

Deloitte.
Insights



The trust enabler

Building cyber-security strategies for
a trusted, digital future

Through the help of the profound expertise of more than 250 colleagues in Germany and a global network of cyber experts, we are able to offer end-to-end cyber services consisting of advisory in strategy, implementation and operations. We help our clients realise the potential of digitalisation holistically in their organisations, to protect valuable assets and to enable innovative business models. We accompany them with a comprehensive range of services to help drive innovation for secure and sustainable growth.

Contact the authors for more information or read more about our cyber risk expertise and services on **Deloitte.com** in English or on **Deloitte.de** in German.

Contents

Introduction	2
What is digital trust?	3
Digital transformation: The trek towards trust	4
Building a cyber-security strategy that enables digital trust	6
1. The rethinking of the enabling potential of technology	6
2. The fragmentation and expansion of responsibility and accountability for digital	7
3. The primacy of data as a governing principle	8
Cresting the peak: From strategy to digital trust	9
Endnotes	10
Acknowledgements	10
About the authors	11
Contact us	12

Introduction

In the age of digital transformation, trust is an elusive asset, but one that's never out of reach for organisations that have initiated the right actions, such as adopting a sustainable, forward-looking cyber-security strategy.

“IT TAKES 20 YEARS to build a reputation and a few minutes of cyber-incident to ruin it.”¹ This statement, as articulately expressed by Stéphane Nappo of Société Générale, illustrates how fragile trust is in the digital sphere. An organisation's best way to deal with the fast-changing threat landscape is an understandable, well-structured cyber-security strategy. This acts as a shield during the constant and rapid upheaval of digital transformation, protecting the business's tangible and intangible assets, including its reputation.

Digital transformation is largely influenced by a set of key factors that are shaping the future and characterised by volatility, uncertainty, complexity and ambiguity (VUCA). In a VUCA world, businesses, individuals and society face new threats and risks – ones that risk managers, C-suite leaders, IT professionals and also policymakers should be concerned about managing. Threats and risks can erode trust in products and services, undermining the carefully built reputation of even the most valuable company.

By analysing drivers and trends that affect the future of digital trust, decision-makers can proactively develop strategies that enable them to cope with the most likely challenges ahead. In Deloitte's Future of Digital Trust study, we identified trends of our digital world, which revealed eight critical implications that the C-suite and other decision-makers should consider when developing future-proof strategies.² This article builds on those implications, showing stakeholders how to mine them for insights that will encourage digital trust; each of the implications should be considered in an organisation's approach to cyber-security.

Some readers might not be aware of the breadth and depth of all of these implications, and others may not have factored all of them into their cyber-security strategies. However, the implications are relevant for modern strategies, and for organisations that strive to proactively mitigate risks attached to processes, technology, people and governance. Behind every successful digital transformation lies an air-tight cyber-security strategy: The compass pointing the way to digital trust.

In Deloitte's Future of Digital Trust study, we identified trends of our digital world, which revealed eight critical implications that the C-suite and other decision-makers should consider when developing future-proof strategies.

What is digital trust?

Think of digital trust as a new prerequisite of good old values, such as reliability, credibility or security, applied in the digital space. Fundamentally, digital trust is an essential factor in an organisation's sustainable and long-term successful digitalisation.

IN A TRUSTING RELATIONSHIP, one does not have to worry about revealing vulnerabilities; each party can rely on the responsible handling of whatever they reveal. In the context of digitalisation, trust is the individual's confidence in an organisation that data will be handled securely and responsibly in the digital environment. Digital trust has taken on new weight as the shift to technological practices and solutions has shattered previously accepted axioms, disrupting industries with new behaviours and attitudes.

To embed digital trust into long-term strategies, two key questions have to be answered: Which driving forces (drivers) and trends will form the future of digital trust in our society and economy, and how can cyber-security be an enabler for a sustainable and trustworthy digital transformation? Let us focus first on the drivers and trends, which lead to implications that help build a strong cyber-security strategy.

FUTURE FORESIGHT METHODOLOGY

It is impossible to definitively predict future developments, but Deloitte's **Future Foresight** business methodology aims to expand our vision and understanding of the forces shaping tomorrow by reducing the 'noise' generated by big buzzwords and developments. With this model, decision-makers and stakeholders can focus on relevant factors that may otherwise escape them, and become empowered to make robust but flexible decisions.

Future Foresight can enable long-term strategy development by building an outside-in foundation. Starting with driving forces, trends are derived and their implications considered (figure 1). Unlike many traditional methods, this process captures the complexities around us. It really helps us get to grips with the most pressing and difficult questions confronting businesses on a daily basis.



Digital transformation: The trek towards trust

If we see digital trust as the peak at the top of an upwards trek, cyber-security strategy lies just below that peak. But to form a winning strategy, we need to acknowledge the mountain of key elements that lie beneath the pinnacle (figure 1). All of these elements described below – driving forces, trends and implications – are explored in detail in our Future of Digital Trust study.³

Driving forces

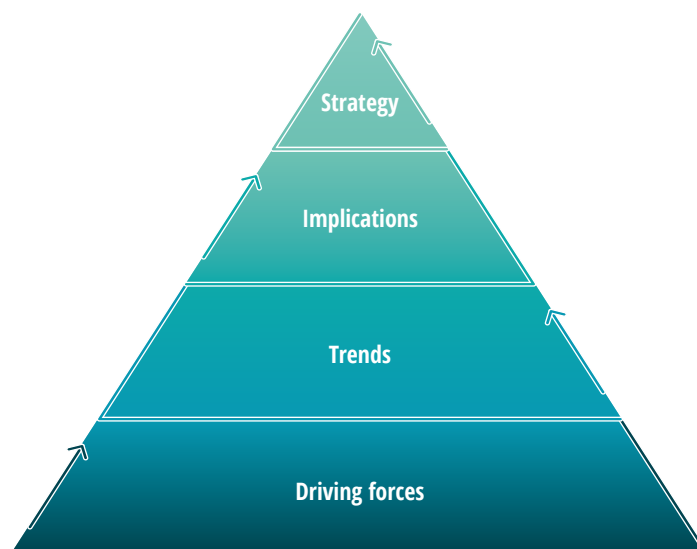
At the base of the mountain are the individual, influencing variables that are already established, emerging or on the distant horizon: the drivers. An example might be the speed of globalisation, or the digital economy.⁴ Drivers can be categorised as social, technological, economic, environmental, political or legal (aka the STEEPL framework). The drivers vary in their impact and the uncertainty of their development. Identifying them helps us outline the highly dynamic environment we are experiencing today and pinpoint the change around us.

Trends

Driving forces link together to form trends that show over-arching developments with the potential to shape the future; they are found across sectors and show the interdisciplinary character of digital trust, which goes beyond technology. Trends consider the nature of the individual driver's interaction and how that can catalyse – or cripple.⁵ For example, in our context, the trend 'oversecuritisation' describes an uncoordinated investment in IT security measures and is influenced by such drivers as offensive and defensive cyber capabilities, data protection and privacy regulations.

FIGURE 1

Hierarchy of key factors influencing digital trust



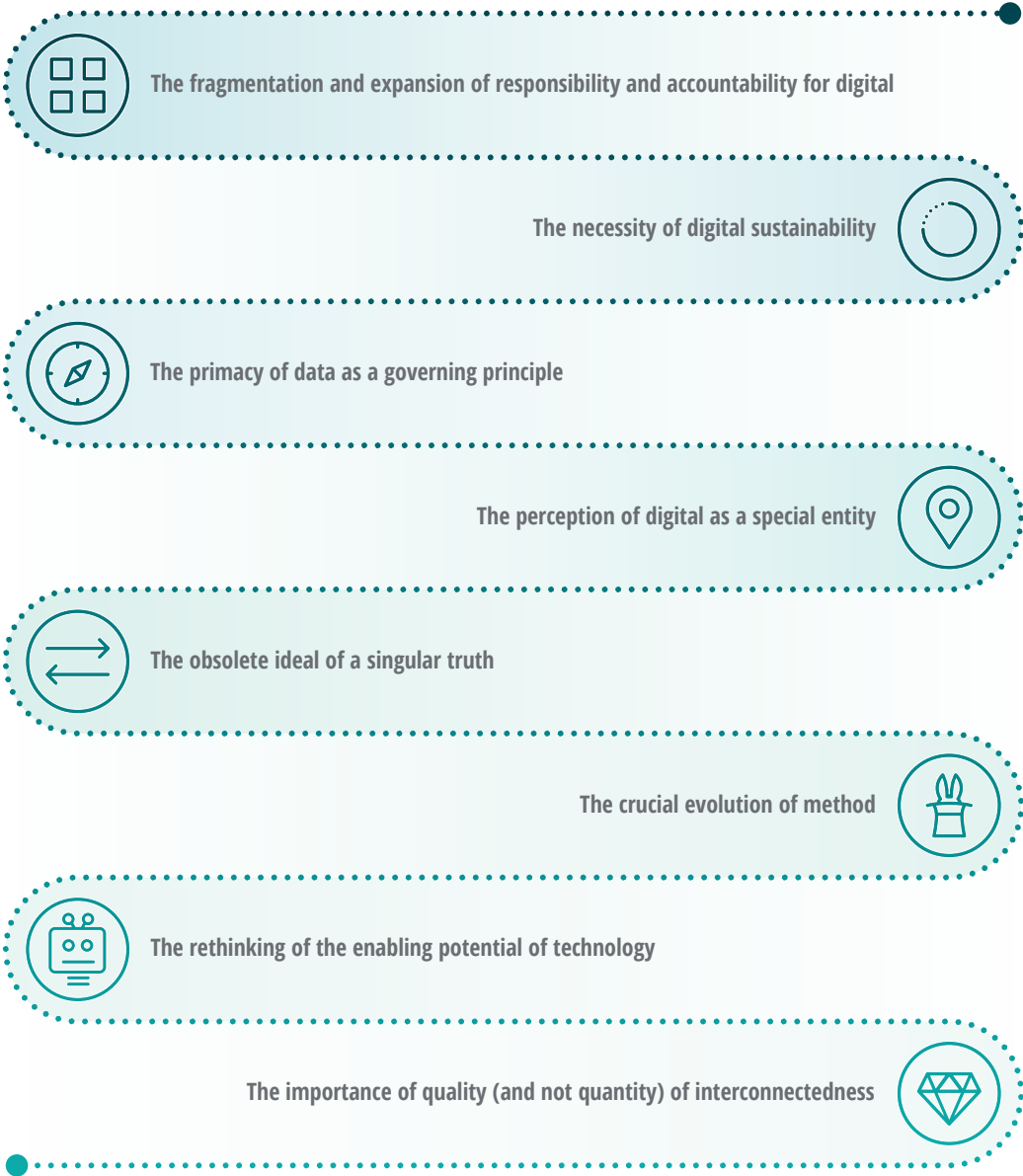
Source: Deloitte, *Future of digital trust: Driving forces, trends and their implications on our digital tomorrow*, March 2021.

Implications

The trends' interaction with each other exposes eight key implications (figure 2) that present various opportunities and challenges across industries, sectors and core business priorities in terms

of digital trust. Analysed individually, the implications illuminate unique points of action for each organisation. Together, they form the bedrock for creating, or revising, long-term cyber-security strategies and policies that will supercharge digital trust.

FIGURE 2
Eight key implications in the context of digital trust



Source: Deloitte, *Future of digital trust: Driving forces, trends and their implications on our digital tomorrow*, March 2021.

Building a cyber-security strategy that enables digital trust

Having understood the relationships among elements that influence digital trust, we can now glean solid insights from the eight implications and consider them in developing future-proof strategies. Below we place three of the eight implications in the context of cyber-security, providing concrete recommendations. The same kind of examination could also be applied to the other five implications.

1. The rethinking of the enabling potential of technology

In the context of cyber-security, two perspectives need to be considered. First, the ever-increasing amount of information is driving up complexity (the biggest enemy of proper cyber-security). Complexity does not scale and will only get worse with the interconnectivity and exponential proliferation of new digital end points. Standards and methods must help reduce those complexities, improve collaboration and automate our responses, using the potential of any new technology that arises.

The second perspective is found by looking through a 'security lens'. Technology advancements are disrupting existing business models and offering new means of attacks. Attackers should not be the only ones exploiting the full potential of new digital tools. Technology must accommodate specific business requirements, threats and risks; this requires a deep understanding of the business needs and the current threat landscape. The cyber-security strategy should enable services and match them with defence tactics and goals to enable a secure digital transformation.

Recommendations derived from this implication for cyber-security strategies:

- **Efficiency:** Automate cyber-security services/functions end to end,⁶ from identification to recovery capabilities. Many cyber-security services and processes are conducted manually, but their efficiency and quality of results can be enhanced with automation technologies or artificial intelligence.
- **Effectiveness:** Follow a risk-based approach and prioritise according to business enablement-related investments. This means spending money where it matters most and generates the most impact.
- **Security:** Build modern security architectures that include the latest technology advancements and resilient services, following principles such as 'Never trust, always verify'. This will enable flexibility and secure adaptation in a fast-changing technology and business landscape.

APPLYING THE INSIGHT

A useful exercise when developing a cyber-security strategy is to extract key questions and steps from an implication's insights. We do this below for one of the eight implications, but a decision-maker should also repeat the exercise for the other seven.

Implication: The rethinking of the enabling potential of technology

Use case: Take a technology architecture management approach with the following steps and corresponding questions.

- Analyse the technology and architecture landscape. (Which technologies and vendors already exist? Where are there gaps that need fixing? Do we have redundancies and overlaps? Can we save money by getting rid of tools?)
- Conduct data source analysis. (Which data sources do we have based on our technology landscape? Which data is already available via the various platforms? Which available data can be further processed, as well as combined?)
- Create automated business intelligence platforms, and conduct real-time analysis and monitoring that enhances security and performs root-cause analysis. (Which use cases can be created based on the existing tools and data? Which insights do we gain by monitoring and analysing these data feeds?)

2. The fragmentation and expansion of responsibility and accountability for digital

The burden of ensuring a trustful digital environment – which includes cyber-security – has shifted from single actors to multiple internal and external stakeholders, either through public pressure or regulations and laws. The burden now sits with a wide variety of private- and public-sector stakeholders who were not traditionally responsible or accountable in the digital sphere.

That means that within a firm, accountability for security can no longer be broken down into separate entities, because of increasing complexity and dependencies. The classical boundaries separating businesses, operational technology, information technology and connected digital products have been erased. To establish digital trust, governance models and accountability should reflect the interconnect-edness of everything in the cyberspace realm.

Recommendations derived from this im-
plication for cyber-security strategies:

- **Co-creation approach:** Modern cyber-security strategies cannot be developed in the often isolated information security department; develop them jointly with the rest of the business and its system, including cyber-security representatives throughout the organisation.
- **Shared responsibilities:** Develop overarching governance and organisation models to include clearly defined cyber roles and responsibilities, both technical and non-technical, across the whole organisation (business, IT, etc). From a product security perspective, cyber-security responsibility for components or systems should be clearly designated and divided among the various stakeholders (e.g. suppliers) across the whole life cycle, from the beginning of development activities until post-production.
- **Prioritisation and customisation:** A strategy should meet business objectives while protecting the most critical assets to establish trust, rather than focusing on broad or solely technology-related controls.

3. The primacy of data as a governing principle

Data is continuously growing and diversifying, and its governance has expanded far beyond privacy and regulation. The staggering influence, relevance and importance of data must be acknowledged proactively in cyber-security strategies – governing, rather than merely guiding. As we shift towards data- and platform-driven digital business models, we are surrounded by smart and personalised services. They generate and use personal information (mobility data, health statistics, financial transaction details, etc.). Building trust in those digital services is key, and data handling must be governed similarly to how we govern our analogue world.

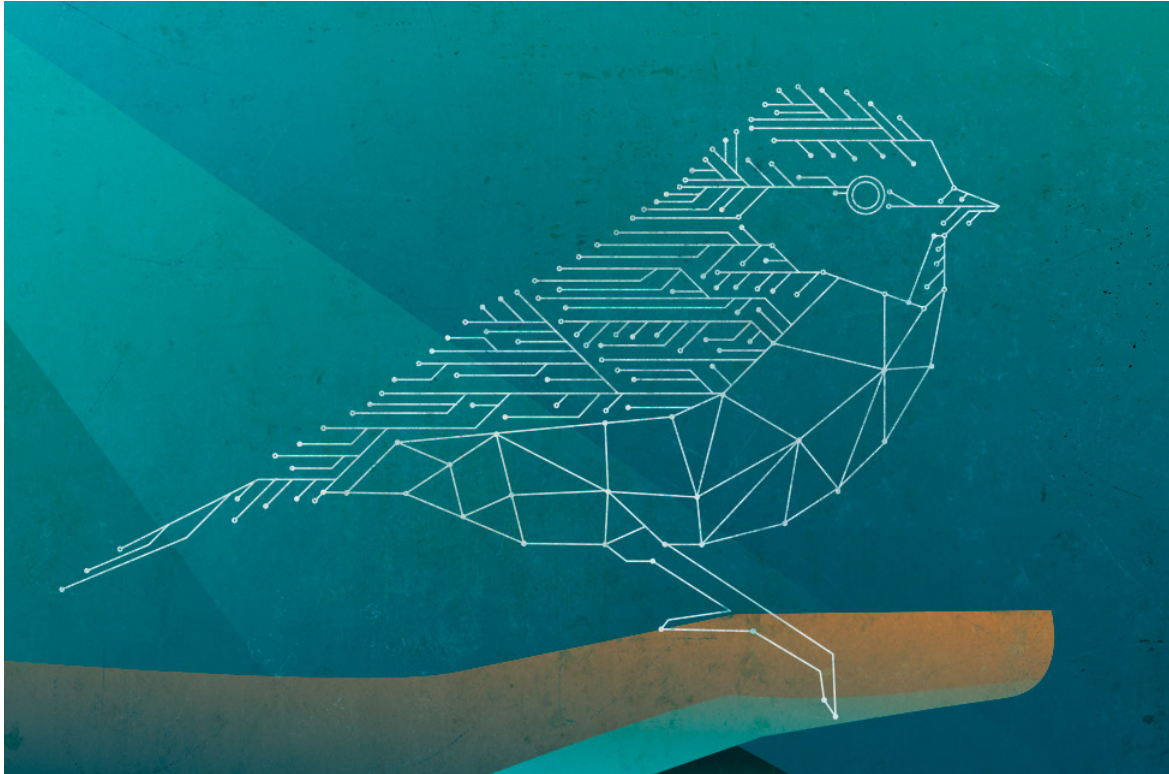
Recommendations derived from this implication for cyber-security strategies:

- **Redefinition of data life cycle management:** In the digital sphere, the life cycles of data must be rethought for application in the endlessly interconnected world – from creation to ultimate destruction/deletion – especially with regard to the ever-increasing number of interfaces and devices/tools communicating with each other.
- **Creation of framework:** Create frameworks for technical and organisational measures that will address the growing amount of data. For example, define and continuously maintain security standards in line with evolving cloud-provider capabilities and cloud usage. Also, continuously monitor compliance with security standards and enable auto-remediation, where possible. Finally, establish high-quality intelligence and monitoring capabilities (such as open-source intelligence, security operations centre or security information and event management structures) to stay vigilant and identify real threats in the digital jungle.
- **Establishment of data governance throughout the data life cycle:** From creation to deletion, governance should cover the various interfaces and consuming entities. For example, designate authorship and ownership of digital data, and define and maintain modern protection requirements for it, especially to guarantee its integrity and confidentiality. This will help build trust at all stages – from data in motion to data at rest. In addition, data transmission across the corporate boundaries should be properly governed and monitored, based on clearly defined data classification schemes (for example, public cloud).

BEYOND TRUST: ROUNDING OUT A SOLID STRATEGY

The implications discussed in this article, and the insights they reveal, mainly focus on digital trust. But 'common sense' elements must still be part of the foundation of a solid cyber-security strategy. These include:

- considering **clear strategic goals** that meet the business requirements by establishing a strategy that follows modern design principles (such as 'Never trust, always verify')
- using **agile principles** that can accommodate the fast-changing environment and adapt to ongoing disruptions and arising trends, during strategy development and implementation
- matching the company and its **risk appetite** to cyber-security demand and business objectives
- fostering a **positive, credible external reputation**; this is key to gaining digital trust, so cyber-security strategies should always help create and preserve an invincible company brand by establishing trustworthy, reliable communication and actions with all internal and external parties.



Cresting the peak: From strategy to digital trust

Day by day, cyber-security is becoming more important. However, business leaders may be overlooking its influence on clients and staff, who worry about their daily interactions with technology as attackers constantly look for new attack surfaces. Digital trust is only likely to be granted to organisations that implement forward-looking, modern cyber-security strategies.

THERE ARE A MOUNTAIN of factors affecting trustworthiness, and at the peak is the promise of a protected digital estate and a protected customer and employee relationship. Cyber-security is an enabler to reach that peak – and to ultimately support the creation and preservation of a trusted and invincible company brand. By considering digital trust's implications on long-term cyber-security strategies, and what should factor into the development process,

decision-makers and stakeholders can turn VUCA on its head. Volatility becomes vision, uncertainty becomes understanding, complexity becomes clarity and ambiguity becomes agility.

For more detailed information about the driving forces, trends and implications, including future scenarios, check out our [Future of Digital Trust study](#).

Endnotes

1. 1st Global Cyber Security Observatory, "CISO of the week, Stéphane Nappo, Société Générale", last accessed 20 July 2021.
2. Deloitte, *Future of digital trust: Driving forces, trends and their implications on our digital tomorrow*, March 2021.
3. Ibid.
4. Ibid.
5. Ibid.
6. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1, 16 April 2018.

Acknowledgements

The authors would like to thank **Max Kaiser**, **Madia Fahim** and the entire **Future Foresight Team** of Deloitte Germany for their contributions to this article.

About the authors

Marius von Spreti | Cyber Risk Leader, Deloitte Germany

Marius is a partner and leads the Cyber Risk practice of more than 200 security professionals at Deloitte Germany. Over the past 20 years, he has been contributing to transformative and innovative client solutions in various roles across all industries. As a cyber expert and business leader, he has built successful teams and has delivered services such as security strategy and risk management, cyber defence, application security, identity management, cloud security, industrial security, incident response and managed security.

LinkedIn: [Marius von Spreti | LinkedIn](#)

Franziska Biberacher | Senior Consultant in Cyber & Strategic Risk

Franziska is a senior consultant in Deloitte's Cyber Risk practice. During her time at Deloitte, she assisted in various IT risk and strategy assessments and supported several remediation programmes, especially in regards to ISO 27001, BAIT and NIST. In addition, she worked on a broad spectrum of cyber-security projects in the area of network and cloud security as well security operations. Based on her experiences, she focuses her efforts on trend sensing as well as associated technologies and methods to help clients build future-proof strategies within Deloitte's Future Foresight team.

LinkedIn: [Franziska Biberacher | LinkedIn](#)

Tim Heinlein | Manager in Cyber & Strategic Risk

Tim works as a cyber risk manager in the German Deloitte Cyber Strategy team and has been supporting clients from various industries for topics centred around cybersecurity strategy and architecture. Building on his experience, he is specialised in Zero Trust strategy and architecture and supports clients to embark on the Zero Trust journey. Prior to working with Deloitte, Tim graduated with bachelor's and master's degrees in electrical engineering and information technology from Technical University of Munich and worked in the field of software development.

LinkedIn: [Tim Heinlein | LinkedIn](#)

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.


Marius von Spreti

Partner, Cyber Risk Leader
Deloitte Germany
mvonspreti@deloitte.de
+49 89 290365999

Deloitte.

Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

 Follow @DeloitteInsight

Deloitte Insights contributors

Editorial: Sara Sikora

Creative: Mark Milward and Lewis Cannon

Promotion: Maria Martin Cirujano

Cover artwork: Traci Daberko

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.