Reg. no. TRAFICOM/18410/09.00.02/2023

19 September 2024

Summary of statements on the Traficom's draft recommendation on cybersecurity risk management measures referred to in the NIS2 Directive for NIS supervisory authorities

Contents

1 The Finnish Transport and Communication Agency Traficom’s draft recommendation

1.1 Statements on Traficom's draft recommendation

The National Cyber Security Centre Finland at the Finnish Transport and Communications Agency (later referred to as ‘Traficom’) requested statements on the draft recommendation on cybersecurity risk management measures referred to in the NIS2 Directive for supervisory authorities. The draft recommendation was circulated for comments in Finnish on the lausuntopalvelu.fi service for eight weeks between 5 April 2024 and 31 May 2024 (register number: Traficom/18410/09.00.02/2023).

Sixteen statements on the draft recommendation were received in total.

The parties issuing statements represented supervisory authorities and entities within the scope of the legislation as well as parties not falling within its scope. Statements on the draft recommendation were issued by the following: Confederation of Finnish Construction Industries RT, Confessional Lutheran Church of Finland, Ministry of Agriculture and Forestry’s Information and Research Division, Finnish Information Security Cluster FISC, FiCom, Finnish Water Utilities Association, Finnish Shipowners’ Association, Confederation of Finnish Industries EK, National Supervisory Authority for Welfare and Health Valvira, Association of Finnish Local and Regional Authorities, Finnish Food Authority, Finnish Energy, Finnish Medicines Agency Fimea and the Information Management Board. Verizon also submitted a general statement on the uniform implementation of the NIS2 Directive in the Member States. The Finnish Safety and Chemicals Agency Tukes had no comments to make.

1.2 Summary of statements

According to the statements received, the draft recommendation was generally found to be supportive of the supervisory authorities and entities. It was felt that the recommendation translates the practical implementation of the risk management obligations imposed by the legislation into concrete terms. As a basic premise, the content of the draft recommendation was regarded as being comprehensive and having a clear structure, as it is consistent with the structure of the Government proposal for an Act on Cybersecurity Risk Management for the corresponding parts. Parties issuing statements found that the presentation in table format supported the comprehensibility of the recommendation. They welcomed the fact that each individual measure of the recommendation was explained and contains a clear reference to the relevant frameworks.

On the other hand, examination of each risk management measure individually and separately from other requirements was also found challenging, as this can guide entities to manage each risk with the same intensity. Parties issuing statements would also like to see more attention being paid to the possibility of the measures offsetting each other. The recommendation was additionally regarded as long in terms of its page count, which is why a summary of the management measures was called for.

The recommendation consciously strives to present each risk management measure as an independent entity and to describe its content, which results in partial overlap between the example implementations. The explanation paragraph included in each individual risk management measure discussed in the recommendation was regarded as serving as a summary.

The terminology of the recommendation was clarified, and the references used in the recommendation were specified as suggested in the feedback. The introductory text of the recommendation was complemented, and detail was added to it insofar as the feedback received concerned the principle of proportionality, management accountability, risk-based approach and relationship between the recommendation and any further technical regulations to be issued by the authorities. In addition, the instructions for reading the recommendation were supplemented with a more specific definition of entities with a higher level of cyber risk.

Perceiving the correspondence between the risk management measures included in the recommendation and the frameworks used in it (standards and sets of assessment criteria) was experienced as a challenge. While a cross-reference document drawn up by Traficom was appended to the recommendation as a response to this feedback, the introductory text of the recommendation were supplemented to avoid a possible misunderstanding of it constituting harmonised standards that would directly meet the requirements of the Act.

Comments on the risk management measures included in the recommendation were provided in both general statements and those specific to individual measures. The recommendation was primarily updated in keeping with the amended Government proposal for an Act on Cybersecurity Risk Management, after which the feedback received on cybersecurity measures during the consultation was taken into account as far as possible by modifying the recommendation or adding detail to it. The observations concerning sector-specific standards and guidelines were added to the recommendation as proposed.

In addition, feedback directly related to the supervision of and resources for risk management measures was received in connection with the consultation, which could not be taken into account in the recommendation. Any feedback concerning supervision and entities' resources will, as far as possible, be passed on to the supervisory authorities as part of Traficom's future role as the single point of contact referred to in the NIS2 Directive.

According to the feedback received, organising the consultation before Parliament had finished debating the Act on Cybersecurity Risk Management was considered problematic, a fact of which Traficom was also aware. Traficom requested comments on the draft recommendation despite the challenging timing of the consultation, as even if the draft was incomplete, it was deemed to translate the implementation of the risk management measures into more concrete terms and to support especially those supervisory authorities and entities who are new to the scope of this legislation.

2 General statements on the draft recommendation

2.1 The recommendation’s support of supervisory authorities and entities

As a whole, the recommendation was regarded as being a good starting point for supervision and supporting the supervisory authorities in the uniform application of national regulation across sectoral boundaries. While the draft recommendation harmonises supervisory practices in different sectors, it allows the supervisory authority scope for case-by-case discretion (Confederation of Finnish Construction Industries RT, Ministry of Agriculture and Forestry, Finnish Information Security Cluster (FISC), Confederation of Finnish Industries EK, National Supervisory Authority for Welfare and Health Valvira, Association of Finnish Local and Regional Authorities, Finnish Medicines Agency Fimea, FiCom).

The recommendation was deemed necessary at the general level, as the example implementations of the draft recommendation cover the risk management measures referred to in the NIS2 Directive, and they were felt to guide, support and harmonise the proportionate assessment and planning of entities' risk management as well as risk management implementation (Confederation of Finnish Construction Industries RT, Ministry of Agriculture and Forestry, FiCom, Finnish Water Utilities Association, Finnish Shipowners' Association, Association of Finnish Local and Regional Authorities).

Parties issuing statements also welcomed the fact that the means of implementation and verification contained in the recommendation vary depending on the entity and the sector, providing examples of what the requirements mean in practice and to which aspects of compliance the supervising authorities will pay attention (Information Management Board, FiCom).

The recommendation was welcomed as a means of optimising guidance because the risk management measures contained in it focus on the uncertainty about the predictability and consistency of official supervision resulting from the decentralisation of supervision (Finnish Information Security Cluster (FISC)).

It was felt that the good practices set out in the recommendation could also be used to guide entities that do not directly fall within the scope of the legislation implementing the NIS2 Directive (Finnish Medicines Agency Fimea). It was believed that the entities could also draw on the applicable parts of the recommendation to assess their service providers and service agreements (Association of Finnish Local and Regional Authorities).

The fact that the legislation also covers many partners who provide external services to entities was also regarded as a positive (Finnish Medicines Agency Fimea).

2.2 The comprehensive content and clear structure of the recommendation

The draft recommendation was generally deemed comprehensive, clear, versatile and practical (Association of Finnish Local and Regional Authorities, Finnish Medicines Agency Fimea, Ministry of Agriculture and Forestry). The fact that the implementation and verification examples in the draft recommendation follow the structure of the NIS2 Directive and are presented in the same order as in the proposed Act on Cybersecurity Risk Management was considered positive (Ministry of Agriculture and Forestry, Finnish Food Authority, FiCom).

The presentation of the content in table format was felt to make the draft recommendation easier to understand (FiCom). The division into separate sections on examples, verification, explanations and references as well as extended instructions was also considered good (Finnish Shipowners' Association). The fact that individual recommendations are explained and that there is a clear reference to the sources associated with each measure, such as standards, was regarded as positive in terms of both supervision and entities (National Supervisory Authority for Welfare and Health Valvira).

Regarding the risk management measures already identified and implemented by entities, it was considered important that the recommendation comprises content from and references to the Cybermeter, which is widely known at the national level (Confederation of Finnish Construction Industries EK). References to other frameworks (standards) were also experienced as useful (Finnish Information Security Cluster (FISC)).

2.3 The specific nature of the risk management measures as a challenge - detail added to parts of the recommendation

Parties providing statements also criticised the structure of the recommendation for examining each individual requirement of section 9 of the Act on Cybersecurity Risk Management separately from other requirements. An assessment of the risk management measures as a whole was called for instead, taking into account any possibilities of measures offsetting each other based on the assessed risks (Confederation of Finnish Industries EK). The recommendation consciously strives to present each risk management measure as an independent entity and to set out its content, which results in partial overlap between the example implementations.

The large page count of the recommendation was felt to make its content more difficult to assimilate and consequently reduce the effectiveness of the guidance, which is why an abstract or summary of the recommendation inserted at the beginning of the document was called for to facilitate its assimilation (Information Management Board). The explanations text included in each individual risk management measure presented in the recommendation was regarded as serving as a summary.

Feedback was also given on the inadequate range of risk management tools in the draft recommendation, in the sense that the probability or impact of all risks cannot be minimised, or minimising them does not make sense. Instead, an identified risk could be accepted on well-reasoned grounds. The recommendation creates the false impression that all risks should be managed with the same intensity (Confederation of Finnish Industries EK). Excessively detailed regulation involves a systematic risk and the risk that entities allocate their limited resources to reporting to the authorities (Finnish Energy). The treatment of risks in general and acceptance of residual risk are discussed separately in section 1.5 of the recommendation. Combined with the specifications concerning risk assessment, considered risk management and the principle of proportionality made in the introductory text of the recommendation, it was deemed that this feedback had been responded to.

2.4 The terminology used in the recommendation was clarified and more specific references were provided

The suggestion made in statements regarding updating the title of the statute used in the draft recommendation to correspond with the Government proposal for an Act on Cybersecurity Risk Management (HE 57/2024 vp) was taken on board (Finnish Information Security Cluster (FISC), Confederation of Finnish Industries EK).

In addition, the fact that the technical terminology related to information security is new to the authorities and entities falling within the scope of the legislation was addressed by adding certain terms that were found difficult (including configuration, hardening, and zero trust principle) to the definitions section of the recommendation (Finnish Food Authority).

As a response to feedback on the variability of definitions and inconsistency or lack of terms, it was also decided to specify that a concept is only defined in the recommendation if it has not already been defined in the Act on Cybersecurity Risk Management (Confederation of Finnish Industries EK, Finnish Energy, Finnish Information Security Cluster (FISC)).

In addition, a reference to a partly outdated guideline in the recommendation (Guideline on security-critical procurements (VM2019:7) was replaced with an updated reference (Recommendation on information security in procurements VM2023:57).

In addition to the Information Management Board, comments on sector-specific standards and instructions were submitted by the Confederation of Finnish Construction Industries RT and the Confessional Lutheran Church of Finland, and the recommendation was modified as suggested.

2.5 The introductory text of the recommendation was supplemented and detail was added to it - risk-based approach and the recommendation's relationship with regulations

On the basis of the feedback received, it could be generally concluded that the recommendation may end up being treated as something separate from the legislation and its rationale, rather than a document that complements the legislation. In particular, it was pointed out that it is not necessary and resource-efficient to require all entities to take all the measures presented in the draft recommendation, or to take them in all activities (Confederation of Finnish Industries EK, Finnish Water Utilities Association). Parties providing feedback would also like the recommendation to make a clearer distinction between statutory requirements and sections that are part of the explanations (Finnish Energy).

It was decided to make it clear in the introductory text that the recommendation was only created to translate into concrete terms the options for verifying the measures that are set out in section 9 of the Act on Cybersecurity Risk Management Act and section 18c, subsections 1–12 of the Act on Information Management in Public Administration and described in detail in their rationales. It was additionally clarified that other provisions closely associated with risk management measures, such as provisions on sector-specific risk assessments, the entity’s considered risk management in which the principle of proportionality is accounted for, and management accountability in the Act on Cybersecurity Risk Management and Act on Information Management in Public Administration also operate in the background.

In the statements received, concerns were expressed over the possibility of the recommendation expanding the requirements of the Act (Confederation of Finnish Industries EK, Finnish Information Security Cluster (FISC), Finnish Energy). The relationship between the recommendation circulated for comments and any technical regulations issued by the supervisory authorities was also considered unclear (Confederation of Finnish Industries EK, Finnish Energy). When the recommendation is implemented in practice, making it clear that the recommendation is not be binding on the authorities or entities was called for (Finnish Water Utilities Association).

As a response to the feedback received, detail was added to the parts of the introductory text that discuss the nature of the recommendation as a guiding and supportive document only and the relationship between the content of the recommendation and any detailed technical regulations to be issued by the supervisory authorities.

2.6 The reading instructions of the recommendation were supplemented and detail was added to them - actors with a higher level of cyber risk

In order to create uniform supervisory practices, it was hoped that the recommendation would take a stand on the kind of entities that are expected to have a higher level of maturity (Ministry of Agriculture and Forestry). Detail was added to the introductory text of the recommendation on the basis of the feedback received.

There will be no obligation to use the frameworks set out in the recommendation, nor is their use restricted in general or in individual sectors. Consequently, the request to specify the type of activities to which each set of assessment criteria included in the statements should be applied was not taken on board (Confederation of Finnish Industries EK).

2.7 The correspondence between the risk management measures and frameworks as a challenge - a cross-reference document was appended to the recommendation

According to their statements, entities have found it problematic that it cannot directly be concluded from the recommendation if implementing the sections associated with the standard requirements referred to in the recommendation produces compliance under the Act on Cybersecurity Risk Management, or if any additional measures will be required (Finnish

Information Security Cluster (FISC)). For this reason, the added value created by the draft recommendation was expected to be smaller than intended (Confessional Lutheran Church of Finland).

While the use of recommendations prepared by other authorities was considered to promote the achievement of the objectives of the Act on Information Management in Public Administration, it was also noted that the Assessment criteria for information security in public administration (Julkri) are not necessarily sufficient to verify the obligations proposed in the Act as such. Consequently, additional references to existing provisions on information security and information management in the Act on Information Management in Public Administration were proposed, which could improve the coverage of compliance verification (Information Management Board). Traficom included references to existing recommendations issued by the Information Management Board in the recommendation, but not direct references to the existing sections concerning information management and information security in the Act on Information Management in Public Administration.

The addition of cross-references, in other words correspondence between fulfilment of frameworks and compliance with the Act on Cybersecurity Risk Management, to the recommendation was called for to support entities and supervisory authorities (Finnish Information Security Cluster (FISC), Finnish Food Authority, Confessional Lutheran Church of Finland). As a response to this feedback, a cross-reference document on frameworks drawn up by Traficom was appended to the recommendation, but in order to avoid misunderstandings, a specification was included in the instructions for reading the recommendation stating that this is not a harmonised standard which would only meet the requirements under the Act on Cybersecurity Risk Management.

2.8 Feedback on supervision - no modifications to the recommendation

The authorities' support was called for in ensuring that the risk management measures will actually lead to reducing digital risks rather than to increasing the administrative burden incurred by entities from the activities. Uniform application of the legislation between the Member States as far as possible and, correspondingly, in different sectors at the national level will play a key role (Finnish Information Security Cluster (FISC)).

It was also hoped that the supervisory authorities would engage in proactive, flexible, interactive and long-term cooperation in the form of guidance, advice and support with the entities in their sectors to determine the marginal conditions of the activities, also ensuring that entities do not oversize their risk management measures. Coordination and cooperation between the supervisory authorities at the national level should also be organised with ensuring consistent quality of supervision in different sectors in mind (Association of Finnish Local and Regional Authorities).

It was also pointed out in statements that mandatory regulation imposed on entities must not prevent the covering of the costs incurred from compliance with the regulation at the expense of other activities (Finnish Energy).

In the supervisory activities of the public administration, compatibility of the new Chapter 4a in the Act on Information Management in Public Administration on cybersecurity obligations and their supervision with existing provisions on information security and information management was seen as a challenge because of the partial parallels between them. Cooperation between the authority supervising public administration and the Information Management Board was also deemed important for the harmonisation of guidelines and recommendations and for more effective supervision (Information Management Board).

Parties issuing statements also proposed that appending harmonised national electronic form templates (such as an inspection protocol template or battery of questions) to the recommendation be considered for sector-specific supervisory authorities' use when applying the Act on Cybersecurity Risk Management and the recommendation (National Supervisory Authority for Welfare and Health Valvira).

In the feedback, adding detail to the risk management measure concerning familiarity among the management by specifying what the management of a multinational concern means was called for. According to statements, a definition of this should be issued as part of the guidelines to make it clear when the management of a concern must be familiar with national requirements (FiCom).

Parties providing feedback requested that attention be paid to the fact that the definition of the NIS2 Directive's scope, which is based on a combination of definitions for sector and size and 'regardless of the size', is considered genuinely challenging. While the draft recommendation does not concern the definition of the scope of the legislation as such, it was hoped that attention could be focused on the entity's assessed actual risk in supervision and in the interpretation of risk management measures. It was hoped that understanding of risks would be taken into account in supervisory activities, in which case the required risk management measures would effectively reduce the likelihood and impact of the risk (Confederation of Finnish Industries EK).

Feedback provided in statements highlighted the importance of adjusting supervision to the size and activities of the entity, taking into account entities' different risks and needs to use various risk management procedures. The supervisory authority should clarify in detail what risk identification, threat analysis and risk management procedure contain. In terms of a possible mandatory security management system and existing international cybersecurity requirements, it would be important that entities could also use existing systems and arrangements in their cybersecurity procedures to avoid duplication (Finnish Shipowners' Association).

Especially from the perspective of supervision, it was hoped that time would be reserved and interactive guidance and support provided for the introduction of risk management measures, especially for entities with more limited financial, personnel and competence resources (Finnish Water Utilities Association).

The feedback directly related to the supervision of risk management measures discussed above could not be incorporated in the recommendation but it has, as far as possible, been passed on to the supervisory authorities as part of Traficom's future role as the single point of contact referred to in the NIS2 Directive.

2.9 Resources as a challenge to supervision and entities - no changes to the recommendation

It emerged in the statements that entities find even the minimum-level implementation of the NIS2 Directive and the Act on Cybersecurity Risk Management a challenge in the prevailing state of public finances (Ministry of Agriculture and Forestry). Entities also pointed out that the resources of entities subject to the NIS2 Directive vary greatly, and the new legislation will bring additional requirements to bear on them (Finnish Water Utilities Association).

According to feedback provided in statements, ensuring compliance is likely to require significant updates of cybersecurity solutions and procedures in the majority of organisations falling within the scope of the regulation, which is why not only more expertise and resources but also the building of a new type of safety culture will be needed (Finnish Association of Local and Regional Authorities).

In general, the plentiful and partly overlapping cybersecurity legislation prompts entities to ask if cybersecurity will actually improve and raises concerns over cost-effective operation (Finnish Energy).

The feedback directly related to resources discussed above could not be taken into account in the recommendation, but as far as possible, entities' feedback has been passed on to the supervisory authorities as part of Traficom's future role as the single point of contact referred to in the NIS2 Directive.

2.10 General statement on the uniform implementation of the NIS2 Directive

Verizon additionally submitted a general statement on the uniform implementation of the NIS2 Directive that factors in other cybersecurity regulation in the Member States. The statement called for cost-effective and technology-neutral implementation of Article 21 on cybersecurity risk management measures that takes into account general international standards and a risk-based approach, which have already been accounted for as the underlying principles of the draft recommendation circulated for comments.

3 Statements on cybersecurity risk management measures

3.1 Cybersecurity risk management policy and assessing the effectiveness of risk management measures

The additions proposed by the Finnish Information Security Cluster aiming to clarify the broader logic of the risk management procedure were incorporated in the recommendation. The Confederation of Finnish Construction Industries RT commented on the significance of building technology in the context of the physical environment and its essential resources and the security of premises. The proposal was accounted for in measure 12, which deals with physical security in detail.

The Confederation of Finnish Industries EK commented on the range of risk management measures as well as on accepting and monitoring a risk, taking into account risks as a whole within the entity’s individual risk-bearing capacity. The content of this section is consistent with the rationale of the Act, which is why modifying the text of the recommendation was not considered possible. However, this feedback was assessed in connection with section 1.5 of the recommendation (Risk treatment), the content of which also already addresses the possibility of accepting risk.

3.2 Information security policy of networks and information systems

FiCom’s feedback on security policy was taken into account, and the requested changes were made to the verification methods.

3.3 Security in network and information systems acquisition, development and maintenance and the necessary procedures for vulnerability handling and disclosure

FiCom commented on section 3.2 (Security in object acquisition), noting that lifecycle management is also dependent on the lifecycle of previously acquired technology, which may be considerable. In addition, FiCom commented on the challenges of limiting time-based access in section 3.8. Traficom was aware of both challenges when drawing up the recommendation. Making the proposed changes to the recommendation was not justified. The implementations presented in the recommendation are given as examples, and they were drawn up with the idea of them being suitable for different sectors and entities of different sizes.

Based on an observation made by FiCom, detail was added to the verification method in section 3.9 for the part of contractual limitations to the penetration testing of a cloud service.

3.4 Product security, overall quality of services, resilience, cyber security risk management measures and cyber security practices of supply chains and its direct suppliers and service providers

-

3.5 Asset management and identification of important operations

According to the statement of the Confederation of Finnish Construction Industries RT, assets also refer to leased premises, software and other resources included in asset management that are in the possession or under the control of the entity. The recommendation was supplemented on the basis of the observations made by the Confederation of Finnish Construction Industries RT.

3.6 Personnel security and cybersecurity training

The Association of Finnish Local and Regional Authorities commented on the background check procedures for individuals, which are not available on a large scale in municipalities or in energy, water and waste utility organisations owned by municipalities, and pointed out a potential bottleneck in implementation. The comment of the Association of Finnish Local and Regional Authorities was not considered to require an update, as the supervisory authority is competent to assess the application of this management measure.

FiCom requested that detail be added to section 6.6 on familiarity among management in terms of how management is defined in a multinational concern. According to FiCom, a definition of this should be issued as part of the guidelines to make it clear when the management of a concern must be familiar with national requirements. FiCom's request has been included in comments on supervision which, as far as possible, will be passed on to the supervisory authorities.

3.7 Access management and authentication procedures

-

3.8 Policies and procedures regarding the use of cryptographic methods and, where appropriate, measures for using secured electronic communication

-

3.9 Incident detection and handling in order to maintain and recover security and reliability

FiCom provided feedback that concerned adding detail to the definition of incidents. The text of the draft recommendation circulated for comments does not clearly distinguish between information security incidents and incidents with information security impacts. This definition is significant when developing the processes for handling incidents and assessing practically all sections of this chapter. The definition used in the draft recommendation comes from the Act on Cybersecurity Risk Management. The definitions in the introductory section of the draft recommendation will be clarified in this respect, while the references already contained in the Act on Cybersecurity Risk Management will be removed from the recommendation to avoid overlaps.

As a response to FiCom’s comments, the formulation of the time period in section 9.3 (Event logging and detection) was modified, but the current expression was considered justified in the implementation example as it was concrete and exemplary.

3.10 Backup management, disaster recovery planning, crisis management and continuity management of operations and, where appropriate, the use of protected backup/emergency communication systems

Finnish Information Security Cluster commented on the clarity and structure of sections 10.2 (Backup copies and backup systems) and 10.4 (Backup communication systems), calling for logically structured and clearly separate measures. The implementation example in section

10.2, in particular, was supplemented based on this feedback. In addition, the terms ‛back-up system' and ‛back-up copy' were added to the definitions.

Finnish Information Security Cluster pointed out that there are repetitions in several sections of Chapter 10 of the recommendation, making the document unnecessarily long in places. A decision was made not to change the current formulation of the recommendation. The overlaps are intentional, with each table making up a separate entity.

3.11 Fundamental information security practices to ensure the security of operations, network and communication systems, hardware, software and applications

Finnish Information Security Cluster pointed out that the recommendation deals with the same issue in several sections and that this reduces its readability. As examples were cited sections 10.3 and 11.11 on the importance of backup copies and testing. The recommendation should clearly indicate the measures required under section 10.3 in addition to the fundamental practices under section 11.11. References to the actual measure were added to the fundamental information security practices of the recommendation. Implementation examples that obviously overlap with examples in other chapters were removed from sections of Chapter 11.

3.12 Measures to secure the physical environment and premises of networks and information systems as well as availability of the necessary resources

The Confederation of Finnish Construction Industries RT pointed out that in Chapter 12 and its subsections as well as in other similar contexts later it should be mentioned that, in addition to communication networks and information systems as well as their physical environment, the measures should also extend to the security of premises as well as the systems and services of essential resources, regarding which the digital security level DT2 set out in the Digital security guideline for buildings corresponds with the fundamental level for premises. DT1 is suitable for residential properties and other low-risk sites. While this guideline was added to the references of the recommendation, no detail was added to the implementation example in this respect. The sections concerning the security of the physical environment and its essential resources as well as the security of premises were revised, also addressing the importance of building services technology in the recommendation.

The Digital security guideline for buildings was added to the references in Chapter 12 of the recommendation as suggested by the Federation of Finnish Construction Industries RT.