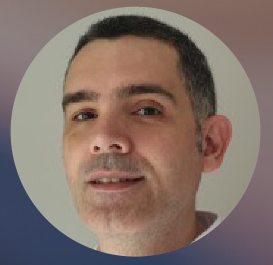
InfoBrief, sponsored by Insight | October 2024

NIS2: What Is Your Deadline?



Matthew Wilkins
Research Director,
European Services

Milan Kalal
Senior Research Manager,
European Services

Richard Thurston
Research Manager,
European Security Services

Dominique Bindels
Consulting Manager,
Custom Solutions Europe

In This InfoBrief

The NIS2 directive significantly broadens the scope of its predecessor, imposing stricter requirements across more sectors and placing risk management at the forefront of CEOs' agendas. Despite high general awareness, detailed knowledge of NIS2 remains limited, leading to slow progress and a lack of board engagement. European organisations face readiness gaps and consistent challenges across industries, exacerbated by policy variations and human factors. The directive necessitates a cultural shift and highlights the often-neglected impact on skills. Consequently, demand is growing for external partners, with service providers being the preferred choice to ensure compliance. The delivery of effective security strategies and stakeholder buy-in are essential for successful engagement.

This InfoBrief, sponsored by Insight, explores the awareness, status, and challenges of European organisations in response to the European Union's NIS2 cybersecurity directive. Together with Insight, IDC assesses organisational awareness and readiness for compliance, the impact of human factors, and the role that external partners can play in assisting organisations on their NIS2 compliance journeys.

Table of Contents

CLICK BELOW TO NAVIGATE TO EACH SECTION IN THIS DOCUMENT.

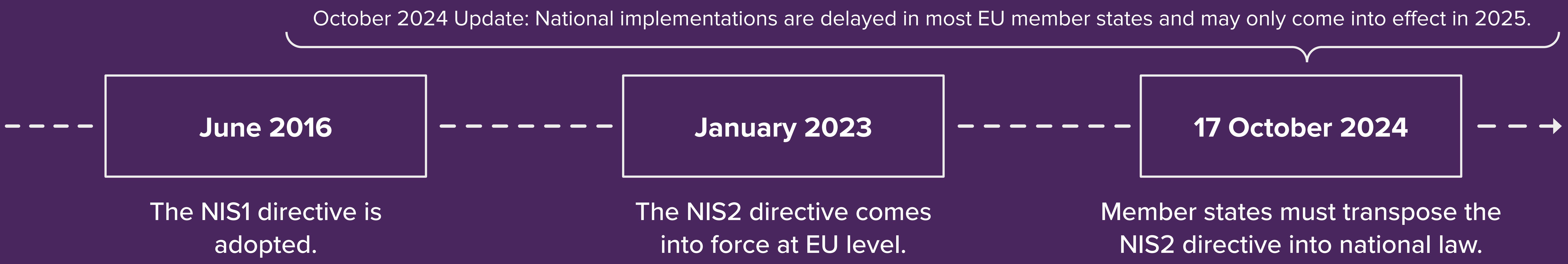
NIS2: What, When, and Where?

The EU Network and Information Security II (NIS2) Directive

What?

- Aims to strengthen cybersecurity risk management and resilience across European Union (EU) critical infrastructure
- Replaces and modernises the existing NIS1 directive
- Now applies to organisations with 50+ employees or more than €10m in annual turnover
- Increases scope from 7 to 18 sectors
- Applies to entities that provide certain critical services or critical infrastructure
- Defines two categories of entity: Essential and Important

When?



October 2024 Update: National implementations are delayed in most EU member states and may only come into effect in 2025.

June 2016

The NIS1 directive is adopted.

January 2023

The NIS2 directive comes into force at EU level.

17 October 2024

Member states must transpose the NIS2 directive into national law.

Where?

- The directive will apply to organisations based in the EU that conduct business inside the EU.
- It will also apply to organisations not based in the EU but that conduct business in the EU.
- Non-EU organisations that do not offer services in the EU are not directly affected by NIS2.

Noncompliance

Noncompliance with the NIS2 directive can result in severe financial penalties, with essential entities facing significant fines. Additionally, management bodies are held accountable for implementing cybersecurity measures and can be personally liable for any failures to comply.

Source: IDC, 2024

NIS2 Has a Broader Scope Than the First NIS Directive

- Increases scope from 7 to 18 sectors
- Applies to entities that provide certain critical services or critical infrastructure
- Defines two categories of entity: **Essential** and **Important**

Essential Entities

- Transport
- Banking
- Financial Markets
- Health Sector
- Public Admin
- Digital Infrastructure
- Energy
- Drinking Water
- Space
- Waste Water

Important Entities

- Digital Providers
- Chemical Manufacture/ Distribution
- Research
- Food Production/ Distribution
- Post & Courier
- Manufacturing
- Waste Management

Additional Sectors in NIS2

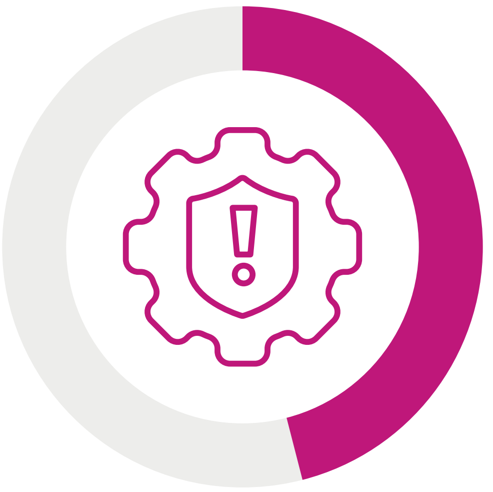
Size threshold: 250 or more employees or more than €50 million annual turnover

Size threshold: 50 or more employees or more than €10 million annual turnover

Source: IDC, 2024

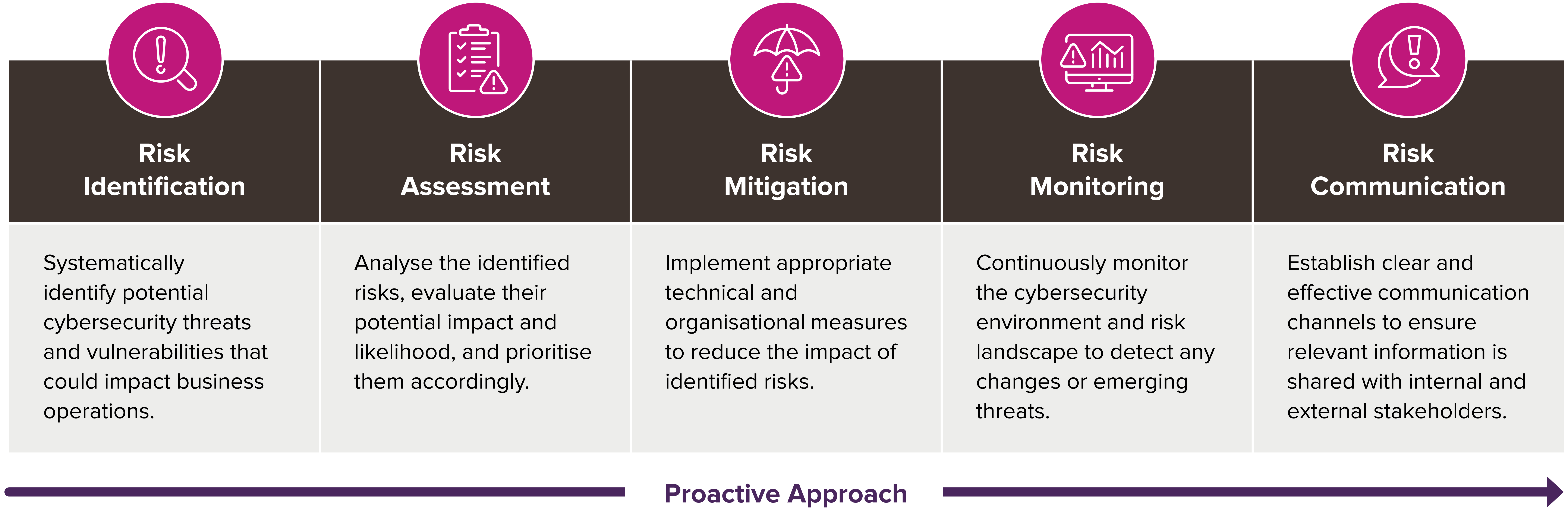
Risk Management Is at the Top of the CEO Agenda

With half of European CEOs citing improving their organisation's risk management posture as their No. 1 priority, risk clearly has the attention of the C-suite. By proactively identifying and mitigating risks, CEOs are striving to ensure business continuity and resilience in the face of uncertainties. Cybersecurity is a manifestation of business risk, one tasked with safeguarding an organisation's assets, reputation, and long-term viability — as threats constantly evolve. Effective risk management in cybersecurity involves not only protecting sensitive data and systems from breaches but also preparing for potential incidents to minimise impact. Integrating risk management with cybersecurity strategies enables CEOs to make informed decisions, allocate resources efficiently, and maintain stakeholder trust.



46%

of European CEOs see improving **risk management posture** as the No. 1 priority



Risk Identification

Systematically identify potential cybersecurity threats and vulnerabilities that could impact business operations.

Risk Assessment

Analyse the identified risks, evaluate their potential impact and likelihood, and prioritise them accordingly.

Risk Mitigation

Implement appropriate technical and organisational measures to reduce the impact of identified risks.

Risk Monitoring

Continuously monitor the cybersecurity environment and risk landscape to detect any changes or emerging threats.

Risk Communication

Establish clear and effective communication channels to ensure relevant information is shared with internal and external stakeholders.

Proactive Approach

Source: IDC, 2024

General NIS2 Awareness Is High, But Detailed Knowledge Is Not

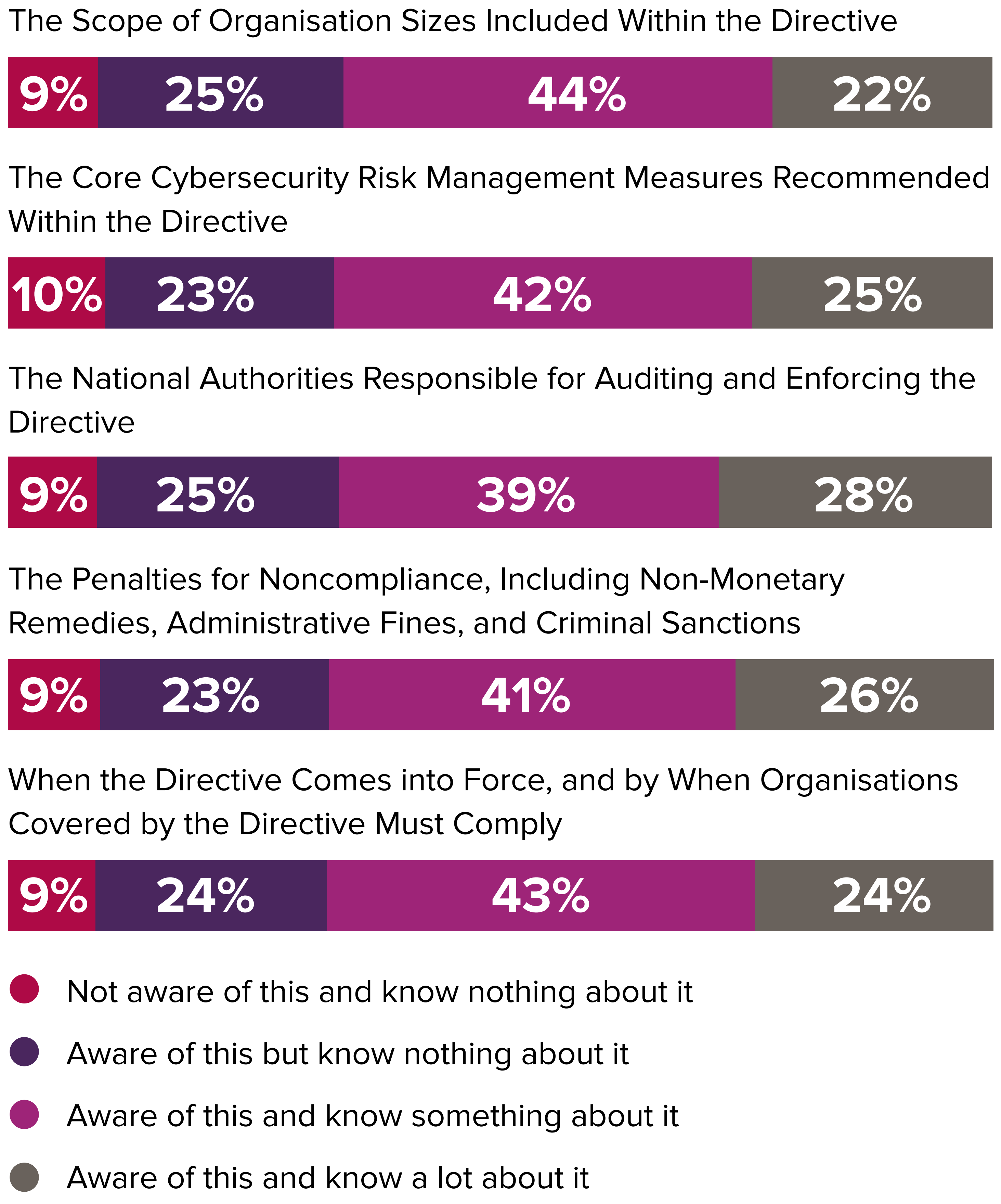
✓ General awareness of the key aspects of the NIS2 directive is high but with varying levels of knowledge.

✓ This demonstrates that the majority of European organisations have the NIS2 directive on their radars and are aware of the key aspects that will affect their organisations.

✗ Conversely, it conveys that one in three European organisations is either unaware or has a very low level of knowledge of a directive that comes into force in the very near future.

✗ The number of European organisations that have detailed knowledge of the key NIS2 aspects is significantly lower, with only one in four firms citing that it is both aware and knows a lot about the directive.

Q. What is your awareness and knowledge of each of the following aspects of the new NIS2 directive?



Aware of this and know a lot about it:

22%

25%

(17% OF UK FIRMS)

28%

(18% of Belgian and Dutch firms)

26%

(18% of Belgian firms and 14% of Dutch firms)

24%

Only one in four firms has *awareness* of and *detailed knowledge* about the various aspects of the NIS2 directive.

Source: IDC, 2024

Organisations Are Struggling with Slow Progress and Board Engagement

Most organisations are making slow progress and are struggling across various areas of NIS2 compliance. These challenges are exacerbated by a lack of board (C-Suite) engagement, which is primarily attributed to a focus on business and growth, with compliance being a low priority — despite the threat of fines for the senior executives of non-compliant organisations.

🇪🇺 **58%**

🇪🇸	🇫🇷	🇧🇪	🇬🇧	🇳🇱
74%	56%	55%	52%	43%

of organisations report that they are making slow progress towards NIS2 compliance.

Q. How happy are you with your organisation's progress towards NIS2 compliance?

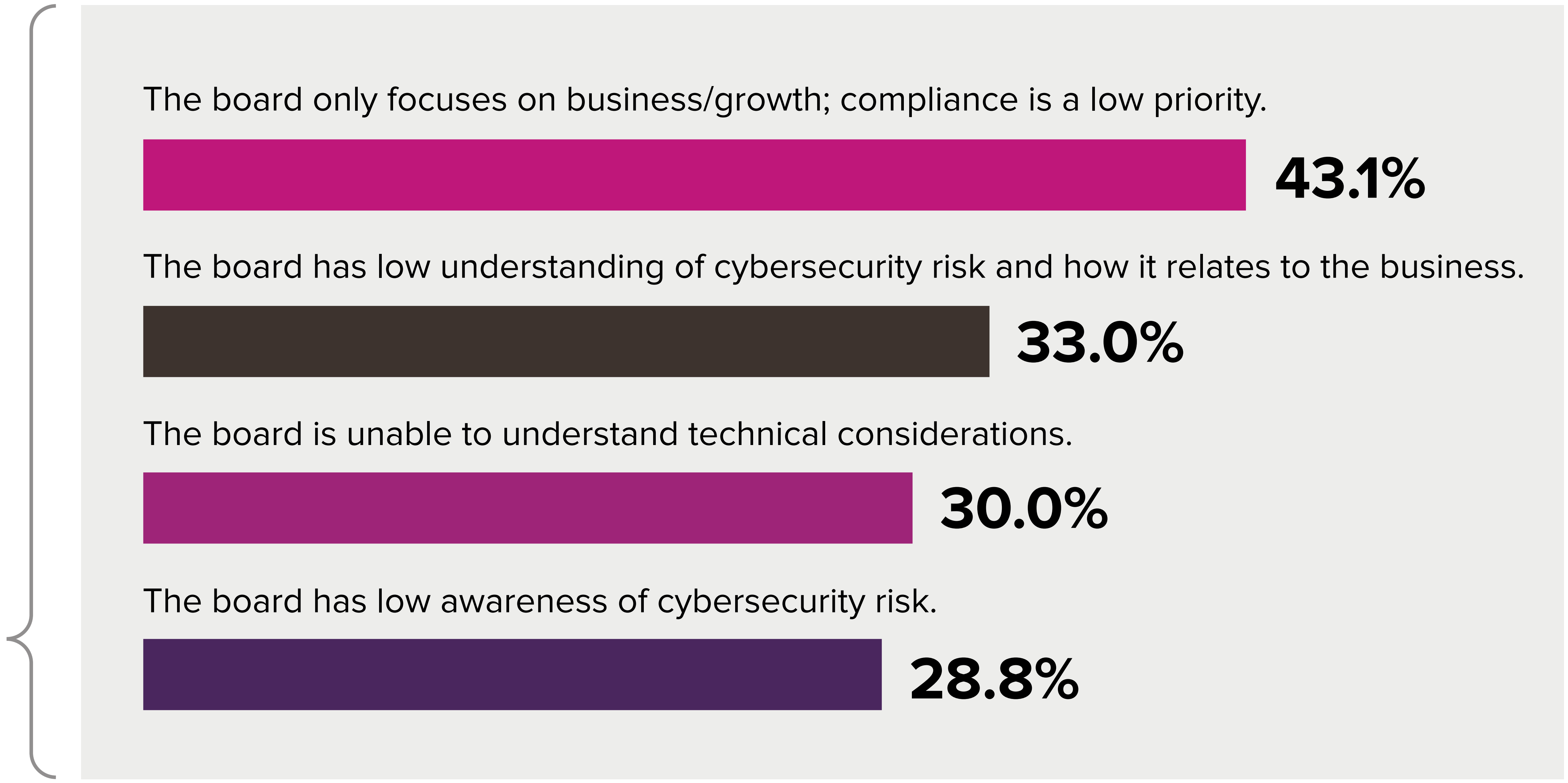
🇪🇺 **42%**

🇫🇷	🇪🇸	🇳🇱	🇧🇪	🇬🇧
40%	38%	38%	38%	34%

of organisations state that their boards are not engaged in NIS2 compliance.

Q. Is your organisation's board aware and engaged regarding NIS2 compliance?

Reasons for Lack of Board Engagement



Q. Why do you believe your organisation's board is not engaged regarding NIS2 compliance?

Source: IDC, 2024

European Organisations Face Readiness Gaps

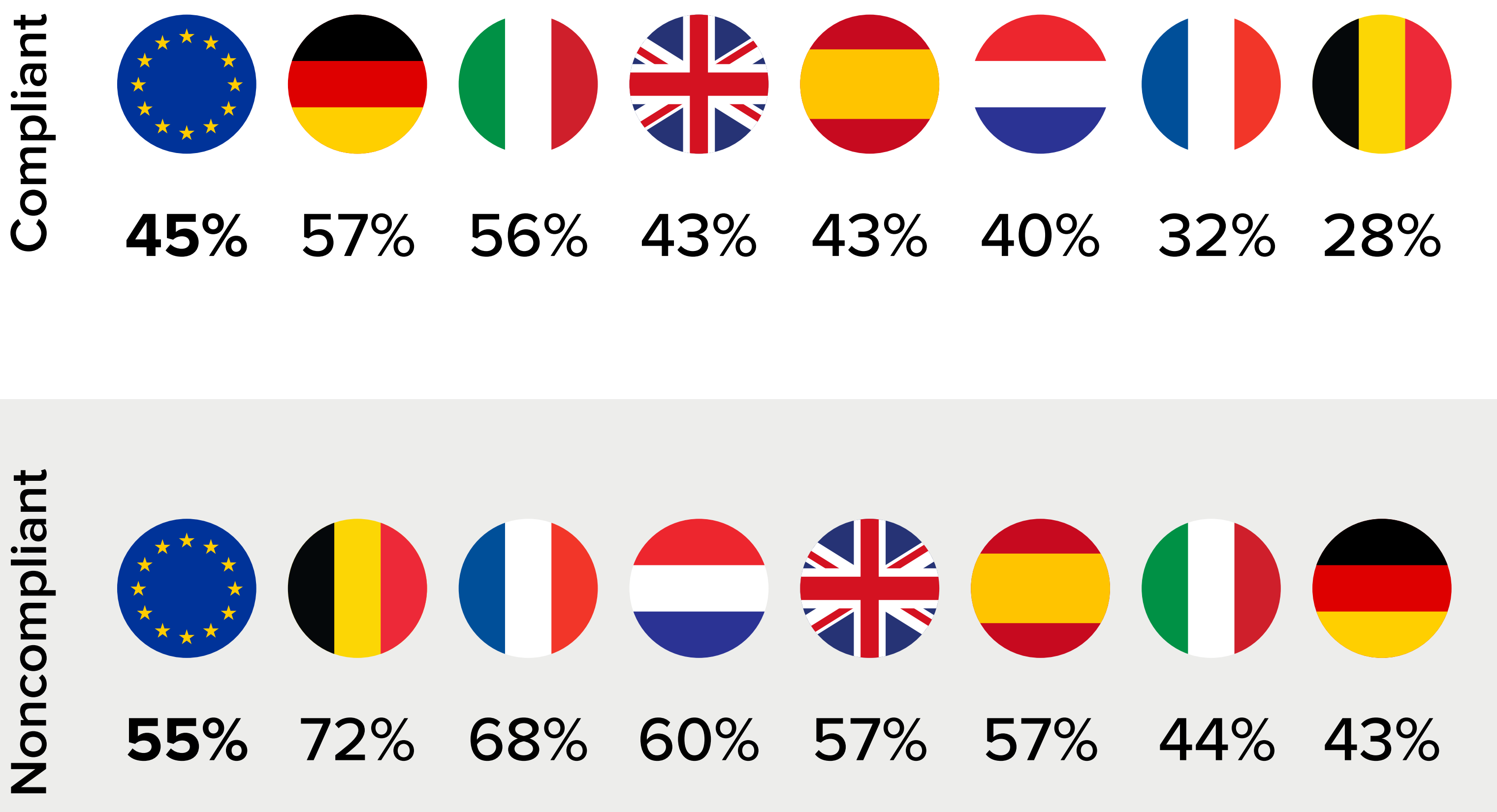
With almost half of European organisations considering themselves compliant with NIS2, there is still work to do. Yet compliance varies greatly by country in the European Union. For example, twice as many **German** organisations consider themselves compliant as **Belgian** firms, and only 32% of **French** firms consider themselves compliant.

Regardless of compliance status, no standout risk or information security management measures are in place (as required for NIS2 compliance) in European organisations. This situation illustrates a lack of a unilaterally agreed strategy regarding measures for NIS2 compliance among European firms.

Security and **IT services providers** are the leading mechanism through which European organisations are made aware of NIS2 implementation at the local or national level, as cited by 4 in 10 firms. Interestingly, **national cybersecurity authorities** are only cited by one-third of European organisations in this regard.

Compliance Status

(self-reported)



Q. Do you believe your organisation is already compliant with the new NIS2 directive?

Measures in Place

Top 3

1	2	3
Security in the acquisition, development, and maintenance of network and information systems	Multifactor authentication, continuous authentication, and secure communication	Policies and procedures to assess the effectiveness of cybersecurity risk management measures
Security in the acquisition, development, and maintenance of network and information systems	Risk management and information system security policies	Incident handling and management

Q. Which of the following risk and information security management measures (as required for NIS2 compliance) does your organisation have in place?

National Level Awareness

Top 2

1	2
44% Aware due to our security and IT services provider actively driving awareness	**32%** Aware due to our national cybersecurity authority actively driving awareness
34% Aware due to our security and IT services provider actively driving awareness	**32%** Aware and participated in the consultation phase

Q. Please indicate your organisation's awareness of NIS2 implementation at the local/national level and the context of that awareness?

Source: IDC, 2024

The Key Challenges Are Consistent Across Industries

But, as European organisations progress in their journeys to NIS2 compliance, the measures they are struggling with are consistently cited across industries.

Policies and procedures are particularly problematic, such as assessing the effectiveness of cybersecurity risk management measures, information system security, and access control.

Most Challenging Compliance Measures

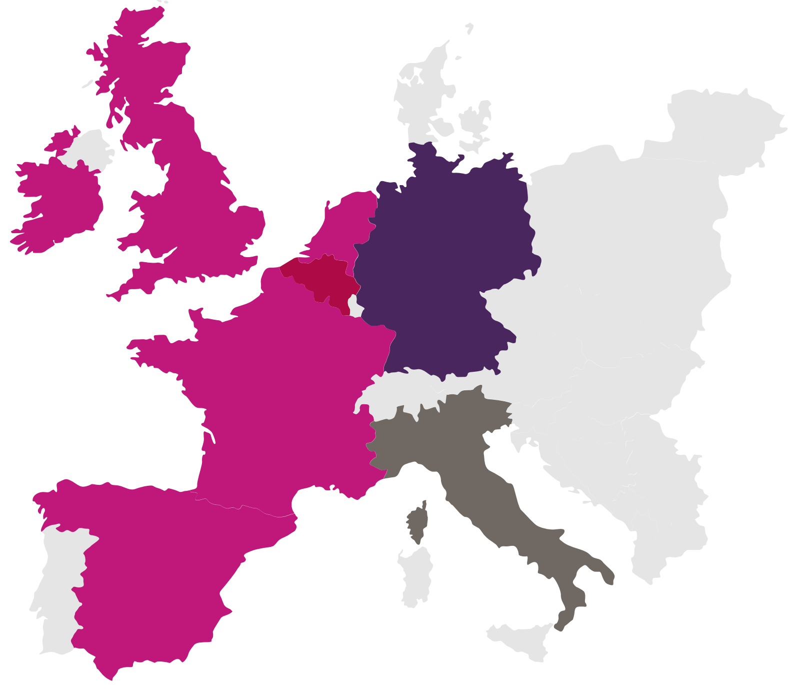
	All Industries	Public Administration	Health	Banking	Manufacturing	Digital Infrastructure
#1	Security in the acquisition, development, and maintenance of network and information systems		Policies and procedures to assess the effectiveness of cybersecurity risk management measures	Risk management and information system security policies	Security in the acquisition, development, and maintenance of network and information systems	Policies and procedures to assess the effectiveness of cybersecurity risk management measures
#2	Policies and procedures to assess the effectiveness of cybersecurity risk management measures	Risk management and information system security policies	Security in the acquisition, development, and maintenance of network and information systems		HR security, access control policies, and asset management	Security in the acquisition, development, and maintenance of network and information systems
#3	Risk management and information system security policies	Policies and procedures to assess the effectiveness of cybersecurity risk management measures	Risk management and information system security policies	Policies and procedures regarding the use of cryptography and encryption	Business continuity and crisis management	Multifactor authentication (MFA), continuous authentication, and secure communications

Q. With which NIS2 measures will your organisation find it most challenging to comply?

Security in the acquisition, development, and maintenance of network and information systems is cited as the No. 1 challenge for small businesses (50–99 employees), medium-size businesses (100–499 employees), and very large businesses (1,000+ employees).

Business continuity and crisis management (back-ups and disaster recovery) are the No. 1 challenge for large businesses (500–999 employees).

However, the most pressing challenges vary by country, with firms in **Germany**, **Italy**, and **Belgium** citing different challenges to organisations based in **France**, the **UK**, the **Netherlands**, and **Spain**.



- ● Security in the acquisition, development, and maintenance of network and information systems
- ● Business continuity and crisis management (back-up and disaster recovery)
- ● Multifactor authentication (MFA), continuous authentication, and secure communications
- ● HR security, access control policies, and asset management

Source: IDC, 2024

Preparation Is Hampered by Policy Variations and Human Factors

Organisations across the EU are encountering substantial obstacles to their efforts to comply with the forthcoming NIS2 regulation. The preparation phase is notably impeded by policy inconsistencies and human factors, including insufficient employee training and awareness. Furthermore, the absence of timely and clear guidance from national authorities exacerbates these challenges, creating uncertainty around compliance requirements. This situation is further compounded by inadequate budget allocations for essential technology investments, significantly hampering progress and increasing the risk of non-compliance and cybersecurity vulnerabilities.

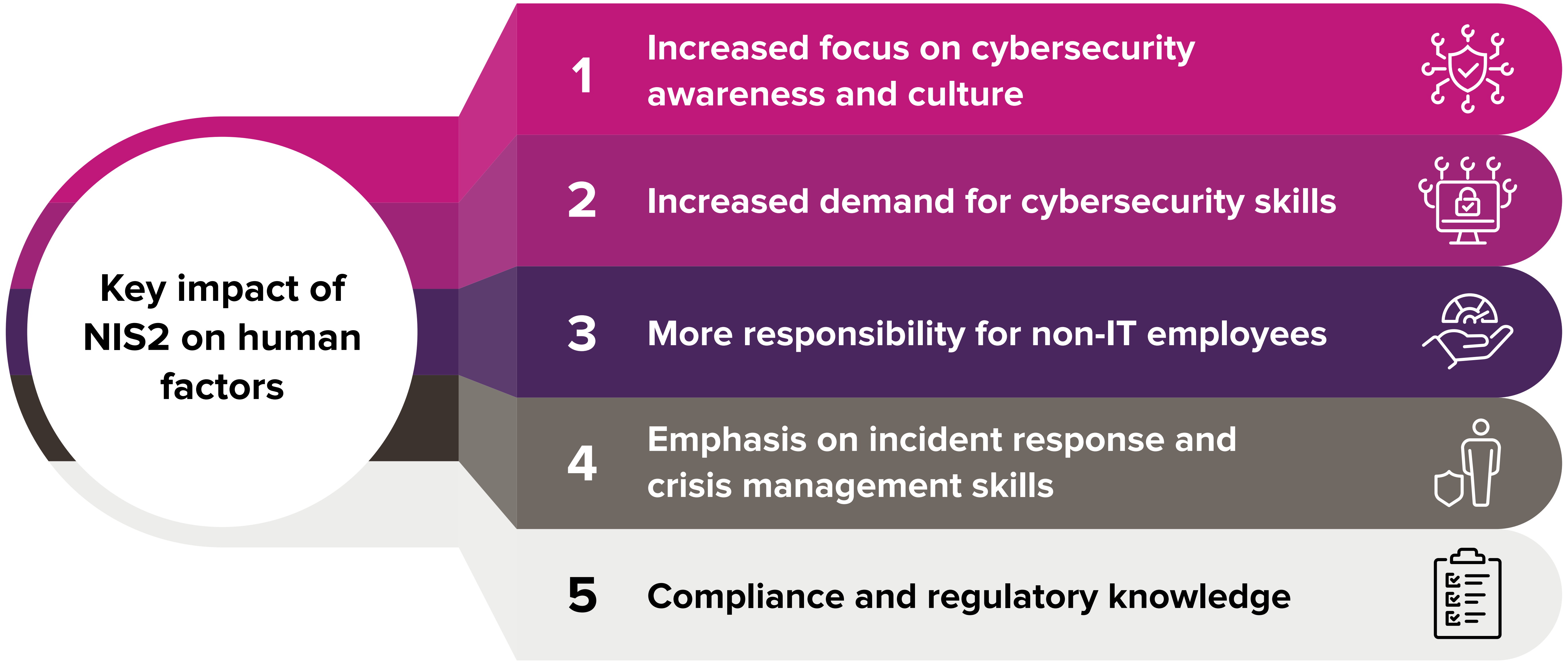
Top Preparation Issues

<table>
<tr><th></th><th>All Countries</th><th>EU</th><th>Germany</th><th>France</th><th>Italy</th><th>Netherlands</th><th>UK</th></tr>
<tr><td>#1</td><td colspan="3">Variations in policies and controls across different EU countries in which we operate</td><td colspan="3">Human factors, including employee training and awareness</td><td>Lack of timely and clear advance guidance from our national security authorities</td></tr>
<tr><td>#2</td><td colspan="2">Human factors, including employee training and awareness</td><td>Lack of budget for technology investments</td><td colspan="3">Variations in policies and controls across different EU countries in which we operate</td><td>Approaching cyber-risk management as a mandatory rather than an optional or recommended undertaking</td></tr>
<tr><td>#3</td><td>Lack of timely and clear advance guidance from our national security authorities</td><td>Lack of budget for technology investments</td><td>Human factors, including employee training and awareness</td><td colspan="2">Lack of timely and clear advance guidance from our national security authorities</td><td>Mapping our status and capabilities in relation to requirements</td><td>Lack of resources for implementing changes to policies, practices, or processes</td></tr>
</table>

Source: IDC, 2024

NIS2 Will Affect Human Factors, Requiring a Culture Shift

While the upcoming NIS2 directive focuses on enhancing technical security standards, it also has significant implications for **human factors and skills** within organisations, as it requires a culture shift towards more **cybersecurity awareness**, **upskilling of employees**, and a deeper integration of **cyber-risk management** into daily operations.



Key impact of NIS2 on human factors

1 Increased focus on cybersecurity awareness and culture

2 Increased demand for cybersecurity skills

3 More responsibility for non-IT employees

4 Emphasis on incident response and crisis management skills

5 Compliance and regulatory knowledge

Ways to overcome human-factor challenges:

Comprehensive training programs: Implement regular cybersecurity training for all employees, tailored to specific roles. This will help ensure that everyone understands their responsibilities.

Strong leadership and governance: Ensure that top management is actively involved in setting a cybersecurity-first culture.

Collaborative risk management: Build cross-departmental risk management teams that include both IT and non-IT staff to align cybersecurity with business objectives.

Investment in upskilling: Provide opportunities for employees to upskill, particularly in cybersecurity, compliance, and risk management roles, ensuring the organisation has the right expertise.

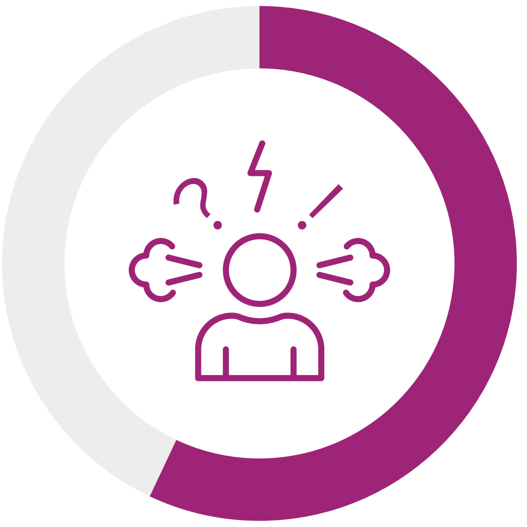
Building a culture of security: Promote cybersecurity awareness throughout the organisation, emphasising that it is not just an IT issue but something that affects everyone.

By addressing these challenges head on, organisations can build a more resilient workforce that is better equipped to handle a complex security landscape and ensure compliance with the new regulation.

Source: IDC, 2024

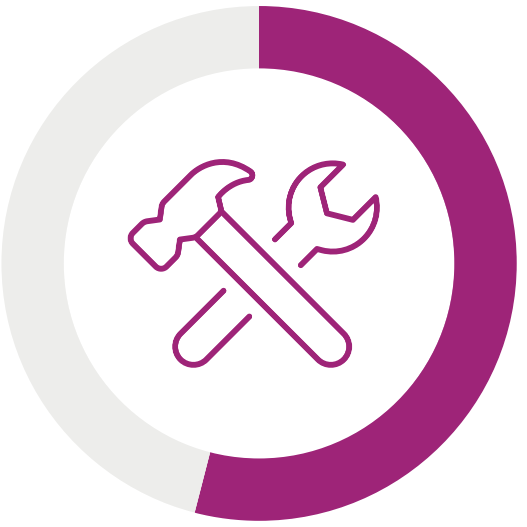
The Impact on Skills Is Considerable Yet Often Neglected

Although employees play a crucial role in helping their organisations comply with the NIS2 directive, **one** in **two** companies is having problems with skills.



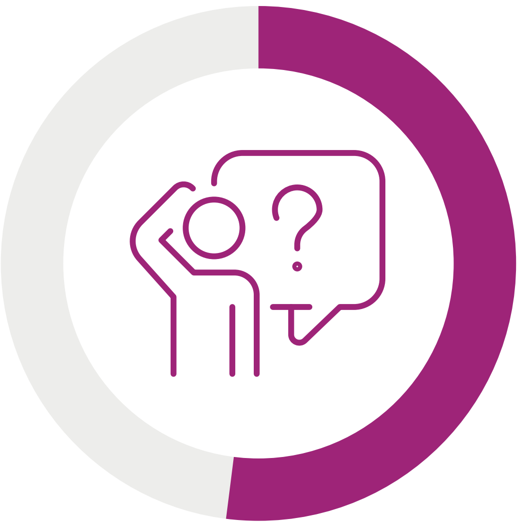
57%

of organisations report that their compliance workload is overwhelming their in-house teams.



54%

of organisations report that they often implement shortcuts or workarounds to meet their compliance deadlines.



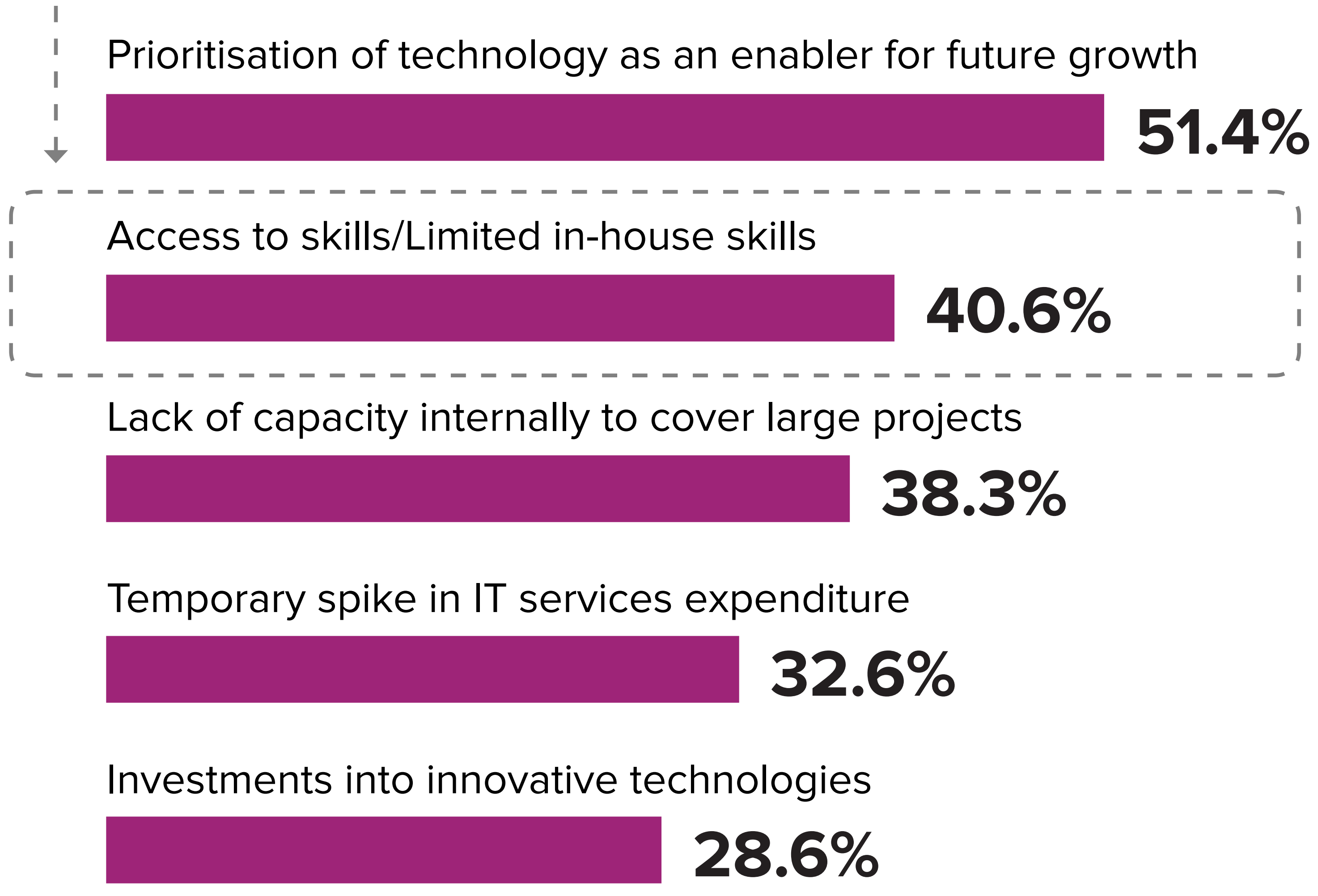
52%

of organisations report that they do not have the in-house skills to become fully compliant.

Q. To what extent do you agree with the following statements?

While skills deficiencies can negatively impact an organisation's journey to NIS2 compliance, engaging with external partners can mitigate skills issues and deliver a positive impact, building on experience with similar engagements.

Reaching out to external providers for a wider range of skills to overcome limited in-house resources is a leading driver of increased services spending among European organisations:



Q. What are the most significant reasons for the increase in external IT services spending in your organisation?

Source: IDC, 2023

Organisations that can get on top of their skills issues will have an advantage over competitors and will potentially achieve NIS2 compliance sooner.

Source: IDC, 2024

Organisations Tend to Outsource NIS2 Implementation But Keep Strategic Capabilities in House

Organisations partnering with managed security providers (MSPs) typically outsource labour-intensive tasks requiring specialised skills, such as security operations. They retain strategic functions like compliance direction, governance, risk management, and data security in house. NIS2 compliance is a significant motivator for organisations not currently using MSPs to consider using them, leveraging the MSPs' expertise and resources.

MSP Engagement

42% are already working with a managed **security services provider**.

54% expect to work with a **managed security services provider** within two years.

Q: Would your organisation consider working with a managed cybersecurity services provider?

Outsourced

40% Cloud security

39% Security operations

39% Technology deployment or strategy to meet NIS2 requirements

39% Technology deployment or strategy to meet NIS2 requirements

38% Cloud security

37% Aligning security strategy with NIS2 compliance

In House

43% Strategic direction on compliance, governance, or risk

41% Ransomware preparedness

43% Data security

43% Security operations

40% Data security

38% Building resilience to stay ahead of new threats

Q: Please indicate what your organisation intends to do for each of the following over the next two years.

Source: IDC, 2024

Security Strategy and Stakeholder Buy-In Drive External Partner Engagements

Partner engagement rates for the NIS2 compliance journey are high.

53% currently work with a partner/advisor.

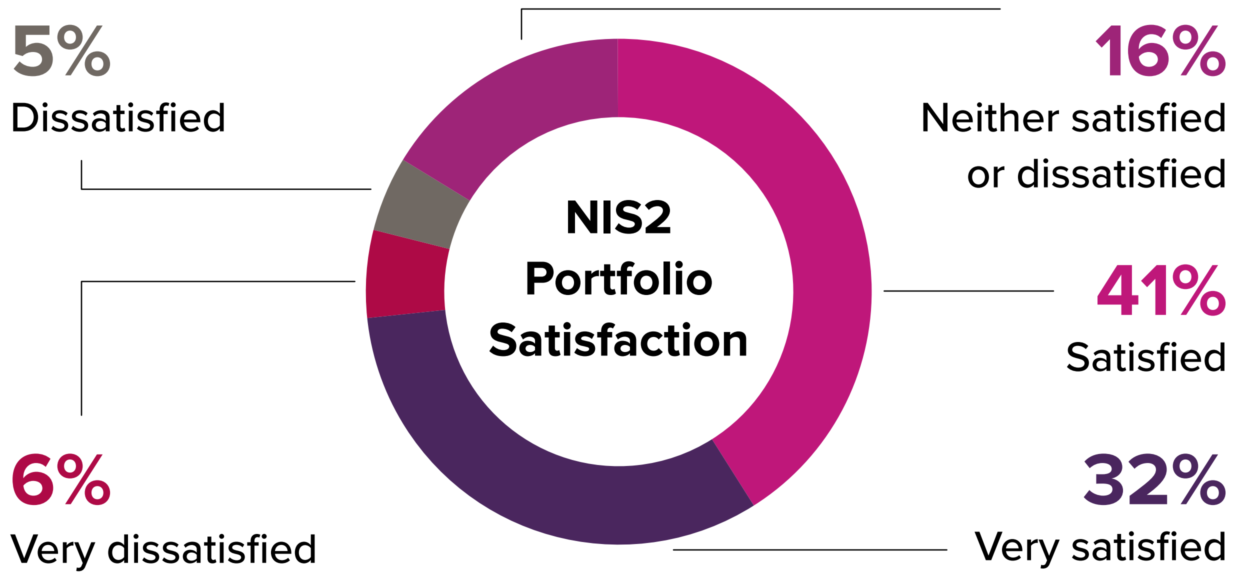
38% plan to work with one in the future.

Half of European organisations are already collaborating with external partners on their NIS2 compliance. Fewer than 10% of European firms do not plan to engage such a partner, highlighting the perceived value of external assistance. However, in Belgium, 18% of organisations do not intend to work with an external partner for NIS2 compliance.

Partner offerings meet the needs of European firms.

73% of European organisations are *satisfied* or *very satisfied* with the NIS2 offerings of their security services partners, indicating very high satisfaction with partner engagement.

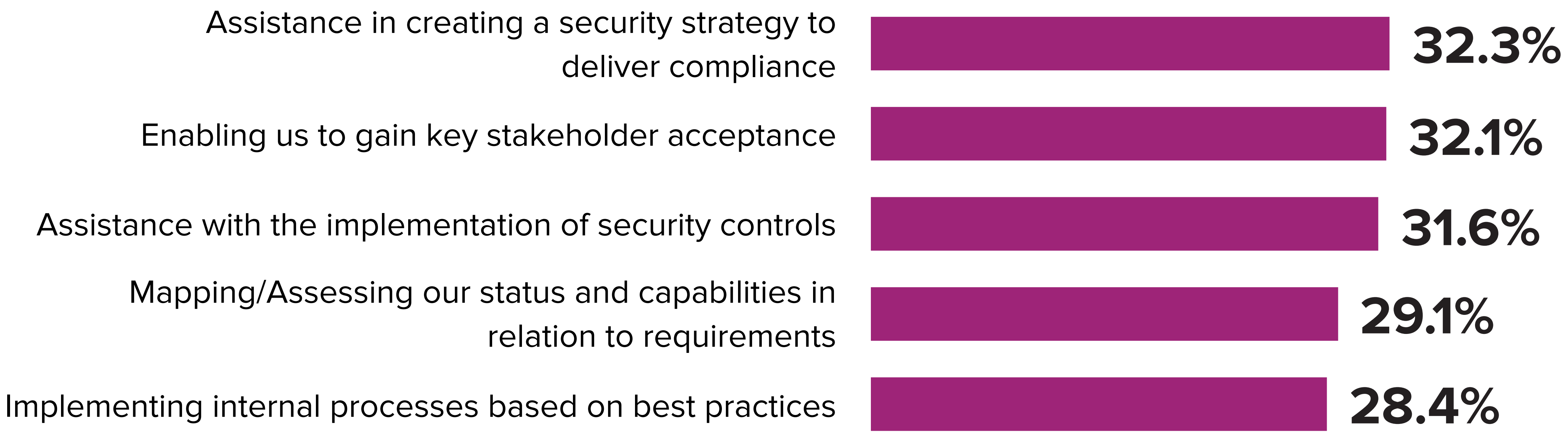
That figure falls to **51% of firms** in the small businesses category, illustrating that partners have work to do in meeting the **needs of smaller firms**.



Q. How satisfied are you with the current offerings of your organisation's security services partners in meeting your organisation's needs regarding NIS2?

To what extent do European firms need external partners to help with their NIS2 compliance journeys?

Q. In which areas related to your organisation's NIS2 compliance journey do you see your cybersecurity services provider playing the most important role? Top 5 plotted



Note: The percentages represent the proportions of respondents that selects the given areas.

Strategic direction and oversight: Security strategy is crucial for compliance, as strong cybersecurity and meeting compliance obligations go hand in hand.

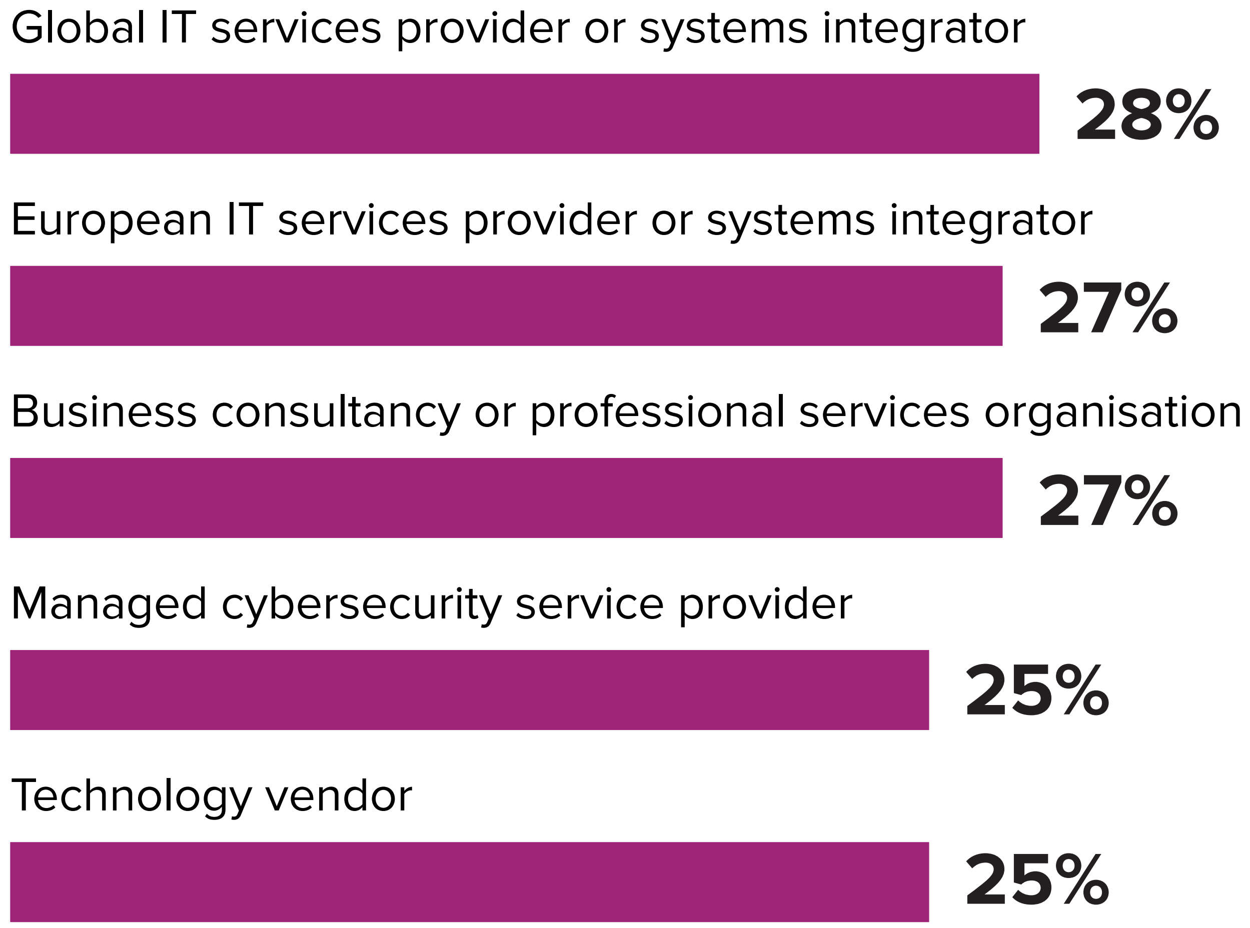
Activities: Ultimately, as European organisations advance in their NIS2 compliance journeys, external partners are assisting with activities such as management sign-off, strategy, benchmarking, implementation, equipment supply, and SecOps.

Value: When selecting external partners for NIS2 compliance, European organisations must evaluate potential partners across a wide range of capabilities. Conversely, service providers must demonstrate their abilities and track records in these key areas of engagement.

Source: IDC, 2024

Services Providers Are Most Preferred for NIS2

NIS2 Partner Preference

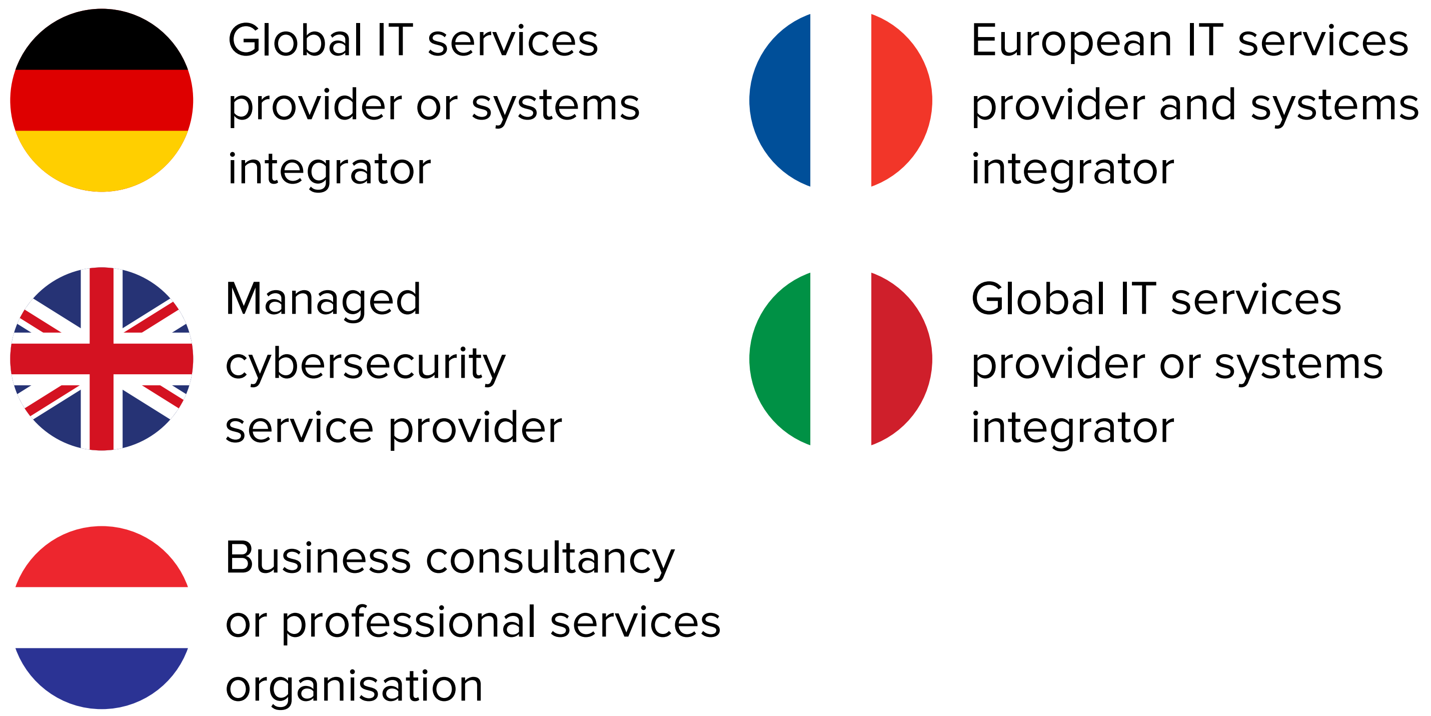


Q. Which external partner types would your organisation prefer for its NIS2 compliance journey?

Preferences for external partner type to help European organisations in their NIS2 compliance journeys are **varied** and demonstrate just how **competitive** the market is for external partners.

Considering Europe overall, IT services providers are the **most preferred partners** for the NIS2 journey – even being ranked ahead of managed cybersecurity services providers.

But variations in preference exist across countries:



Global IT services provider or systems integrator

European IT services provider and systems integrator

Managed cybersecurity service provider

Global IT services provider or systems integrator

Business consultancy or professional services organisation

The leading preference for Belgian firms is "*a company that knows the compliance requirements of our country really well*". This demonstrates **prioritisation** of compliance regulation knowledge.

Sources of information on NIS2?

30% of European firms cite IT services providers as the leading source of information on NIS2.

Small businesses leverage their **industry peers** and **ecosystem partners**, while large businesses cite **industry regulators** as the leading source of NIS2 information.

While partner preference by company size illustrates an overall preference for **IT services providers**, it also indicates how small organisations in Europe are equally willing to work with a **managed security services provider** and that large businesses prioritise compliance knowledge over partner type.

Small business *(50–99 employees)*	Global IT services provider, systems integrator, or managed cybersecurity service provider
Medium-size business *(100–499 employees)*	European IT Services provider or systems integrator
Large business *(500–999 employees)*	A company that knows the compliance requirements of our country really well
Very large business *(999+ employees)*	Global IT services provider or systems integrator

Ultimately, the closely ranked preferences illustrate that no single type of partner **excels** in meeting the NIS2 needs of European organisations. This makes the selection decision **harder** for organisations looking for help but also reveals the need and opportunity for all partner types to **improve** their messaging and offerings.

Source: IDC, 2024

Recommendations

As organisations continue to evolve in their digital transformation journeys and become digital businesses, data becomes critical IP and of increasing importance to the business, customers, and partners.

In keeping with this, the European Union enacted the Network and Information Security directive in 2016, which was updated in 2023, as NIS2. Organisations conducting business activities in the EU are affected and, as a result, have a set of NIS2 requirements placed on them.

Progress in attaining NIS2 compliance is slow across Europe, with organisations in the region facing many issues. External partners are a source of assistance and are already being leveraged by European organisations on their NIS2 compliance journeys.

Act now: Despite delays in nations transposing NIS2 into national law, organisations should not delay their compliance efforts. Continue preparing by conducting thorough assessments of current cybersecurity measures, identifying gaps, and implementing necessary improvements.

Raise awareness: Conduct training sessions and workshops to bridge the awareness and knowledge gap, ensuring that all relevant staff understand the directive’s requirements and implications. Utilise external experts if necessary to expedite this process and ensure comprehensive understanding across the organisation.

Involve senior management: With 58% of European organisations reporting slow progress in NIS2 compliance and 42% stating their boards are not engaged with NIS2, making compliance progress is a key issue for European firms.

Engage proactively: Address human factors by developing and clearly communicating cybersecurity policies and procedures. Ensure top management is actively engaged, and foster a strong cybersecurity culture within the organisation. This will enhance your overall cybersecurity posture and facilitate compliance with NIS2 requirements.

Rely on partners: To address internal skills deficiencies, organisations should leverage the expertise of strategic partners, such as IT services providers. This approach can mitigate skills gaps, enhance compliance efforts, and help avoid potential penalties.

Evaluate thoroughly: Satisfaction with NIS2 offerings from security services partners is high among European organisations. In selecting potential NIS2 partners, organisations must evaluate prospective providers across all parameters, including strategy, benchmarking, implementation, and SecOps.

Message from Insight

Insight

As a leading solutions integrator with extensive knowledge of security solutions and the EU regulatory landscapes, Insight is well equipped to guide organisations towards robust security controls and seamless compliance ahead of the upcoming NIS2 requirements. Recognising the urgent need for cohesive communications at every level, we can help you create a shared common understanding of NIS2 across your organisation. We focus on driving meaningful change, emphasising risk reduction over superficial reporting, and optimising the returns on your investments.

Let Insight be your strategic ally in navigating the complexities of NIS2 and achieving a proactive cybersecurity approach to the directive.

Survey Demographics

Company size:

10%

59–99 employees

33%

100–499 employees

21%

1,000+ employees

36%

500–999 employees

Vertical Industries:

1%	Space
6%	Digital providers
10%	Digital infrastructure
8%	Energy
10%	Banking
4%	Financial market infrastructures
10%	Public administration
8%	Health
11%	ICT service management
20%	Manufacturing
11%	Transport and logistics
0.3%	Water, wastewater, waste management

Country Split:

8%	Belgium
17%	France
17%	Germany
17%	Italy
8%	Netherlands
17%	Spain
17%	United Kingdom

Decision Influence:

67%	Decision maker
33%	Digital providers

Roles:

34%	IT security manager or director
47%	IT manager or director
8%	VP of head of operations
2%	VP or head of risk or compliance
6%	Chief Information officer or chief technology officer
2%	Chief information security officer
7%	Chief operations officer
8%	Chief risk officer or chief compliance offer

Source: IDC 2024, n = 600, CAWI survey method

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets.

With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight help IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

Founded in 1964, IDC is a wholly-owned subsidiary of International Data Group (IDG, Inc.), the world's leading tech media, data, and marketing services company.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell, and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC

IDC UK
5th Floor, Ealing Cross, 85 Uxbridge Road, London, W5 5TH, United Kingdom
T 44.208.987.7100

X @idc   @idc   idc.com

© 2024 IDC Research, Inc. IDC materials are licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

Privacy Policy | CCPA