Have you considered the legal issues that accompany the cloud?

The move to multicloud delivers many business benefits, but it also increases complexity. They include legal considerations, such as data privacy and e-discovery issues. This paper outlines an approach to mitigating legal risk.

The security of confidential data in the public cloud is seen as a significant risk by enterprises in many sectors. This nervousness goes above and beyond standard security concerns. Regulations regarding cloud computing are not standardized and do not fall under a single legal jurisdiction. Instead, enterprises face a plethora of ever-changing laws that vary between regions.

Take, for example, the Personal Information Protection Law (PIPL), which came into effect in China last year. Like Europe's GDPR regulation, it is designed to protect personal data and regulate its processing and use. Or the California Privacy Rights Act (CPRA), which comes into effect in January 2023, and will enable consumers to have the right to know, control and protect their personal information. This will include expanding breach liability.

Global reach has created governance issues

The different laws applicable across various jurisdictions are one of the big legal issues enterprises encounter with the cloud. The US Cloud Act, for example, gives law enforcement authorities the power to request access to data stored by cloud providers, even if it is stored outside the United States. On the other hand, India has followed Europe and embedded many components of GDPR into its Personal Data Protection bill.

Such legislation can be a barrier to the widespread adoption of cloud solutions in heavily regulated sectors such as health and finance. For example, the Patriot Act and the Cloud Act are seen as significant risks that could result in an organization's customers' data being compromised.

In addition, with cloud service providers now operating on such a large scale and data housed in data centers across the globe, it is often difficult for enterprises to identify the data's exact jurisdiction.

The major risks associated with cloud

While the cloud brings with it many benefits, including agility, flexibility, and scalability, it comes with risks you need to govern and manage. Organizations must fully comprehend these risks and mitigate them if they are to sleep easily regarding the cloud's unique capabilities. These include:

1. Enterprises moving to the cloud are trusted custodians of the data in their possession. They must take responsibility for handling their data without risking their own, customers', and stakeholders' reputations
2. Cyber risk through the failure of information technology systems and solutions
3. Operational risks due to failed processes, policies, systems, or events may disrupt everyday business operations
4. Legal risks include data security and liability, contractual obligations, local regulations, and data protection in humanitarian action

By 2023, 80% of organizations faced with complex global regulations will increase security compliance automation investment by 25% to ensure all policies and regulations are met consistently.[1]

orange™ Business

Determine where your data is stored

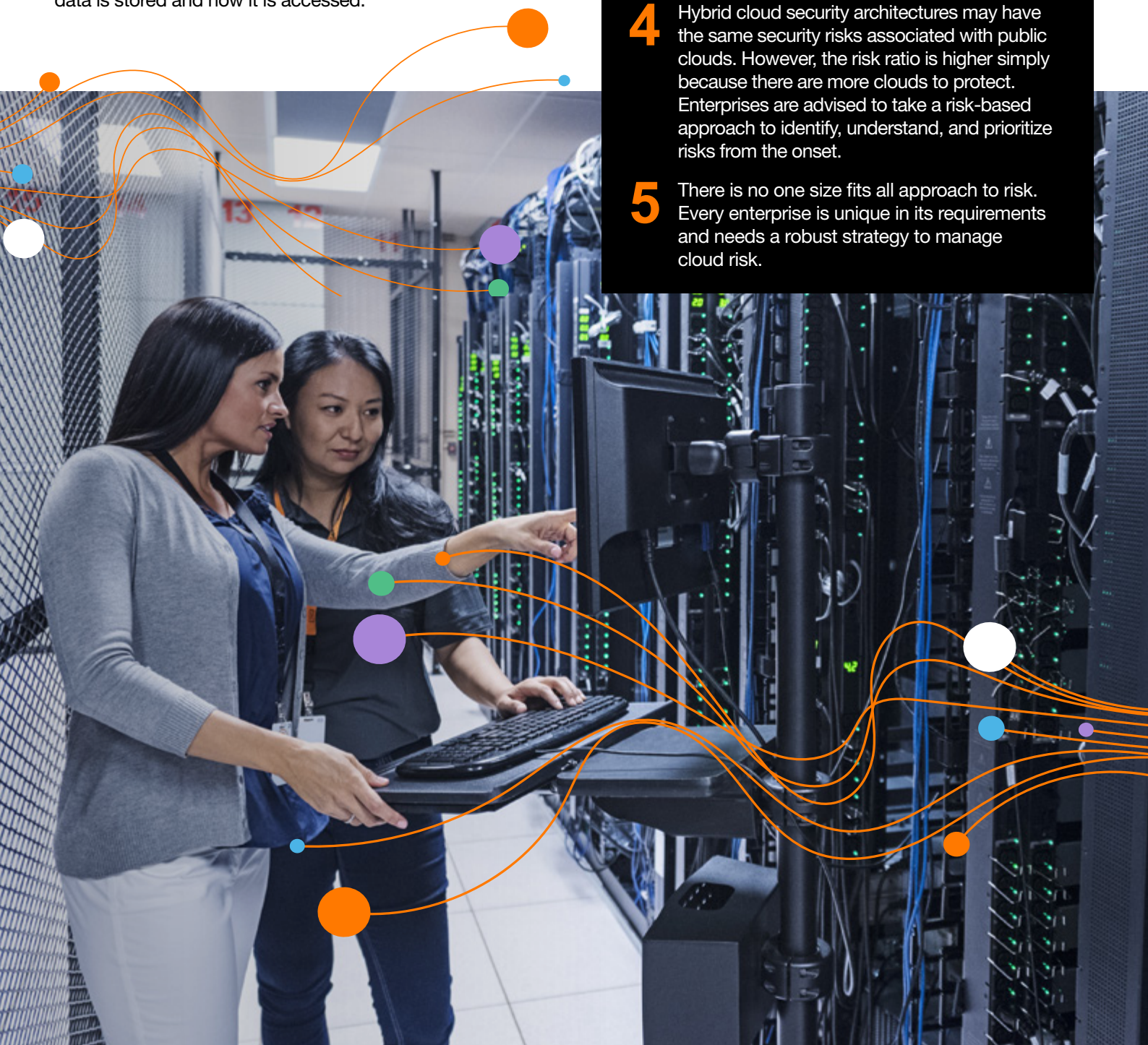
The first step in understanding your risk is determining where it is stored and what regulations will impact you. With the Cloud Act, for example, if your data is stored in the US, it is subject to the rulings of the US authorities. The Cloud Act, however, affects all organizations that engage in cross-border data storage. If your data is stored in the EU or another non-US jurisdiction, then you need to be clear that our data may be subject to future warrants and disclosure orders issued as part of the Cloud Act. In this case, companies must evaluate their cloud storage practices and implement policies and procedures to mitigate, assess and respond to US and foreign information requests.

5 steps to limiting risk in the cloud

When looking at moving data to the cloud, you must understand that while some risk management moves to the cloud service provider (CSP), accountability for the actual risk still sits firmly with the enterprise. It is therefore vital that you do a robust risk assessment and understand where all data is stored and how it is accessed.

Here are five considerations when it comes to assessing risk in the cloud:

1. Due to technical and legal factors, you must have an international view of your cloud estate as there are so many regulatory jurisdictions that may come into play. Obtain risk assessments for each cloud service.
2. Both the cloud environment and regulatory landscape is changing fast. Keeping abreast of what is happening to ensure compliance and mitigate risks is a continuous process that must be regularly reviewed.
3. Migrating any data to the cloud comes with its own unique challenges. Data should be encrypted and correct access permissions reviewed to avoid any issues. This helps to ensure data is kept secure throughout the whole migration process.
4. Hybrid cloud security architectures may have the same security risks associated with public clouds. However, the risk ratio is higher simply because there are more clouds to protect. Enterprises are advised to take a risk-based approach to identify, understand, and prioritize risks from the onset.
5. There is no one size fits all approach to risk. Every enterprise is unique in its requirements and needs a robust strategy to manage cloud risk.



Why choose Orange Business to mitigate regulatory risk in the cloud

Wherever you are on the cloud maturity scale, Orange Business can help you address the legal risks associated with operating in the cloud. These include:

Risk qualification

Our team of experts can help you quantify your level of risk. This includes the likelihood of data disclosure. For example, a customer operating in Switzerland wanted to know if any requests for disclosures had been made under the Patriot Act. We found that no requests for content data issued by the US Government have been fulfilled by AWS or Azure subsidiaries in Switzerland. From this, we could analyze if the level of risk was acceptable.

Data classification

All data must be classified before a move to the cloud is considered. While most data sits happily in the cloud, some data is not suitable for the cloud under any circumstances. This may be highly sensitive government data, for example. Or GDPR data which should be stored in the cloud in the country it was created. We can classify your data across its lifecycles to ensure it is protected in the best way possible. Workloads are cataloged and segmented accordingly where possible.

As part of this assessment, we can recommend hosting and managed services for medium to highly sensitive data classifications and provide data tagging advice.

Hybrid cloud recommendations to reduce risk

We take a solution-agnostic approach, providing our customers with the best cloud solution that best fits the regulatory landscape they are operating in. This includes the best technical mix to lower risk across regions.

Deciding which data should reside with a particular cloud provider is a huge decision and can influence your business's future success. We work with all major cloud providers, as well as specialist private and sovereign cloud providers. We have our shared data centers alongside an ecosystem of partners, to ensure you have the best cloud solution for your business while minimizing regulatory risk.

Orange Business expertise

- **15 years of experience operating private, public, and pan-European sovereign clouds**
- **8,500 experts worldwide to manage your digital transformation**
- **Specific tools and technicians skilled in connectivity, multicloud networking, and security**
- **160 countries with local sales and support**
- **24 x 7 cloud support via five major service centers across the globe**
- **Business practices with in-depth knowledge of big data and analytics, AI, ML, IoT**
- **Extensive experience in designing, building, and running digital infrastructure and cloud solutions**
- **Orange helps develop European standards, including GAIA-X and the European Commission's High-Level Expert Group (HLEG) on AI**
- **Orange Business is an AWS Advanced Consulting Partner with the AWS Direct Connect Service Delivery and the capacity to address AWS cloud transformation needs on a global scale**

We provide a modular approach to managing your multicloud estate, so you choose the services most relevant to your business needs. We can integrate, operate and support your cloud applications. Contact us here **https://www.orange-business.com/en/any-request**

1. IDC Future of Trust 2021

orange™ Business

aws PARTNER Advanced Tier Services