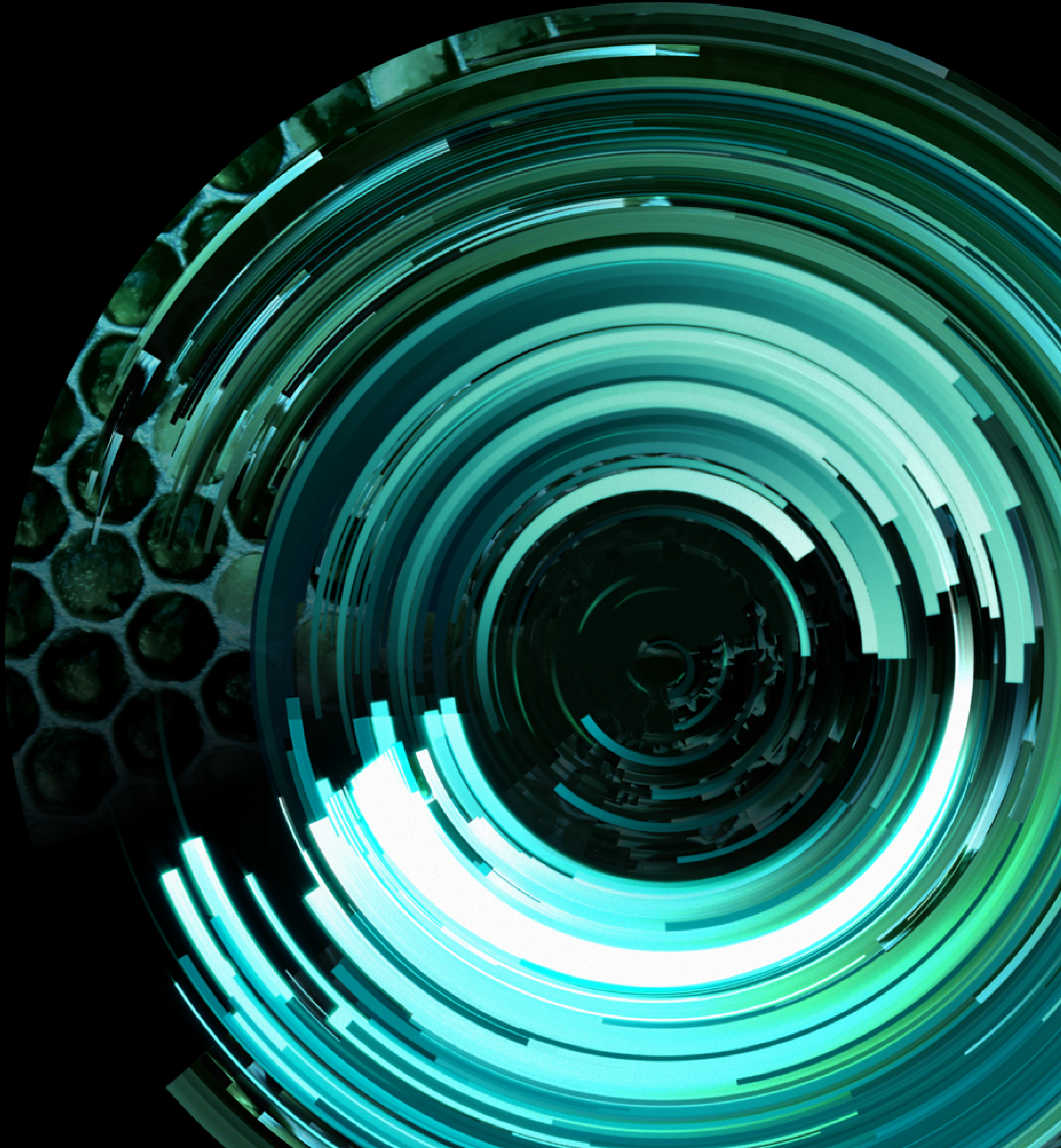
Deloitte.

Cloud Sovereignty White Paper

Unleashing the potential of sovereign cloud: A gateway to resilience and adaptability



Cloud Sovereignty

Sovereignty may take many forms and have different meanings. There is no widely accepted definition and organisations are reflecting on it through multiple perspectives depending on their business and digital context. However, the adoption of public cloud has become prevalent for every organisation as an enabler of agility and innovation, no matter which type of context, industry or region.

The geopolitical context plus global and regional crises are leading organisations to seek resilience and realise cloud value with the right balance of control and innovation. A sovereign partner ecosystem is key to accelerating business transformation without losing the autonomy and control that customers need on their data and applications.

Cloud sovereignty thus unlocks new opportunities as a safe gateway to resilience and adaptability from the cloud with greater flexibility to adapt to changing requirements and technology advancements.

Described in full

Cloud Sovereignty can be described as the political, business and technological dimensions of data protection and data security, as well as the control of and independence from operations, data, software, infrastructure and communications providers. A sovereign cloud must combine strategy, governance and technical controls to ensure resilience, flexibility, autonomy and compliance with regulatory requirements.

Public and private Sovereignty

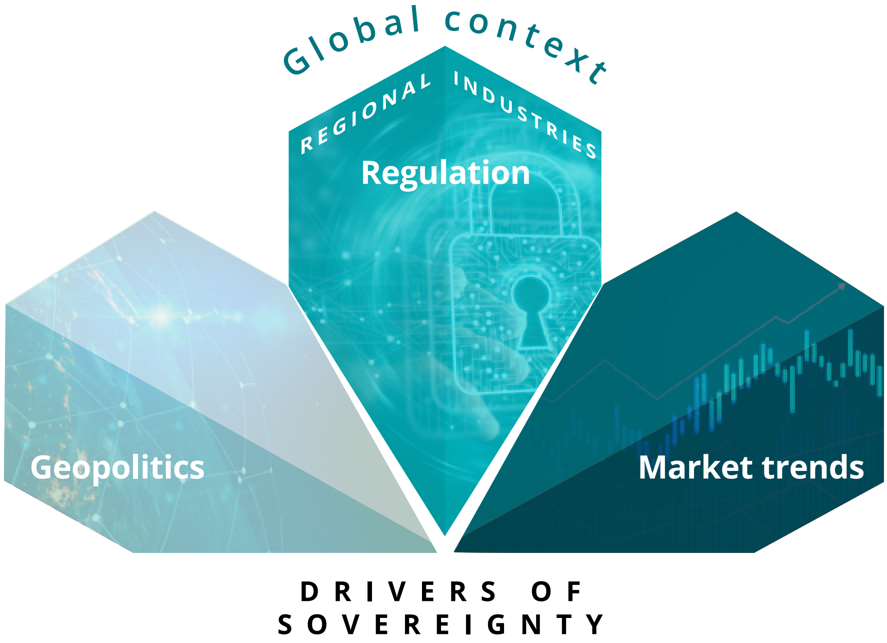
The importance of cloud sovereignty is not limited to public services but has become a top concern for private industries due to the increasing pressure from industry and regional regulators in the light of recent geopolitical events.

Sovereignty mismanagement in highly regulated industries can lead to severe consequences (data breaches, fines, brand reputation). For instance, critical infrastructure and energy, which have become more technology-driven with Industry 4.0, require stringent cloud sovereignty for operational compliance in order to prevent business disruptions.

Public and private organisations need both to maintain control over their operations and assets in the cloud to ensure productivity, resilience, and maintain their competitive advantage within a context of uncertainty.

The driving Trident for Sovereignty

Geopolitics, market and regulation shape the sovereignty requirements of organisations. The sovereignty posture of each one reflects their strategy to address their unique challenges that need to be overcome along the Cloud adoption.



Geopolitics

Global & regional crises have shown vulnerabilities when relying on key products from foreign countries or materials or components depending on enhanced supply chain resilience

European Union: Strategic autonomy has become a top priority for the EU due to commercial tensions with China and the US

US Cloud Providers: US-based multinational cloud providers might impact Operations for certain companies with Russian interests in response to the Russia-Ukraine war

Regulation

Data protection of citizens has become a focal point for regulators. This can be seen through regulations like GDPR, CCPA, PIPL, or PDPB

European Court decisions: Schrems II ruling by the European Court invalidated the use of the EU-US Privacy Shield

The US new regulations: US CLOUD Act may allow the US law enforcement to subpoena data stored in non-US regions. The UK has already engaged in an Executive Agreement to facilitate this

Market trends

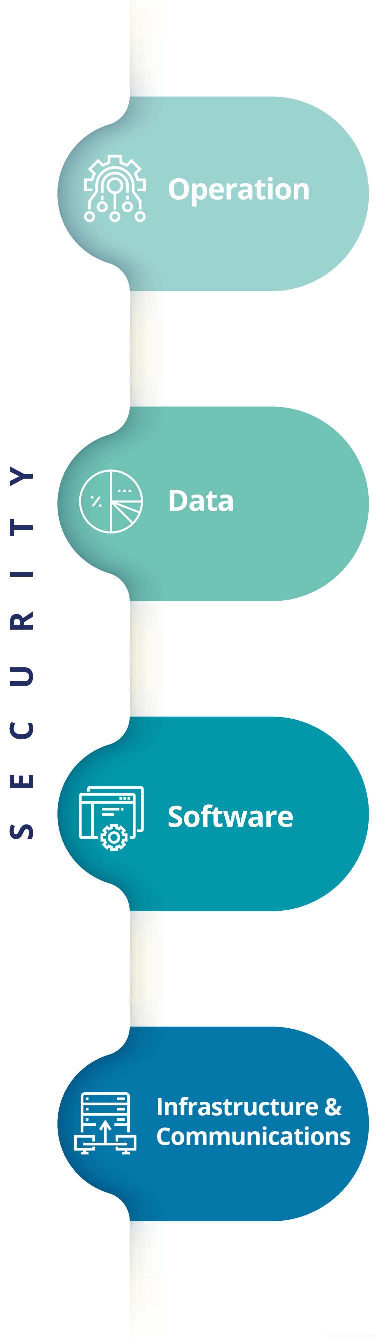
Data ecosystems can facilitate opportunities such as extending the partnership along the value chain and build vertical marketplaces

New challenges for Cloud buyers have raised related to management of sovereign IT policies, enforcement, and security across vendors either for public, local or on-premise

Mainframe modernisation: the mainframe continues to offer a compelling value proposition with new use cases that require data sovereignty along the hybrid cloud-edge continuum (Analytics, IoT)

Assessing Sovereignty

In order to evaluate technical cloud sovereignty in organisations, Deloitte has developed a comprehensive framework that covers the entire cloud stack and includes five distinct domains. This framework is applicable to organisations across all industries, including public and private sectors, and can be used to assess an organisation's level of maturity in cloud sovereignty.



Operational Sovereignty

Visibility and control over provider operations. Prevent unauthorised access to data through monitoring and controlling IT services, as well as the underlying configuration to deliver and operate securely and effectively cloud services.

Examples

Sovereign public clouds, resilience frameworks, sovereign landing zones.

Data Sovereignty

Ability to maintain control over data, including where and the way it is stored, how it is protected and processed, and who has access to it. Organisations can only achieve full data sovereignty as data owner. Otherwise, they must rely on agreements with third-parties, which limit the degree of such sovereignty.

Examples

Sovereign data encryption (BYOK, HYOK), security-enabled object storage, single-tenant data flexibility, confidential computing.

Software Sovereignty

Ability to operate and orchestrate software or solutions independently from a manufacturer's product roadmap. This includes maintaining control over the source code, development processes, and software updates, as well as the ability to shift between platform providers.

Examples

Smart-packaging, software as an appliance, software supply chain awareness.

Infra/Comms Sovereignty

Technological and operational sovereignty over your organisation's infrastructure including data and software layers as an enabler to have full control over physical and logical access. Utilising open standards for infrastructure and communications maximises adaptability and, resilience and survivability of your IT and organisation to shift between scenarios.

Examples

Open IaaS, hybrid cloud services, Open networking, Trusted execution.

SECURITY

Cross Dimension

Overarching controls over the rest of the domains to ensure security is covered in all layers of the framework.

Examples

DevSecOps, IAM, Double Key Encryption (DKE), IDS/IPS.

Deloitte's Cloud Sovereignty Framework

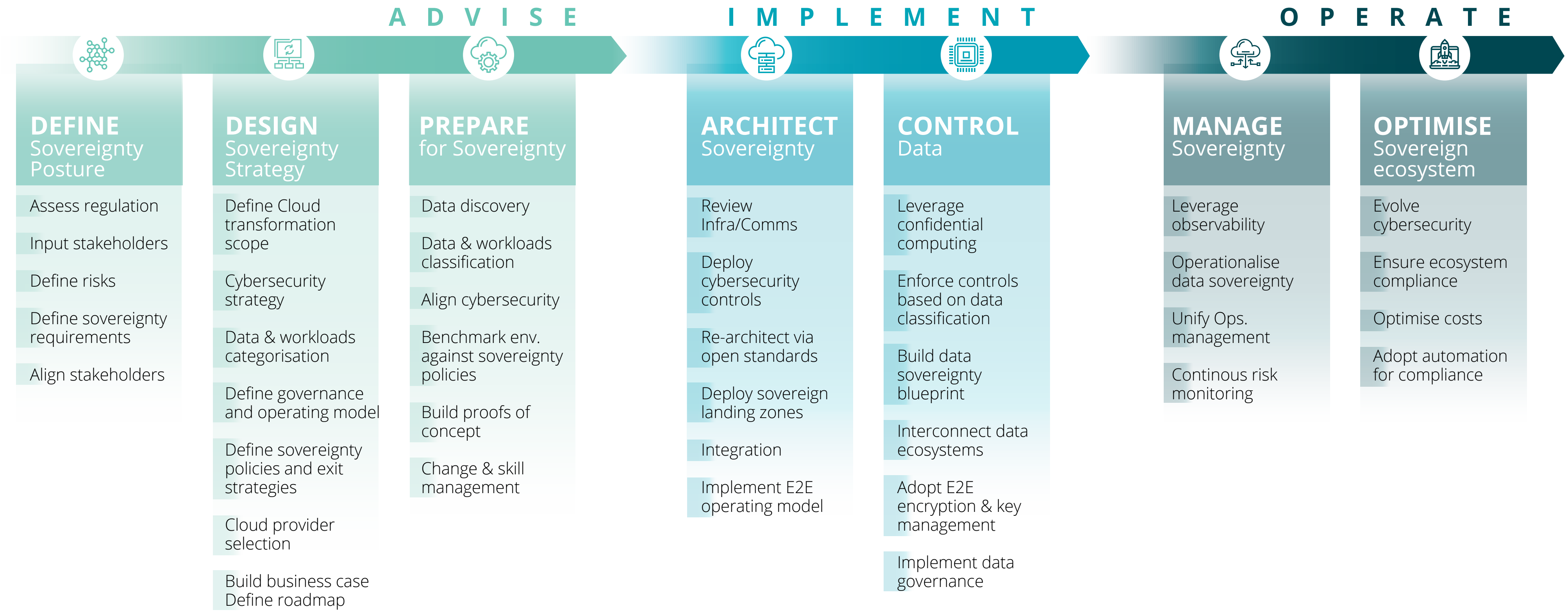
By breaking down domains into specific areas of the framework, organisations can better understand the challenges of adopting Sovereignty in the Cloud and focus investments depending on the organisation's unique sovereignty needs and objectives.

SECURITY

Operation	**Ecosystem and Governance** Ensure governance and operational sustainability in the ecosystem of cloud suppliers	**Autonomy** Running solutions effectively independently from the Cloud model and provider	**Resilience** Capabilities of adaptability to recover from adverse occurrences affecting sovereignty	**Operational Compliance** Operational monitoring over regulatory duties and vendor contracts
Data	**Control** Having legal rights and complete control over the data that you own, as well as control over data that you use	**Traceability & Observability** Ability to trace your data and monitor its usage across the entire landscape	**Sensitivity & Confidentiality** Prevent disclosure of sensitive data in correspondence to its sensitivity level	**Residence** Choose the geographical location of data and ensure it resides within jurisdiction, and restrict access through encryption when it is not possible to control
Software	**Portability** Ability to migrate workloads across different environments	**Interoperability** Platform capabilities to operate effectively across different cloud services and providers	**IP** Having software independence with open IP or in-house development and the ability to participate in market-driven innovation	**Reversibility** Ability of repatriate workloads and avoid one-way limitations of workload deployments
Infrastructure & Communications	**Compute** Use standard compute infrastructure to enable portability	**Storage** Use standard storage infrastructure to support data sovereignty, traceability and observability	**Networking** Use standards of communications and interconnectivity security features to support operational sovereignty	

The Journey to Sovereign Cloud

The Journey to mastering Cloud Sovereignty encompasses three phases for a gradual deployment beginning with the organisation's unique sovereignty posture and design of the strategy, the preparation of the architecture up to its implementation and, finally, the effective management for its continuous optimisation.



ADVISE

DEFINE Sovereignty Posture

- Assess regulation
- Input stakeholders
- Define risks
- Define sovereignty requirements
- Align stakeholders

DESIGN Sovereignty Strategy

- Define Cloud transformation scope
- Cybersecurity strategy
- Data & workloads categorisation
- Define governance and operating model
- Define sovereignty policies and exit strategies
- Cloud provider selection
- Build business case Define roadmap

PREPARE for Sovereignty

- Data discovery
- Data & workloads classification
- Align cybersecurity
- Benchmark env. against sovereignty policies
- Build proofs of concept
- Change & skill management

IMPLEMENT

ARCHITECT Sovereignty

- Review Infra/Comms
- Deploy cybersecurity controls
- Re-architect via open standards
- Deploy sovereign landing zones
- Integration
- Implement E2E operating model

CONTROL Data

- Leverage confidential computing
- Enforce controls based on data classification
- Build data sovereignty blueprint
- Interconnect data ecosystems
- Adopt E2E encryption & key management
- Implement data governance

OPERATE

MANAGE Sovereignty

- Leverage observability
- Operationalise data sovereignty
- Unify Ops. management
- Continous risk monitoring

OPTIMISE Sovereign ecosystem

- Evolve cybersecurity
- Ensure ecosystem compliance
- Optimise costs
- Adopt automation for compliance

The future of Cloud Sovereignty

Data sovereignty has always been a critical component for organisations. However, the vision of sovereignty is now expanding to integrate risks of the business and supply chain across the entire cloud stack and the partner and provider ecosystem.

To face the challenges of the hybrid-edge continuum, a comprehensive approach beyond data sovereignty that includes the lenses of operations and software is required to foster resilience and operational autonomy, regardless of the cloud environment or delivery model.

Moreover, emerging cloud technologies such as AI, machine learning, and automation will gradually play a pivotal role in enforcing sovereignty compliance and managing risks effectively to build seamless end-to-end sovereign cloud architectures.

In summary, Cloud Sovereignty is a safe gateway to resilience and adaptability that will help organisations achieve greater control over their cloud assets, improve compliance and operational autonomy while taking advantage of emerging technologies.

Deloitte believes sovereignty is a Journey that needs to be embedded in current cloud strategies, in order to revaluate the implications and to be better prepared for future events. Ultimately, we will have to design and architect for sustainable and sovereign platforms.

Contacts

Alfons Buxó
Partner
abuxoferrer@deloitte.es

Bram De Schouwer
Partner
bradeschouwer@deloitte.com

Didier Descombes
Partner
ddescombes@deloitte.fr

Andreas Schwall
Director
aschwall@deloitte.de

Alvaro Martin
Manager
amartindelvalle@deloitte.es

Sébastien Scholaert
Consultant
sscholaert@deloitte.com

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 415,000 people worldwide make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

© 2023. For information, contact Deloitte