BDO

Techtonic States

SECURE YOUR BUSINESS EDGE

REPORT CHAPTER 3

BDO DIGITAL

CONTENTS

The New Business Edge: The strategic integration of advanced technologies and data-led decision-making to drive resilience, agility and long-term growth.

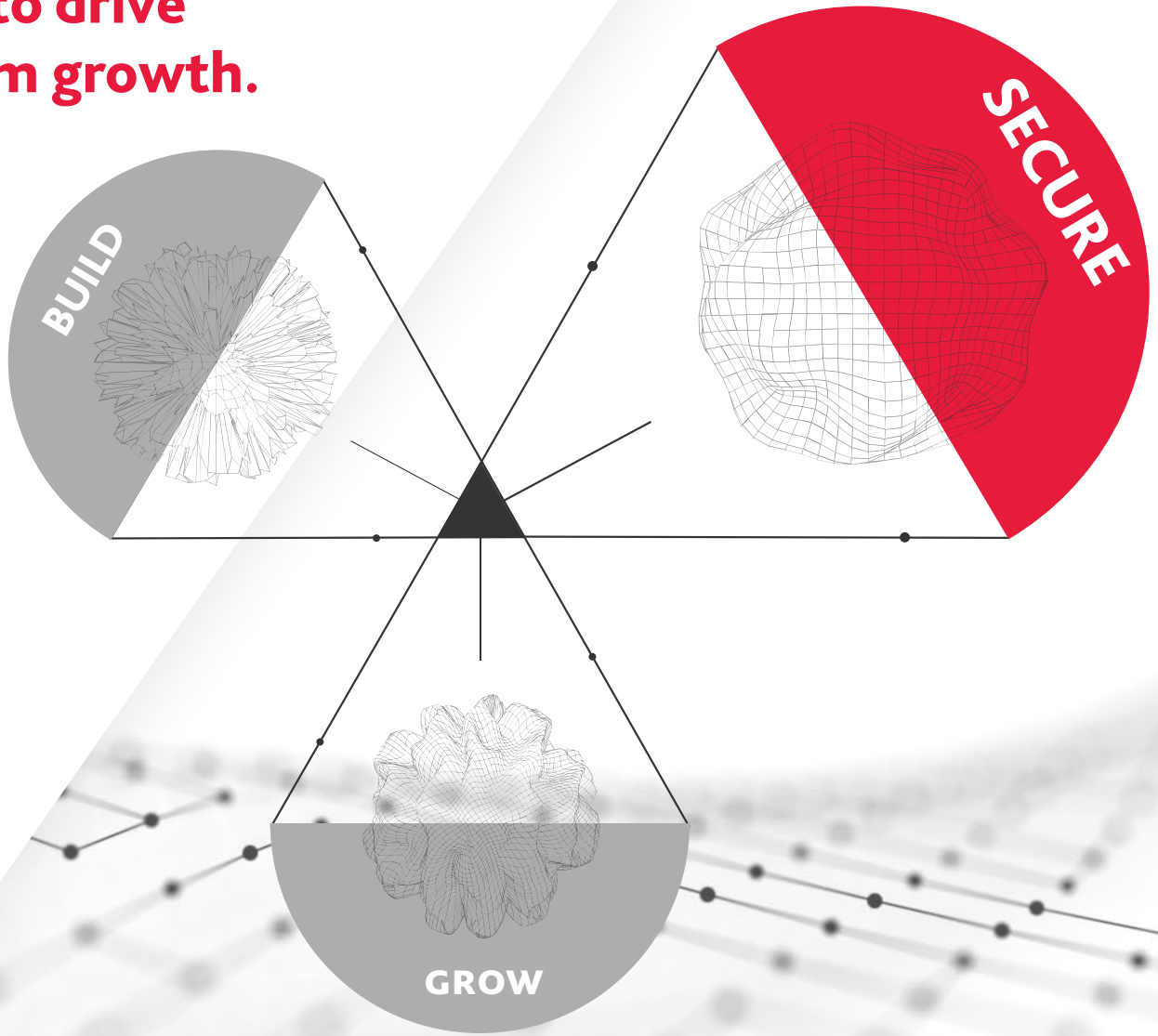
Our latest *Techtonic States* report reveals that, looking ahead to 2028, leaders anticipate a 'World Fragmented' – defined by fractured markets, disrupted supply chains, and rising geopolitical tension. But no matter what the future holds, one thing is clear: the risk landscape is shifting fast. Technological disruption is at the heart of this change, opening new frontiers while simultaneously exposing new vulnerabilities.

Just 55% of leaders say their leadership understands AI risks – yet BDO's **2025 Global Risk Landscape Report** shows 69% of companies are risk-averse, up from 61% in 2024. In today's volatile environment, excessive caution could be the riskiest move.

Businesses must move boldly but securely – ready to disrupt and be disrupted. The leaders will be those that balance innovation with strong governance, tech ethics, and layered cybersecurity. This proactive approach to risk is central to gaining the New Business Edge.

This chapter explores how forward-thinking organisations can turn resilience into a strategic advantage – protecting their edge today and securing their growth for tomorrow.

The three dimensions of the New Business Edge



01

Governing AI for **Responsible Growth**

As AI adoption accelerates, it is amplifying existing business risks and introducing new ones. To adopt these tools with confidence, businesses must assess the risks early and build risk management into their strategy. However, our research reveals that only 55% of business leaders believe their organisation's leadership has a clear understanding of the risks associated with AI. This gap in awareness could prove costly.

Where do leaders believe the greatest risks lie, and how are they planning to address them?

The top risks of AI implementation, according to leaders

01	Data privacy	71%
02	Security risks	70%
03	Job displacement	61%
04	Data quality and availability	60%
05	Overreliance on technology	39%

The top measures organisations are taking to mitigate AI risk

01	Investing in data privacy	73%
02	Investing in data security	72%
03	Ethical AI guidelines	42%
04	Job role redesign	28%
05	Investment in upskilling	21%

With AI increasing the scale and complexity of data use – often without clear visibility – it's no surprise that data privacy, quality, and security are key concerns. As organisations collect and process more information than ever, the risks of breaches and misuse increase, making strong protection against both external and internal threats essential. This is putting a blocker on innovation, with almost half (48%) reporting that data security concerns are preventing their organisation from investing in more AI technologies.

Businesses must treat data not just as an asset, but as a responsibility. High-quality, well-governed data is not just important for operational efficiency, but for ethical and resilient decision-making. If left unchecked, poor data quality can gradually erode trust and only reveal itself in moments of crisis.

Responsible data practices, transparency, and accountability are the foundations for safe, ethical and effective AI use. Business leaders recognise this, with 68% believing robust governance frameworks and security measures are essential to technological innovation.

Your people are central to implementing these practices and mitigating risk, and yet just 28% of leaders say their organisation will focus on job role redesign, and only 21% plan to invest in upskilling. Without a workforce equipped to adapt to AI-driven change, businesses face increased exposure to security vulnerabilities, unmotivated teams, and displacement of critical talent. Building digital literacy, critical thinking, and ethical decision-making now will enable teams to work smarter, faster, and safer with AI.

> *Poor data quality leads to bad decisions and operational blind spots. And when it comes to AI, the stakes are even higher. AI systems are only as good as the data they're built on, so if that data is flawed, biased or insecure, the outcomes will be too. Success also depends on equipping teams with the skills to adapt and thrive in an AI-driven world.*

KOEN CLAESSENS
Global Risk Advisory Leader, BDO

02

A Rising Tide of **Cyber Threats**

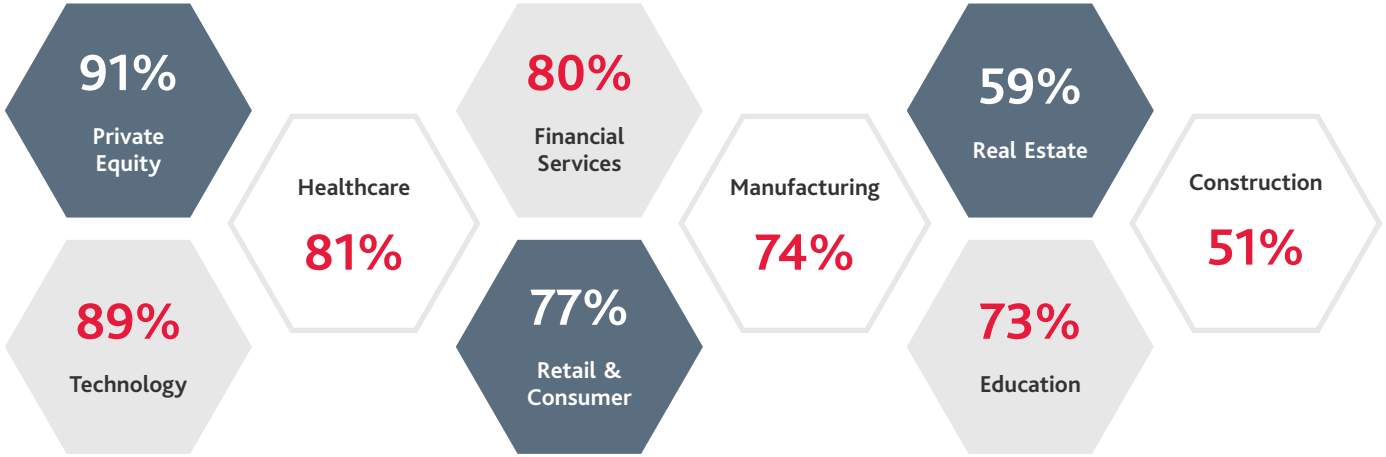
Cyber risk remains firmly at the top of the agenda for business leaders, and for good reason. As digital transformation accelerates, so do the threats that come with it: 68% of leaders say technological advances are intensifying cyber risks and generating new forms of cybercrime.

More than a quarter (27%) of leaders believe that cyber threats – including cyber fraud, espionage and ransomware attacks – will be the single most impactful risk to their organisation in the next three years. And the pressure is mounting fast: 76% expect their organisation's cybersecurity risk to increase over the next 12 months.

This sense of urgency isn't uniform across all sectors. Industries with high-value data, complex supply chains, or critical infrastructure – such as private equity, technology and healthcare – are feeling the heat most acutely. But no sector is immune. As threat actors become more sophisticated and attack surfaces expand, every organisation must brace for impact.

RISING CYBER RISK: SECTOR SPOTLIGHT

The proportion of leaders who expect their organisation's cyber risk to increase over the next 12 months



Currently, a third of leaders (33%) say their organisation is not equipped with the infrastructure and/or skills to tackle the scale of cybersecurity threats. However, over half (56%) expect their organisation's investment in cyber security to increase over the next 12 months, by an average of 7%. As threats grow more complex, embedding security into strategic decision-making will be key to unlocking innovation, safely and confidently.

Risk shouldn't be a blocker to innovation, but a guide for it. Too often, security is left out of strategic conversations, but security teams aren't here to say no – they're here to help you move faster, with confidence.

ROCCO GALLETTO
Global Cybersecurity Leader, BDO

Cybersecurity isn't just an IT issue; it's a business resilience issue.

03

Tech Ethics: **The Missing Pillar of Corporate Responsibility**

Too often the pressure is only set to grow, with more than two-thirds (68%) of leaders believing the pressure relating to corporate responsibility will increase between now and 2028.

When considering the importance of various corporate responsibility factors for their organisations' growth, leaders rank financial responsibility first, followed by ethical business practices and stakeholder engagement. Meanwhile, tech ethics and data ownership rank sixth, with just 59% of leaders believing this is important for their organisation's growth today. And looking ahead, just 52% of leaders believe it will be important for their growth in 2028.

But in a future where AI and other advanced technologies are key drivers of competitive advantage, overlooking these ethical considerations could become a serious vulnerability. Customers, employees and stakeholders want to know that AI systems are operating in ways that are equitable and explainable. And as governments around the world introduce laws and guidelines around AI use, such as the EU AI Act, businesses will need to demonstrate ethical practices to avoid legal penalties.

MARKET SPOTLIGHT

Leaders who see tech ethics and data ownership as important for their organisation's growth

	Now	In three years' time (2028)
USA	70%	65%
SPAIN	64%	57%
AUS	62%	51%
UK	62%	55%
NL	60%	49%
CA	60%	46%
LATAM	57%	53%
SG	56%	53%
GER	51%	42%
INDIA	46%	52%

Today, out of necessity, business leaders are focusing on immediate geopolitical and economic challenges, often leaving little headspace for long-term issues like data governance and accountability. But as companies make more decisions using AI, tech ethics will become central to maintaining trust, ensuring compliance, protecting reputation and enabling sustainable innovation. The businesses that lead on these fronts won't just meet rising expectations; they'll shape them.

RIC OPAL
Global BDO Digital Leader, BDO USA

04

Five Steps for **Managing Risk and Building Resilience**

Effective risk management starts with a clear-eyed understanding of the challenges ahead and a commitment to building organisational resilience. This section outlines five essential steps that empower businesses to assess their true risk exposure, strengthen governance, and foster collaboration across teams. By integrating these strategies, leaders can confidently navigate uncertainty and build a foundation for long-term success.

Five steps for managing risk and building resilience

01

Start with a risk reality check

Before developing a risk treatment plan, assess your true exposure and readiness. Engage cyber risk management teams early in any transformation to guide a speedy, safe journey. When evaluating cyber risk, go beyond counting incidents—investigate close calls, root causes, and response gaps. Not all risks are equal, so focus on what matters most and prioritise based on potential impact.

02

Rethink your data governance framework

Robust data governance is built on visibility. It means knowing exactly what data you have, where it comes from, where it lives, who owns it, who has access to it, and how it's protected. Once the framework is in place, it's crucial you put as much energy into embedding and sustaining it, making it part of how your business runs every day.

03

Invest in your people

They are both your strongest defence and your greatest vulnerability. Hire for curiosity and adaptability, then empower your people with the time, tools and trust to learn, grow and collaborate. When people feel valued and understand their role in protecting and advancing the organisation, they become active champions of its success.

04

Stay ahead of regulation

In fast-moving areas like AI, regulation is always playing catch-up with innovation. Don't let this slow you down. Scenario planning can help to anticipate change and design systems with future compliance in mind. This includes addressing cloud, data and AI sovereignty early – ensuring your infrastructure respects jurisdictional boundaries and protects sensitive data to avoid costly rebuilds later.

05

Break down team silos

Risk doesn't live in one department, and neither should your response. Align enterprise risk management, compliance, IT security and the board with a shared language and collective goals. When teams collaborate, risk becomes more manageable, and strategy becomes unstoppable.

05

The Role of **BDO**

Your business wants to innovate faster, supported by embedded cybersecurity and compliance that protects and enables across the innovation journey. Be confident knowing you've taken the right steps to include cyber risk management as your guide to a safe and secure future to enable your organisation to thrive.

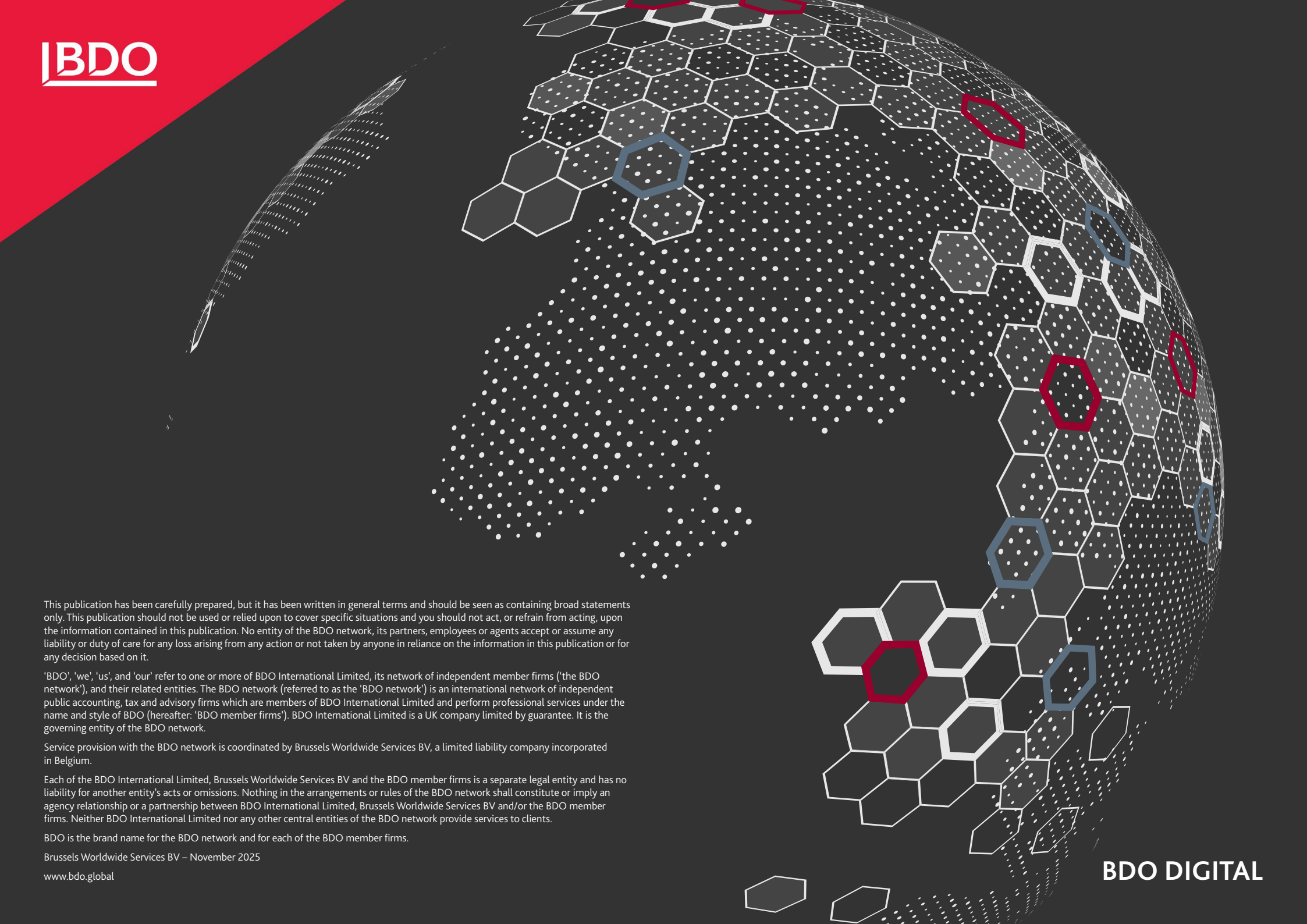
From robust risk management and data protection to resilient recovery and regulatory compliance, we help you safeguard your assets, future-proof your infrastructure, and turn cybersecurity into a catalyst for confidence and competitive advantage.

Visit the **BDO Global website** to read more about our Risk Advisory and Cybersecurity services or get in touch with our team.

To find out more about the 2025 Techtonic States study, read the first two report chapters

CHAPTER 1: THE NEW BUSINESS EDGE ▶

CHAPTER 2: BUILD YOUR BUSINESS EDGE ▶



Brussels Worldwide Services BV – November 2025

www.bdo.global

BDO DIGITAL