NIS 2 & Beyond: Risk, Reward & Regulation Readiness

Key insights from European IT leaders to navigate the NIS 2 Directive

Contents

Executive Summary

Today's threat landscape is unprecedented in scope, with advances in technologies like AI emboldening bad actors to find and exploit security vulnerabilities more quickly than ever before. Faced with this dangerous and rapidly evolving environment, more organizations are recognizing the limitations of their current reactive cybersecurity.

To promote a more proactive approach to cybersecurity, regulations like the updated **Network and Information Security Directive, known as NIS 2**, have been introduced to provide organizations across 15 relevant sectors with the essential security processes and frameworks necessary to enhance their cyber hygiene practices.

In April 2024, Zscaler conducted a survey across six European markets, engaging more than 875 IT leaders to assess the progress of organizations in meeting the NIS 2 compliance requirements ahead of the October 17, 2024, deadline. The findings reveal a **troubling disconnect between the confidence levels of European companies and their comprehension of the NIS 2 compliance prerequisites**, despite the directive's significance.

This gap raises alarms about the possibility of a last-minute rush to compliance, which could shift focus away from other vital cybersecurity concerns, thereby intensifying existing vulnerabilities. **How can organizations quickly accelerate their compliance efforts? And should they consider broader perspectives beyond NIS 2?**

This report will seek to answer these questions.

Key Findings

Zscaler NIS 2 & Beyond:
Risk, Reward & Regulation Readiness – Results Overview

80% of European IT leaders feel confident their organization will meet NIS 2 compliance requirements by this year's deadline and **14%** claim to have already met them

Only **53%** of IT leaders believe their own teams fully understand what the requirements for NIS 2 compliance are, and even fewer **(49%)** believe leadership fully understand them

One third (32%) of IT leaders say NIS 2 regulations are one of the leadership team's top priorities, and **52%** say they are becoming a higher priority

62% of IT leaders believe NIS 2 represents a significant departure from their current strategy

Only **31%** of IT leaders would rate their existing cyber hygiene as excellent

The three areas IT leaders are having to make the most significant changes to become compliant are: updating their **technology stack/ cybersecurity solutions**, and **educating employees** and **leadership**

44% of IT leaders believe that tools and services have a critical role to plan in a successful NIS 2 implementation

Two fifths of organizations have yet to implement a zero trust architecture as part of their cybersecurity approach

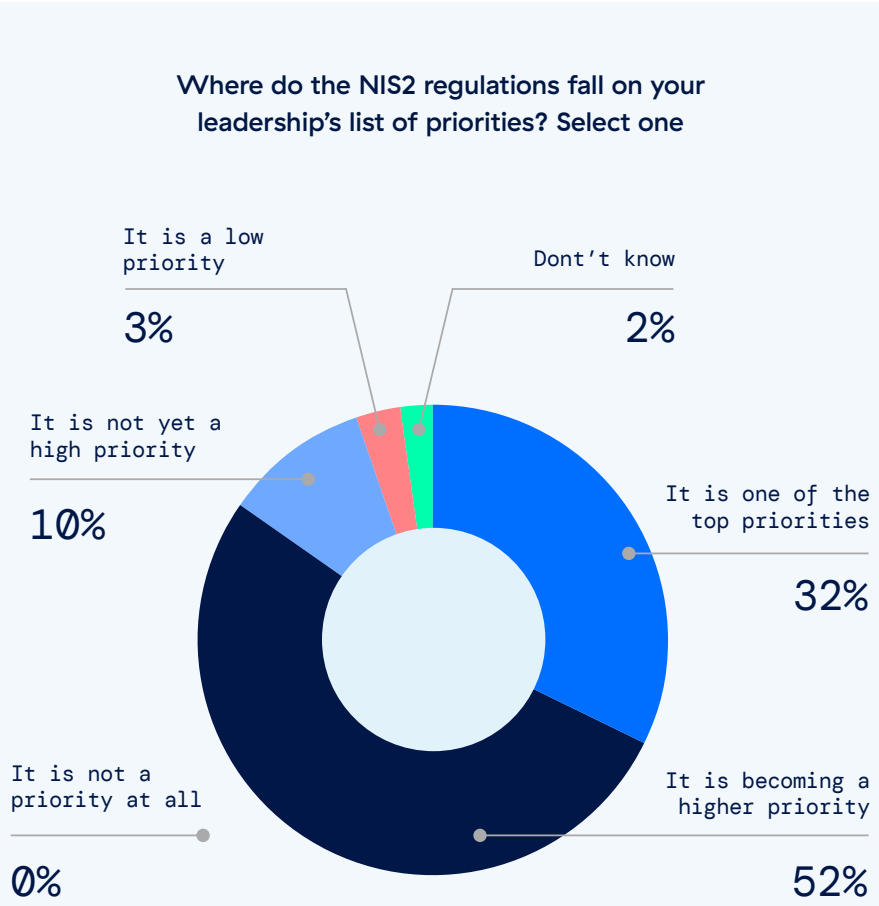
71% of IT leaders say that keeping today's organizations cyber secure requires a mindset change that won't be brought about by a compliance exercise

53% of IT leaders do not believe the NIS 2 regulations go far enough considering the scale of the cybersecurity challenge

Confidence And Disconnect: Surveying NIS 2 Readiness In Europe

An examination of the initial survey data paints an optimistic picture of the preparedness of European entities for NIS 2 compliance. The figures indicate that the vast majority (80%) of IT leaders across Europe are confident in their organization's capability to meet NIS 2's conditions within the stipulated time frame, and a fraction above 1 in 10 (14%) say they have already fulfilled the compliance requirements.

However, a more granular scrutiny of the situation uncovers inconsistencies and friction points around both organizations' understanding of the regulations and efforts to achieve compliance.

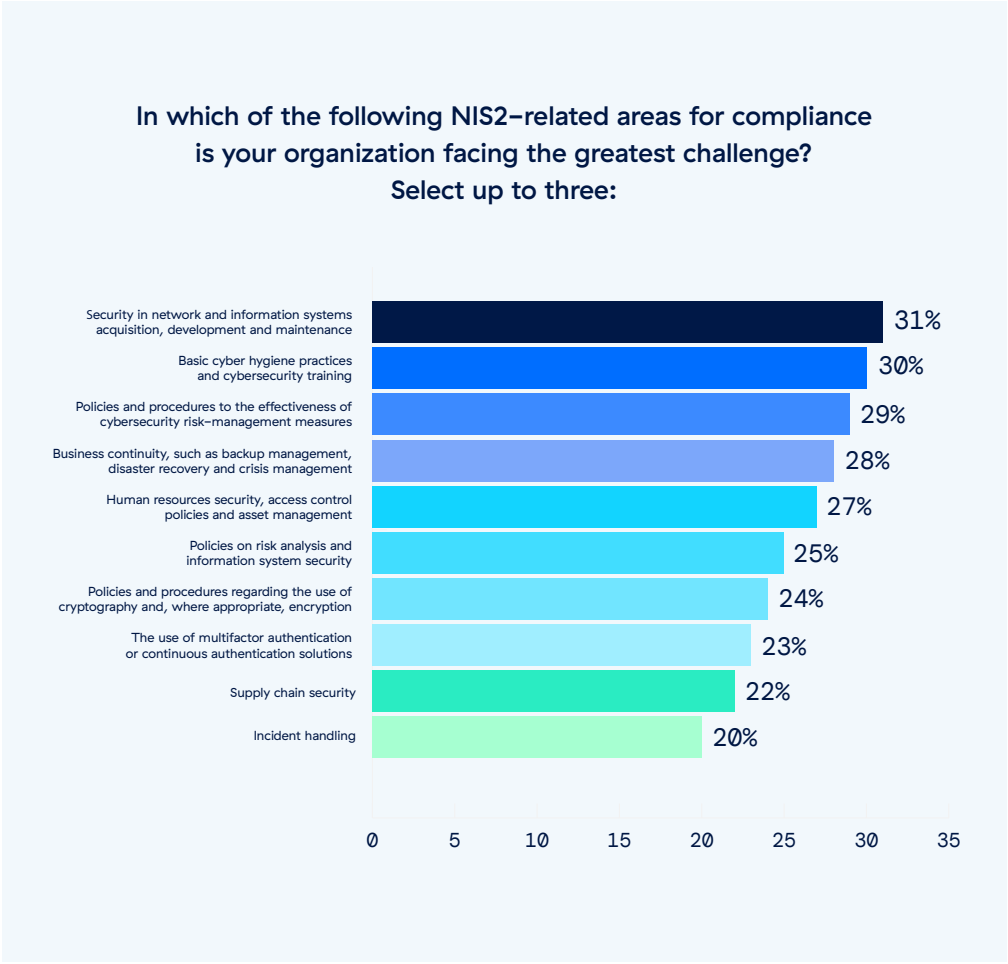


Despite the professed assurance of meeting the upcoming deadline, just 53% of IT leaders are convinced of their own teams' thorough comprehension of NIS 2 compliance, and even fewer (49%) are confident about their leadership's understanding of the same. Meanwhile, despite its apparent prioritization—and company leadership potentially being held personally liable if their business is not compliant under NIS 2—half (56%) of IT leaders report a lack of sufficient support from their leadership in meeting compliance deadlines, suggesting a **disconnect between strategic intent and practical implementation.**

A further disconnect was also revealed between how the directive is being positioned and how IT leaders might view it. Despite NIS 2 being an evolution of an existing framework, **62% of IT leaders believe it represents a significant departure from their current cybersecurity practices**—suggesting that many businesses may not have been keeping up with evolving technology solutions and have instead been maintaining the bare minimum security requirements. This assumption is affirmed by the fact that less than one-third (31%) of IT leaders rated their existing cyber hygiene as excellent, and two-fifths admitted that their organization has yet to implement a zero trust

This leaves organizations with significant ground to make up. The survey highlights critical places that need extensive updates to achieve compliance, such as **updating technology stacks, enhancing employee and leadership training, and advancing cybersecurity measures.** It also reveals that the three areas of the directive causing the greatest challenges are: security in network and information systems acquisition, development, and maintenance; basic cyber hygiene practices and cybersecurity training; and policies and procedures to the effectiveness of cybersecurity risk-management measures.

The NIS 2 directive emphasizes the responsibility of organizations to ensure network and information system security with a culture of governance and comprehensive risk management. As such, the relevant entities must adopt proactive technical, operational, and organizational measures to manage the risks posed to the security of network and information systems.



With the deadline on the horizon, organizations face hastened compliance efforts, potentially at the expense of other vital cybersecurity facets. **60% of survey participants voice apprehensions that the concentrated efforts on NIS 2 compliance may result in the neglect of other critical areas of security.** Consequently, it is imperative for organizational leaders to extend substantial support to IT departments, ensuring a holistic approach to compliance that mitigates risks of vulnerabilities and operational setbacks.

> "While there appears to be a quiet confidence across the region that businesses will reach NIS 2 compliance within the rapidly approaching deadline, our research suggests that this confidence could be built on shaky foundations... Leadership needs to act now and provide their IT teams with the necessary support to avoid missing key steps in their compliance journey and risking serious financial consequences across EMEA"
>
> —BRIAN MARWIN, SENIOR VICE PRESIDENT EMEA SALES, ZSCALER

NIS 2 Response: What Does Action Look Like?

In the context of NIS 2 and further upcoming regulations, many **organizations will need to fundamentally reevaluate and revamp their cybersecurity strategies** if compliance mapping shows gaps in their security processes.Though 44% of IT leaders believe that tools and services have a vital role to play in a successful NIS 2 implementation—the truth is that compliance has to transcend the adoption of new technologies.

The objective of regulations like NIS 2 is to enhance the overall security posture within organizations in the critical infrastructure sectors by raising it to a minimum base layer of common protection. While it is possible therefore to be wholly NIS 2 compliant on paper, organizations who approach it with this goal alone will end up having a **low level of operational security.**

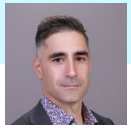
True **cybersecurity superiority** necessitates a meticulous reassessment of current security processes, compelling organizations to fortify their defenses beyond the conventional thresholds. Despite the regulatory demands, certain organizations appear to be maintaining a passive, reactionary security approach, addressing issues only when forced.

The updated directive forces organizations to review their current security processes and, if necessary, move them up to what is now considered the current base layer of protection. Organizations that have done their homework already just have to go through an effort to prove compliance. However, the majority will need to raise the bottom rung of security processes because they have survived with only the minimum level of security up to this point.

"For organizations in heavily regulated industries such as financial services, NIS2 and DORA regulations will not require massive changes in security frameworks as these teams will already have a high level of compliance. For those who are outside of those environments, it may feel too daunting to move to a centralized cloud security platform, or implement true zero trust, as it will feel like another layer of complexity.

However, having a central platform for your applications, security and tools can minimize the number of variables you might have and could make it far easier for your organization to become compliant if you don't have a full grasp of all your company assets."

—JAMES TUCKER, HEAD OF CISOS IN RESIDENCE, EMEA, ZSCALER



NIS 2 compliance is only the first step. To reinforce their defenses, organizations are compelled to transition from a reactive posture of threat mitigation to a proactive one, where risks are anticipated and preemptively neutralized.

Does NIS 2 go far enough?

Government directives like NIS 2 are created to raise the security floor to a common base level across Europe. This doesn't mean they will lift the ceiling of security. The research shows that many IT leaders understand this and also recognize that NIS 2 doesn't go far enough.

A significant majority

71%

of IT leaders say that keeping today's organizations cyber secure requires a mindset change that won't be brought about by a compliance exercise.

Furthermore

53%

question the sufficiency of NIS 2 regulations considering the scale of the cybersecurity challenge, underscoring the need for more robust measures.

Ultimately, **addressing NIS 2 compliance demands more than just procedural tweaks; it calls for a foundational shift toward proactive risk management and cybersecurity vigilance.** It is only through the adoption of this proactive approach that organizations can effectively contend with the dynamic threat environment and ensure the protection of their digital infrastructure.

Next Steps For Compliance: NIS 2 & Beyond

The EU estimates that more than 160,000 companies and 15 sectors will have to comply with NIS 2 as they fall into the extended organizational categories. All will be subject to "stricter requirements for risk management and incident reporting, wider coverage of sectors, and more hard-hitting penalties for non-compliance."

The directive is focused on critical physical and digital infrastructure within EU member states, but it also has reach. It applies not only to organizations within the EU, but also to any organization worldwide that provides services to any of the protected sectors within the EU. As with SEC regulations, there are strict rules for prompt incident reporting.

The NIS 2.0 Directive comes into force in October 2024, mandating that management bodies within organizations in specific categories implement cybersecurity risk management measures. The company size varies by sector, but ranges from a minimum of 50 employees for Important Entities (IE) and a minimum of 250 employees for Essential Entities (EE). EU member states can impose administrative fines for instances of NIS noncompliance. For essential entities, EU member states can impose administrative fines of up €10 million or 2% of total worldwide annual turnover in the preceding financial year for noncompliance. For important entities, fines can reach €7 million or 1.4 % of total worldwide annual turnover in the preceding financial year.

Impacted categories extend to:

NIS 2.0
Energy
Transport
Banking
Financial market infrastructure
Health
Drinking water
Wastewater
Digital infrastructure
ICT service management (B2B)
Public administrations
Space
Postal and courier services
Waste management
Manufacture, production, and distribution of chemicals
Food production, processing, and distribution
Manufacturing
Digital providers
Research

Six Steps to Drive the Compliance Process

To prepare effectively, organizations should follow these six steps:

1 Map your business risk and assets

Begin by determining if your organization falls under the scope of NIS 2. This involves understanding the new directive's categories and compliance measures. Every eligible company must register proactively with the relevant authority. While registration processes vary across EU members, grasping the Directive's fundamentals is crucial for preparation. Once registered, devise a plan to implement the Directive's requirements.

2 Map requirements against your existing frameworks

Leverage established cybersecurity frameworks like ISO 27001 or CIS to streamline NIS 2 compliance efforts. Mapping these frameworks against NIS 2 requirements offers a systematic approach. This alignment reduces the effort for organizations already adhering to cybersecurity frameworks, as many NIS 2 requirements overlap with existing ones.

3 Set up your NIS 2 team

Assign responsibility for the NIS 2 compliance process to the CISO or equivalent authority. Delegate tasks to a diverse project team comprising subject matter experts from various functions. These experts ensure comprehensive coverage of NIS 2 requirements, including crisis management and cybersecurity aspects specified in the Directive.

4 Review your inventory management and risk footprint visibility

Conduct a thorough review of your organization's technology inventory and assess associated risks. Inadequate visibility into technology assets poses a significant challenge to compliance efforts. Implement a centralized asset management system to enhance visibility and streamline compliance activities. Address organizational complexity and align IT and operational technology (OT) workloads.

5 Transfer any existing audit results to NIS 2

Leverage audit results from compliance efforts with other regulations to expedite NIS 2 compliance. Identify areas of alignment between existing audit results and NIS 2 requirements to streamline the process. Collaborate with knowledgeable partners to bridge any gaps and achieve compliance efficiently, minimizing disruption to operations.

6 Remove infrastructure complexity

Simplify your technology landscape by consolidating disparate technology stacks and adopting leading cloud-based security platforms. This consolidation reduces complexity and enhances compliance efficiency. Integrate relevant platforms covering cybersecurity aspects to create a cohesive IT ecosystem. Ensure seamless integration between platforms to reduce complexity further.

Industry Snapshot

The survey also sought to identify how industry segments compared in their NIS 2 readiness. Asking the entities how they would rate their organization's current cybersecurity hygiene, the results highlighted that industries with the highest overall security standards—such as the financial market infrastructure, banking, and chemical sectors—were rating themselves with the highest marks. Only around half of the respondents in the health and transportation sectors, as well as digital providers and public administration, were confident in their cyber hygiene.

NIS 2 is considered a top priority for leadership in **ICT services (44%)**, **financial market infrastructure (43%),** and **banking (38%)**, and is becoming a higher priority for those sectors that rate their cyber hygiene not as advanced, like **public administration (54%)**, **transportation (66%)** or **health (67%)**. The confidence level of IT leaders in their team's understanding of the NIS 2 requirements ranked the highest in **ICT services (63%)**, followed by **food (60%)** and **chemicals (56%)**. However, the sectors that have fallen behind in their **security practices—health (48%)**, **transportation (50%)**, and **public administration (54%)**—were only somewhat confident in their teams understanding of the requirements. This gradient indicates that there is more work to be done to reach compliance readiness by those segments that state their cyber hygiene is not as excellent.

Key:
↑ = Higher than European average
↓ = Lower than European average
* = Lowest/highest country result
s = same

Key Findings

62%(↓) of IT leaders in the chemicals sector feel confident their organization will meet NIS 2 compliance requirements by the deadline, even though this is also the sector with the largest share of respondents claiming to have already met the requirements **(29%)**

35% (↓) of IT leaders in the health industry believe their own teams fully understand the requirements for NIS 2 compliance

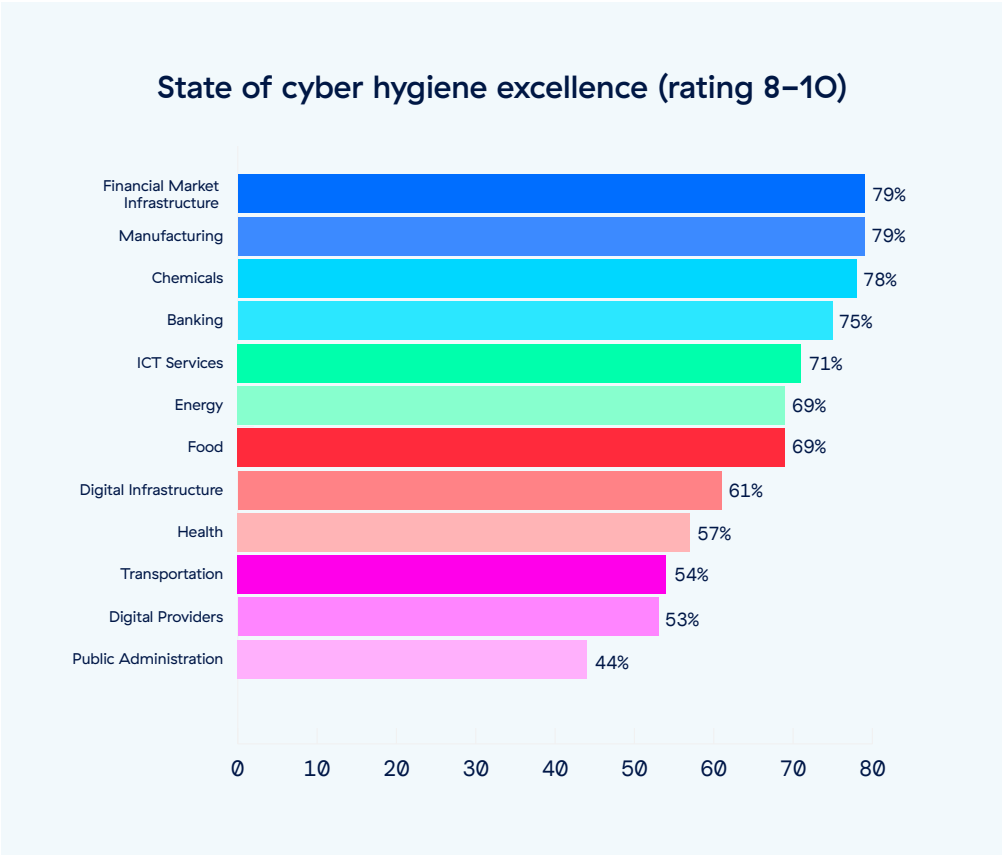
73% (↑) of IT leaders in the food production, processing, and distribution sector believe NIS 2 represents a significant departure from their current strategy, whereas only **48% (↓)** of respondents in the transport sector felt the same

55% (↑) of IT leaders in the transport sector have yet to implement a zero trust architecture as part of their cybersecurity approach

Only 49% (↓) of respondents in the public administrations sector believe their organization was advanced in its NIS 2 preparedness

60% (↓) of IT leaders in the energy sector say that keeping today's organizations cyber secure requires a mindset change that won't be brought about by a compliance exercise

67% (↓) of IT leaders in the food production, processing, and distribution sector do not believe that the NIS 2 regulations go far enough considering the scale of the cybersecurity challenge



Benelux

Key:
↑ = Higher than European average
↓ = Lower than European average
* = Lowest/highest country result
s = same

Key Findings

76% (*↓) of Benelux IT leaders feel confident their organization will meet NIS 2 compliance requirements by the deadline—**23% (*↑)** claim to have met them

Only 44% (*↓) of Benelux IT leaders believe their own teams fully understand the requirements for NIS 2 compliance, but curiously, slightly more **49% (s)** believe leadership fully understand them

A third (32%) (s) of Benelux IT leaders say NIS 2 regulations are one of the leadership team's top priorities. **56% (↑)** say they are becoming a higher priority

64% (↑) of Benelux IT leaders believe NIS 2 represents a significant departure from their current strategy

Only 21% (*↑) of Benelux IT leaders would rate their existing cyber hygiene as excellent

The three areas Benelux IT leaders are having to make the most significant changes to become compliant are: updating their **technology stack/cybersecurity solutions**, and **educating leadership** and **employees**

47% (↑) of Benelux IT leaders believe that tools and services have a critical role to play in a successful NIS 2 implementation

Almost two-fifths 37% (↑) of organizations have yet to implement a zero trust architecture as part of their cybersecurity approach

72% (↑) of Benelux IT leaders say that keeping today's organizations cyber secure requires a mindset change that won't be brought about by a compliance exercise

68% (*↑) of Benelux IT leaders do not believe that the NIS 2 regulations go far enough considering the scale of the cybersecurity challenge

Commentary

Despite low confidence levels, the Benelux region appears to have travelled further in its compliance journey than most countries in Europe, with almost a quarter of respondents claiming to have already met the requirements. However, for those that have yet to meet them, there is a big gap in understanding within local IT teams compared to the other countries and perhaps an even bigger gap in existing security standards with Benelux companies recording the lowest rate of cyber hygiene excellence.

"While the upcoming regulations will help to raise the bar for the bare minimum that companies must do to ensure compliance, CISOs shouldn't become too blindsided and forget to maintain wider cyber hygiene. There is a risk that security teams will be too busy trying to reach compliance in a specific area of the business that they start to neglect the parts that are already up to scratch. For organizations who have been proactive with their cybersecurity up to this point, they will already be compliant. But that shouldn't let them rest on their laurels. Bad actors will only continue to push the boundaries and so too should the defenders in repelling them."

—TONY FERGUSSON, EMEA CISO IN RESIDENCE (NEUR), ZSCALER

France

Key:
↑ = Higher than European average
↓ = Lower than European average
* = Lowest/highest country result
s = same

Key Findings

81% (↑) of French IT leaders feel confident their organization will meet NIS 2 compliance requirements by the deadline—**12% (↓)** claim to have met them

Only 51% (↓) of French IT leaders believe their own teams fully understand the requirements for NIS 2 compliance, and even fewer **(41%) (↓*)** believe leadership fully understand them

Only 19% (↓*) of French IT leaders say NIS 2 regulations are one of the leadership team's top priorities **but 60% (↑)** say they are becoming a higher priority

61% (↓) of French IT leaders believe NIS 2 represents a significant departure from their current strategy

Only 26% (↓) of French IT leaders would rate their existing cyber hygiene as excellent

The three areas French IT leaders are having to make the most significant changes to become compliant are: updating their **technology stack/cybersecurity solutions**, and **educating employees,** and **processes**

39% (↓) of French IT leaders believe that tools and services have a critical role to play in a successful NIS 2 implementation

Over two-fifths (43%) (↑*) of French organizations have yet to implement a zero trust architecture as part of their cybersecurity approach

71% (s) of French IT leaders say that keeping today's organizations cyber secure requires a mindset change that won't be brought about by a compliance exercise

50% (↓) of French IT leaders do not believe that the NIS 2 regulations go far enough considering the scale of the cybersecurity challenge

Commentary

French organizations are aligned with the European average in their confidence of achieving compliance by October, but there is a stronger sense that their leadership teams don't have a strong enough understanding of the regulation requirements or consider NIS 2 compliance high enough on their list of priorities. IT leaders in France also believe their cyber hygiene is lower than the European average, and France has the highest number of organizations that have yet to implement a zero trust architecture. This suggests that French organizations may face the biggest challenge to reach compliance.

"With the Paris Olympic Games around the corner, and a complex geopolitical landscape causing a rise of cyber risk, many large French organizations have already engaged in a reinforcement of their cybersecurity plans, including an adoption of zero trust. This is providing them with the confidence that they are on track to meet expectations of new compliance frameworks such as NIS2 and DORA. This confidence is reflected by 3 out of 4 respondents (75%) answering that France is advanced in its preparedness for the NIS 2 directive."

—IVAN ROGISSART, DIRECTOR SALES ENGINEERING, EMEA SOUTH, ZSCALER

Germany

Key:
↑ = Higher than European average
↓ = Lower than European average
* = Lowest/highest country result
s = same

Key Findings

79% (↓) of German IT leaders feel confident their organization will meet NIS 2 compliance requirements by the deadline—**15% (↑)** claim to have met them

Only 56% (↑) of German IT leaders believe their own teams fully understand the requirements for NIS 2 2 compliance, and even fewer **48% (↓)** believe leadership fully understand them

Only 26% (↓) of German IT leaders say NIS 2 regulations are one of the leadership team's top priorities but **57% (↑)** say they are becoming a higher priority

Only 43% (↓*) of German IT leaders believe NIS 2 represents a significant departure from their current strategy

Only 29% (↓) of German IT leaders would rate their existing cyber hygiene as excellent

The three areas German IT leaders are having to make the most significant changes to become compliant are: updating their **technology stack**/**cybersecurity solutions**, and **educating employees** and **leadership**

37% (↓) of German IT leaders believe that tools and services have a critical role to play in a successful NIS 2 implementation

Two-fifths (40%) (s) of German organizations have yet to implement a zero trust architecture as part of their cybersecurity approach

71% (s) of German IT leaders say that keeping today's organizations cyber secure requires a mindset change that won't be brought about by a compliance exercise

47% (↓*) of German IT leaders do not believe that the NIS 2 regulations go far enough considering the scale of the cybersecurity challenge

Commentary

In general, German IT leader responses trend very similarly to the average European results—they show confidence in achieving compliance despite gaps in understanding. Less than half of respondents, however, felt that the Directive would require significant change to current policies in order to reach compliance, suggesting that German organizations might be further along in their security journeys than the majority of countries in Europe.

"It's not uncommon for German companies to sell themselves short when it comes to compliance and security achievements, which is reflected by the low percentage of IT leaders who rated their cyber hygiene to be excellent. Despite this self-assessment, those basics are usually well set up in large enterprises. But the 'backbone of the German economy', the mid-sized companies, face a different challenge. Their mindset is to keep overhead costs low, so they have often delayed investments in modern IT and cybersecurity and will thus be highly impacted by NIS 2 requirements."

—CHRISTOPH SCHUHWERK, CISO IN RESIDENCE EMEA (CEUR), ZSCALER

Italy

Key:
↑ = Higher than European average
↓ = Lower than European average
* = Lowest/highest country result
s = same

Key Findings

77% (↓) of Italian IT leaders feel confident their organization will meet NIS 2 compliance requirements by the deadline—**13% (↓)** claim to have met them

Only 48% (↓) of Italian IT leaders believe their own teams fully understand the requirements for NIS 2 compliance, and curiously, slightly more **(49%) (s)** believe leadership fully understand them

35% (↑) of Italian IT leaders say NIS 2 regulations are one of the leadership team's top priorities and **47% (↓)** say they are becoming a higher priority

71% (↑) of Italian IT leaders believe NIS 2 represents a significant departure from their current strategy

Only 23% (↓) of Italian IT leaders would rate their existing cyber hygiene as excellent

The three areas Italian IT leaders are having to make the most significant changes to become compliant are: updating their technology **stack/cybersecurity solutions (28%)**, **educating leadership (16%)**, and **policies (16%)**

36% (↓) of Italian IT leaders believe that tools and services have a critical role to play in a successful NIS 2 implementation

Over two-fifths (42%) (↑) of Italian organizations have yet to implement a zero trust architecture as part of their cybersecurity approach

63% (↓*) of Italian IT leaders say that keeping today's organizations cyber secure requires a mindset change that won't be brought about by a compliance exercise

59% (↑) of Italian IT leaders do not believe that the NIS 2 regulations go far enough considering the scale of the cybersecurity challenge

Commentary

Italian IT leaders generally align with the European results but are slightly less confident that they will reach compliance by October 2024. Italy also had a lower percentage of respondents who rated their organization's cyber hygiene as excellent and a greater number of IT leaders claiming it would require a significant departure from their current security strategy to reach compliance. These results suggest that Italian organizations have not been reviewing and updating their security processes regularly and will need to put in significant effort to raise their standards ahead of the deadline.

"Italy saw the largest deviation from the European average when rating cyber hygiene excellence, with only 23% of Italian IT leaders rating it highly. From my consulting experience, organizations need support with the adoption of the appropriate policies to implement the desired security level. Vendor sprawling leads to great complexity of IT infrastructures and the lack of required technologies could lead to roadblocks or delays in achieving the compliance in the expected timeframe. The zero trust framework is a step in the right direction for Italian organizations, with 58% of businesses already adopting it and 39% with plans to do so."

—STEFANO ALEI, TRANSFORMATION ARCHITECT, EMEA SOUTH, ZSCALER

UK

Key:
↑ = Higher than European average
↓ = Lower than European average
* = Lowest/highest country result
s = same

Key Findings

82% (↑) of UK IT leaders feel confident their organization will meet NIS 2 compliance requirements by the deadline—**15% (↑)** claim to have met them

57% (↑*) of UK IT leaders believe their own teams fully understand the requirements for NIS 2 compliance, and **56% (↑*)** believe leadership fully understand them

46% (↑*) of UK IT leaders say NIS 2 regulations are one of the leadership team's top priorities, and **43% (↓)** say they are becoming a higher priority

74% (↑*) of UK IT leaders believe NIS 2 represents a significant departure from their current strategy

45% (↑*) of UK IT leaders would rate their existing cyber hygiene as excellent

The three areas UK IT leaders are having to make the most significant changes to become compliant are: updating their **technology stack/cybersecurity solutions**, **educating leadership**, and **educating employees**

54% (↑*) of UK IT leaders believe that tools and services have a critical role to play in a successful NIS 2 implementation

39% (↑) of UK organizations have yet to implement a zero trust architecture as part of their cybersecurity approach

80% (↑*) of UK IT leaders say that keeping today's organizations cyber secure requires a mindset change that won't be brought about by a compliance exercise

54% (↑) of UK IT leaders do not believe that the NIS 2 regulations go far enough considering the scale of the cybersecurity challenge

Commentary

Results in the UK generally trended more positively than the rest of Europe, with IT leaders feeling more confident about reaching compliance and believing that a higher percentage of both IT teams and leadership fully understood the requirements of NIS 2. UK respondents also believe most strongly that a mindset change is needed to keep organizations secure—something that is perhaps reflected in their comparatively high levels of cyber hygiene excellence.

> "From my experience working with UK organizations, they appear to be slightly ahead of continental Europe in preparedness for NIS 2 and general adoption of technology trends. There is an element of the British 'keep calm and muddle on' mentality, with many companies being more willing to accept these changes and roll with the punches. The business leaders I speak to are looking for practical and efficient ways to comply without having to strip everything back and start their security processes again. There is also a bigger appetite from UK organizations to capitalize on new technologies faster to support their ongoing security framework. Meanwhile, the rest of Europe is worrying about achieving NIS 2 compliance due to their extensive level of planning actually preventing any forward progress at this stage. This continental approach may provide dividends in the long run, but definitely delays the process."
>
> —MARC LUECK, CISO IN RESIDENCE EMEA, ZSCALER

Spain

Key:
↑ = Higher than European average
↓ = Lower than European average
* = Lowest/highest country result
s = same

Key Findings

83% (↑*) of Spanish IT leaders feel confident their organization will meet NIS 2 compliance requirements by the deadline—**12% (↓)** claim to have met them

56% (↑) of Spanish IT leaders believe their own teams fully understand the requirements for NIS 2 compliance, and **51% (↑)** believe leadership fully understand them

31% (↓) of Spanish IT leaders say NIS 2 regulations are one of the leadership team's top priorities, and **57% (↑)** say they are becoming a higher priority

59% (↓) of Spanish IT leaders believe NIS 2 represents a significant departure from their current strategy

36% (↑) of Spanish IT leaders would rate their existing cyber hygiene as excellent

The three areas Spanish IT leaders are having to make the most significant changes to become compliant are: **updating their technology stack/cybersecurity solutions**, and **educating employees** and **leadership**

51% (↑) of Spanish IT leaders believe that tools and services have a critical role to play in a successful NIS 2 implementation

35% (↓) of Spanish organizations have yet to implement a zero trust architecture as part of their cybersecurity approach

67% (↓) of Spanish IT leaders say that keeping today's organizations cyber secure requires a mindset change that won't be brought about by a compliance exercise

47% (↓*) of Spanish IT leaders do not believe that the NIS 2 regulations go far enough considering the scale of the cybersecurity challenge

Commentary

Spanish IT leaders were the most confident that their organizations will reach compliance by October and were also higher on average than most countries in believing that both IT teams and leadership fully understand the compliance requirements. Like their UK counterparts, Spanish organizations appear to be further along in their security evolution than other countries in Europe, but they differ from the UK in believing that the new regulations are a significant departure from what they already have in place.

> **"Regulatory initiatives like NIS 2 have a twofold positive effect on the security of organizations in Spain. On one side, the entities gain a better overview of the state of their security infrastructure, and on the other side, this security awareness will help to encourage further investment from the C-suite to improve the security posture. This survey underlined this trend, as 89% of Spanish respondents believe their leadership's current approach to cybersecurity is proactive, which is the highest of all European countries surveyed. However as the budget is not unlimited, IT teams do get challenged to spend money efficiently—hence, the reduction of infrastructure complexity is of utmost concern and a security platform based approach gets more attention."**
>
> —PABLO VERA ARANGO, REGIONAL DIRECTOR IBERIA, ZSCALER

Securing Front Foot Advantage

> "For us to truly unlock innovation in cybersecurity, regulation must work alongside it to encourage the adoption of a forward-thinking mindset that will see businesses modernize in line with the pace of new, transformative technologies. It'll take real vision, but leaders can't afford to stick to the status quo if the next decade is anything like the last."

—NATHAN HOWE, GLOBAL VICE PRESIDENT, INNOVATION, ZSCALER

For too long, businesses have operated reactively, addressing cyberthreats as they arise rather than proactively strengthening their defenses. However, the introduction of regulatory frameworks like NIS 2 and the upcoming DORA signals a shift, urging organizations to adopt a proactive approach to cybersecurity.

By methodically identifying gaps in existing security frameworks and presenting actionable steps, security teams can effectively communicate compliance requirements to the C-suite. Additionally, consolidating technology stacks and implementing cloud-based security solutions offer practical strategies to mitigate ongoing risks and improve cyber resilience.

While regulations prompt organizational change, it's vital to recognize that compliance alone doesn't drive innovation but rather ensures adherence to established standards. Therefore, regulatory audits should be integrated into an ongoing cycle, enabling security teams to stay updated on evolving threats and continually optimize security frameworks.

Embracing a proactive mindset and transforming cybersecurity approaches offer organizations a significant advantage. This not only facilitates smoother and more cost-effective compliance but also leads to risk reduction and improved business resilience. By prioritizing proactive risk management and cybersecurity preparedness, organizations can confidently navigate evolving threats and safeguard digital assets against emerging cyber risks in a fast evolving, and increasingly unstable world.

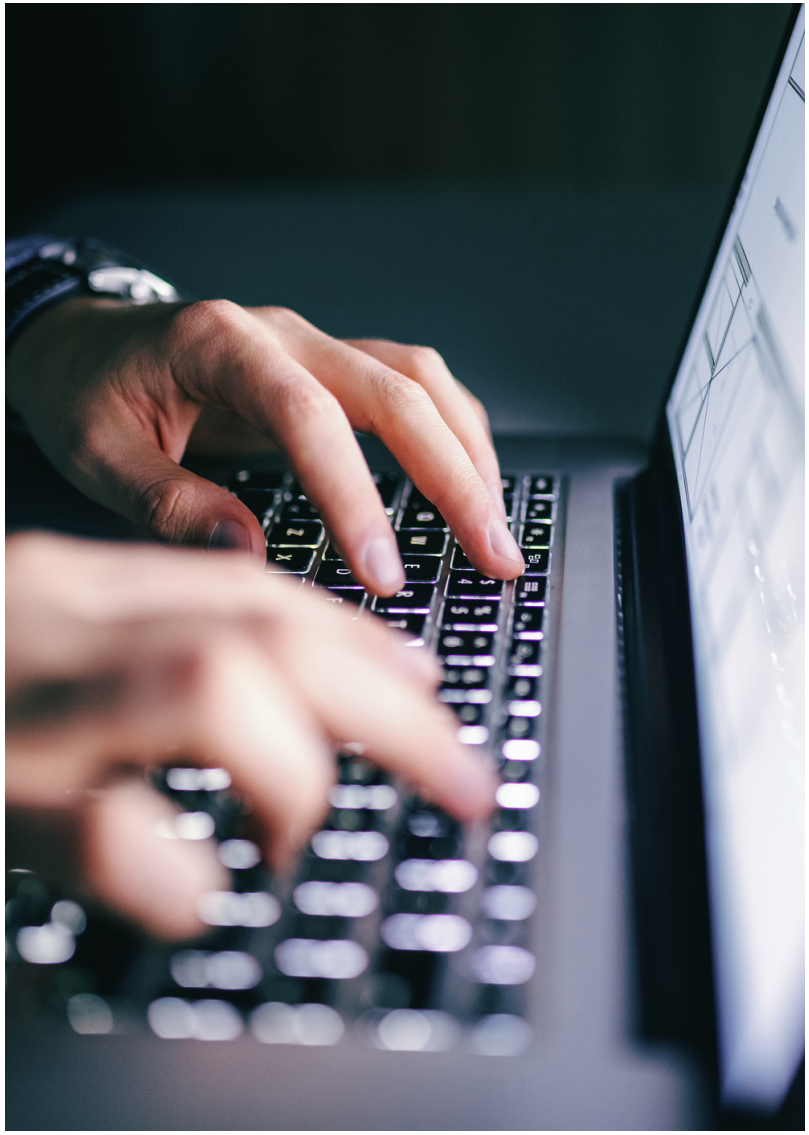
How Can Zscaler Help?

The Zscaler Zero Trust Exchange™ platform reduces the complexity associated with traditional network security, making it easier for organizations to meet the requirements of the NIS 2 Directive.

Employing granular segmentation to compartmentalize a network, enforcing least-privileged access to restrict user permissions, and maintaining continuous traffic monitoring are proactive measures Zscaler supports via the Zscaler Zero Trust Exchange™ platform that help to identify and respond to threat actors, minimizing potential damage and impact of attacks.

Implementing a zero trust architecture helps reduce an organization's attack surface, prevent lateral movement, and lower the risk of a breach. By abstracting security from the network infrastructure, Zscaler allows organizations to securely connect the right user to the right application without exposing their networks to the internet. This significantly mitigates the risk of attacks while helping organizations meet NIS 2's mandates for secure data handling, access controls, and incident management.

- **Zscaler Internet Access™** provides AI-powered protection for enterprise users, devices, and web and SaaS applications across all locations as part of the Zero Trust Exchange.
- **Zscaler Private Access™** safeguards applications by limiting lateral movement with least-privileged access, user-to-app segmentation, and full inline inspection of private app traffic.
- **Zscaler Risk360** delivers a comprehensive and actionable risk framework that helps security and business leaders to quantify and visualize cyber risk across the enterprise.
- **Zscaler Cloud IPS**, integrated with technologies like firewalls and sandboxes, provides comprehensive threat protection against various attacks, leveraging custom and industry-leading signatures for real-time monitoring and policy enforcement. Moreover, organizations can proactively identify and remediate vulnerabilities using Zscaler capabilities such as ZIA Advanced Threat Protection and Mobile Malware Protection policies, while Risk360 offers insights into the external attack surface and lateral propagation risk, enabling informed decisions to enhance an organization's security posture and reduce their mean-time-to-respond (MTTR).



Research methodology

In April 2024, Zscaler commissioned Sapio Research to conduct a survey of more than 875 IT decision–makers (IT leaders) across 6 markets (Benelux, France, Germany, Italy, Spain, UK). These IT leaders work at companies of 500+ employees and span 15 sectors governed by the NIS 2 regulations, e.g., financial market infrastructure, energy, public administrations, and health.

Experience your world, secured.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE—based Zero Trust Exchange is the world's largest inline cloud security platform. To learn more, visit www.zscaler.com

Zscaler Ltd, 7 Bishopsgate, London, EC2N 3AR, UK