PONE BIOMETRICS

NIS2 Directive

Achieving NIS2 compliance

How the OFFPAD secures your path to conformity

January 2025

Image source: www.freepik.com

WHAT IS NIS2?

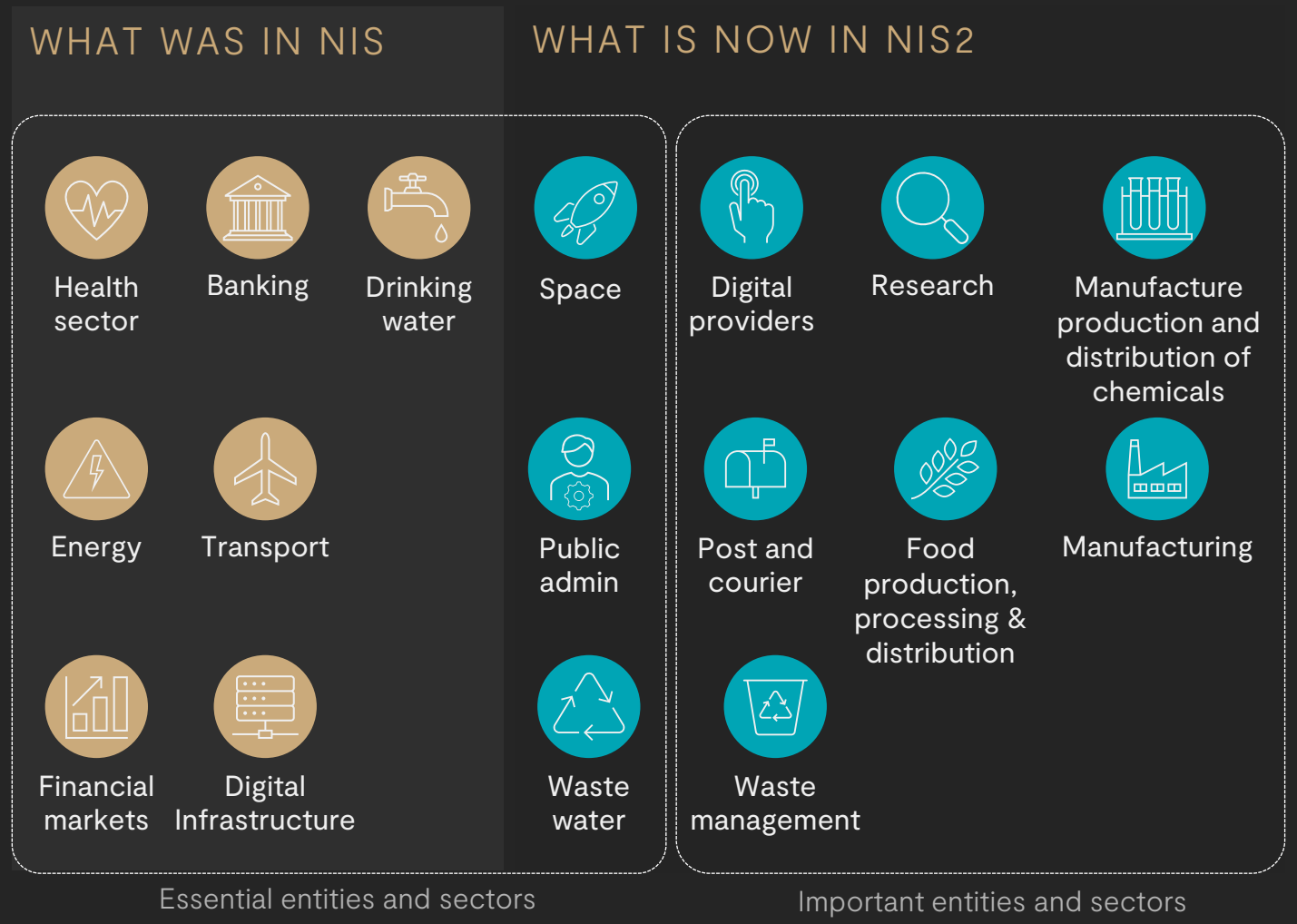
As cybersecurity threats continue to evolve, posing increasing risks to individuals and businesses, regulations are advancing to address these challenges and raise baseline security standards. NIS2 (Network and Information Security Directive 2), the latest directive from the European Union, represents a significant milestone in this effort.

A COMPREHENSIVE OVERHAUL TO STRENGTHEN CYBER RESILIENCE IN THE EU

Building on its predecessor, the NIS Directive (2016), NIS2 marks a substantial overhaul of the EU's cybersecurity regulatory framework. Its primary goal is to enhance the overall cyber resilience of member states and the organizations that operate within or engage with them.

Image source: www.freepik.com

WHAT' NEW IN NIS2?



NIS2 broadens the scope of the original directive by extending its jurisdiction to include more sectors and entities, particularly those deemed 'essential' or 'important' to the EU's internal market. For organizations falling under this expanded scope, NIS2 introduces heightened security expectations.

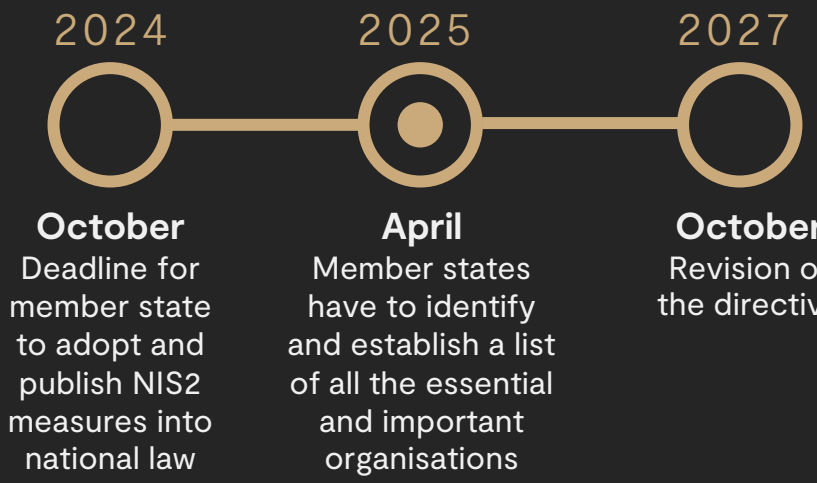


Image source: www.freepik.com

KEY REQUIREMENTS

ENHANCED SECURITY MEASURES

Organizations must implement comprehensive risk management practices and robust cybersecurity strategies.

INCIDENT REPORTING OBLIGATIONS

NIS2 mandates faster and more detailed reporting of cybersecurity incidents.

CORPORATE ACCOUNTABILITY

Businesses must adopt measures to ensure leadership accountability for cybersecurity risks.

BUSINESS CONTINUITY

A stronger emphasis is placed on continuity and resilience planning to mitigate potential disruptions.

CONSEQUENCES OF NON-COMPLIANCE

NIS2 INTRODUCES STRINGENT PENALTIES

For failing to meet its requirements, including significant fines and the risk of litigation. These consequences underline the directive's importance and the need for proactive compliance.

Essential entities and sectors

10M€ or 2% turnover

Important entities and sectors

7M€ or 1.4% turnover

Non-compliance with NIS2 can result in substantial fines of up to €10 million or 2% of annual turnover for essential entities and €7 million or 1.4% for important entities. Additional costs include legal fees, operational downtime, and recovery expenses from cyber incidents. Non-compliance can also lead to lost revenue, increased insurance premiums, and significant reputational damage.

Image source: www.freepik.com

Image source: www.freepik.com

THE NEED TO BE PREPARED

A COMPLEX IMPLEMENTATION

As an EU Directive, NIS2 will be interpreted and implemented differently by each member state, creating additional complexity for businesses operating across borders. Despite these challenges, the directive's message is clear: organizations must act now to align with its requirements.

PREPARING FOR NIS2

Preparation is critical. Businesses must assess the directive's impact on their operations, evaluate their current security posture, and establish a clear roadmap for compliance. By taking these steps, organizations can not only avoid penalties but also strengthen their overall cybersecurity resilience.

OFFPAD: THE FIRST STEP TO COMPLIANCE

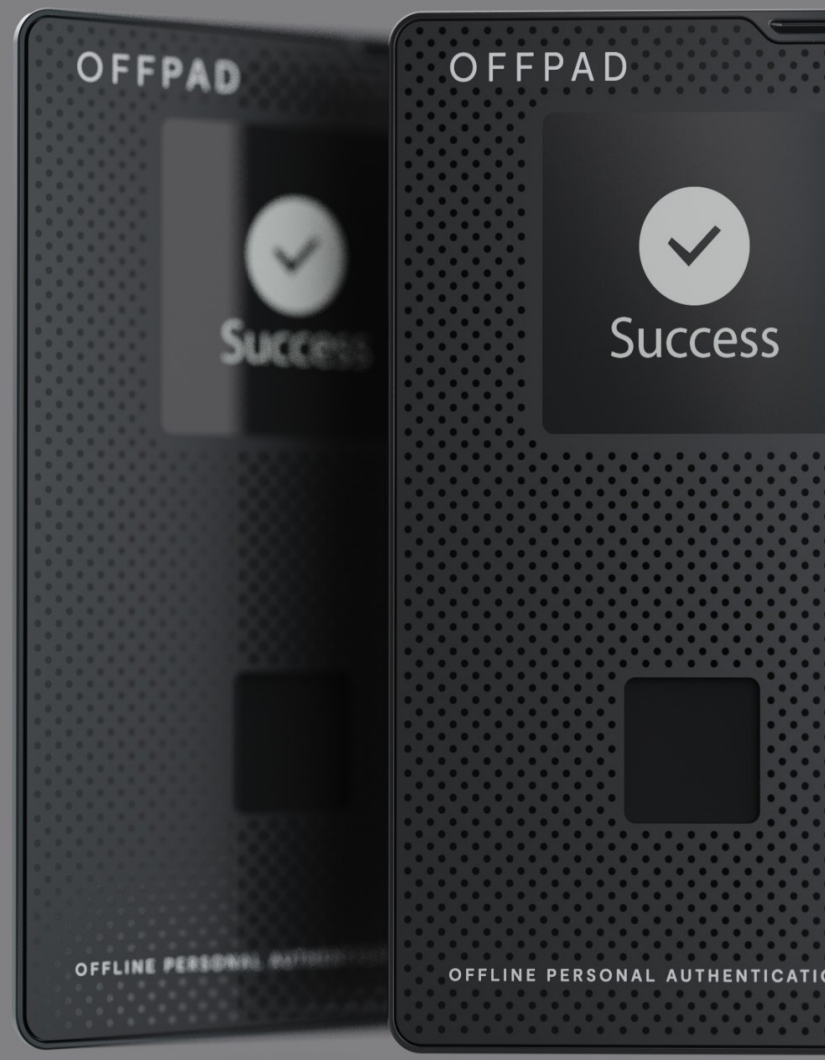
RISK MANAGEMENT AND MITIGATION
Under NIS2, organizations must adopt comprehensive risk management strategies

STRONG ACCESS CONTROL
NIS2 mandates robust access control mechanisms to prevent unauthorized access to critical systems and data.

INCIDENT PREVENTION AND RESPONSE
NIS2 requires organizations to prevent and respond to cybersecurity incidents effectively.

AUDIT READINESS AND ACCOUNTABILITY
NIS2 emphasizes corporate accountability and audit readiness for cybersecurity practices.

FLEXIBILITY ACROSS IT ENVIRONMENTS
It ensures organizations can implement strong MFA across all platforms, supporting the scalability and standardization NIS2 requires



SIMPLIFYING NIS2 COMPLIANCE WITH SECURE AND ROBUST AUTHENTICATION

Enhance security, prevent breaches, and ensure compliance with NIS2 through biometric multi-factor authentication and seamless integration.

THE ULTIMATE DEFENCE AGAINST CYBER THREATS & NIS2 COMPLIANCE

UNBREAKABLE AUTHENTICATION

Ditch passwords and weak SMS codes. OFFPAD delivers passwordless security that can't be intercepted, ensuring only you can access your accounts.

EFFORTLESS SECURITY

No more password struggles or complex app setups—just plug in your OFFPAD, touch to authenticate, and you're in.

UNIVERSAL COMPATIBILITY

One key for all your devices! OFFPAD works seamlessly across Windows, macOS, Linux, and major browsers and services like Google, Microsoft, and GitHub.

PRIVACY FIRST, ALWAYS

Your personal data stays yours. OFFPAD stores no personal information—only encrypted keys and biometrics, which never leave the device.

ULTIMATE PHISHING PROTECTION

Say goodbye to phishing threats! OFFPAD only authenticates legitimate websites, keeping hackers locked out—even if they trick you into visiting a fake site.