econocom
asystel – bdf – bizmatica

Complidoo Vs NIS2

just switch

CONFIDENTIAL DOCUMENT

GET SOLUTION

NIS2

The Network Security Directive (EU) 2022/2555, called NIS2 (Network and Information Security) became law across the European Union in October 2024, imposing strict cybersecurity responsibilities on numerous large and medium-sized enterprises and other organizations of national importance.

As a directive, it must be implemented by the member countries of the European Union, through an implementing decree, which the Italian government adopted in September 2024.

The new regulatory framework reinforces what was already provided for by the previous NIS framework, which is therefore repealed, maintaining the following obligations for Member States:

- definition of a national cybersecurity strategy
- designation or establishment of one or more competent authorities responsible for cybersecurity and supervisory tasks
- designation or establishment of multiple competent authorities responsible for managing large-scale cybersecurity incidents and crises
- designation or establishment of one or more CSIRTs

Scope

The NIS2 Directive applies to public or private entities operating in essential and important sectors, as listed in Annexes I and II of the Directive, and which are considered medium-sized enterprises or exceed the thresholds for medium-sized enterprises.

A medium-sized enterprise is defined as:

- employing between 50 and 250 people,

and

- having an annual turnover not exceeding 50 million euros, or an annual balance sheet total not exceeding 43 million euros.

Scope

Among the sectors to which NIS2 applies in the ICT field are the following:

- ICT service management (business-to-business)
  a) Managed service providers
  b) Managed security service provider

- Digital infrastructure
  a) Internet Exchange Point providers
  b) DNS service providers, excluding operators of root name servers
  c) TLD name registries
  d) Cloud computing service providers
  e) Data centre service providers
  f) Content delivery network providers
  g) Trust service providers
  h) Providers of public electronic communications networks
  i) Providers of publicly available electronic communications services

Pega is among these entities as a provider of cloud computing services.

Jurisdiction

Although Pega does not have a physical presence in Italy, it falls within the scope of NIS entities because the regulation applies also to those entities that, while not established within the EU territory, offer services within it.

Such entities are therefore required to designate a representative in the Union, established in one of the Member States where their services are offered and subject to the relevant jurisdiction.

In the absence of such designation, the competent national NIS authority may initiate legal action against non-compliant entities.

Principles and obligations

The Directive imposes specific obligations and responsibilities on essential and important entities in order to enhance the level of security and resilience of the organization and, consequently, of the Country “system” as a whole.

- Organization registration and data update
- Accountability of management bodies
- Risk management, including supply chain risk
- Training and awareness
- Incident notification
- Adoption of cybersecurity measures

INFORMATION SECURITY

econocom
asystel – bdf – bizmatica

How to

It is therefore necessary for NIS entities to plan the activities required to establish a system for managing security and incidents, bearing in mind that the security of an information system cannot be achieved by considering only technological aspects, but also organizational and physical ones.

The management system must include requirements aimed at:

- identifying and managing the risks to which the organization is exposed
- defining roles and responsibilities, including those of top management
- managing resources, including training
- managing relationships with suppliers and customers
- handling security incidents
- managing business continuity
- defining appropriate security measures to be implemented
- establishing an audit program
- defining a management review process

PRESENTATION OF THE SOLUTION

econocom

asystel – bdf – bizmatica

Our solution for centralised management of compliance and risk

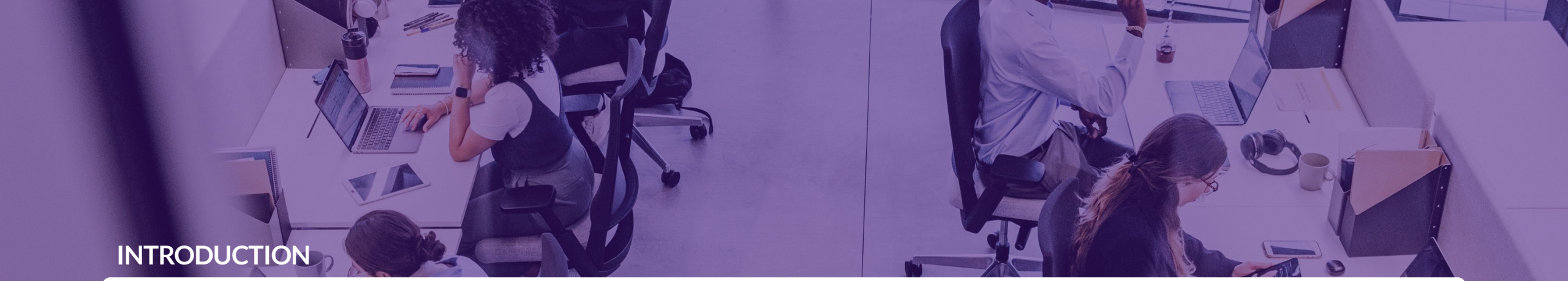
The collaboration between **GetSolution**, and **Asystel-BDF** gave birth to Complidoo, *an innovative, integrated, modular and scalable application* that supports companies in the proper management of GRC processes.

Complidoo

Governance, Risk and Regulatory Compliance Management for Italian companies

- Why a GRC platform is a strategic choice for companies ?

Complidoo



INTRODUCTION

In a world where **information** is the most valuable asset and **digitalization** is constantly on the rise, companies are faced with an **increasingly complex regulatory landscape**. Information security, risk management and regulatory compliance are **not only an obligation, but also a strategic lever** to build and maintain trust with customers and partners. Compliance with current regulations, both national and international, becomes a challenge that requires **careful management and constant monitoring**: new risks emerge every day as regulations evolve.

In Italy, companies of all sizes are confronted with stringent regulations, from the **GDPR to the recent NIS2 directive**, to avoid penalties that can severely affect not only budgets but also reputation. This white paper explores how **Governance, Risk & Compliance (GRC)** platforms can respond to these challenges, providing an **agile and integrated tool** to ensure high quality processes and robust protection against operational and reputational risks.

Regulatory context

Italian companies, like their European counterparts, face a **regulatory patchwork** covering areas such as data protection, IT security, quality management and consumer protection. Among the main regulations in this area are:

GDPR (General Data Protection Regulation) - It regulates the management and protection of personal data, requiring companies to demonstrate transparency and maintain strict control over how they collect and process data.

NIS2 *(effective from October 2024)* - Introduced to strengthen cybersecurity resilience in critical infrastructures, it imposes security standards to counter growing digital threats, extending responsibilities to a wider number of sectors and introducing more incident reporting requirements.

DORA (Digital Operational Resilience Act) - It imposes cyber resilience requirements on EU financial institutions to prevent and manage digital operational risks, including vendor controls and incident reporting

AI Act (Artificial Intelligence Act) - regulates the development and use of artificial intelligence (AI) in the EU, ensuring that AI is safe, respects fundamental rights and promotes user trust.

Regulatory context

There are also a number of international standards that companies choose to adopt as a means of ***accountability*** against security, quality and business continuity requirements, such as:

ISO 27001 (Information Security Management) - International standard setting requirements for information security management systems, applicable to all types of organizations.

NIST Cyber Security Framework (CSF2.0) - is a set of standards, guidelines and best practices to help organizations manage and mitigate cyber risk.

ISO 22301 (Business Continuity Management) - Represents an international standard for preventing, managing and recovering from business disruptions, ensuring business resilience and continuity of essential services.

ISO 9001 (Quality Management System) - It represents an international standard for quality management systems, guiding companies to improve processes, customer satisfaction and operational efficiency

The mentioned certificates not only help companies **to demonstrate compliance** with European **regulations**, but also **strengthen their credibility** by assuring customers and partners of high standards of data and critical infrastructure protection.

The situation of Companies:

- **Lack of integrated tools** to manage compliance with various regulations (NIS2, GDPR, DORA...)
- **Lack of specialised and up-to-date skills** in the areas of cybersecurity, risk management and regulatory compliance, indispensable for dealing with complex regulations (NIS2, GDPR, DORA...)
- **Overload of compliance functions** to gather the necessary information due to the difficulty in finding the information and disjointed approaches

Hotspot

The difficulty of regulatory compliance

Complying with regulations represents a real organizational, economic and operational commitment. The main difficulties arise not only in achieving the required compliance but even more so in **maintaining the processes and procedures described**, which must be continuously updated. Coordinating the requirements of several regulations can lead to **inefficiencies, administrative burdens and an increased risk of error**.

Each procedure must be documented accurately and easily accessible, **requiring time and res**ources, especially in the absence of **appropriate technological tools**.

Hotspot

The difficulty of regulatory compliance

To comply with regulations such as **GDPR** or **NIS2** and maintain certifications such as **ISO 27001** or **ISO 22301**, companies need to **consolidate processes** and define **roles and responsibilities** within **governance** activities.

What are the critical aspects for companies?

- **Gathering all the information** necessary for adaptation and **sharing** with all the functions involved
- Have an **integrated methodological approach**
- **Continually monitor risk** and **develop risk management plans** that also consider threats from **suppliers and partners** along the supply chain.
- **Ensure effective management of security incidents**, with timely notifications to regulators in the event of violations.

Hotspot

The Consequences of Non-Compliance

The penalties for non-compliance are significant and can have a devastating impact, **both in economic and reputational terms.**

Companies that do not comply could face fines of up to 4% of global annual turnover or up to EUR 20 million.

This makes compliance not only a matter of protection, but a reputational and economic necessity.

To prevent possible penalties, companies must adopt a **structured and proactive approach** to IT security and compliance management.

The GRC platform: the solution for centralizing compliance and governance

A GRC (Governance, Risk and Compliance) system is a platform that supports companies in the integrated management of corporate governance, risk mitigation and compliance with regulations and standards, both internal and external.

Designed to improve efficiency, reduce costs and centralize the management of critical areas, a GRC system is the ideal solution to address the requirements imposed by various regulations and certifications.

Thanks to their modular structure, the system can be adapted to the specific needs of the company, reducing the need for manual checks and minimizing errors.

Companies' needs to manage Compliance and Governance aspects

1. Having a solution capable of centralizing all the regulatory requirements to be put in place through an integrated approach

2. Organize fulfilment management through guided procedures, distributing specific tasks to resources

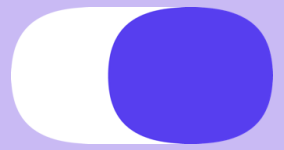
3. Automatically compile documentation to be produced

4 Digitalizing evidences of fulfilments

5 Centrally store the information and documentation produced, making it easier to use and faster to access

6 Monitoring the progress of all actions undertaken

7 Empowering certain corporate functions with regard to regulatory compliance



DEMO Solution

Our solution for centralised management of compliance and risk

Complidoo offers **systemic support** to the organisation and effective and efficient management to **govern the risk** associated with business operations and the complexity of regulatory requirements and the associated data pool, necessary to **ensure compliance** with the various regulations, while allowing **integration with the various management** systems adopted by the company, and managing in parallel any specificities of the present application context. For companies, it represents the ideal tool for corporate governance; in fact, thanks to the **relationship between its modules and an interdisciplinary approach**, it is possible to adopt an integrated management system.

Complidoo is an innovative solution that includes:

- The distribution of activities between the different business functions by sending tasks to the different users
- Collaboration functionality to facilitate user activities
- Automating processes by reducing human error and accelerating the process itself
- The ability to collect and analyse risk and compliance data in a single platform, providing greater visibility and control
- the possibility for companies to stay up-to-date with changing regulations and quickly adapt their internal policies
- Monitoring of ownership and deadlines through customisable dashboards
- Different service delivery modes, including SaaS or On Premises management
- High customisation possibilities for specific company needs
- The possibility of integration with other systems already present in the company, extending functionality and streamlining the information flow

Baseline

- **Data Protection**
- **Resource Management** Module
- Definition of **Security Measures**
- **Supplier Qualification** Module
- **Monitoring & Auditing** Module
- **Risk Management** Module
- **Incident Management** Module
- **Corrective Actions/Warnings Management** Module

Complidoo

GRC System

Additional modules

- Document Management Module *(Archive and LTA)*
- **RdC Management** Consulting
- **Contract Management** Module
- **Communication Management** Module
- **Service Desk** Management Module
- **Cyber Security** Management Module
- **OnBoarding** Module
- **Ondemand** service

Complidoo

GRC System

The advantages of Complidoo: a winning strategy

1. It **simplifies the management of regulations**, making the compliance process more efficient and less complex.

2. It represents a **strategic opportunity** to improve efficiency and operational security.

3. Provides **continuous and proactive monitoring**, reducing compliance risks and strengthening corporate resilience.

4. Protects the company from unexpected costs and reputational threats by ensuring constant control.

5. Optimizes company resources, limiting manual checks and increasing the speed and accuracy of compliance processes.

6. Strengthens the trust of customers and partners, positioning the company as responsible and trustworthy through secure information and transparent processes.

7. Allows the company to **focus on core activities**, with systematic and effective compliance management.

8. It **generates detailed reports and audits on demand**, providing companies with all the data they need to prove their compliance in the event of inspections or requests by authorities. These tools also facilitate the **automation of incident reporting procedures**, as required e.g. by NIS2, reducing response times and ensuring regulatory compliance.

Q & A

Complidoo

Thank you

econocom

asystel – bdf – bizmatica