Cubbit

How to stay compliant in the cloud with GDPR, ISO 27001 & NIS2:

a sovereign-friendly guide for IT managers

Table of contents

Introduction

In the digital age, data universally represents the new oil, a resource whose production volume is set to triple by 2026 compared to 2021. This exponential growth represents both a great opportunity and a crucial challenge. As of today, the success of an organisation is also and especially measured by its ability to protect and prevent against external or internal threats (e.g., ransomware, cyber attacks, and various types of disasters), by its capacity to react, as well as by the risks ensuing from non-compliance with the new and increasingly complex national and European regulatory framework regarding data protection and the security of digital infrastructures.

This challenge arises particularly in highly regulated sectors such as healthcare and public administration, where the need for data protection and regulatory compliance is paramount. In addition, strategic sectors such as Defence, Aerospace and Oil & Gas have to safeguard their data assets in an ever-expanding digital frontier.

This guide is designed to assist IT managers and CIOs in tackling the complexities of data sovereignty and compliance in 2024. It aims to provide the essential knowledge and tools needed to protect organisations' data assets, considering the particularly significant challenges and consequences of this period.

The following pages explore the challenges of data sovereignty in depth, offering a detailed analysis of concepts such as data residency, data repatriation, and data gravity. Understanding these concepts is crucial to developing effective strategies that balance operational efficiency, IT security and regulatory compliance.

In the context of the regulatory landscape of 2024, the guide provides an overview of the main regulations that require attention, including GDPR, the NIS2 Directive, and the ISO 27001 standard. Each regulation is examined in detail, offering clarity on its meaning, applicability, the consequences of non-compliance, and the steps to take to address regulatory challenges.

Key Definitions

1. Digital Sovereignty

The term digital sovereignty refers to the concept whereby a country regulates and exercises governance over its digital resources, including data, infrastructure and information technology. In broader terms, digital sovereignty can include control over the internet, digital platforms, communication networks and emerging technologies such as artificial intelligence.

Digital sovereignty aims to reduce dependence on external actors and preserve national security, as well as to safeguard security and autonomy in matters related to the digital domain.

2. Data Sovereignty

Data sovereignty refers to the concept that information produced, collected, processed, converted, and stored in digital form is subject to the laws and governance structures of the country where it was generated. This aspect translates concretely into the ability to exercise control authority over the entire data lifecycle. Closely related to this concept are data security, *cybersecurity, privacy* protection, the safeguarding of sensitive information, and the implementation of measures and processes that ensure the continuous availability of information.

Understanding data sovereignty is crucial in today's digital landscape, where data is collected in one country and then transferred and processed in another. Regulatory conflicts can arise in such contexts, especially if data protection and privacy laws differ between countries.

From this viewpoint, understanding data sovereignty becomes key to ensuring secure data management, both in transit and at rest, while simultaneously complying with the applicable regulatory requirements.

3. Data Residency

Data residency refers to the physical or geographical location where data is stored, but not processed. It holds fundamental importance in data governance as it can impact the legal and compliance aspects of data storage and processing.

As countries enact regulations requiring specific data to be held within their borders, **the choice of a specific data residency is a prerequisite for compliance with data privacy and security regulations.**

4. Data localisation

Data localisation refers to the practice of storing and processing data in a specific geographical location, usually within a country or region. This practice can be implemented to comply with a law or regulation on data protection or to meet regulatory requirements that demand data be maintained within certain jurisdictions. Data localisation can impact data sovereignty as it may entail the existence of physical constraints imposed on organisations for the storage and processing of data.

This practice differs from data residency, which instead implies a strategic decision by companies to store data in a specific geographical location, often based on regulatory, performance or tax considerations.

5. Data repatriation

Data repatriation refers to the transfer and migration of data, applications, or workloads from a public cloud environment to an on-premise (local) or regional infrastructure. The concept of data repatriation also encompasses the movement of IT resources from a public cloud environment outside the country of operation to a local data centre, including on-premise facilities, local public clouds, or *colocation facilities*.

The decision to repatriate data is often determined by various factors, such as cost considerations, performance and latency issues, data governance and compliance requirements, security risks, and evolving business needs.

Data repatriation requires careful planning, assessment, and execution to ensure a smooth transition, with no disruption to business operations and no potential data loss.

6. Data Protection Regulations

Data protection regulations include, as applicable, any national, federal, European Union, state, or other privacy and data security laws or regulations. The most relevant regulation is the Regulation (EU) 2016/679, **General Data Protection Regulation *("GDPR")***. The GDPR, applicable to the personal data of those residing within the European Economic Area, has introduced a modern risk-based approach and the principle of *accountability*. In this way, the European Union aims to ensure that the free movement of personal data can only occur through lawful and transparent processing, giving individuals control over their personal information throughout the entire data lifecycle. Non-compliance with the GDPR can result in severe sanctions, including fines of up to 20 million euros or 4% of the annual global turnover if higher.

Non-compliance with data protection regulations varies according to the applicable local, national, or international laws. Some consequences can extend well beyond fines, such as legal actions, damage to reputation, loss of customer trust, loss of sensitive data, obligations to notify breaches to supervisory authorities and affected individuals, operational limitations, exclusion from public tenders, and ultimately leading to business cessation.

7. Data gravity

Data gravity describes the phenomenon where the volume of data within a specific area increases, thereby attracting more data, services, applications, and other elements. Similar to the gravitational pull between celestial bodies, large data sets act like "planets", with associated components, such as services and applications, functioning as "moons" being drawn towards them.

As the mass of data increases, other elements, applications, services, or workloads are attracted. This concept is particularly relevant in the realm of cloud computing, where the location of data can influence the design and overall efficiency of IT solutions. Hence, the question naturally arises: **how to store data in a cost-effective, secure, and compliant manner, while simultaneously extracting the maximum possible value from it?**

Indeed, while data gravity offers advantages in terms of proximity and diversity of data, it also introduces **challenges in the management of the data itself.** The accumulation of extensive data sets can increase complexity, making tasks such as data migration more complicated. Organisations must address these challenges to ensure efficient management, access, and analysis of data, resulting in a positive final impact on business operations and strategies.

Cloud compliance in 2024: where to keep an eye on for structuring an efficient and compliant data governance

1. GDPR

The GDPR was adopted on 27 April 2016, came into effect on 24 May of the same year, and has been operational since 25 May 2018. It aims to strengthen the protection of personal data of citizens of the European Union (EU) and residents, both within and outside the EU borders.

The GDPR has expanded the catalogue of rights and fundamental freedoms, raising the level of protection of natural persons with regard to their personal data, while at the same time tightening the sanction regime that for companies can amount to up to 4% of the total annual global turnover of the previous year.

In 2024, the evolution of technology, such as artificial intelligence and the Internet of Things (IoT), will certainly make GDPR compliance more complex. Enterprises will need to adapt quickly to ensure that new technologies comply with data protection regulations.

2. NIS2

On 16 January 2023, the European Union adopted a new directive on Network and Information Security (Directive (EU) 2022/2555, or NIS2). NIS2 must be transposed by the EU member states by 17 October 2024. This means that by the end of 2024, entities falling within the scope of NIS2 will be required to comply.

The NIS2 Directive complements the various European data protection and privacy regulations and guidelines, with the primary goal of enhancing cybersecurity measures, particularly in areas defined as critical.

This is achieved by expanding its scope to include a wider range of stakeholders, extending its reach to operators of essential and important services, both public and private.

Essential and important entities will be required to take appropriate and proportionate technical, operational and organisational measures to manage security risks to the computer and network systems they use in their operations or in the provision of their services, and to prevent or minimise the impact of incidents for the recipients of their services and for other services. A number of minimum measures are identified; these include the assessment of supply chain security, including security aspects concerning the relationship between each entity and its direct suppliers. There are also penalties of up to 10 million euros or 2% of global annual turnover (whichever is higher) for essential companies and EUR 7 million or 1.4% of global annual turnover (whichever is higher) for important companies.

3. ISO 27001

The international standard **ISO/IEC 27001** defines the requirements for establishing, implementing, managing and continuously improving an Information Security Management System (ISMS) within an organisation. Its main objective is to help organisations protect the confidentiality, integrity, and availability of information, while ensuring effective management of data security risks. The standard provides a risk-based approach and offers a flexible structure that can be adapted to the specific needs and size of an organisation. For these reasons, this standard is a useful tool for demonstrating *accountability* in view of GDPR *compliance* and beyond.

In the context of cloud service providers, possession of an ISO/IEC 27001 certification underlines the provider's commitment to information security, data protection and efficient management, making it an essential consideration for users. Possessing an ISO/IEC 27001 certification, although voluntary in itself, is in some sectors a minimum requirement to be able to operate, i.e. offer goods and services. This is especially true in the public administration sector.

Although non-compliance with the ISO/IEC 27001 standard does not lead to penalties per se, it can cause reputational damage, contractual liabilities, penalties related to non-compliance with the GDPR, as well as the loss of business and competitive opportunities, as we will see below in detail.

The GDPR in detail

1. What is GDPR?

The GDPR, or General Data Protection Regulation, is a European Union regulation aimed at ensuring the protection and privacy of individuals' personal data. Entering into force in May 2018, the GDPR establishes clear rules on how organisations process personal data, giving individuals more control over their data.

With the GDPR coming into force, the concept of “accountability” takes centre stage. This highlights the importance for those processing personal data to take direct responsibility for all stages of processing. Concretely, this implies that organisations must be able to clearly demonstrate and document compliance with privacy regulations, ensuring transparent and accountable management. Concurrently, new paradigms are emerging such as “*privacy by design*” and the risk-based approach, which promote the design of processes and services with privacy embedded at an early stage.

The appointment of a data controller is subject to stricter rules, together with the obligation to appoint a Data Protection Officer (DPO) in specific cases. The Regulation introduces additional obligations to provide information and request consent, ensuring greater clarity and transparency for the individuals involved.

The scope of the rights granted to the individual is broadened, emphasising the importance of giving individuals more control over their personal data. Finally, strict criteria are established for the transfer of data outside the European Union, promoting a more careful and conscious handling of information beyond EU borders.

Administrative fines are strengthened, with maximum amounts varying according to the provisions violated, prompting a tougher approach to privacy violations.

2. To whom it applies

The GDPR applies to your organisation, company or branch in two scenarios: if it is based in the EU and processes personal data as part of its activities, regardless of where the data is actually processed; or, even if it is located outside the EU, if it offers goods or services (free or paid for) or monitors the behaviour of individuals within the EU.

3. Consequences of non-compliance

Non-compliance with the GDPR can entail a number of significant risks that can affect an organisation's financial and reputational sphere. Fines can reach up to 20 million euros or 4% of global annual turnover, whichever is higher. Supervisory authorities may also impose temporary or permanent suspension of processing, directly impacting the organisation's operations.

In addition to financial penalties, civil liability represents another risk, with the possibility of facing compensation claims from individuals affected in case of violations of their rights. GDPR violations can ultimately severely compromise the organisation's reputation, negatively impacting the trust of customers, partners, and stakeholders. This can result in the loss of existing and potential customers, as well as reduce business opportunities and partnerships.

The financial impact associated with fines and legal expenses, coupled with the legal and criminal risks stemming from serious or repeated violations, further exacerbates the complexity and consequences of non-compliance. Conversely, organisations compliant with the GDPR can enjoy a competitive advantage in terms of trust and respect for privacy.

4. How to be compliant

Proper personal data management requires adherence to some key principles:

- **Lawfulness, fairness, and transparency.** The processing of personal data must be lawful, fair, and transparent to individuals concerned. Information about the processing must be easily accessible and understandable.
- **Specific, explicit, and legitimate purposes.** Personal data must be collected for specified, explicit, and legitimate purposes and must not be processed in a way incompatible with those purposes.
- **Data minimisation.** The processing of personal data must be limited to what is strictly necessary for the purposes of the processing. Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- **Accuracy.** Personal data must be accurate and, where necessary, kept up to date. Every step must be taken to ensure that inaccurate data is deleted or corrected without delay.
- **Storage limitation.** Personal data must be kept only as long as strictly necessary for the purposes of processing.
- **Integrity and confidentiality.** Personal data must be processed in such a way as to ensure security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.
- **Accountability.** The data controller is responsible for compliance with the principles and must be able to demonstrate it.

Risk assessment is an essential part of GDPR compliance as it allows potential threats to the security and privacy of personal data to be identified, understood, and mitigated.

Storing data in the cloud can be a useful, efficient, and GDPR-compliant tool, but it is essential to choose a provider that can offer certain minimum requirements:

- **Data Encryption:** The provider should offer encryption of data in transit and at rest to ensure robust protection.
- **Data Localisation:** The ability to establish the physical location of data in the EU can be crucial to comply with data protection regulations.
- **Security and Privacy Policies:** The provider should have robust security and privacy policies, including data breach management protocols.
- **Security Certifications:** Compliance with recognised security standards, such as **ISO/IEC 27001, ISO/IEC 27017** and **ISO/IEC 27018**, are indicators of the robustness of security measures.
- **Control Tools:** Provide tools that allow the user organisation to exercise proper control over the stored data and monitor its access.

By choosing a cloud service provider carefully and considering these aspects, an organisation can effectively integrate cloud data management into its approach to GDPR compliance.

ISO 27001 in detail

1. What is ISO 27001?

ISO/IEC 27001:2022 is the globally recognised standard that outlines the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). Possession of an ISO 27001 certification demonstrates that an organisation has implemented and maintains an ISMS in compliance with the standards defined by the regulation. This system extends across a wide range of aspects related to information security within the organisation. In particular, the ISO 27001 certification covers data protection, risk management, security policies and procedures, staff training, and other aspects related to cybersecurity. In summary, the ISO 27001 certification confirms that an organisation has implemented appropriate measures and practices to protect sensitive information and effectively manage risks associated with information security.

2. To whom it applies

The scope of the certification is specified during the certification process and clearly indicates which parts of the organisation and which processes are included in the perimeter of the Information Security Management System. Clearly and transparently determining what is covered by the certification ensures that it is easily understandable to all interested parties, including clients, business partners, and regulatory authorities.

The ISO 27001 certification for a cloud service provider must be designed to ensure a holistic approach to information security, addressing both physical and logical aspects, as well as including *best practices* in design, code development, and hardware management. Specifically:

1. **Physical Security:**
   - Access control to physical facilities hosting the cloud storage infrastructure.
   - Physical protection of servers, data centres, and storage devices.
   - Security of server rooms, including cooling and power supply measures.
2. **Logical Security:**
   - Design and implementation of logical access controls to ensure that only authorised users can access data.
   - Encryption of data in transit and at rest.
   - Monitoring of activities and logs to identify potential threats and breaches.
   - Implementation of cybersecurity policies and procedures.
3. **Design and Code:**
   - Software and development security: assessing and managing security risks throughout the software development lifecycle.
   - Code review to identify and correct potential vulnerabilities.
   - Secure management of credentials and permissions.
4. **Hardware Security:**
   - Assessment and management of risks related to hardware security such as protection against physical tampering of storage devices.
   - Implementation of security measures to prevent unauthorised access to hardware devices.
   - Secure management of hardware assets and storage devices.

3. Consequences of non-compliance

Non-compliance with the ISO 27001 standard can have consequences, such as:

- **Reputational damage**: Non-compliance can harm the organisation's reputation, as it demonstrates insufficient attention to information security, an increasingly critical aspect in the digital age.

- **Contractual liability**: In many cases, compliance with standards like ISO/IEC 27001 is a contractual requirement. Non-compliance could therefore lead to contractual liabilities or business losses with partners or clients who require specific security standards.

- **GDPR-related sanctions**: If the organisation processes personal data and does not meet GDPR security requirements, it could be subject to significant sanctions. Compliance with standards like ISO/IEC 27001 can help mitigate this risk.

- **Loss of business and competitive opportunities**: The absence of ISO/IEC 27001 certification could result in the loss of business opportunities and competitiveness, demonstrating insufficient commitment to information security.

In general, investing in compliance with standards such as ISO 27001 can not only help mitigate information security risks, but can also provide strategic benefits, improving stakeholder trust and the competitiveness of the organisation in the market.

4. How to be compliant

ISO 27001 certifications are issued by independent certification bodies, also known as certification entities or accreditation entities. The typical procedure for obtaining ISO 27001 certification involves the organisation that seeks certification hiring an independent certification entity to conduct an audit of its ISMS.

When considering a cloud service provider, the customer should also verify the possession of two complementary certifications that include:

- **ISO 27017 - Code of practice for information security in the cloud**: This standard provides specific guidelines for information security related to cloud services, taking into account the unique aspects and challenges associated with this environment.
- **ISO 27018 - Code of practice for the protection of personal data in the cloud**: It focuses on the protection of personal data in the cloud environment, offering specific guidance for cloud service providers that handle personal information.

NIS2 in detail

1. What is NIS2?

In January 2023, the European Union adopted the new version of the Directive on the Security of Network and Information Systems (EU Directive 2022/2055), known as "NIS2". The NIS2 Directive aims to enhance the cybersecurity and resilience of EU organisations. Member States will have until 17 October 2024 to transpose the NIS2 Directive into their national legislation. For organisations, however, the time has already come to prepare for ensuring compliance with the new directive.

The goals of the NIS2 Directive in brief:

- **Strengthening cybersecurity**: NIS2 aims to raise the collective level of cybersecurity of EU member states to address the growing cyber threats.
- **Extension of scope and uniform application**: The new Directive expands its scope to more sectors and focuses on providing guidelines to ensure a uniform transposition into the national laws of EU member states.
- **Preparation and awareness**: The involved organisations must prepare by defining a compliance path and optimising their cybersecurity awareness through the promotion of a security culture in crucial sectors, such as energy, transport, banking and digital infrastructures.

2. To whom it applies

NIS2 applies to the new categories of "*essential entities*" and "*important entities*". In the first category, Public Administrations are now included, in addition to operators in the energy, health, space, banking and financial, transport, digital infrastructure, and water sectors, unlike the previous legislation. The second category includes postal and courier services, waste management, the chemical sector, the agri-food sector, digital services, and other sectors.

In particular, the subjects, both public and private, that provide services or carry out activities within the European Union exceeding the limits set for medium-sized enterprises and operating in the "*sectors of high criticality*" identified in the list fall directly within the scope of the NIS2 Directive.

Then, by 17 April 2025, the Member States will define the list of essential and important entities, including domain name registration service providers. Subsequently, this list must be reviewed every two years and, if necessary, updated.

Essential entities will be subject to surveillance measures from the introduction of NIS2, while important entities will be subject to ex-post surveillance measures, meaning only if the authorities receive evidence of non-compliance, measures will be taken.

3. Consequences of non-compliance

Non-compliance with NIS2 entails significant consequences for organisations within its scope. Failure to comply with the directive can result in hefty fines. Essential businesses risk fines of up to 10 million euros or 2% of their total global annual turnover. Important businesses face penalties of up to 7 million euros or 1.4% of their total global annual turnover, whichever is higher. Moreover, NIS2 emphasises accountability, with management potentially held responsible for negligence or non-compliance, marking a paradigm shift in the consequences of cybersecurity failures.

NIS2 introduces stricter penalties for non-compliance:

- For **essential entities**, financial penalties can reach 10 million euros or 2% of the total global annual turnover of the previous fiscal year, whichever amount is higher.
- For **important entities**, monetary penalties can reach 7 million euros or 1.4% of the total global annual turnover of the previous fiscal year, choosing the higher amount between the two.

4. How to be compliant

Organisations will need to identify the services, processes, and critical assets that provide the services that fall under the scope of the NIS2 Directive and then identify the appropriate technical, operational, and organisational measures to protect information systems and networks by adopting a multi-risk approach.

Compared to the GDPR, the NIS2 Directive indicates in greater detail that the measures must include at least the following elements:

1. Risk analysis policies and computer system security.
2. Incident management.
3. Operational continuity and crisis management *(backup and disaster recovery)*.
4. Supply chain security.
5. Security in the acquisition, development, and maintenance of computer and network systems, including the management and disclosure of vulnerabilities.
6. Strategies and procedures to assess the effectiveness of cybersecurity risk management measures.
7. Basic computer hygiene practices and cybersecurity training.
8. Policies and procedures relating to the use of encryption and cryptography.
9. Human resources security with access control strategies.
10. Use of multi-factor or continuous authentication solutions, secure voice, video, and text communications.

This more rigorous risk management also entails defining an incident management plan to adhere to the notification process for the competent authorities. By collaborating with regulatory authorities and following industry best practices, organisations can address the complexities of NIS2 compliance, contributing to a more resilient and secure digital ecosystem.

Data sovereignty and cloud compliance: the ultimate checklist for 2024

A) Favour cloud providers offering sovereign-friendly solutions
B) Geo-fencing
C) Check compliance and certifications
D) Data durability and data availability
E) Data Protection and Management
F) Minimise vendor lock-in
G) Best practices for digital hygiene
I) Adopt an incident reporting plan
L) Customer service

A) Favour cloud providers offering sovereign-friendly solutions

Companies, especially public institutions that require secure IT systems and the protection of sensitive data and business information, should be extremely critical in choosing their cloud service provider. In this context, it is necessary to carefully examine where the headquarters and data centres of the potential cloud provider are located to determine under which jurisdiction that data may fall.

B) Geo-fencing

Carefully check the data management policies (especially regarding data movements) and the location where data is stored.

Ensure that the cloud storage providers you select offer robust geo-fencing capabilities for the area where the data is stored to align with digital sovereignty requirements. If you are an MSP, a reseller, or a distributor, this opens up new earning opportunities. You can work with healthcare, the public sector, and strategically important companies such as those operating in the defence, aerospace, and oil & gas sectors.

C) Check compliance and certifications

Adopting European services compliant with GDPR and ISO 27001, with data stored only in the EU, opens a new world of opportunities for strategic sectors where everything is (often) still stored only locally.

In our conversations with CIOs and IT managers from healthcare and strategic industries, we have found that adopting a cloud storage solution compliant with these requirements not only helps them comply with NIS2 (and avoid related fines, as well as damage to reputation and image) but also allows them to strengthen their cybersecurity by correctly applying the 3-2-1-1-0 backup rule and following all best practices to protect data from ransomware and disasters.

Moreover, be cautious about your providers' use of non-compliant third-party services and request all possible certifications and evidence. Indeed, many cloud storage providers claim to be ISO 27001 certified, but they are not 100%. They limit themselves to using ISO 27001 certified data centres: be careful in your choice before incurring unexpected and hefty fines.

D) Data durability and data availability

When it comes to data control, it is crucial to consider industry standards.

A key element to take into account is resilience. In this context, the metrics to consider include:

- Durability, a value expressing the probability that the data will not be lost, must be at least 99.999999999% (the canonical '11 9')
- Availability, a value expressing the probability that the data is immediately accessible when retrieval is attempted, must be greater than 99.9%

These standards will not only help you comply (and thus avoid fines) with GDPR, NIS2 and ISO 27001, but also improve your disaster recovery capabilities and *recovery time objective (RTO)*.

9 tips for corporate data governance

1. Check and test backups on a daily basis.
2. Use immutable storage (object lock) for protection against ransomware.
3. Always ensure that you are using a backup with versioning.
4. Adopt geo-distributed cloud storage, so that data is always available without additional costs, even if one or more locations go offline following a disaster.
5. Ensure that your data is protected by strong client-side encryption like AES-256 or end-to-end.
6. Keep a copy on offline and air-gapped storage.
7. Ensure the protection of endpoints on backups and servers.
8. Maintain multiple recovery points with backup copy jobs.
9. Apply Veeam's 3-2-1-1-0 backup rule on more than one immutable storage.

E) Data Protection and Management

Develop a robust data protection and management strategy, including data classification, access controls, and periodic audits. Adherence to the principle of least privilege (PoLP) and the implementation of IAM policy are of great help.

Additionally, implement data lifecycle management practices to ensure the relevance, integrity, and preservation of data.

F) Minimise vendor lock-in

Reduce vendor lock-in by choosing providers compatible with market standards (e.g., the S3 protocol for object storage), which facilitates data portability. Additionally, favour services designed to integrate hybrid and multi-cloud strategies. Don't be swayed by the surface-level appeal of commercial offers on the market: evaluate hidden costs such as egress fees without having to compromise on high performance between edge and cloud.

G) Best practices for digital hygiene

Data breaches and downtime can sometimes occur. In these cases, demonstrating that you have done everything possible to protect your data is crucial to avoid fines and business closure, especially when working with critical customer information.

Here are 6 crucial practices you should consider:

- Regularly train employees.
- Minimise the attack surface through the principle of least privilege.
- Apply patches to vulnerabilities in the software you use.
- Use multi-layered security (such as firewalls, antivirus, intrusion detection systems).
- Adopt unique passwords and enable multi-factor authentication.
- Implement features that enable granular access like IAM policy.

I) Adopt an incident reporting plan

Each country has specific legal requirements for reporting incidents. Therefore, you should carefully consult the official websites and check what you have to do when reporting incidents.

Consult the official websites of GDPR, NIS2, ISO 27001, and all regional laws. Additionally, contact their staff to know exactly what to do. It's better that all this is done and documented before an attack occurs.

L) Customer service

The choice of a provider should not be limited to solely assessing the product or service offered. Various reports from IT professionals increasingly highlight the importance of having a team that is expert in the field, capable of dedicating time to listening and responding promptly and in the customer's language.

It is increasingly common for large companies to provide a standardised service and adopt an impersonal and distant approach towards customers. The lack of human interaction is particularly felt in crucial moments, for example during the installation of the solution or when it is necessary to activate an emergency recovery.

For this reason, it is essential to assess the availability offered by the support team, their ability to speak your own language, and the knowledge and skills that this team has developed and can provide to its clients.

Conclusion

In the rapidly evolving landscape of cloud storage, the challenges of ensuring data sovereignty and compliance have never been so critical. With the start of 2024, organisations are facing the monumental task of navigating complex regulations, safeguarding data resources, and mitigating risks in an environment where data is both a valuable asset and a potential vulnerability.

In this brief guide aimed at IT managers, we explored key concepts such as data localisation, data residency, data repatriation, and data gravity. These concepts are fundamental for regulatory compliance and for devising effective strategies that balance operational efficiency and data security.

Navigating the regulatory landscape of 2024, we detailed GDPR, the NIS2 Directive and the ISO 27001 standard, focusing on the key aspects, purposes, scope, and consequences of non-compliance, offering IT managers solid practices to ensure data protection.

The checklist provided in this guide is a practical tool for organisations wishing to improve their data *governance* in 2024. From assessing cloud service providers based on jurisdiction and certifications to implementing geo-fencing measures and the importance of encryption, the checklist offers concrete actions to strengthen data protection strategies.

As a concluding note, organisations must remain vigilant and proactive in the face of evolving threats and the changing regulatory landscape. The importance of choosing reliable and compliant technological partners can be a fundamental choice.

In this context, Cubbit emerges as a pioneer in geo-distributed cloud storage, offering hyper-resilient and sovereign solutions in line with GDPR, NIS2, and ISO 27001 certifications. Cubbit's commitment to data security, encryption, and compliance positions it as a strategic ally for organisations intending to safeguard their data assets in the digital era.

Cubbit

About Cubbit

Cubbit is Europe's 1st geo-distributed cloud storage: hyper-resilient, sovereign, 100% S3 compatible — with no costs for egress, deletion, and redundancy.

Unlike traditional cloud storage, where data is stored in a few centralised data centres, every data saved on Cubbit is encrypted, fragmented, and replicated across multiple geographic locations within a single country or geographic perimeter — safe from ransomware and localised disasters.

The service is compliant with GDPR and **certified ISO 9001** and **ISO/IEC 27001, ISO/IEC 2017**, and **ISO/IEC 27018**.

Cubbit supports object lock, versioning, IAM policy, and lifecycle configuration features.

Thanks to its compatibility with S3, Cubbit can be integrated in a few clicks with any S3 compatible stack such as Veeam, Nakivo, and Synology, enabling **immutable** and highly secure **backup** lines.

To date, over 5,000 clients in 70+ countries rely on Cubbit, including partners, institutions, and world-renowned companies like Exclusive Networks (a European leader and cybersecurity distributor listed on the Paris Stock Exchange with $4.9B in revenue) and Leonardo (a global leader in defence and security with $14B in revenue).

If you want to learn more and discover how Cubbit can help protect your company's data and backups, you can activate a free trial with no credit card required. And if you need custom support or consulting on storage and cybersecurity topics, you can book a free 15-minute consultation.

Disclaimer and limitation of liability

Please note that the information contained in this guide is provided by Cubbit S.r.l. for informational and educational purposes only and should not be construed as legal advice or opinion, and should not be interpreted as such. We cannot guarantee that the information is up-to-date or reflects the latest regulatory developments.
For information specific to your business situation, we recommend that you seek the assistance of a professional advisor.

Registered Office: Via della Zecca 1 - 40121 - Bologna (BO) - Italy
Shipping & Meeting address: Via Altabella 17 - 40125 - Bologna (BO) - Italy

business@cubbit.io

www.cubbit.io