keepit

NIS2 and SaaS applications

Your compliance checklists for meeting NIS2's business continuity requirements

Table of contents

Your NIS2 compliance checklists for SaaS applications

Is your company a medium-sized enterprise or larger* AND falls into the group of essential entities?

If yes

This means you're part of Europe's critical infrastructure and need to comply with the NIS2 Directive. The penalties for non-compliance are severe: EU member states can give penalties of up to 10 million Euro or 2% of yearly turnover. And beyond those financial consequences, management can be personally held liable.

If no

Are you sure? Just because you're not in the EU, you may still fall under NIS2 regulations. NIS2 compliance is also relevant for organizations in the supply chain of companies working in the EU. Make sure you don't fall under its regulations if you're doing business with a European company.

Visit our website to learn more about NIS2 or...

...schedule a meeting if you'd like to see how we can help you on your journey towards compliance

**More than 50 employees and an annual turnover exceeding 10 million*

Think you still have time to comply?

EU member states need to transpose the requirements into national law by October 17, 2024

Once the law is passed in member states, the measures must already be implemented by organizations. Implementation of NIS2 requirements is an ongoing project that requires processes and changes in the organization — and that takes time.

Be proactive and get started while there's still time.

What should you do now?

Regardless of your answers, it's advisable for all companies, especially those operating within or closely related to critical sectors, to adopt robust cybersecurity measures.

The evolving cybersecurity landscape and the interconnected nature of digital services mean that comprehensive security practices are essential for resilience against cyberthreats.

To help you on your journey, here are three useful checklists for you to devise a plan of action for NIS2 compliance:

- → **Checklist for complying with Article 21**
- → **Checklist for securing SaaS applications**
- → **Checklist for choosing a SaaS data backup vendor**

Checklist for complying with Article 21

Entities must implement security measures, assess risks, and comply with cybersecurity standards

Article 21 of the directive stresses management's responsibility to prepare a cyber strategy and implement cybersecurity risk-management measures,

> "based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents."
>
> NIS2 Directive

This includes an evaluation of risk exposure and an informed decision of acceptable risk levels. With the following questions, you can verify if your organization has undergone a proper risk analysis process and documented its acceptable risk appetite.

ARTICLE 21-2(A)

Ask your organization these questions:

Policies on risk analysis and information system security

□	Have you defined organizational goals and the acceptable risk levels for your organization?
□	Have you conducted a formal risk assessment for the systems, applications, and infrastructure that support your business-critical processes? Do you know your internal and external risk factors?
□	Have you documented the risk analysis process to clearly show that management has considered risks and evaluated threats, vulnerabilities, and potential impacts?
□	Have you implemented controls to address these risks or documented risks as accepted?
□	Have you documented business continuity policies and plans to ensure your organization can maintain or quickly resume operations after disruptive incidents?

Checklist for complying with Article 21 C

Organizations can prepare for NIS2 by focusing on backup management and disaster recovery as integral components for business continuity

Article 21 of the directive explicitly mandates the establishment of "robust backup and disaster recovery plans" to ensure business resilience and business continuity. This is defined as the following:

> **A plan for managing business operations during and after a security incident. This means that backups must be up to date. There must also be a plan for ensuring access to IT systems and their operating functions during and after a security incident.**
>
> NIS2 Directive

At minimum, the best practice would be to back up vital data, create a strong disaster recovery plan, and then test these processes to know that they work as expected (meaning you have protected your business-critical data, and it can be recovered).

The following questions will help consider if you've established sufficient procedures to protect your data and have solid disaster recovery plans in place for when disaster strikes.

See check list on next page →

ARTICLE 21-2(C)

Ask your organization these questions:

Business continuity, backup management and disaster recovery, and crisis management

□ Have you mapped out all your business-critical processes and the systems and data that support them? Have you identified critical data that needs to be protected for business continuity?

□ Have you implemented backup management processes to ensure the availability and recoverability of critical data in the event of incidents and disruptions?

□ Are you confident you have backups of all business-critical data supporting critical processes — across on-premises, native cloud, and public cloud environments?

- For example, is your M365 data such as Outlook, OneDrive, SharePoint, and Teams business-critical to keep your organization running during an attack?
- What about identity systems such as Entra ID — being able to access your accounts is surely business critical?

□ Have you implemented disaster recovery plans and procedures with clear strategic prioritization of what to recover first to ensure timely restoration of operations?

□ With this plan, are you confident you can recover within agreed Recovery Time Objectives (RTOs) when an incident happens to ensure business continuity?

□ Does your disaster recovery plan specifically include your business-critical SaaS applications? (This is an area many organizations overlook, as discussed in our recent webinar.)

□ Have you established backup retention periods based on recovery objectives and compliance mandates?

□ Do you regularly test your business continuity and disaster recovery plan — at least annually — and can you document that testing occurred, as well as its results?

Testing is a key element of continuity, because with regular testing, your business ensures that data recovery is possible in the event of a real crisis — this is best practice data security and compliance in line with the NIS2 framework.

Read our comprehensive testing phase guidelines here

Checklist for securing SaaS applications

Increased SaaS usage complicates disaster recovery: Assess and secure SaaS risks per NIS2 compliance guidelines

The surge in SaaS application usage, along with the cloud data they create, has led to increased complexity in disaster recovery planning. Certain risk factors for SaaS applications need to be considered in your cyber security strategy, and you need to ensure you have secured these environments against breaches and unauthorized access.

To help provide an overview of the measures needed to protect your operations and the SaaS application data your organization relies on, these questions can help you create a risk profile per SaaS application you're using to identify the application risks and establish ways to mitigate the risks, in accordance with NIS2 requirements.

Ask your organization these questions:

Vendor risk management and compliance

□	Have you assessed the SaaS provider's security posture, incident response procedures, and compliance with relevant standards such as ISO 27001 and the NIST 800-X series?
□	Have you assessed the security of third-party integrations and APIs connected to the SaaS application?
□	Have you implemented appropriate safeguards for data exchange with third-party services?
□	Have you ensured the SaaS application complies with all relevant data protection regulations such as GDPR or CCPA?
□	Have you agreed on service level agreements (SLAs) with the SaaS provider to ensure they meet security and availability requirements, and have you included clauses for regular security assessments and audits in these?

Ask your organization these questions:

Data encryption and monitoring

□	Have you classified SaaS data based on sensitivity and criticality and implemented appropriate security measures based on the classification of the data?
□	Have you verified that data at rest and in transit is encrypted using strong encryption protocols?
□	Have you verified that encryption keys are managed securely, and access is restricted to authorized personnel only?
□	Do you continuously monitor the SaaS application to detect and respond to security threats in real time?

Ask your organization these questions:

Access control and audits

□	Have you implemented role-based access control (RBAC), limiting data access based on user roles and responsibilities?
□	Have you implemented multi-factor authentication (MFA) for accessing the SaaS application and backup management interface?
□	Do you conduct regular security audits and reviews of SaaS applications to identify and remediate vulnerabilities?
□	Do you document these audits and track findings to ensure continuous improvement of security measures?

Once you understand the risk profile of each SaaS application, you can develop a resilience strategy to comply with the NIS2 business continuity, backup, and disaster recovery requirements — assuring that the security posture for the environment is strong enough to meet your corporate needs, as well as protecting and backing up the data in those environments.

Listen to our webinar on how to create a SaaS resilience strategy

Checklist for choosing a SaaS backup vendor

Assessing your SaaS backup vendor is crucial for NIS2 compliance, ensuring data protection, and robust disaster recovery processes.

As organizations prepare to meet the stringent requirements outlined in NIS2, selecting a suitable backup vendor is key to successful compliance.

By following data protection best practices, not only do you ensure compliance with regulatory requirements such as NIS2, but you also strengthen your overall data protection and comprehensive recovery capabilities. You can use these questions to guide you during the sales process when considering a specific vendor.

Ask your organization these questions:	
Security	
□	Have you reviewed the provider's data protection policies and procedures, as well as its disaster recovery policy documentation?
□	Have you verified that the backup service complies with all relevant EU data residency regulations? Can you select the region you want your data to be stored in, and can you ensure it will never leave this region?
□	Can you be sure that the backup service complies with all relevant data protection regulations (e.g., GDPR, CCPA)?
□	Have you assessed the security posture of the backup service provider and their compliance with relevant security standards such as ISO 27001?
□	Have you agreed on SLAs that include specific metrics such as backup frequency, data retention, and restoration times? Do these include clauses for regular security assessments and compliance audits?

Ask your organization these questions:

Data backup

- □ With this vendor, can you perform regular automated backups multiple times a day to minimize potential data loss?
- □ Can you ensure that only necessary data is backed up, for example, through incremental backups, adhering to data minimization principles?
- □ Can you ensure that data is encrypted both at rest and in transit using strong encryption protocols, and are your encryption keys managed securely?
- □ Does the vendor leverage immutability as a security measure for protecting data so you can rely on your backups being complete and uncorrupted?
- □ Have you established backup retention periods based on recovery objectives and compliance mandates?
- □ Have you verified that backup retention policies meet your data retention requirements and regulatory obligations?
- □ Have you ensured off-site backups are stored in geographically separate locations to mitigate the risk of regional disasters?
- □ Do you have mechanisms in place to verify the integrity of your backed-up data?
- □ Have you assessed the physical and logical security of the locations where your backup data is stored? Does your vendor ensure separation from SaaS vendors and support air-gapping measures by storing backups on a separate infrastructure?
- □ Can you confirm that access to backup data is restricted based on user roles and responsibilities to reduce the risk of unauthorized access?
- □ Have you implemented multi-factor authentication (MFA) to access backup management interfaces?
- □ Can you monitor and log backup processes to detect any anomalies, report on them, and respond to disruptions or security threats?
- □ Can you ensure that logs of backup jobs are retained for an appropriate amount of time and are protected from unauthorized access?
- □ With this provider, can you document your regular testing of backup and recovery processes to prove compliance with NIS2 standards?

The importance of data protection and backup

A well-structured backup policy is indispensable in any organization's IT strategy, serving as a safeguard against data loss or corruption.

It provides assurance that critical data remains protected, retained, and recoverable promptly. By adhering to the best practices outlined in these questions, organizations can bolster their data resilience, uphold their commitment to data security, and navigate the complexities of compliance.

Choosing backup vendor is a critical step in ensuring compliance with the NIS2 Directive. By following the checklist of best practices outlined in this article, businesses can mitigate risks, safeguard critical data, and maintain operational resilience in the face of cybersecurity threats. As the deadline for NIS2 compliance approaches, businesses must prioritize the selection of a backup vendor that meets their specific requirements and aligns with industry best practices.

Selecting a backup vendor

A backup provider not only ensures compliance with regulatory requirements but also strengthens overall data protection efforts in today's digital landscape.

Ultimately, selecting a backup vendor is more than a compliance checkbox; it's an investment in the long-term security and resilience of your organization's data infrastructure. By considering the questions included here in a vendor selection process, businesses can mitigate risks, safeguard critical data, and navigate the evolving landscape of cybersecurity threats with resilience and confidence.

keepit

How Keepit can help

Here at Keepit, we:

- Are European born and built. Guarantee full compliance with current and future EU regulations, such as NIS2 and GDPR.
- Own and operate our infrastructure and data center regions across the globe — including two EU locations (Denmark and Germany) and locations in the UK and Switzerland.
- Ensure full data sovereignty with a no-transmission guarantee, regardless of privacy shield status.
- Deploy leading security measures, such as air gapping, immutability by default, and encryption both in transfer and at rest.
- Help you protect all your important SaaS workloads to ensure business continuity.
- Are recognized by Forrester for our significant experience with data privacy and compliance needs

Talk to us today

FORRESTER®

> *”Best fit for companies that need Microsoft 365 protection and GDPR expertise”*

Forrester New Wave™: SaaS Application Data Protection, Q4 2021