Stratix

NIS2 for NRENs

A Call to Action

POSITION PAPER

Position Paper for the GN5-1 project partners
commissioned by GÉANT Association

Hilversum, 12-7-2023

Management Summary

The European Union has revised Directive (EU) 2022/2555 on Network and Information Systems Security (NIS2[1]). Member states are now busy implementing the directive, with the deadline set for 17 October 2024[2]. NIS2 applies to more sectors, and imposes more obligations, than the original NIS Directive (EU) 2016/1148.

In many cases, NIS2 will also apply to National Research and Education Networks (NRENs).

NIS2 can be advantageous for the NRENs – secure and robust networks are in the interest of their users and of society at large. However, its implementation can be complex and resource-intensive. NIS2 brings a risk-based and procedural approach to security that could be at odds with current practice.

This position paper looks ahead to the questions that need answering during the implementation phase of NIS2.

Firstly, NRENs must identify whether they fall under the scope of NIS2, and if so, under which category. This report provides some answers, but cannot do this for every organisation.

NRENs must find ways to not only become compliant but also minimise the impact of NIS2 on their organisation. We present several options for this. Discussions between technical people and legal people are inevitable.

A good starting point towards compliance will be one of the existing network and information security frameworks. GÉANT Association (GÉANT) and its member organisations have developed the GÉANT Security Baseline[3] and are making good progress on comparing NIS2 with Security Baseline. The ISO 27001 standard is also useful, but is much broader and thus not as fit for purpose as the Security Baseline. There is no ideal solution.

We also recommend that NRENs engage in talks with their governments. In many countries, the NRENs deal with the Ministry of Education and its regulator(s). For NIS2, NRENs must engage with organisations they are less familiar with. Customers, such as universities, face the same questions, therefore coordination between NRENs and their customers is advisable.

To summarise: NIS2 will not go away. It will lead to changes in your organisation and require a new balance between binary technical thinking and nuanced regulatory reasoning. Now would be a good time to embark on this voyage.

[1] Directive (EU) 2022/2555 (NIS2 Directive) https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[2] https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

[3] https://security.geant.org/baseline/

Contents

1 Introduction

In January 2023, the revised European Directive on Network and Information Systems Security (NIS2) came into force, with the goal of increasing cybersecurity across the whole European Union.

This directive expands the scope of the original NIS, and will have significant consequences for the research infrastructures within Europe. Some NRENs will certainly fall under NIS2, others partially or not at all.

NIS2 can be advantageous for the NRENs – secure and confident networks are in the interest of users and of society at large. However, implementation and compliance can be complex and resource intensive.

GÉANT, as the GN5-1 Work Package 8 (WP8) leader, wishes to help GN5-1 project partners (particularly the NRENs) in establishing their position regarding the NIS2 Directive, in order for them to respond effectively to the implementation in their respective countries.

GÉANT has therefore asked Stratix to create a position paper that can help organisations determine the key issues, risks, and possible responses to NIS2. This position paper looks ahead to the questions that need answering during the implementation phase of NIS2.

The paper is a recommendation from Stratix, as an independent party, which the recipients can follow as they see fit. Stratix has prepared this report from April through July 2023, using a combination of desk research and interviews with experts from NRENs, GÉANT and national regulators. We extend our gratitude to everyone who helped us. *Dankon!*[4]

[4] Esperanto for ‘Thank You!’

2 NIS2 in brief

2.1 The Directive

The NIS2 directive (EU) 2022/2555 is a revision of the NIS directive from 2016 (EU) 2016/1148[5] - which is still in force but will be repealed next year. Brussels reached a political agreement in November 2022. The directive entered into force in January 2023, which means that Member States now have until October 2024 for implementation.

2.2 Broader in scope than the original NIS

The NIS2 purpose is to "achieve a high common level of cybersecurity" across the EU Member States. The directive is a response to growing concerns about cyberattacks and the impact of cybercrime on society. All kinds of networks have been proven vulnerable, across economic sectors.

NIS2 expands the scope of NIS to more organisations and digital services. Annex I and Annex II of the directive define which networks are under consideration, including those for energy, water and transport, but also digital infrastructure and ICT service management. The directive is also much more specific in many areas. NIS2 sets requirements for management, risk control, business continuity and reporting to authorities, for all entities in scope.

Organisations in scope are considered "essential" entities or "important" entities, based on size and what services they offer. The important entities are to take an "all-hazards" approach to cybersecurity, and to set up a reporting process for any incidents with a significant impact.

In general, NIS2 will bring a risk-based and procedural approach to many more entities than previously included. A base of common sense, good faith and a balance between security (not very convenient) and convenience (not very secure), as was often seen in the past, will no longer be sufficient.

2.3 NIS Coordination Group and ENISA

NIS2 sets up new coordination mechanisms at the European level. ENISA, the European Agency for Cybersecurity, will oversee NIS2 as EU regulator. ENISA will coordinate information sharing and peer review, maintain a database of known vulnerabilities, write annual reports and more.

The governing body is the NIS Coordination group, where Member States work together with ENISA and the European Commission[6]. The Coordination Group will support Member States and the European Commission during the implementation phase. It will also exchange best practices and information with public and private stakeholders.

[5] https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[6] NIS2, Article 14

2.4 National implementation in progress

Member States have to implement NIS2 and transpose the text into national law by 17 October 2024[7]. By that date, the European Commission will also publish implementing acts, clarifying certain elements.

Some Member States have started to prepare, but it’s early days.

The implementation of the earlier NIS directive proved challenging, and led to differences between Member States. Although one stated aim of NIS2 is to reduce the differences between countries, implementation of NIS2 is still likely to be different in each country.

As usual, the influence of EU law extends far outside the EU27. This is also true for GÉANT members in countries outside the EU.

[7] NIS2, Article 41

3 Potential issues for NRENs

NIS2 is certain to influence NRENs in a number of ways, depending on what services they offer, and other factors, including the size of organisation. Clients, such as universities and research bodies, and their suppliers will also be affected.

Firstly, NRENs must identify whether they fall under the scope of NIS2, and under which category. This report summarises the criteria, but national differences make every case unique.

3.1 Are NRENs in scope?

The scope of the NIS2 directive is much wider than that of the original NIS directive. the GN5-1 project partners (NRENs) may or may not be in scope, depending on size, organisational structure, ownership structure and legal situation, and the products and services offered[8].

The first step taken by an NREN should be to find out whether or not NIS2 is applicable.

3.1.1 Size does (not) matter

NIS2 comes with size thresholds, because the European Commission knows that the regulatory burden may be too high for small enterprises.

The NIS2 directive does not apply to small and micro-enterprises[9], *except* for providers of a few specific services. This means that NRENs with fewer than 50 employees, and an annual turnover under EUR 10 million, and/or an annual balance sheet under EUR 10 million may not be in scope. According to the GÉANT NREN Compendium, many NRENs are below these limits.

The directive does apply to medium-sized enterprises (up to 250 employees and EUR 50 million turnover and/or 43 million balance sheet), however, they may not be regarded as essential entities, depending on their service offering.

With NIS, governments were able to set thresholds in such a way that small and medium enterprises (SME) were exempt, even though they provided critical digital services. This time, the thresholds are stricter. That means that even small NRENs may fall under NIS2, if they are providers of critical services.

In addition, some articles of NIS2 state that an entire organisation is in scope, even if only a small part of it handles sensitive data.

3.1.2 Some NRENs are a public entity

Regardless of size, however, the directive applies to any NREN which is a "public administration entity" (according to the definition in NIS2 Article 6, Clause 35).

[8] NREN Compendium 2021, (2022), https://resources.geant.org/wp-content/uploads/2022/07/Compendium-2021-web.pdf

[9] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises http://data.europa.eu/eli/reco/2003/361/oj

At first glance, all NRENs would seem to fit the definition, but this is not certain (it depends, among other things, on the precise interpretation of "bodies governed by public law", which has been subject to debate). An NREN which is part of a ministry or controlled by a ministry is clearly a "public administration entity", whereas an NREN which acts as a private company, funded through revenues from the universities, may not be.

3.1.3 Some NRENs may be a public network

In some cases, an NREN may be regarded as "provider of publicly available electronic communications services" (a category explicitly mentioned in the directive as highly critical), while NRENs in other countries may not. This will depend on the exact wording of the definition in national legislation, and even on interpretation by the courts.

SURF in the Netherlands has seen this before. In 2007, telecoms regulator OPTA (now ACM) forced SURFnet to register as a public provider of network services. A court verdict in 2012 overturned this decision and lifted all obligations.

In our investigation we have found that some NRENs are already facing questions about this topic.

3.2 Many services in scope

NRENs also vary in what services they offer to their users. We know that many NRENs currently offer services that are explicitly mentioned in NIS2. These include:

- DNS (authoritative resolution for third parties, or publicly available recursive DNS[10])
- Public TLD / Registry services
- Certificates/trust provision
- Internet Exchange services
- Public ISP services
- Cloud computing services
- Data centre services

The European Commission will publish implementing acts by October 2024, including one on public recursive DNS.

Even the smaller NRENs may find that they are in scope for NIS2, regardless of size, if they offer any of the above services.

Note that the NIS2 scope for DNS services has been revised since the earlier draft. GÉANT and several NRENs (as well as research institutions) spotted an issue with this draft[11], which stated that there would be unintended consequences for DNS providers that only provide the service for their own websites. This issue has been resolved in the final version, with this type of DNS provider now being out of scope.

[10] NIS2 Recital 32, and Article 6 (20)

[11] https://connect.geant.org/2021/01/22/running-you-own-dns-service-there-may-be-changes-ahead

3.2.1 NREN already in scope of NIS

NRENs have always been active developers of ‘the Internet’, from an academic curiosity to what is it today. This is why the NREN manages parts of the national IT infrastructure in many countries.

For example: in Austria, ACOnet and University of Vienna run the Vienna Internet eXchange (Vix.at). KIFÜ in Hungary controls large swaths of backbone infrastructure for the public and private sector.

For these organisations, NIS2 was not the first piece of security regulation they have encountered. ACOnet and KIFÜ were already in scope for NIS. Nevertheless, every new regulation in this area will require effort during implementation and constant monitoring afterwards.

3.3 A patchwork of EU Law

The NIS2 directive is not the only standard addressing information security. The European Union has developed a number of regulations, addressing security risks for different sectors within society, including the following:

- GDPR – the General Data Protection Regulation[12] – sets the requirements for the handling of sensitive user data by any organisation.
- CRA – the Cyber Resilience Act[13] - is expected to bolster cybersecurity rules to ensure more secure hardware and software products. It was developed in parallel with NIS2, but aimed at products with digital elements. The CRA is still being debated between Member States and in the European Parliament.
- CER – the Critical Entities Resilience directive[14] – will help protect vital society functions including data networks against natural disasters and man-made contingencies. Published on 14 December 2022, it has the same deadline for implementation as NIS2, i.e. 17 October 2024. GÉANT and members have already identified overlap between NIS2 and CER.
- The Directive on Digital operational resilience[15] (DORA) for the financial sector is yet another example of new sectoral rules.

In many areas, these regulations overlap. Sometimes they use common language and common sense, like requirements for strong authentication. In other places, the language and definitions are just-not-identical, potentially leading to contradictions or too specific measures.

The European Network and Information Security Agency (ENISA) was created in 2004. In 2019, a new EU Regulation[16] gave it a permanent status as the European Agency for Cybersecurity. ENISA is dedicated to achieving a high common level of cybersecurity across Union law.

[12] https://eur-lex.europa.eu/eli/reg/2016/679/oj
[13] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
[14] https://eur-lex.europa.eu/eli/dir/2022/2557/oj
[15] http://data.europa.eu/eli/reg/2022/2554/oj
[16] https://eur-lex.europa.eu/eli/reg/2019/881/oj

3.3.1 National or sector-specific regulations

To complicate matters even further: NIS2 is a broad regulation that will add to existing national and sectoral regulations.

For example, the Dutch government has developed policies for the protection of 'vital' infrastructure[17], including networks for energy and water, transport, banking and telecommunications. The Netherlands was ahead of CER and NIS2 in this. Confusingly, the word vital is translated into English as 'critical' but it's not the same as 'critical' in the CER. Nor is it the same as 'essential' or 'important' in NIS2. Solving this synonym-bingo will be crucial.

3.4 A patchwork of government departments

NIS2 will expand its scope quite dramatically. NIS was limited to certain sectors of the economy and thus a smaller set of government organisations. This time, pretty much any digital infrastructure will be in scope, so the number of government departments and regulators involved will increase.

The government perspective is that tens of thousands of private companies could suddenly be in scope for NIS2. This is not a small matter, as explained in an interview with a regulator. The patchwork of new EU Laws makes scoping difficult as well.

In most countries, NRENs deal with their 'historical' government organisations. The same can be said for many clients or organisations connected to the NREN network, who will also be in scope. The Department of Education may be the primary government department for universities and research institutions. University hospitals, however, also deal with the Ministry of Healthcare.

Information security/cybersecurity are often in a different government domain than Education. Depending on history, services and users, government domains involved may include Defence, Economic Affairs, Justice, Internal Affairs, Foreign and Commonwealth Affairs (GB) and Infrastructure.

For many regulators that NRENs know well, the subject matter will also be new. Inside government, responsibilities will be redefined. Regulators may or may not be able to offer assistance, based on capacity and priorities.

3.5 NIS2 will be felt outside the EU

The 27 Member States have reached an agreement over NIS2. The GÉANT network extends into 100+ countries[18]. Other governments may or may not implement NIS2 directly, but will indirectly feel its influence.

Some countries implement EU law, like Norway and Iceland. Others are not bound by NIS2, but will implement the basics to stay aligned with the single market. The UK implemented NIS

[17] https://english.nctv.nl/topics/critical-infrastructure-protection
[18] https://about.geant.org/membership/membership-map/

because it was still in the EU. It is planning to implement a NIS update very similar to NIS2[19]. The UK NREN (and GÉANT member) JISC has already started working on the subject[20].

Candidate countries will implement EU regulations with the goal of EU membership. One NREN said that the translation from the leading English (or French) text into the national language led to contradictions between existing law and NIS2, contradictions that are codified into legal text and hence difficult to solve.

These differences will make it harder to find a consistent approach for every NREN and solutions that work for everyone.

3.6 The CSIRT network will change

One of the changes in NIS2 is that the CSIRT network will be fortified. Each Member State shall designate or establish one or more Computer Security Incident Response Teams (CSIRTs)[21]. Assisted by ENSIA, the teams should work to improve information sharing, incident reporting, coordinated response etc.

At the time of writing, ENISA listed 556 teams in the European Union, 47 of which had an NREN as a constituent[22]. In some countries, several universities are listed. Thus NRENs are already familiar with a CERT or CSIRT, but the hierarchy and requirements will certainly change with NIS2.

A sectoral team under existing governance could be very small, and thus poorly equipped for the changes coming up. Some NRENs may gear up and continue to be a CSIRT, others may come under supervision.

3.7 Supply Chain effects

It must be noted that some suppliers or clients may be designated as essential or important entities under NIS2. NIS2 requires entities in scope to analyse their networks including supply chains and ask the right questions about risks and mitigating measures.

NRENs can procure services that are covered by NIS2. That means a supplier can be an essential or important entity.

NRENs also supply services to universities and other stakeholders. This could lead to the case where an NREN is not directly in scope for NIS2, but still has to implement some of the same measures, because a customer or a supplier is a NIS2 entity. These obligations will have to be addressed in (renegotiated) private contracts.

[19] https://www.mwe.com/insights/regulating-cybersecurity-across-the-eu-and-the-uk/

[20] https://www.mwe.com/insights/regulating-cybersecurity-across-the-eu-and-the-uk/

[21] NIS2, Article 10

[22] https://www.enisa.europa.eu/topics/incident-response/csirt-inventory/certs-by-country-interactive-map, retrieved on 29 June 2023.

Member States may decide to bring universities into scope that work in research areas like 5G/6G or quantum computing. Thus, universities would be obliged to check that their supply chain is NIS2 compliant.

It should also be noted that ‘critical research activities’ are not specified in NIS2. Discussions have shared that universities are unhappy with the prospect that their entire organisation will be in scope, rather than just a few faculty departments.

> Member States may provide for this Directive to apply to: (a) public administration entities at local level; (b) education institutions, in particular where they carry out critical research activities.[23]

[23] NIS2, Article 2.5

4 Solutions to consider

NRENs must find ways to become compliant, or otherwise, find ways to minimise the impact of NIS2 on their organisation. There are a number of options:

NRENs can change their own organisation by realigning their product and service offering, or embrace change and find ways to influence the road to compliance via regulatory measures.

4.1 Changes in the organisation

4.1.1 Reshuffle services within the organisation

NIS2 distinguishes between essential services and important services. The essential services fall under a stricter regime and will probably come with ‘ex-ante’ oversight. The regulator will play a more active role (if it can find the time and priorities).

Important services fall under a lighter regime and ‘ex-post’ oversight. This could mean that incidents are investigated. The government regulator may or may not be able to offer help and guidance.

Moving essential services into a separate entity may limit some of the impact of NIS2 to that specific entity.

Note that according to Recommendation 2003/361/EC, setting up a separate entity under control of the NREN does not affect the size criteria (a combination of an entity controlled by a another entity is considered a single enterprise for the size category, unless it can truly operate independently[24]) It however does allow the remainder of the NREN to stay outside of the scope of NIS2 if the only services it offers are moved into the new entity.

Both options could fit the scenario when the regulator has to set priorities and will not help. The directive allows regulators to set priorities following a risk-based approach[25]. We hear that regulators are bracing for impact of a much bigger NIS2 that can put tens of thousands of essential organisations under supervision.

4.1.2 Sector-specific regulations may supersede NIS2 rules

The Danish NREN, DeiC, has been told by its government that NIS2 will *not* be applicable. This organisation falls under sectoral regulations already, coming from the healthcare sector.

Article 4 of the NIS2 directive says:

> “Where sector-specific Union legal acts require essential or important entities to adopt cybersecurity risk-management measures or to notify significant incidents and where those requirements are at least equivalent in effect to the obligations laid down in this Directive (…)”

[24] NIS2, Recital 16
[25] NIS2, Article 31

This potential escape clause warrants further investigation by NRENs. It would still require compliance work, but not a full NIS2 exercise.

4.1.3 A 'home country' for international networks

Article 37 of the directive is relevant for organisations that are located in or provide services in more than one Member State.

> Where an entity provides services in more than one Member State, or provides services in one or more Member States and its network and information systems are located in one or more other Member States, the competent authorities of the Member States concerned shall cooperate with and assist each other as necessary.

The competent authorities shall cooperate, provide a 'single point of contact' and offer mutual assistance when requested. This could mean that NRENs in a larger network that cooperate closely, could fall under a 'Home Regulator'. The NIS2 implementation will be guided by one Member State and at least some of the regulatory effort will be shifted to that entity.

This could be relevant to several networks, including GÉANT and NORDUnet. NORDUnet supplies connectivity between the five Nordic NRENs, and is based in Copenhagen. It is likely that NORDUnet will be in scope for NIS2, but for its members that is still to be decided.

This topic could also be relevant to entities such as EGI, a federation of computing and storage resource providers for research and development.

4.2 Halt or buy-in certain services

The amount of regulation for the tech and internet sector will continue to grow. Transaction costs and the effort to show and maintain compliance with NIS2 may simply become too high to justify continuing products that were developed in the past without this level of oversight.

One interviewee expressed his regrets that it is no longer possible to build networks or services like he used to. "Legal and regulatory people simply don't speak the same language as software engineers."

If halting services altogether is not wanted or feasible, it could be an option for an NREN to assume the role of a broker for these services, rather than building or acquiring them. Note that NIS2 still requires companies to analyse the level of network and information security with their suppliers. Purchasing services can shift the burden of proof to suppliers, but an NREN may still be responsible. Taking a broker role (arranging the terms of contract without being a party to it) may help circumvent such responsibilities.

4.3 Embrace change

The opposite approach is also possible. NIS2 could be a catalyst for change: it can be used as a way to take up new responsibilities in cooperation with other stakeholders. To change the organisation, to find budget and start doing things differently.

One of the sources for this report took a pragmatic view, saying that reaching compliance doesn't require actually changing much in the organisation. Rather, it is key to carefully document the processes of an organisation and be able to explain why they are compliant.

As discussed earlier, (cf. section 3.2.1) many NRENs have experience with NIS or other existing regulations. An NREN that already runs a CSIRT may consider becoming a CSIRT under NIS2 and influence the outcome, knowing that NRENs are certain to fall under a CSIRT and ENISA as EU agency anyway. ENISA has done a lot of work for NIS and NIS2 and is able to provide advice and best practices[26].

This is not a straightforward choice however, as the requirements will be different, for example, on incident reporting: a CSIRT *has* to report every incident almost immediately, whereas a CERT does not.

4.4 A range of cybersecurity frameworks to choose from

NRENs can adopt a well-proven existing certification scheme. After all, many of the basic requirements are common sense. Using an established framework can be helpful. Public and private organisations have already developed a broad range of standards in response to earlier regulations, which addresses different risks for different sectors.

The European Union Agency for Cybersecurity, ENISA, has set up a framework[27] which communication service providers can use to show compliance with the security aspects of the European Electronic Communications Code (EECC), but which can also be used for other purposes.

Based on this framework, ENISA has created a more specific security baseline for 5G networks[28], and is currently working on a similar baseline for cloud computing.

The European Commission has also developed the 5G Toolbox[29] in response to concerns about mobile network security and the influence of High Risk Vendors (HRV) vendors from outside the EU. While the so-called Strategic Measures are geopolitically sensitive, the Tactical Measures are a detailed and risk-based blueprint for computer and network security.

4.4.1 National frameworks

Governments in Europe have also developed their own national frameworks, written in the national language and referencing national law, such as *Baseline Informatiebeveiliging Overheid (Baseline for Government Information Security)* in the Netherlands.

In Germany, the Bundesamt für Sicherheit in der Informationstechnik (BSI) develops standards and best practices. In the UK, the Cyber Assessment Framework (CAF)[30] provides guidance for organisations responsible for vitally important services and activities.

[26] For example: https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc
[27] https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc
[28] https://www.enisa.europa.eu/publications/5g-security-controls-matrix
[29] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2020:0050:FIN
[30] https://www.ncsc.gov.uk/collection/caf

The Center for Internet Security (CIS)[31] is also an influential body. It is a resource for every level of government in the United States and has developed standards and best practices that are widely used around the world.

The National Institute of Standards and Technology (NIST) is a US federal agency active in this field, also with global influence.

4.4.2 Private frameworks

GÉANT has developed its own approach to Business Continuity Management (BCM) and Information Security Management: the GÉANT Security Baseline[32]. This approach is based on international standards, generally accepted principles and measures, but is also adapted to the needs of NRENs.

The GÉANT Security Baseline has three, Security Maturity levels. The first defines a GÉANT-wide minimum of security and is expected to be met by most NRENs by default and implemented by all NRENs in the short term. This first level contains basic requirements that form the basis for an effective security programme within an organisation.

NRENs should ensure compliance with this level and implement missing requirements as quickly as possible. Implementing GÉANT Security Baseline will achieve much of what is necessary for NIS2.

In addition, many NRENs are familiar with the ISO/IEC 27000 series of information security standards, some are even certified for ISO27001 for the whole or part of their organisation. IEC 62443, while primarily designed for industrial automation and control, provides a slightly different approach, which can be adapted for use in networking and network automation.

One caveat, however, both the GÉANT Baseline and the ISO standard are control frameworks, designed to implement measures that improve security. An organisation should start with a risk-based analysis to not only find its weak spots, but to also implement a risk-based process (Plan-Do-Check-Act cycle) to ensure ongoing efforts to find and fix security issues.

[31] https://www.cisecurity.org/

[32] https://security.geant.org/baseline

5 Recommendations

NIS2is not going away, and will increase the amount of regulatory oversight. Organisations should to start preparation now, if they seek to influence the outcome. The implementation phase only started this year and will run until 17 October 2024, so there's still time.

5.1 Accept that the world has changed

The challenge will be to implement the changes without too much extra paperwork.

You may need to bring in new expertise in regulatory affairs and policy making, in order to perform a risk-based approach. Granted, it is frustrating to get seven opinions from five different legal advisors. As one interviewee said: "In law, 'AND' is NOT a logical operator!"…

5.2 Implement a framework

A good starting point towards compliance is the implementation of existing network and information security frameworks. ISO 27001 addresses risk management.

GÉANT and member organisations have developed the GÉANT Security Baseline and are making good progress of comparing ISO 27001 with NIS2. ISO 27001 is useful, though not as fit for purpose as the GÉANT Security Baseline. The ISO 27001 family is much broader in scope and contains a long list of requirements (controls) that are often 'pass or fail'. Compliance is dependent on following the latest version and all its annexes.

In an effort to compare frameworks, GÉANT members are analysing the requirements of the Baseline, ISO27001, BCM and NIS2[33]. A preliminary assessment showed that ISO27001 alone will not be sufficient.

NIS2 will also bring obligations for governments. These include strategic and organisational measures that a control framework simply does not address. The reporting obligations[34] are a case in point – 'without undue delay and in any event within 24 hours' will hinge on national implementation.

There will also need to be a gap analysis, showing what NRENs will need to address from NIS2 that cannot be fully covered by either the Security Baseline or ISO27001.

5.3 Work together in the GÉANT network

While there are significant differences between NRENs, there is scope for a coordinated approach. NRENs can share best practices, learn from each other, agree on common positions to

[33] As discussed in the Spring Meeting for SIG-ISM Members held on 3 May 2023 in Trondheim, Norway.

[34] NIS2, Article 23

present to their governments, and develop common frameworks to implement the NIS2 obligations.

GÉANT will play a role, and indeed has already taken steps, setting up the Wiki pages on NIS2[35] and holding regular meetings[36]. The Wiki on NIS2 will be expanded in due course. GÉANT Infoshare meetings will also be held on a quarterly basis to discuss developments and new insights.

GÉANT is well placed to facilitate cooperation, gather information and share knowledge. Active contribution to that discussion will be valuable.

5.4 Work together with your user organisations

NRENs provide their services to universities, schools, university hospitals, scientific organisations, government branches and many other clients. Those organisations may also fall under NIS2 (in particular research organisations) and feel the impact.

Many of your clients have just become aware of NIS2 themselves and are looking for answers. For an NREN it's possible to discuss NIS2 within their branch organisations and with their regulators.

An NREN is probably not in a position to lobby on behalf of clients. But working together will help to get your voice heard.

5.5 Talk to your government

Government organisations are also facing challenges in multiple fields. The directive must be transposed into national law. It takes time to check every article in existing laws and update every reference. At the same time, the regulators must redefine their tasks and find ways to cooperate, set priorities and adapt their procedures for NIS2 and other upcoming legislation.

At this point in time, many governments are still in a very early stage of drafting national legislation - if they have started at all.

There are also still opportunities to engage with stakeholders and the legislators to see if the national law and implementation can be steered in a helpful way. Or to see whether other sectoral regulations can be used to argue the case that NIS2 should not be applicable.

It's understandable that NRENs do not have the time and budget to review and draft legislation, therefore cooperation with other stakeholders is a good idea, as is asking the regulator for guidance.

[35] https://wiki.geant.org/display/SIGISM/NIS-2+Directive

[36] GÉANT Infoshare II on NIS-2, (2023), https://wiki.geant.org/download/attachments/586645525/230111%20NIS2%20Infoshare%20V4.pdf

CONTACT

About Stratix

Stratix is an independent research and consultancy company specialised in communication infrastructures and services. For 30 years we have been focusing on sectors where ICT networks play an important role: telecommunications and media, but also energy, scientific research and real estate. Within these segments we support a variety of clients with tactical and strategic issues, including government organisations, telecom providers, telecom users, investors and interest groups.

The Stratix team consists of experienced consultants with extensive knowledge of the technical, financial-economic, regulatory and social aspects of communication infrastructures. From these perspectives, we analyse your issue - whether it's market research, policy advice, guidance with a tender & contract or an investment decision. In order to base our advice on data from actual practice, Stratix maintains the broadband atlas of the Netherlands on its own initiative. Stratix has an extensive network within industry, government and academia, and always focuses on finding the most suitable team for the assignment(s) to make the connection between science, policy and practice in its work. Stratix' mission is to provide real perspective.

Stratix is not affiliated with service providers, suppliers or any other organisation. Its structure and business model guarantees the quality of our work and fast, flexible solutions.

Stratix

Stratix B.V.
Villa Looverhoek – Julianalaan 1
1213 AP Hilversum
The Netherlands

Telephone:	+31.35.622 2020
E-mail:	office@stratix.nl
URL:	http://www.stratix.nl
Reg. no.:	57689326
IBAN:	NL85ABNA0513733922
BIC:	ABNANL2A
VAT:	NL8526.92.079.B.01