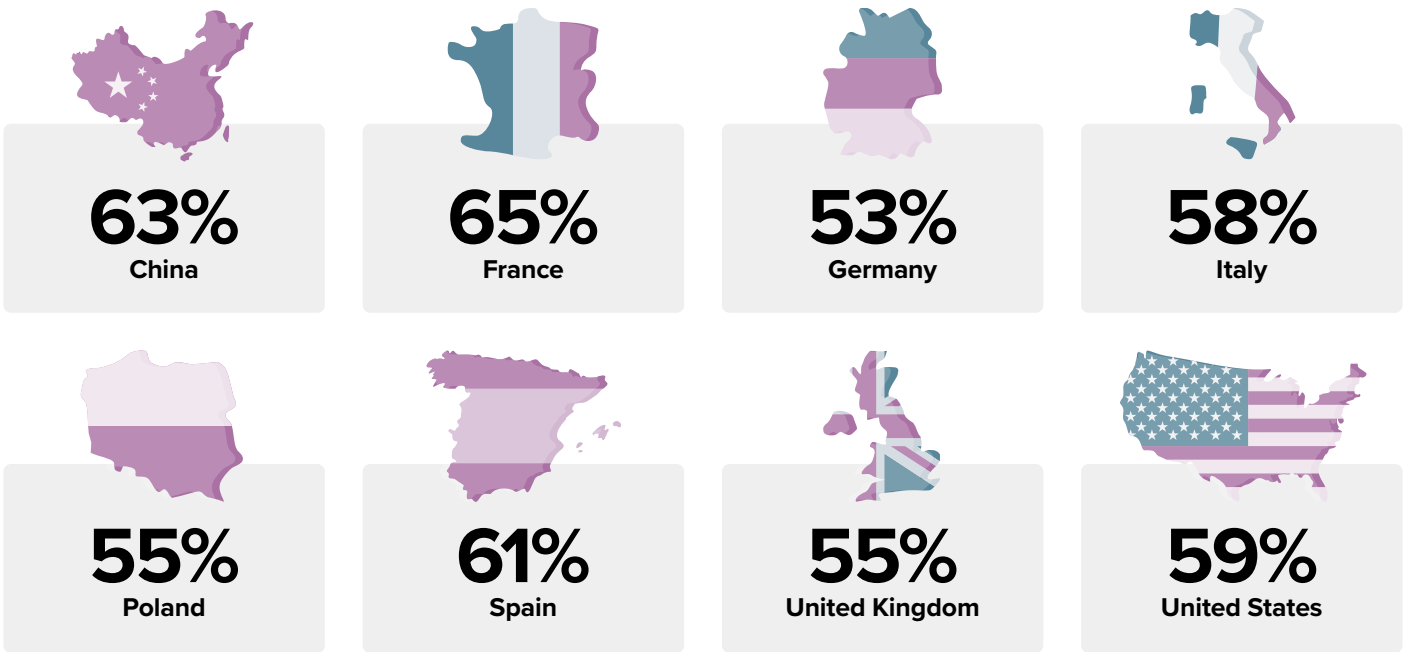
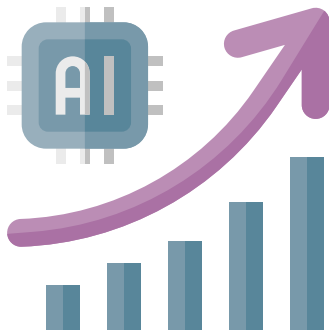


Ian Livsey is IRM's chief executive officer.

The latest stories and news affecting the wider business environment as interpreted by our infographics team

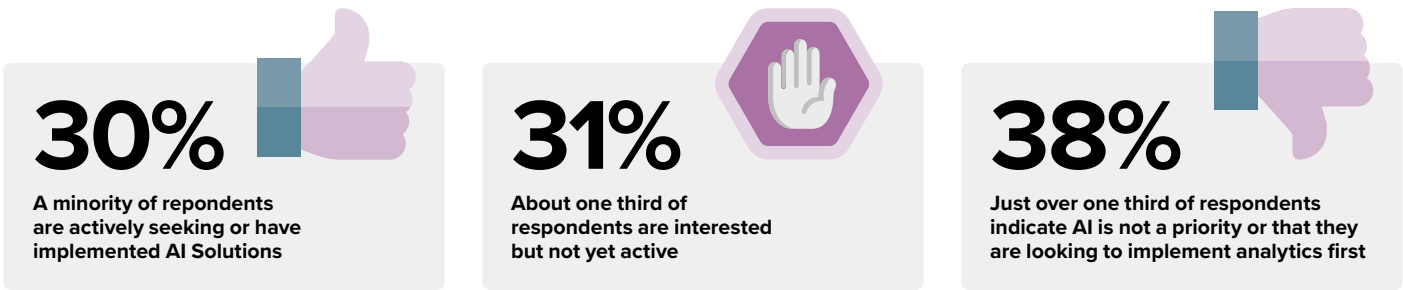
Suppliers say AI will “significantly increase” productivity gains

AI should also improve the functioning of global value chains, reduce costs and increase export opportunities



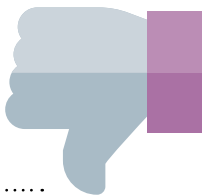
Source: Allianz Trade Global Survey 2024

But the reality is that most businesses are not fully engaged with AI

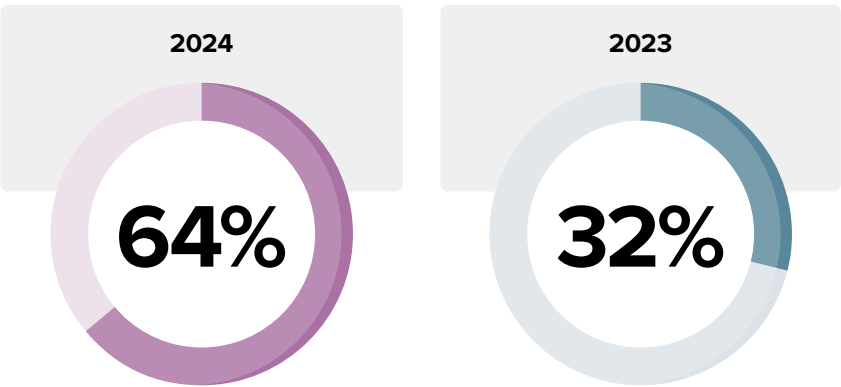


Source: The 2024 state of risk report, Origami

Employees give thumbs down to employer experience claims

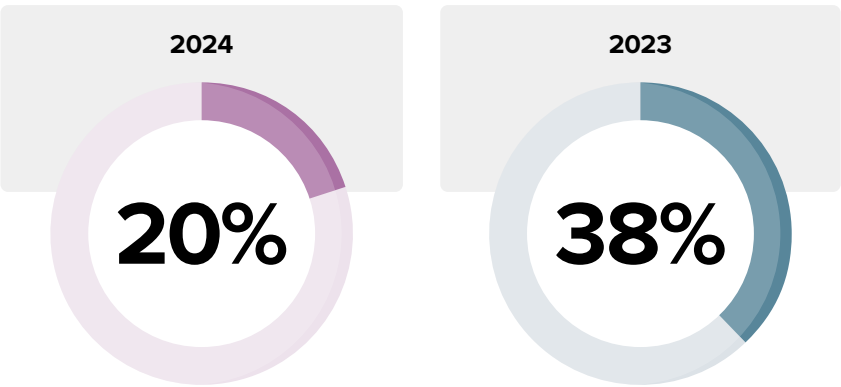


HR and reward professionals saying they deliver excellent employee experience

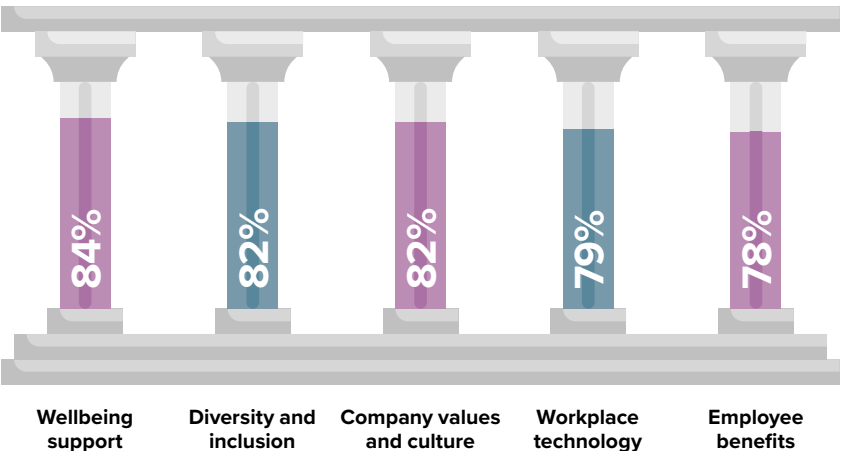


But are increasingly out of touch with workforce

Employees rating employee experience as excellent:

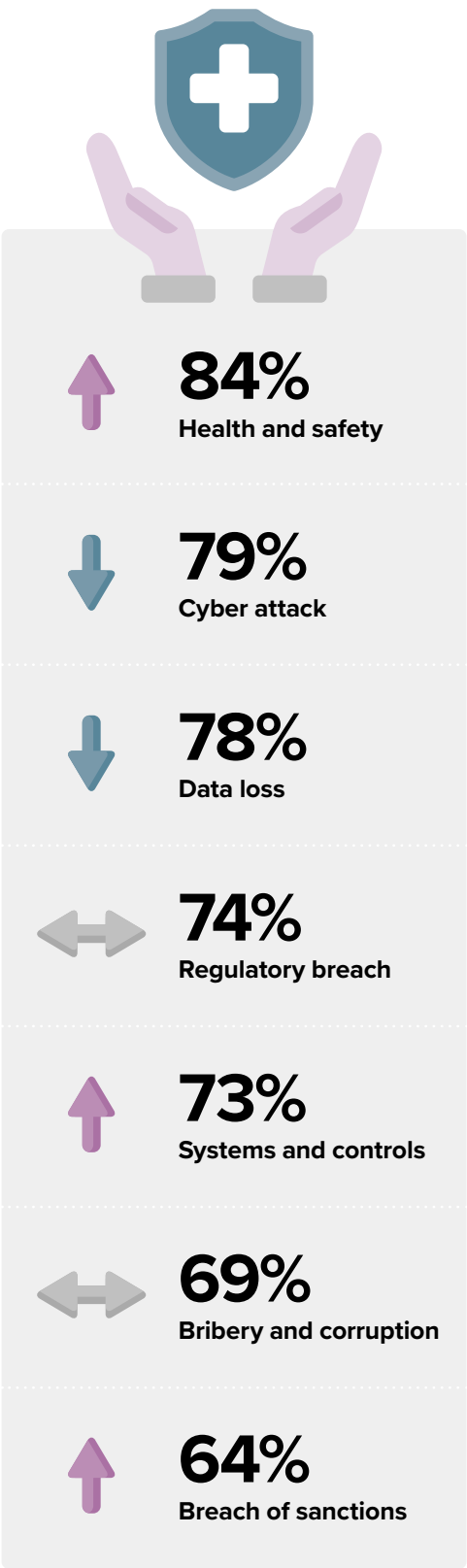


The most important pillars of a great employee experience:



Source: The expectation exponential, Benefex

Health and safety top concern for directors in 2024



Source: Global directors' and officers' survey report 2024, Clyde and Co, WTW

Securing biodiversity

BY ARTHUR PIPER



Moves to halt the extinction of species and protect biodiversity are gathering momentum, and businesses are under pressure to take a lead

The biodiversity of the planet is under attack. While calculations differ, species are going out of existence rapidly. For example, WWF and ZSL have estimated that between 1970 and 2018, there was a **69 per cent decline** in wildlife populations. As more geographical areas are cleared for human industry and habitation, the rate of decline could continue.

But the statistics are only a first stab at assessing the scale of the problem. The numbers are difficult to assess because the

The truth is that climate change and biodiversity loss are linked in complex ways. The exploitation of land and water can create drought, pollution, and temperature change at the same time as killing species. In fact, WWF identified changes in the way land is used as the biggest driver of biodiversity loss. Not only can utilising land displace species from their traditional habitats, but simply creating more fragmented landscapes often destroys fragile ecosystems. This means that to arrest or reverse declining trends in biodiversity, governments and

the latter to be met by 2030 by the countries that ratified the framework. The goals do not just focus on reducing the extinction rate and rates of loss but also aim to educate people about why nature should be valued and to share the monetary benefits of genetic research (see *2050 vision for biodiversity*). There are 23 separate targets, the most important being to bring at least 30 per cent of the world's lands, inland waters, coastal areas, and oceans under effective conservation and management. Other measures include reducing global food

Not only can utilising land displace species from their traditional habitats, but simply creating more fragmented landscapes often destroys fragile ecosystems

survey ([based on the Living Planet Index](#)) covers only a relatively small percentage of the world's species – 11 per cent of mammals, 6 per cent of fish and 3 per cent of amphibians and reptile species, with nothing on insects, fungi, coral, or plants, according to the [Our World in Data project](#).

Yet, even on this limited evidence, the picture looks grim. WWF's biannual *Living planet report*, last published in 2022, put it like this: "While we need to urgently act to restore the health of the natural world, there is no sign that the loss of nature is being halted, let alone reversed. The declining trend in vertebrate populations continues, despite an array of political and private sector commitments."

organisations need to think and act differently about co-habiting with other species on the planet.

Taking action

In December 2022, delegates from 196 countries agreed to adopt the Kunming-Montreal Global Biodiversity Framework (GBF) at the biannual COP15 (COP Biodiversity) in Montreal, Canada – a United Nations-backed project to address biodiversity issues. ([Its better-known sister event](#) COP Climate is an annual meeting, with COP28 expected to take place in Baku, Azerbaijan, in November this year.)

[The agreement at COP 15](#) was highly significant, as it put in place concrete goals and specific targets around biodiversity –

waste, cutting subsidies that could harm biodiversity, and requiring transnational companies to monitor, assess, and disclose the impact of their operations, supply chains, and portfolios on biodiversity. And, of course, the agreement is toothless without action from the signatories.

Policy action

Governments in the UK and Europe have made moves to achieve such goals. Back in 2021, the UK government committed to becoming "[nature positive](#)" by 2030. That entails reversing current declines in biodiversity to help species and ecosystems begin to recover. In November 2022, the UK's statutory nature conservation bodies issued a joint statement

supporting the goals and targets set out in COP15 – but the so-called biodiversity indicators that are meant to measure progress are devolved. That means each of the UK's four countries are setting their own targets, and there have been delays and arguments along the way.

Europe's 2030 Biodiversity Strategy also predates COP15 by a couple of years and is part of its 2019 Green Deal package. There are already a range of initiatives – on birds and habitats, for example – that exist in the European Union. In addition, new legislation, such as the Nature Restoration Law – passed by the European Parliament in March this year – aims to restore 20 per cent of the EU's land and sea by 2030. But the aim of both the UK's and Europe's over-arching goals that are now enshrined in COP15 is to force action on the ground. That will entail developing more specific rules on, say, fishing conservation, while driving individual countries to align their biodiversity policies with the global framework and ensuring that organisations within those regions comply.

That could prove tougher than planned. As this edition of *Enterprise Risk* goes to press, Europe-wide elections will be getting underway. Green policies such as the Green Deal are under attack – often around cuts to carbon emissions. However, in countries such as Croatia, where the government is aiming to restrict fishing quotas, and Finland, where forests are a key part of the economy, popular resistance to nature restoration is growing. There is a growing feeling that while governments like to talk tough on nature, some policy weakening is putting ambitious goals out of reach.

Business pressure

Europe is ahead of the UK in nature-related reporting requirements. The EU's Corporate Sustainability Reporting Directive (the first reports under which are due next year) includes

2050 VISION FOR BIODIVERSITY

GOAL A

- The integrity, connectivity, and resilience of all ecosystems are maintained, enhanced, or restored, substantially increasing the area of natural ecosystems by 2050
- Human-induced extinction of known threatened species is halted, and, by 2050, extinction rate and risk of all species are reduced tenfold, and the abundance of native wild species is increased to healthy and resilient levels
- The genetic diversity within populations of wild and domesticated species is maintained, safeguarding their adaptive potential.

GOAL B

- Biodiversity is sustainably used and managed and nature's contributions to people, including ecosystem functions and services, are valued, maintained, and enhanced, with those currently in decline being restored, supporting the achievement of sustainable development, for the benefit of present and future generations by 2050.

GOAL C

- The monetary and non-monetary benefits from the utilisation of genetic resources, and digital sequence information on genetic resources, and of traditional knowledge associated with genetic resources, as applicable, are shared fairly and equitably, as appropriate with indigenous peoples and local communities, and substantially increased by 2050, while ensuring traditional knowledge associated with genetic resources is appropriately protected, thereby contributing to the conservation and sustainable use of biodiversity, in accordance with internationally agreed access and benefit-sharing instruments.

GOAL D

- Adequate means of implementation, including financial resources, capacity-building, technical, and scientific cooperation, and access to and transfer of technology to fully implement the Kunming-Montreal global biodiversity framework are secured and equitably accessible to all Parties, especially developing countries, in particular the least developed countries and small island developing States, as well as countries with economies in transition, progressively closing the biodiversity finance gap of \$700 billion per year, and aligning financial flows with the Kunming-Montreal Global Biodiversity Framework and the 2050 Vision for Biodiversity.

Source: *Convention on biological diversity*



The agreement at COP 15 was highly significant as it put in place concrete goals and specific targets around biodiversity



“ **There is a growing feeling that while governments like to talk tough on nature, some policy weakening is putting ambitious goals out of reach**

detailed disclosure requirements on biodiversity and ecosystems. More specifically, it includes disclosure requirements on impacts and interdependencies in terrestrial and aquatic ecosystems (freshwater and marine), species (fauna and flora), and diversity between and within ecosystems and species. Companies must also report on the risks and opportunities as well as associated strategies, measures, and financial implications.

In addition, in September 2023, the taskforce on nature-related financial disclosures (TNFD) published its first recommendations with direct

inspiration from COP15. The initiative built on work from such organisations as the International Sustainability and Standards Board and GRI to create sustainability disclosures in four key areas – governance, strategy, risk management and metrics (see *TNFD’s recommended disclosures*).

The recommendations are not binding, and as yet, no UK regulatory authorities are requiring businesses to report using these guidelines. So, why bother? After all, regulatory compliance – especially in the EU – is at an all-time high in a number of other areas.

Early adopters of the

recommendations that took part in a trial organised by TNFD could provide an answer. With incoming regulations on deforestation due in the EU, the British retailer Tesco decided to see whether the guidance would be useful in mapping its palm oil supply chain and in identifying sensitive areas. As well as being keen not to contribute to forest loss, the retailer also wanted to support local small-holder producers who could fall foul of the EU’s certification regime. Using TNFD’s so-called leap approach, the business was able to better assess its biodiversity footprint across 120 regions in Indonesia and map that onto its supply chain dependencies.

“Tesco intends to use the insights from this work to help gather the origin information we need to be able to make targeted interventions on the ground,” the retailer said. “The work will also help Tesco more



TNFD'S RECOMMENDED DISCLOSURES

GOVERNANCE

Disclose the organisation's governance of nature-related dependencies, impacts, risks, and opportunities.

Recommended disclosures

- A** Describe the board's oversight of nature-related dependencies, impacts, risks and opportunities.
- B** Describe management's role in assessing and managing nature-related dependencies, impacts, risks and opportunities.
- C** Describe the organisation's human rights policies and engagement activities, and oversight by the board and management, with respect to Indigenous Peoples, Local Communities, affected and other stakeholders, in the organisation's assessment of, and response to, nature-related dependencies, impacts, risks and opportunities.

STRATEGY

Disclose the effects of nature-related dependencies, impacts, risks and opportunities on the organisation's business model, strategy and financial planning where such information is material.

Recommended disclosures

- A** Describe the nature-related dependencies, impacts, risks and opportunities the organisation has identified over the short, medium and long term.
- B** Describe the effect nature-related dependencies, impacts, risks and opportunities have had on the organisation's business model, value chain, strategy and financial planning, as well as any transition plans or analysis in place.
- C** Describe the resilience of the organisation's strategy to nature-related risks and opportunities, taking into consideration different scenarios.
- D** Disclose the locations of assets and/or activities in the organisation's direct operations and, where possible, upstream and downstream value chain(s) that meet the criteria for priority locations.

RISK & IMPACT MANAGEMENT

Describe the processes used by the organisation to identify, assess, prioritise and monitor nature-related dependencies, impacts, risks and opportunities.

Recommended disclosures

- A** (i) Describe the organisation's processes for identifying, assessing and prioritising nature-related dependencies, impacts, risks and opportunities in its direct operations.
(ii) Describe the organisation's processes for identifying, assessing and prioritising nature-related dependencies, impacts, risks and opportunities in its upstream and downstream value chain(s).
- B** Describe the organisation's processes for managing nature-related dependencies, impacts, risks and opportunities.
- C** Describe how processes for identifying, assessing, prioritising and monitoring nature-related risks are integrated into and inform the organisation's overall risk management processes.

METRICS & TARGETS

Disclose the metrics and targets used to assess and manage material nature-related dependencies, impacts, risks and opportunities.

Recommended disclosures

- A** Disclose the metrics used by the organisation to assess and manage material nature-related risks and opportunities in line with its strategy and risk management process.
- B** Disclose the metrics used by the organisation to assess and manage dependencies and impacts on nature.
- C** Describe the targets and goals used by the organisation to manage nature-related dependencies, impacts, risks and opportunities and its performance against these.

Source: [TNFD](#)



Regulations have come so quickly that the data systems and the controls around them are either non-existent or still at a low level of maturity in most sectors

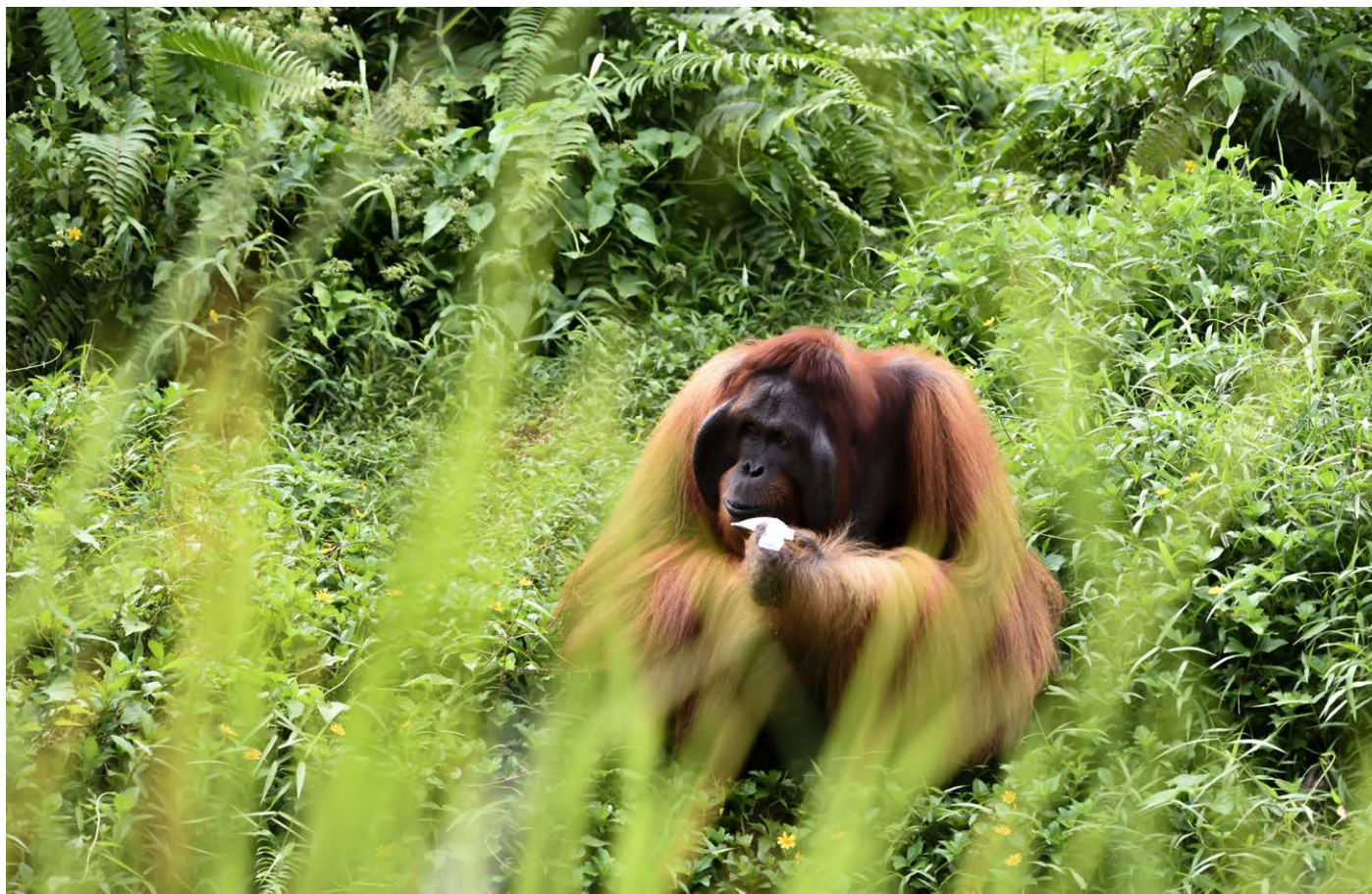


Image credit: Simone Milwatz / Unsplash.com

accurately assess nature-related risk in its palm oil supply chain, both for its DCF commitment and for future disclosure.”

This type of exercise is what is known as a double-materiality assessment. The organisation looks at both the risks it faces externally and also how its actions impact the local environment where its activity takes place. While more time-consuming and costly, this approach is likely to provide a much richer and nuanced view into the risk landscape and how risks interact at both a global and local scale. Organisations should expect more focus in these areas, as the [International Sustainability Standards Board](#) announced in April 2024 that it would start

a project on risk disclosures around biodiversity, ecosystems, and ecosystem services.

Investor landscape

Investors are also waking up to the impacts of reduced biodiversity on long-term financial health. [The Institute and Faculty of Actuaries](#), for example, published a policy briefing in July 2023, setting out its active support for greater action and disclosure. The [EU published in 2023](#) a risk management framework for financial institutions specifically dealing with nature and biodiversity. Banks are also re-examining their balance sheets in light of their commitments to carbon neutrality across portfolios. It is easy to imagine

the need to hit biodiversity targets also becoming a potential hurdle for accessing capital sometime in the next decade.

Risk managers are going to have their work cut out, adding a further layer of complexity around non-financial reporting in this area. Regulations have come so quickly that the data systems and the controls around them are either non-existent or still at a low level of maturity in most sectors. A skills shortage will also add to the difficulty of getting up to speed in this area. But the rewards of good compliance are potentially high for the environment – and with social attitudes to green-friendly businesses on the rise, the financial benefits may be worthwhile too. 🌱

Pathways to smarter governance

BY AMENA ALBASHER

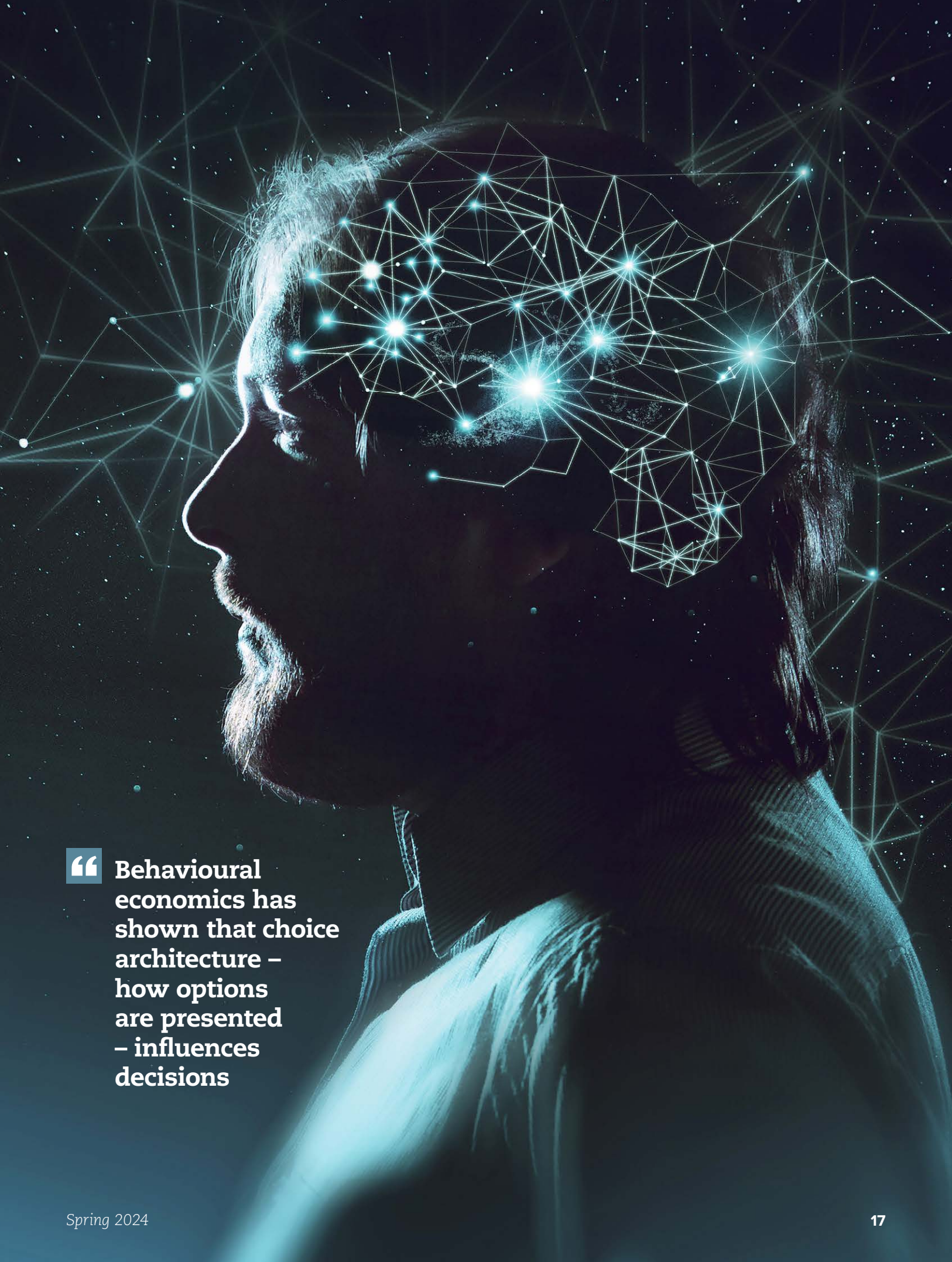
Principles from behavioural economics can be integrated into governance frameworks to address human biases, ethical challenges, and decision-making processes

Behavioural economics is revamping the way we approach economic decision-making. It is a combination of knowledge from psychology, neuroscience, and economics that explains the fact that people often make irrational decisions that are in contrast with traditional economics models. By including cognitive biases, heuristics, and the strong impact of social, emotional, and circumstantial factors, behavioural economics has a more pragmatic approach to forecasting human economic behaviour.

At its core are principles such as loss aversion, which refers to people's tendency to strongly prefer avoiding losses to acquiring gains. Policymakers can use loss-framing rather than gain-framing, for example, to nudge more prudent and farsighted decisions on matters such as mitigation against climate change. Another main idea is the status quo bias – the tendency of people to maintain current circumstances rather than change them, even though better alternatives exist. Debiasing techniques can be devised to make potential advantages

of change more prominent, thus overcoming this bias.

Behavioural economics has shown that choice architecture – how options are presented – influences decisions. Easily implemented approaches, such as making attractive choices the main default or highlighting the benefits in a visual manner, have changed the behaviour of savings at retirement, energy consumption, and so much more. Researchers have even created ways to make use of psychological biases, such as overconfidence, to boost investments and risk-taking behaviour in particular situations.



“ Behavioural economics has shown that choice architecture – how options are presented – influences decisions

These perceptions are not all theoretical – they are increasingly being used by governments and businesses to design their manipulations of economic behaviour without using too many rigorous laws. Behavioural public policy has led to higher tax compliance, energy savings, increased retirement savings, and other instances of socially good behaviours. Admittedly, the journey seems difficult, as it involves issues with ethics, privacy safeguards, and proper implementation. However, there is a need to develop and implement measures to guard against these risks to ensure that the principles of behavioural economics are implemented effectively.

Governance frameworks

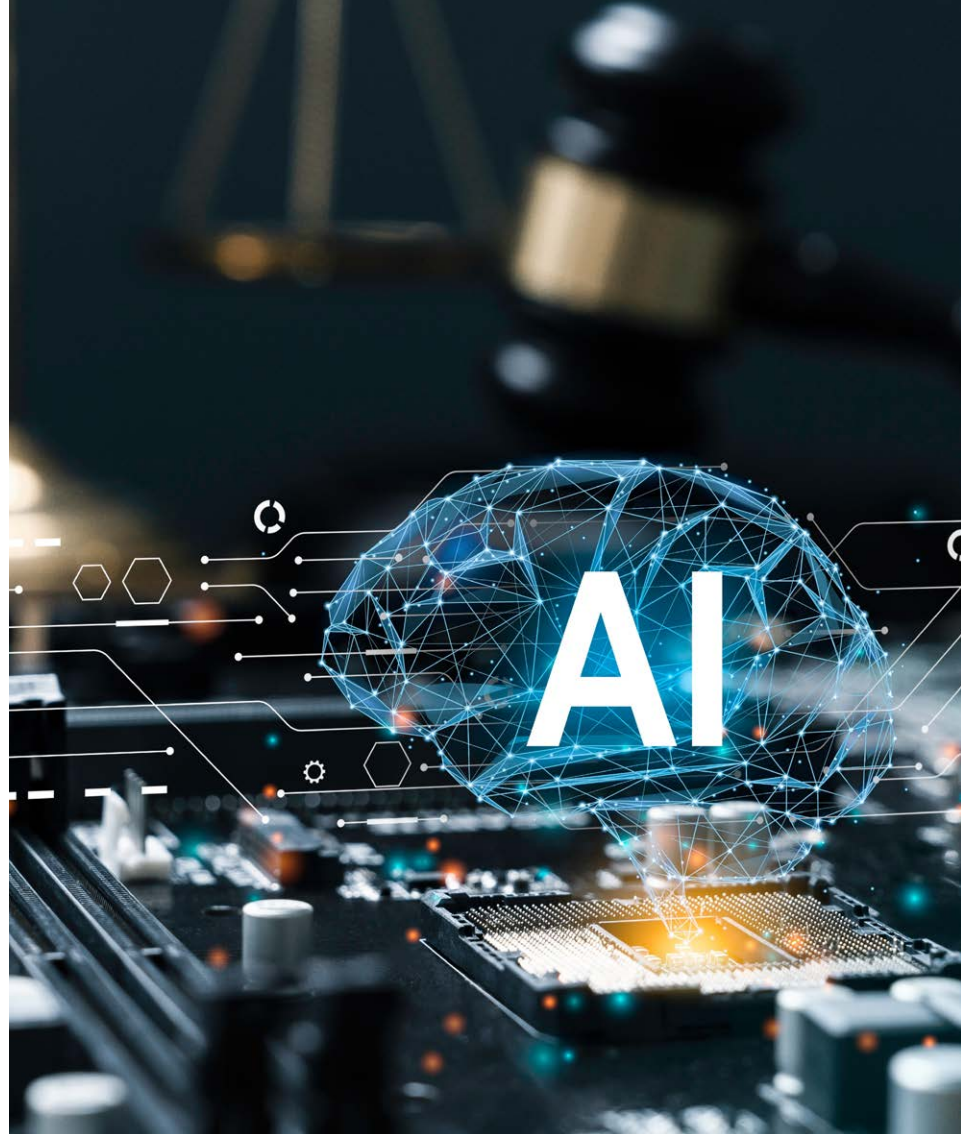
The behavioural economic theories of management play a critical role in making decisions, ethics, and taking out human bias in the organisational setup. Furthermore, behavioural economics can help fix the functioning of governance institutions by considering that a well-meaning and democratic system can also be influenced by cognitive limitations and human biases. This integration allows for variances in human decision-making to be addressed, debiasing methods to be implemented, multiple views supported, and critical thinking to be enhanced. Lastly, behavioural economics theories, such as the nudge theory, can lead to a choice that is both effective and ethical and can also be autonomous.

The Volkswagen emissions scandal demonstrates the importance of adhering to governance systems and human biases, for the consequences can be dire. Researchers have found that emission standards

evasion was supported by and encouraged a poisonous cocktail of groupthink, overconfidence bias, and short-term gain-obsessed complacency, even with very strict compliance measures. Group think dynamics made the minority go unheard, and this hubris affected the actual risk calculation. What this controversy can demonstrate is that the search for and elimination of such biases should be done actively with the use of behavioural science insights. Applying the principles of biased techniques, such as groupthink, contrarian points of questioning, and the restructuring of the objectives

from short-term profitability to long-term sustainability (while incorporating loss aversion and temporal discounting principles), will help create ethical decisions. The Volkswagen case shows how significant human bias can be in governance practice.

Moreover, the principles of behavioural economics are instrumental in designing appropriate policies for AI-driven economies. Considering such cognitive biases as present bias and loss aversion, governance frameworks can employ nudges to make AI development incentives in line with long-term social objectives beyond a narrow profit



“ The principles of behavioural economics are instrumental in designing appropriate policies for AI-driven economies



techniques have turned out to be very useful resources for opposing the power of cognitive biases and thus creating more objective and fair policies. For instance, within central banks, institutions such as the Federal Reserve have been implementing structured decision-making procedures that emanate from comprehensive data analysis, rigorous debates, and established communication protocols. These measures are designed to counterbalance judgmental decision-making by encouraging an ultimately more cooperative and evidence-based approach to monetary policymaking.

Moreover, another debiasing tactic could be linked to public policy and budget. This problem of resource allocation happens

by the application of techniques like ensemble forecasting and scenario planning. This art of diminishing prejudices is done by considering several viewpoints and finding alternative solutions. Debiasing programmes are no miracle cures but are continuing mechanisms that require constant checks and comparisons to ethical and objective principles in order to prevent mistakes and adjust them for economic stewardship.

Nudging ethics and sustainability

The nudge strategy has been introduced as one of the new techniques of gentle influence with the aim of promoting green and ethical economic models at individual and organisational

“ Transparency, increased frequency of the assessment, and strict compliance with ethical rules create the ethical foundation of nudging

motive. For instance, mandating AI systems to switch to privacy-preserving settings creates pressure towards data ethics rather than short-term data monetisation, resulting in loss aversion. Both standardised and behavioural frameworks are also effective in neutralising the status quo bias and other distortions brought about by framing effects. Applying behavioural economics to AI governance through choice architecture may lead to a better weighing of societal considerations.

Debiasing techniques

The recognition of human biases in the field of economics, as well as decision-making and governance, is one of the biggest challenges of economics because bias can result in suboptimal outcomes and can erode the fairness and effectiveness of policies. Debiasing

mostly among governmental and public organisations when they are supposed to decide where to allot their resources. Through cost-benefit analysis and impact assessment, sunk cost fallacy or status quo bias is prevented. The strategies focus on thoroughly investigating diverse policy alternatives and their implications, with the goal of improving the depth of understanding and objectivity of the policymaking process. Through this approach, these policy makers can develop and implement holistic policies that cater to the very needs of those affected.

What is more, such tools have been used in economic predictions and modelling, too. Economists and analysts can be too optimistic or decide everything by making mistakes. The blunders associated with forecasting are being corrected

levels. Contrary to hard command and control approaches, soft nudges formulate interventions based on findings in behavioural economies that use psychological triggers to indirectly move people without infringing on their freedom of choice. These rules, governance, and allocation of resources can be effectively controlled by policymaking bodies and governments to direct individuals to make more appropriate decisions. Adopting sustainable options as the norm, or distributing important information clearly, may also induce partakers to carry out their environmental responsibilities voluntarily, not as a result of force.

Additionally, nudges may be used as a tool to drive informed and smart decisions with regard to public finance. Strategies, such as automatic enrolment in retirement saving plans or tax-



“ In organisational governance, loss aversion can be applied to encourage more responsible and ethical decisions

advantage investment accounts, are examples of approaches that can lead people to contribute towards their long-term economic and sustainability goals. By following set templates, and with the use of consciously designed options, nudges help us to overcome present bias and short-termism and the other cognitive limiters of financial planning and effective policymaking at both the personal and government levels.

Balancing individual freedom of choice with achieving certain objectives requires fine-tuning the nudging approach for economic government. Transparency, increased frequency of assessment, and strict compliance with ethical rules create the ethical foundation of nudging, which is at the same time fair and efficient.

Nudging techniques and their overexploitation may be the basic reason why people in economic governance and policymaking processes behave ethically, sustainably, and responsibly. Lastly, nudging techniques can play a critical role in ensuring that individual behaviour aligns with societal expectations.

Enhancing decision-making

The loss aversion concept, which considers loss to be more painful than gains of the same value, can be the most effective tool in governance and organisation when applied properly. By formulating decisions in terms of loss rather than gain, policymakers and organisational leaders will undoubtedly encourage more cautious and prudent decision-making. By consciously choosing

to use this principle, organisations can be better positioned to contribute to more responsible and sustainable governance, as well as forward-thinking systems.

The application of loss aversion in public policy and the regulatory environment is a tool that can be used to promote right and sustainable decisions. For example, policymakers could show the impacts of no action, such as economic disruptions, environmental degradation, and health issues, as consequences of the lack of mitigation measures against climate change. Highlighting possible losses may promote thinking about preventive measures and long-term strategies rather than short-term economic gain or inertia.

In organisational governance, loss aversion can be applied to

encourage more responsible and ethical decisions. Likewise, companies can articulate the risks entailed in unethical and unsustainable practices, such as reputational damage, legal liabilities, and consumer trust loss, as major losses to be evaded. Another way can be through highlighting the possible losses that may result in pushing top-level executives and stakeholders to make better choices that are more ethical and responsible, leading towards long-term sustainability.

Additionally, loss aversion can be extended to financial decisions in organisations and institutions. Instead of only focusing on the potential gains involved in investments or financial approaches, decision-makers can be given some information on the possible losses a risky or unwise financial decision could cause. Typically, the framing of the issue can make the administration become more conservative in their decision-making, pushing for long-term financial stability and responsible resource allocation.

Overcoming practical challenges

Although it is full of promise, the application of behavioural economics in the frameworks of governance also has its problems. One challenge comes from the innate complexity of human behaviour and the challenge of predicting how individuals will react to various interventions. Organisations should consider these principles with humility and constantly assess the effectiveness of applying thorough experimentation and data processing.

Similarly, another challenge is surmounting resistance to change and doubts about the effectiveness of the unusual methods. There is often resistance from those who see behavioural insights as strange and not proven because traditional governance frameworks usually rely on existing norms and standards. According to

MIT Sloan Management Review, those organisations that attach importance to the process of continuous learning and adaptation to new information do better regarding the implementation of behavioural economic principles.

To deal with these problems, organisations have to give top priority to continuous education and open communication. They can do this by explaining the principles well and showing the possible advantages that will

and prevent misapplication and possible infringement of personal rights through behaviour control methods. Through the combination of rigorous science and an innovation-based attitude, firms can gain the advantages of behavioural economics and thus be prepared to prevent complications from unexpected consequences.

The use of behavioural economics in the creation of governance frameworks has great



The crux of behavioural insights implementation is developing a culture within the organisation that adopts experimentation and iterative learning

lead to the creation of trust and acceptance from stakeholders. Similarly, the ability to adapt and learn from mistakes is also essential. Small-scale pilots and learning prototypes are important tools to help organisations develop and prove the worth of their behavioural insights before scaling them across the organisation – as shown by successful programmes at companies like Google and Microsoft.

The crux of behavioural insights implementation is developing a culture within the organisation that adopts experimentation and iterative learning. Instead of looking to copy behaviours from other organisations as an ideal, they should maintain an agile test-and-learn mindset. This results in speedy testing of interventions and their monitoring and continuous refinement on the basis of real-world data and feedback loops. Bring together multidisciplinary groups that will combine behavioural science expertise with operational knowledge for this to be done with empirical rigour. Ethical review boards and safety safeguards should also be adopted to evaluate

promise for realising a responsible, ethical, and sustainable future. Through a deeper insight into cognitive biases and human psychological idiosyncrasies, we can design governance systems more in sync with humane principles. The upcoming years are sure to witness an increase in behaviourally based policies and interventions that span across various domains of economic governance. Nevertheless, this job entails a delicate balancing act of giving and taking while respecting data privacy rights. Eventually, behavioural economic tools will enable governance systems to operate harmoniously with how people behave, fostering a fair, transparent practice in which society and long-term growth will be the main objectives. 🌐



Amena AlBasher is an experienced GRC risk management expert, holding a master's degree in health administration from Cornell University. She has spearheaded numerous GRC programmes across diverse industries as a lead and advisory member.

IRM's strategy for the African continent

BY DOROTHY MASEKE

May 10th saw a historic in-person event with our East African, Nigerian, Zimbabwean and South African Groups for IRM's Strategy for the African continent combined with IRM's maiden board visit to Kenya

The event's opening breakfast meeting offered a unique opportunity for around 150 senior-level professionals specialising in risk, quality assurance, compliance, audit, and accounting to convene. It served as a platform for networking and collaboration among professionals from banking, insurance, SACCOs, the public sector, pharmaceuticals, healthcare, NGOs, and regulatory bodies across East Africa and beyond. Guests heard from keynote speaker Geoffrey Odundo, executive advisor, CPF Financial Services Group and other leading risk management experts who represented the institute.

His presentation focused on Africa's growth and opportunity areas, including prospects for accelerated economic growth, building an economic case for East Africa. East Africa's

growth is fuelled by the service industry, tourism, and now hard commodities like minerals.

New world of risk

East Africa is the fastest-growing region in Africa, and this introduces a new world of risks from globalisation and climate impact to heightened inflation and geopolitical risks. The agenda addressed critical topics, such as emerging risks, integrated risk management, and the transformative role of technology. Participants gained valuable insights into IRM's internationalisation plan, focusing on its Africa strategy and its implications for members across the continent.

Aligned with IRM's overarching goals of expanding global reach and influencing risk management practices, this endeavour is the start of driving the development of the risk



management profession, elevating risk awareness, and championing best practices throughout Africa.

Key stakeholders

The board also met with key stakeholders in Kenya, as it seeks to build strategic alliances and partnerships with professional and academic institutions. There were also high-level discussions with policy makers in a bid to enhance risk management within the public sector – a key area of focus

“ In Africa, businesses face diverse and often volatile operating environments, making effective risk management essential for survival and growth



and expertise within the IRM.


This initiative is timely and historic and holds immense importance for businesses, society, and the economy in Africa. The IRM Board has also recently appointed Charity Mandiopera, Senior Credit Risk Officer at ZB Financial Holdings Limited (Zimbabwe).

Dorothy Maseke, already a deputy chair of the IRM Group, will be the inaugural chair of IRM Africa, and she will have strategic oversight of the establishment of a registered educational body in Africa (see “Global board boost” in the Spring 2024 edition of Enterprise Risk).

In Africa, businesses face diverse and often volatile operating environments, making effective risk management essential for survival and growth. IRM plays a crucial role in this regard by providing tailored education and resources to

businesses and individuals, enabling them to identify, assess, and mitigate risks efficiently while developing risk intelligent leaders of the future.

IRM qualifications hold significant importance for risk managers and companies, as they provide internationally recognised standards and best practices in risk management. By equipping professionals with these qualifications, IRM enhances the capacity of individuals and organisations to navigate complex risk landscapes with confidence and expertise.

By adopting robust risk management practices supported by IRM qualifications, businesses can enhance their resilience, ensuring continuity in operations, even amid disruptions. 



Please contact: Dorothy.Maseke@theirm.org



The DNA of a controls lifecycle

BY MAYANK GOEL

The UK's revised corporate governance code sets out stricter board responsibilities over the threats organisations face. Taking six critical steps can help risk managers create a controls lifecycle that underpins successful compliance

The UK's Financial Reporting Council (FRC) is responsible for setting the UK's corporate governance code, which is applicable to companies with a premium listing in the UK. The code, which was last revised in 2018, defines corporate governance as the mechanism by which companies are directed and controlled by their board of governance.

Given that governance implementation can vary across companies, the code does not set out a rigid set of rules but instead offers flexibility through a “comply or explain” approach. Following a focused consultation on internal controls, assurance and resilience in support of the UK government's plans to restore trust in audit and corporate governance, the FRC published the 2024 code, which will be effective in phases to financial years beginning on or after January 1, 2025.

In January 2024, the FRC published a revised Corporate Governance Code and accompanying guidance that focuses on the importance of effective internal controls and risk management for boards of directors. The code also requires a meaningful and contextualised explanation statement in the annual report by the boards. This must highlight how the code's principles have been applied to the company's risk management and material internal controls, and the resulting outcomes as well as any departures from

the code. While there are other changes in code, such as expanded reporting on company culture, diversity characteristics expectations and greater remuneration transparency, the remainder of this article focuses on the impact of the revised risk and internal controls expectations in the revised code.

Key changes

The most significant changes in the revised code relate to establishing a formal risk management framework and maintaining as well as reporting on the effectiveness of risk management and material internal controls. The existing code only required the board to monitor the company's risk management and internal

controls and review their effectiveness at least annually.

In addition to the existing expectations, the revised code now requires boards to make an annual internal controls declaration on how they have monitored and reviewed the effectiveness of risk management and material controls – this is contained in provision 29. Boards will also be required to report on issues arising due to ineffective material controls, remediation plans and updates on previously reported issues. By design and taking a non-prescriptive approach, the code does not define what constitutes material control but instead defers it to the board to determine in the context of their company.

To support boards and management with the

IMPLEMENTING AN INTERNAL CONTROLS FRAMEWORK

IDENTIFICATION

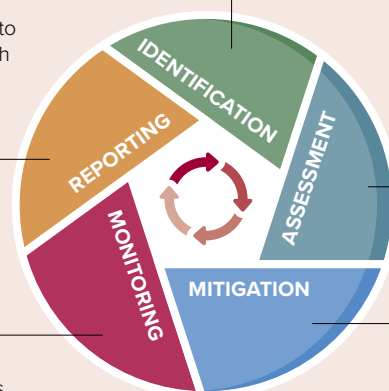
Identify the risks and objectives that need to be addressed through internal controls.

REPORTING

Report on health of internal controls environment to stakeholders.

MONITORING

Periodically assess and enhance controls.



ASSESSMENT

Determine adequacy of any existing controls that may address identified risks.

MITIGATION

Understand root cause of control failures and implement mitigating steps.

“ Risk managers will need to assess whether they have the necessary framework, processes and documentation to evidence the declarations made by the board

CHOOSING AN APPROPRIATE FRAMEWORK

The following steps may help risk managers choose an appropriate risk management framework:

- Understanding the various standards available, such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Integrated Framework and its broader enterprise risk management framework, which includes not only internal controls but also strategic, financial, operational and compliance risks
- Aligning with business objectives and regulations. For example, a healthcare provider would have different considerations than a financial services provider
- Making continuous improvements based on outcome of periodic risk assessments.

implementation of these changes, which could be extensive depending on the organisation, risk managers will need to assess whether they have the necessary framework, processes and documentation to evidence the declarations made by the board. In addition to determining which controls are material, the level of testing required will need to be ascertained.

The changes to the UK Corporate Governance Code are akin to US Sarbanes Oxley (SOX) law but less prescriptive, and provision 29 comes into effect on January 1, 2026. Unlike SOX which is focused just on financial activities, the UK code is broader and extends to financial, operational, compliance and non-financial activities. A number of large companies, especially in regulated industries, already have a formal risk management programme in place with existing direct communication and reporting between the board and the central risk function.

Such companies might find it easier to operationalise the new changes. However, for smaller companies or companies who were previously not subject to the code, they will need to kick off enterprise-wide programmes to adopt and operationalise a controls framework that is fit for purpose, tailored to their specific industries and addressed to the unique risks associated with the industry (see *Choosing an appropriate framework*).

Once selected, a typical framework follows a controls lifecycle. Consistently identifying (based on reasonable documented criteria), assessing, testing and documenting material controls at least annually is crucial for risk managers to help boards achieve code compliance.

Six steps

Step one involves identifying the risks and objectives that need to be addressed through internal controls. Risks can be sorted into several categories, such as credit,

market, strategic, financial or non-financial, and may arise from business-as-usual operations, financial reporting, data and information technology systems. This step should be performed through a top-down risk assessment in line with the risk appetite, considering quantitative and qualitative factors that are consistently applied and the criteria documented.

Step two happens once risks and objectives have been identified. The presence and adequacy of existing material controls should be determined to mitigate the identified risks (see *What material controls should do*).

Step three entails assessment, which includes evaluating the design and operating effectiveness of controls to determine whether they are working as expected. Controls to satisfy code would need to be tested annually through testing procedures, such as sample testing, test-of-one, walkthroughs or reperformance at least by internal audit. The code leaves it up to individual boards whether an external audit review of controls is required and to what extent. The updated code requires disclosure of material controls not operating effectively, along with any action taken or proposed to enhance the control.

Next comes risk mitigation. Based on the results of the assessment, any identified and confirmed control deficiencies should undergo a root cause analysis so that it is not only understood what went wrong but also why any controls failed. This analysis should be performed holistically to determine whether a similar deficiency is present for other material controls.

Once the analysis is complete, mitigation plans

should be developed, tracked and implemented to strengthen controls, address underlying root causes and mitigate risks to an acceptable level. Remediation timelines may vary depending on the complexity of the gap, thus it is important to have

written reports and visual representations of KPIs/KRIs, but it is important that the report be clear and concise as well as contextualised to the specific circumstances material to the company. As previously noted, the updated code requires the board

WHAT MATERIAL CONTROLS SHOULD DO

- Be company-specific; no one control fits every company
- Be aligned to principal risks faced by a company's business model
- Ensure compliance with applicable regulations
- Consider the impact to company's stakeholders if the control should fail
- Include financial and non-financial matters (i.e. technology, data etc.)
- Be periodically reviewed to ensure relevance.

For more information:

[UK Corporate Governance Code \(frc.org.uk\)](https://www.frc.org.uk/Corporate-Governance-Code), [Corporate Governance Code Guidance \(frc.org.uk\)](https://www.frc.org.uk/Corporate-Governance-Guidance)

“Consistently identifying, assessing, testing and documenting material controls at least annually is crucial for risk managers to help boards achieve code compliance

the appropriate governance of remediation activities. The updated code requires that the annual report provide a summary of how previously reported issues have been addressed.

Monitoring

Step five requires an ongoing process of monitoring to periodically assess whether the controls need to be adjusted based on changing business needs and external factors, and to give assurance to the board that the framework is aligned with the company's objectives. The code guidance recommends that in addition to management-level reporting of risks and internal controls, the board should conduct its own monitoring based on its interactions with auditors and other sources.


Reporting the internal controls lifecycle to stakeholders within and outside of the company is the final step. Effective risk reporting provides stakeholders with transparency into the company's risk profile and the overall effectiveness of its risk management framework. Risk reporting can be in various formats or a combination of

to provide a description of how it has monitored and reviewed the effectiveness of the framework. It also requires a declaration of the effectiveness of material controls and a description of any material control weakness.

Greater transparency

The proposed changes to the code aim to enhance the transparency of risk management practices and could be a significant undertaking for smaller companies. Given the not-so-distant effective date of the updated internal controls requirements, organisations with less-mature risk management programmes looking to implement an internal controls framework should consider items such as taking an iterative approach to controls implementation (rather than “boiling the ocean”), determining the feasibility of operating a three-lines-of-defence model, or at least an independent testing function, maintaining documentation of internal controls, including policies, procedures and evidence of control effectiveness, and responding to control deficiencies by implementing clear action plans.

The updated code acknowledges

that companies have varied needs when it comes to internal controls, and thus the “comply or explain” principles-based approach still remains the foundation of the code. Further on, it makes it clear that a good explanation for departures from code provisions may be more beneficial to stakeholders than a check-the-box code compliance approach. This should allow organisations to find alternative approaches to comply with code principles. 

 **Mayank Goel is vice president, compliance manager at MUFG in New York.**

Disclaimer: The views expressed in this report solely reflect the personal views of the primary author of this article, about the subject matter referred to herein, and such views may not necessarily reflect the thoughts and opinions of MUFG Bank, Ltd and its affiliates or management team. No part of such author's compensation was, is or will be directly or indirectly related to the specific recommendations or views expressed herein. This should not be construed as investment advice, a recommendation to enter into a particular transaction or pursue a particular strategy, or any statement as to the likelihood that a particular transaction or strategy will be effective, and it does not take into account the specific objectives or the particular needs of any specific person who may receive this information. You should consult an independent financial, legal, accounting, tax, or other advisor as may be appropriate regarding the subject matter herein. MUFG Bank, Ltd. hereby disclaims any responsibility to you concerning the content herein and does not warrant the accuracy of the content for any particular purpose and expressly disclaims any warranties of merchantability or fitness for a particular purpose. Neither the author nor MUFG Bank, Ltd has independently verified the accuracy of this content, and such information may be incomplete or condensed and is provided “AS IS”.

Regulatory overdrive

BY SARAH WINT

The European Union has been creating a raft of digital regulations to help protect businesses and consumers against hackers. But that is likely to come with an unprecedented regulatory burden for many organisations

While technology always moves faster than lawmakers can protect people against its worst side effects, the European Union has been working harder than most to catch up. This year will see risk managers busy with the first implementation of core planks of that regulation.

First, the NIS2 Directive is a major attempt to create a high common level of cybersecurity across the EU. The original NIS Directive (implemented in 2016) attempted to help organisations build their cyber resilience, but while it had some success, implementation was patchy both across Member States and in different sectors.

In addition, the pandemic

intensified digitalisation and, therefore, made society more vulnerable than ever to major online and operational disruptions. “Any disruption, even one initially confined to one entity or one sector, can have cascading effects more

Co-ordinated response

NIS 2 requires Member States to put in a better cybersecurity infrastructure. That includes, for example, setting up a national computer security response team and a competent national cybersecurity authority – the



Organisations need to improve their risk management processes under NIS 2

broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the whole internal market,” stated an EU report into the impact of COVID-19 on the effectiveness of NIS.

latter to boost co-operation between Member States and among different sectors.

For individual businesses, NIS 2 is much more demanding. Organisations need to improve their risk management processes

30

DORA'S FIVE AREAS OF FOCUS

- **ICT risk management:** risk management is at the heart of DORA as financial firms must identify, assess, and mitigate ICT risk, including the ability to continuously monitor systems, data, and connections. Known issues must be addressed quickly and, where they become serious, they must be reported. See DORA's chapter II, articles 5 to 16.
- **Incident reporting:** the Act aims to standardise incident reporting in the sector and is explicit about how the reporting framework must include both internal and external elements. In practice, businesses must be able to quickly identify problems and report them internally to key stakeholders. Following an impact evaluation and risk mitigation process, disruptive events must be reported to the regulators – and, with data breaches, to customers. See DORA's chapter III, articles 17 to 23.
- **Resilience testing:** the Act says that financial institutions need to periodically test their ICT risk management frameworks through digital operational resilience testing. That includes having in place processes to conduct, for example, effective scenario-based tabletop testing, vulnerability assessments, performance testing, and threat-led penetration testing. The results of these tests must be fed back into the business so that any weaknesses can be properly corrected – thereby creating a virtuous circle of gradual improvement. See DORA's chapter IV, articles 24 to 27.
- **Third-party risk management:** a key aim of DORA is to extend the levels of security expected of financial institutions to their technology suppliers. The onus is on the firms themselves to ensure that such IT partners adopt high standards of digital security and operational resilience. That means ensuring that contracts are reviewed so that they contain commitments from third parties to adhere to such standards – and for the firms to document any risk areas they discover among such vendors. Firms cannot depend on a single vendor for their requirements, despite many migrating in recent years to cloud-based services. See DORA's chapter V, articles 28 to 44.
- **Information sharing:** while not a mandatory requirement, DORA also encourages firms to voluntarily share information and intelligence on cyber threats with other financial institutions. See DORA's chapter VI, article 45.

“ Third-party risk and access control are likely to be areas of significant effort

to include, for example, incident management, stronger supply chain security, better network security, and improved access control and encryption. A prompt and accurate reporting system needs to be able to inform the regulator of breaches within 24

hours – and organisations need to have a business continuity plan that includes system recovery and emergency procedures. While some of these are already areas of intense focus, third-party risk and access control are likely to be areas of significant

effort if they are to be compliant by 17 October 2024 when the provisions become mandatory.

Penalties are stiff: up to 2 per cent of annual turnover or £8.6 million, whichever is higher. And directors that fail to ensure adequate risk management steps are to face personal liability under the directive.

UK businesses providing goods and services within the EU are affected by NIS 2. While those who do not are exempt, the UK is also strengthening its cyber resilience regulations when parliamentary time allows. The Department for Science, Innovation and Technology put additional [proposals relating to the UK's data infrastructure out for consultation in December 2023](#).

Operational focus

Financial organisations are busy getting ready for Europe's Digital Operational Resilience Act (DORA), which applies to any financial firms doing business in or with the EU from January 17, 2025. The purpose of the regulation is to strengthen the digital infrastructure upon which the financial world operates. Policymakers realised that while most financial firms are well regulated, they often relied for their processes on technology platforms and systems – often supplied by third-party vendors – that fell outside the scope of the financial authorities. Given that society increasingly relies on this infrastructure, the EU decided to tighten its risk management requirements.

DORA focuses on five core areas: risk management, incident reporting, operational resilience testing, third-party risk management, and information sharing (see DORA's five areas of focus).

Governing the gadgets

With a growing number of businesses adopting connected devices across their organisations, the [EU Parliament approved legislation](#) to boost the security

“ The purpose of the regulation is to strengthen the digital infrastructure upon which the financial world operates

of digital products in March 2024. The Cyber Resilience Act (CRA) is designed to build better security and standardise what businesses and consumers can expect from the goods they buy and use in their operations (see, *Cyber Resilience Act core requirements*).

The European Commission is to draw up two lists of products based on the potential risk they pose – they will be regulated by a risk-based process. During the bill’s passage through parliament, MEPs ensured products such as identity management systems software, password managers, biometric readers, smart home assistants, and private security cameras would be covered by the new rules. Products will also be expected to have security updates installed automatically and separately from functionality updates – and must have been thoroughly risk-assessed prior to release.

Data is key

The EU’s Data Act came into force on 11 January 2024 and is paired with the Data Governance Act, which became applicable in September 2023. “While the Data Governance Act regulates processes and structures that facilitate voluntary data sharing, the Data Act clarifies who can create value from data and under which conditions,” according to the EC.

The key aim of the Data Act is to allow the users of smart devices access to the information those technologies create and collect. For consumers, that will mean that they can share, for example, the data on a broken watch with any repair service they want to use – not just with the manufacturer. In addition, consumers will be able to collate data from different devices, no matter who manufactured them.

Such data portability is expected to increase both competition and fairness over the future use and accessibility of data across Europe.

From a UK perspective, those

immediately affected will be manufacturers of IoT devices that are sold in the EU, data holders who make information available to users in the EU, and organisations such as cloud

CYBER RESILIENCE ACT CORE REQUIREMENTS

The CRA sets out crucial security criteria that products with digital elements (PDEs) have to comply with, including:

- **Security by design and default** – appropriate level of cybersecurity based on the risks must be embedded in a PDE from the beginning. A PDE must be placed on the market with a secure-by-default configuration, including the possibility to reset the product to its original state, including a default setting that security updates be installed automatically, with a clear and easy-to-use opt-out mechanism.
- **Unauthorised access prevention** by appropriate control mechanisms, such as authentication, identity, or access management systems.
- **Protection of the confidentiality** of stored, transmitted, or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms.
- **Protection of the integrity** of stored, transmitted, or otherwise processed data, commands, programs, and configurations against any manipulation or modification.
- **Minimisation of data** – process only data, personal or other, that are adequate, relevant, and limited to what is necessary in relation to the intended purpose of a PDE.
- **Protection of the availability** of essential functions, including the resilience against and mitigation of denial-of-service attacks.
- **Resilience against service attacks** and attack surface limitation to minimise the potential entry points for cyberattacks.
- **Vulnerability management** – a PDE must be placed on the market without any known exploitable vulnerabilities. Post-market-launched vulnerabilities can be addressed through security updates.
- **Data portability** – users must be provided with the option to securely and easily remove all data and settings and, where such data can be transferred to other products or systems, this must be done in a secure manner.

Source: [A&O Shearman](#)

MINIMUM REQUIREMENTS FOR HIGH-RISK AI

At a minimum, developers and implementers whose technology falls within the high-risk category should be prepared to comply with the following requirements of the AI Act:

- Register with the centralised EU database
- Have a compliant quality management system in place
- Maintain adequate documentation and logs
- Undergo relevant conformity assessments
- Comply with restrictions on the use of high-risk AI
- Continue to ensure regulatory compliance and be prepared to demonstrate such compliance upon request

Source: [Holland & Knight](#)

service providers that process EU data. Some pundits expect the longer-term effect of the Data Act to mirror that of GDPR, which has impacted global regulations on data privacy and protection.

General purpose AI regulation

In May this year, the EU's Council of Ministers rubber-stamped the world's first legislation aimed at governing general purpose AI – [the AI Act](#). As with most EU legislation, the act is likely to come into force in about two years after it is passed – so around May 2027.

The AI Act aims at extra-territoriality to govern the use of AI within the EU wherever the providers and developers of the software may actually reside. That means that those UK businesses providing such services in Europe will be

affected – as will the tech giants in the US. The Act will need to be read in line with GDPR, which governs the processing and use of private information.

Given the rapid development of AI – ChatGPT has come along during the regulation's development, for example – it is not surprising that the regime it enforces will be risk based. That means that regulatory activities apply to systems based on their likely impact on users. The first tier applies to those applications deemed to have unacceptable risk. AI-based systems that cause people to make harmful decisions, or exploit vulnerable people, use biometric data to categorise people based on race, political opinions, sexual orientation and so on, and those that create or expand facial recognition databases by scraping images from CCTV or

the internet are banned outright.

Those that present high or limited risk fall into the second and third tiers. The high-risk category covers many systems that are in use today, according to law firm Holland & Knight, and are likely to cause significant work for businesses that use them. “High-risk applications of AI technology may include biometric identification systems, educational/vocational training or evaluation systems, employment evaluation or recruitment systems, financial evaluations or insurance-related systems,” the firm said.

The boundary between the risk that these systems pose and the ones in the lower, third tier will be subject to more guidance. The EC has 18 months to create these more detailed categorisations – but that could leave businesses with only six months to get ready if they fall foul of the stricter regulations (see, [Minimum requirements for high-risk AI](#)).

The limited risk category has the lightest-touch regulation. But it is also worth noting that the act also provides for additional transparency rules across all categories, specifically labelling AI systems that interact with humans as machines in many cases.

Risk managers looking to improve their skills in this fast-moving sector could consider taking [IRM's Digital Risk Certificate](#), which offers a sound grounding on everything from cybersecurity to ethics. Now that legislators have caught up with recent technological developments, there are likely to be many more regulations to come. 📰



The AI Act also provides for additional transparency rules across all categories, specifically labelling AI systems that interact with humans as machines



IRM Advisory

**Advice, Guidance
and Mentoring**

**Level up your risk
performance**

IRM Advisory will advise, guide and mentor you in levelling up your risk performance by helping you get the most out of your risk frameworks and programs.

From understanding your risk appetite to setting the proper risk levels and developing an enterprise-wide risk culture.



Scan me!

hub.theirm.org/advisory
advisory@theirm.org



Sick of work

BY ARTHUR PIPER

With cyberattacks and AI often dominating headlines, social risks often rank poorly in surveys – which is why it was surprising to see health and safety making a strong showing in a recent poll

Surveys are generally seen as lagging indicators because they are a snapshot of what people were thinking in the weeks during which they are completed. So, when a category that has not dominated the news and social media suddenly makes an appearance, alarm bells should be ringing.

That happened recently when Clyde & Co's annual global directors' and officers' liability report 2024 showed that health and safety has leapfrogged cyberattacks, data loss and regulatory breaches as the top concern for respondents. Ranking health and safety first (at 86 per cent) in the survey clearly baffled the report authors.

"It is unclear what the precise reason is for this rise in concern, but, certainly in the UK, 2023 saw highly-publicised fines levied on major corporations (e.g. Network Rail, Morrisons, Serco and Transport for London)," the

report said, "alongside a noticeable uptick in enforcement notices issued by the Health and Safety Executive (HSE) and reports of the HSE's impressive 94 per cent conviction rate of individuals."

Pandemic effects

Given that the report is global, that does not fully account for the renewed focus on safety in

physical and mental health – only slightly down on peak levels in 2022 at the tail-end of the Covid-19 pandemic," according to the FT's own research. Ill health indicators included alcohol consumption, obesity and lack of sleep.

While organisations may decide to focus on individual wellness initiatives, the FT indicated that broader structure



Ranking health and safety first (at 86 per cent) in the survey clearly baffled the report authors

the boardroom. As the authors go on to point out, a report by the *Financial Times* (FT) across a range of industries found that poor health has persisted since the pandemic.

"UK employers lost the equivalent of 50 days of work per employee last year because of poor

problems with human resources strategies are likely to be involved. "While employers in Britain and elsewhere spend billions of pounds each year on wellness interventions focused on individual staff, growing evidence suggests that the most significant influences are structural factors



“ Human resources professionals seem to have become bad at delivering results in employee engagement programmes – at the same time as believing they are doing sterling work

related to autonomy, sense of purpose, pay, working conditions, and supportive management,” the newspaper said.

Out of touch

Worryingly, human resources professionals seem to have become bad at delivering results in employee engagement programmes – at the same time as believing they are doing sterling work.

Almost two-thirds (64 per cent) of HR professionals said their organisations delivered an “excellent” employee experience compared with only 20 per cent of employees who said the same, according to a survey by Benefex.

Something has gone wrong over the past 12 months. Last time the survey was done, employers slightly underrated their performance (34 per cent said they provided an excellent experience, compared with 38 per cent of employees). That is a

much healthier position to be in – especially as since then, 81 per cent of employees have decided that experience at work was more important than a year ago.

In fact, other polls have shown that many workers are also increasingly receptive to the idea of returning to the office. A Castleforge polling of more than 1,800 office workers in winter 2023 found that 59 per cent of young workers (aged 18-24) said they worked less productively at home. And 43 per cent also reported feeling socially isolated while working away from the office and experienced negative effects from a lack of human interaction – supporting the idea that employees’ experience at work has become more important overall.

Disconnect

That suggests that too many HR departments are out of sync with these trends and are designing employee experiences that people generally do not like.

So what do people want? Benefex found that while salary (78 per cent) and benefits (59 per cent) remain the two key factors when choosing an employer, employees also said that wellbeing (55 per cent), flexible working (53 per cent), high ethical standards (51 per cent) and employee recognition (50 per cent) were also important.






“Expectations around benefits are rising at a rapid rate,” the report said. “More than 90 per cent of employees state that it’s important that their benefits protect them if they get sick, help them to achieve work-life balance and support their financial, physical and emotional wellbeing.”

HR risk management is often cast as a process that is meant to safeguard the company from the behaviour of bad employees. Perhaps it is time for some organisations to begin safeguarding employees from the deadening effect of poorly designed employee experience programmes. ☹

Change tomorrow with industry leading GRC software

Camms.






With powerful, agile and integrated solutions in governance, risk, compliance and strategy, Camms' business software will help you make the right decisions, manage risks and focus on what matters. Working with tens of thousands of users at organisations across five continents, and with over 25 years of experience, Camms thrive on watching their clients achieve results and stay a step ahead. Helping firms meet goals, influences business decisions and board strategy is in Camms' DNA. To learn more, visit www.cammsgroup.com.

 Daniel Kandola
 +44 (0) 161 711 0564
 sales@cammsgroup.com
 www.cammsgroup.com
 Suite 4.3, Parsonage Chambers
3 The Parsonage
Manchester, M3 2HW
United Kingdom

Cost-effective technology for risk & compliance professionals



1RS provide cutting edge 1RS ERIC (Risk & Compliance), 1RS CASS and 1RS SMCR solutions, which have been designed and built by Risk and Compliance professionals with over 25 years of experience. Our solutions are supported by experts, and we continually update the products to reflect best practice and changes in regulatory expectations. We are trusted by banks, vehicle finance, wealth management, investment banking and management, brokers, and more throughout the United Kingdom and Europe. For more information, visit <https://1rs.io>

 Andrew Firth
 +44 (0) 20 7175 6177
 hello@1rs.io
 1rs.io
 38 Borough High Street
London
SE1 2AL

Enterprise risk management and risk analysis software



riskHive are an established global provider of professional cloud, intranet and desktop solutions for the management and analysis of RAID (risks, issues, assumptions and dependencies). Being low maintenance, highly configurable and cloud based, the Enterprise Risk Manager application can get you online in under 24 hours, supporting your existing processes and terminology. Easily import existing risk information to quickly produce a consolidated risk portfolio. Relied on by customers ranging from New Zealand through the Middle East to Northern Europe riskHive deliver a truly global ERM solution with a truly enterprise 'all-in' licence.

 Ian Baker or Doug Oldfield
 +44 (0) 1275 545874
 ian.baker@riskhive.com
doug.oldfield@riskhive.com
 www.riskhive.com
 riskHive Software Services Ltd.
Dilkush, Farlers End
Bristol, BS48 4PG

Risk, audit & compliance software

Symbiant®






Symbiant is a market leading provider of Risk, Audit & Compliance software. They have a full range of modules that can be connected for a wholistic view. Customise your own layouts and reports or use the ready-made options. All modules are a fixed £100 per month. Contracts are only 30 day. Visit the website to watch the quick overview videos or to arrange a no obligation web demonstration.

 Mark Long
 +44 (0) 20 8895 6410
 irm@symbiant.co.uk
 www.symbiant.co.uk
 20-22 Wenlock Road
London
N1 7GU

Risk management software



Since 2014, Origami Risk is the only company that has been consistently recognised for delivering client success, innovation, and stability, while bringing new ideas and advanced features to the RMIS market. Origami Risk's innovative software is designed with the latest technology and a focus on performance and ease-of-use, providing integrated solutions to the entire insurance value chain, serving Risk Managers, Brokers, TPAs and Carriers. It features powerful workflow, advanced reporting and analysis tools, and intuitive features to improve productivity and better manage total cost of risk—saving our clients time and money and enabling them to be more successful. Learn more at www.origamirisk.com

 Neil Scotcher
 +44 (0) 16179 17740
 nscotcher@origamirisk.com
 www.origamirisk.com
 30 Moorgate
London
EC2R 6PJ

Risk management software



In today's rapidly evolving world, business models and organisations are facing increased change and unprecedented levels of scrutiny. With change comes complexity, challenging risk managers to redefine the way they lead an organisation's approach to and implementation of risk management. Protecht helps organisations through deep understanding, monitoring and management of risk. We provide the complete risk solution—comprised of world-class enterprise risk management, compliance, training and advisory services—to government organisations, key regulators and businesses of all sizes across the world. With 20+ years at the forefront of risk and compliance solutions, millions of incidents managed across thousands of individual risks, and over 25 thousand people attending our training courses to date, we're one of the most respected and influential voices in risk.

 N/A
 +44 (0) 20 3978 1360
 info@protechtgroup.com
 www.protechtgroup.com
 77 New Cavendish Street
The Harley Building
London W1W 6XB
United Kingdom

Clever feelings

Human intelligence is inherently biased, which may prove essential when working with machines

As more human intelligence is embedded into AI systems, one increasingly wonders about the nature of human intelligence. Large language models (LLM) are based on huge quantities of human-generated data, in which the human intellect is fundamentally embedded. They are also made by very clever people – so the results of their processes should theoretically be amazing and trustworthy.

Sadly, that has turned out not to be true. Such programs often make things up – or are at least cavalier about the veracity of their statements – and cannot tell you what sources of information they have used to come to their conclusions. They freely replicate the biases they draw on in source data without a second thought.

From a recent discussion with an AI expert, Toffler understands that the way LLMs work means that such faults are a feature of these programs – not a bug – and are therefore likely to remain a problem.

Foggy thinking

On the plus side, the fact that such programs often make things up and cannot tell you what sources of information they have used to come to their conclusions is an encouraging sign that LLMs do accurately reflect how many people think much of the time. A glance at a favourite social media



feed will bear that statement out.


So, it is troubling to note that, given these shortcomings in both people and machines, one of the ways that they are meant to co-operate is for people to provide critical thinking on the information LLMs provide. In other words, people are required to give the information a rigorous pruning to get rid of any potential biases that the humans provided the machines with in the first place.

The Cambridge Online Dictionary defines critical thinking as “the process of thinking carefully about a subject or idea, without allowing feelings or opinions to affect you.” Readers may feel warm inside to note that one of the “smart” vocabulary phrases related to critical thinking is risk management.

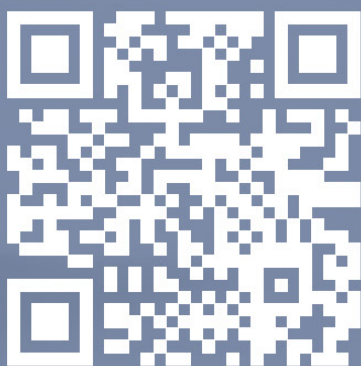
Bias built in

Unfortunately, cognitive neuroscientists such as Antonio Damasio realised back in the 1990s that the very feelings and opinions that create biases have played an important role in

human development. If people are biased towards seeing everything as a potential food source, for example, they are more likely to survive. To make this possible, Damasio argued, the nervous system processes incoming data from the outside world and tags items of interest with little emotional charges that make them more interesting to us than they otherwise might be. Bias can therefore not only be seen as a fundamental part of being human but as something that is both built in and useful.

If humans are to apply critical thinking, then, to LLMs, they must also approach that task with an understanding that they may be bringing different types of intelligence to the task. That may include a bias towards objectivity. But another, more important, bias may be one that leans towards empathy. As we have learnt from high-profile IT system failures, humans’ ability to feel sorrow, pity, or joy may be an essential tool to bring when working with machines. 

Build your career as a risk professional



Scan me!

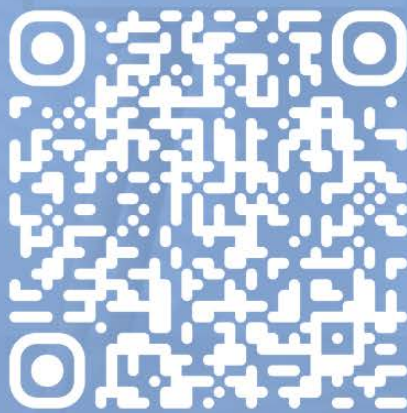
Training with the IRM

With training courses covering a wide range of enterprise risk management topics, our courses are delivered by industry experts so you can immediately apply the latest in best practice techniques. As well as being practical and interactive, the courses allow you to log CPD hours and some offer accreditation.

www.theirm.org | Tel: +44 (0)20 7709 9808 | Email: enquiries@theirm.org

irm

Join over
8,000 risk
management
professionals



Scan me!

IRM Membership

Join us and you'll benefit from a host of networking and professional development opportunities. You'll also have access to a wealth of articles, guides, reports and other practical tools and resources to develop your skills and keep you up-to-date. A full list of our membership grades and professional designations can be found on our website.

www.theirm.org | Tel: +44 (0)20 7709 9808 | Email: membership@theirm.org

irm