Radiation and Nuclear Safety Authority

101/0002/2016

12.2.2021

Guide YVL A.12, Information security management of a nuclear facility

1 Introduction

Information security refers to the entity aimed to ensure the operation of the organisation and to develop the quality of the operation of the organisation. Information security is controlled through the information security management system (ISMS). In order to function, the management system should be part of the organisation's risk management and activity management system.

Information security management and the management system are discussed in standard series ISO/IEC 27000, which the update of this Guide aims to take into account, especially concerning vocabulary. The special requirements of nuclear facilities are discussed in chapter 4 of the Guide, the requirements of which apply to systems and equipment important to safety.

Documentation dealing with information security and its submission is not classified according to the safety classification because safety classification is not done for information security. For example, a device belonging to safety class EYT can be significant to information security.

2 Scope of application

Guide YVL A.12 sets forth the regulations concerning information security at nuclear facilities, and the requirements for their application. The Guide is applied to nuclear facilities in all stages of their lifecycles. The Guide is intended for use by licence applicants and licensees, and it shall be applied to other organisations that have an impact on information security at nuclear facilities, as well as to other use of nuclear energy. Other users of nuclear energy include uranium producers, possessors of small amounts of nuclear commodities and licensed nuclear information, and research facilities participating in research of the nuclear fuel cycle that are included in the scope of nuclear safeguards. General requirements and the regulatory control performed by STUK are also described in the A series YVL Guides and in the YVL Guides

- B.1 Safety design of a nuclear power plant
- B.2 Classification of systems, structures and components of a nuclear facility
- B.7 Provisions for internal and external hazards at a nuclear facility
- C.5 Emergency arrangements of a nuclear power plant
- E.7 Electrical and I&C equipment of a nuclear facility.

By virtue of Section 55 of the Nuclear Energy Act (990/1987), the Finnish Radiation and Nuclear Safety Authority (STUK) is the authority that regulates safety at nuclear facilities in Finland. Pursuant to Section 9 of the Nuclear Energy Act (990/1987), the licensee is responsible for the security arrangements insofar as they do not fall under the responsibility of the authorities.

3 Justifications of the requirements

The general obligations concerning security arrangements are presented in the Nuclear Energy Act (990/1987) and the Radiation and Nuclear Safety Authority Regulations on the Security in the Use of Nuclear Energy (STUK Y/3/2020) and on the Safety of a Nuclear Power Plant (STUK Y/1/2018). The international nuclear industry agreements that have been signed by Finland, other intergovernmental agreements, and the commitments made by Finland also include a number of obligations.

Guide YVL A.12 presents requirements for the information security management of a nuclear facility and specifies requirements presented in Regulation STUK Y/3/2020. According to Section 4(5) of Regulation STUK Y/3/2020, the updated version of Regulation STUK Y/3/2016, which replaced the Government Decree on Security in the Use of Nuclear Energy (734/2008), *appropriate information security principles shall be used in the design and maintenance of systems and components*. Otherwise, the provisions of the Act on the Openness of Government Activities (621/1999) on the publicity of documents shall apply, and this also covers information security. The non-disclosure obligation regulated in Section 78 of the Nuclear Energy Act applies to the plans concerning nuclear security arrangements.

The Guide uses terms *licensee* and *licence applicant* due to the different phases of the life cycle of a nuclear facility, among other things. Even if a requirement concerns the licensee, it also obliges the licence applicant (e.g. requirement 312).

3.1 Chapter 3 Information security management

Information security management can be used to describe the organisation's actions and methods to demonstrate the organisation's commitment to the maintenance and development of information security. Guide YVL A.12 presents requirements for an information security management system, in which external actors and their responsibilities shall be taken into consideration in addition to the description of the information security organisation. The organisation shall identify the stakeholders relevant for the information security management system (e.g. subcontractors, consultants and contractors) and the requirements set by them. The requirements of Guide YVL A.12 are in line with standard ISO/IEC 27001.

The licence applicant shall understand its operating environment and decide on the application and restrictions of the information security management system in order for the system's functionalities to correspond with actual conditions. The interfaces and dependencies of operations carried out by both the licensee and other organisations shall be described in the documentation.

3.1.1 Section 3.1 Information security management system

The licensee shall define the information security management policy, which may be an individual document or part of a larger set of documentation. Based on the policy, the licensee shall create an information security management system that is part of the management system. The management system specifies information security principles, among other things.

The information security management system shall cover the actions and procedures related to information security. The previous version of the Guide (2013) used terms *administrative* and *technical information security*, while the new Guide only uses term *control* in accordance with standard ISO/IEC 27000. When preparing the information security management system, international and national standards shall be taken into account. Standards are listed in the references of Guide YVL A.12.

The purpose of the information security management system is to maintain and develop secure processes that take into account the target maturity for the organisation's processes and the boundary conditions set by it. The management system shall cover all equipment and systems relevant for information security. The information security management system includes information systems, communications systems and electrical and I&C systems. The equipment in the system may be networked or self-standing. Even if the management of the office network and plant I&C network in itself were separated, the management system shall cover the entire plant environment along with connection points.

The information security management system shall include the guidance and supervision of external resources in terms of information security. Personnel background checks must be carried out and access rights to the systems and premises must be limited according to the task. At the end of employment, the rights shall be removed in a timely manner; the measure also manages the insider threat.

The information security management system shall include the objectives for information security. Objectives refer to compliance with the principle of continuous improvement. Continuous monitoring and the maintenance of objectives shall be paid attention to, as threats to information security are constantly changing. The implementation plans shall include the responsibilities and duties of the different parties involved, required resources, implementation/maintenance schedules and actions as well as the evaluation and development of actions.

According to Guide YVL A.12, information shall be protected against unauthorised use, modification and deletion as required by the classification. The information security audit tool (KATAKRI) and the VAHTI instructions provide the means and procedures used to protect non-public information given to the licensee by the authorities. The procedures according to Council Decision 2013/488/EU (modified via Decisions 2014/233/EU and (EU) 2019/2247) shall also be used to protect non-public information given to the licensee by the authorities. The processing and storage of confidential documents shall be in accordance with their classification.

Before disclosure of documentation containing information that is safety-classified by an authority, confidential or derived from these types of information to a third party, the licensee or licence applicant shall apply for the approval of the authority that created the material for disclosure of the information.

In connection with the update, the requirements of instruction YVL A.12 on the protection of objects have been rewritten, but the requirement level has not changed in practice. The licensee shall carry out and maintain a risk and threat assessment in accordance with the management system. On the basis of the assessment, the assets to be protected shall be identified and adequate controls shall be defined for

them. Requirements 314 and 315 refer to threat and risk assessment, analysis, controls and methods. Controls and methods can only be chosen after analysing what threat or risk they are intended to address. When conducting a threat and risk assessment, the failure analyses required by Guide YVL B.1 may be used as a basis for assessing the impact of information security breaches. However, these failure analyses do not necessarily cover all effects of intentional activity. In addition to information security experts, experts in plant processes and in I&C and electrical systems should be involved in the impact assessment of I&C and electrical systems.

Guide YVL A.12 does not require classification, categorisation into zones or any other predefined model for the risk assessment or for the protected assets, but the licensee shall determine the appropriate method for its own plant and operations. For example, IAEA Guideline NSS 17 provides examples of categorising assets into zones. Although no actual zones are required, requirements 405a–h of YVL A.12 require a physically unidirectional connection between the security system and other I&C architecture and between the I&C architecture and the external network. In addition to the actual I&C systems, any computers necessary for the maintenance and periodic testing of systems and equipment, as well as various design tools, shall be taken into account when evaluating the assets to be protected. Requirement 404 explicitly requires that electrical and security surveillance systems as well as emergency communication systems shall also be protected. In addition to the systems and equipment mentioned above, related information, such as the documentation and parameters of the systems, shall be adequately protected in accordance with requirement 404a.

3.1.2 Resource management

Work planning, sufficient resources and employees' training and expertise have also been recognised as important from the point of view of information security. Requirements for the training of nuclear personnel are presented in Guide YVL A.3 (e.g. requirements 311a and 605). Requirement 322 of Guide YVL A.12 specifies the training and competence of persons responsible for information security. According to requirement 321, the key personnel and resources related to information security management shall be employed or owned by the licensee. According to requirement 323, the level of information security and assignment of responsibilities of both the licensee and external resources shall be at a level that at least corresponds to the licensee's standards for similar activities.

Guide YVL A.12 specifies the requirements presented in Guide YVL A.3 for resources and competence with regard to two matters. In accordance with requirement 321, the key personnel or resources related to information security shall be directly employed or owned by the licensee. If the operation or maintenance of information systems is outsourced, the risks of outsourcing shall be assessed. In addition, requirement 323 requires the supplier to have at least the level of information security that corresponds to the licensee's standards for the activity to be outsourced. It should be noted that different functions, such as the maintenance of design tools or parametrisation of security surveillance systems at the plant, may have different levels of information security requirements.

3.1.3 Section 3.4 Assessments, audits and reviews of the information security management system

In order to verify the adequacy of the information security management system, the licensee shall arrange an annual self-assessment. The self-assessment may be carried out by area, but in such a way that all areas of the management system are covered over a period of three years.

In addition to the self-assessments, the licensee shall organise an independent extensive information security audit over a period of four years. For this purpose, the licensee shall assemble a group of experts independent of its activities. Due to the independence of the expert group, special attention needs to be paid to its orientation and the scope and depth of the inspection.

The licensee shall notify STUK of any self-assessments, independent assessments, audits and reviews in good time to allow STUK to monitor their implementation at its discretion. The audits and reviews and their results shall be documented. The documents shall be accessible to inspection by STUK, for example, on the licensee's premises.

3.1.4 Section 3.5 Improving the information security management system

The principle of continuous improvement shall be applied to the information security management system. Continuous improvement shall utilise and take into account the operating experience from information security management in the licensee's own field of business and other fields of business. The information security knowledge of the licensee shall be up-to-date. The safety impact of new threats shall be assessed proactively.

The management shall promote ways to develop and maintain the safety culture that involve the entire personnel in the implementation and continuous improvement of the information security management system. This can also be seen as part of the safety culture. The old version of the Guide mentioned the licensee's management, but the current version emphasises that the management of other actors must also ensure that the information security management system is complied with and improved within their own organisations. The licensee's management shall ensure that any improvements made to the management system are aligned with the set goals.

3.2 Chapter 4 Protecting systems that are important to safety

The information security and architecture of any equipment and systems that affect the safety of a nuclear facility, such as the information systems, communications systems and electrical and I&C systems, shall be designed and implemented in a manner that employs sufficient physical, technological and administrative security arrangements to prevent unauthorised access as well as is reasonably achievable.

Systems and equipment that directly or indirectly affect the information security of the nuclear facility shall be identified and their significance to information security assessed. Systems that do not directly affect nuclear safety, but through which indirect influence is possible, must therefore also be taken into account when

assessing the significance of these systems. Such systems may include an office network, design tools and databases and security surveillance systems. Special attention needs to be paid to the information security significance of computers needed for the maintenance or parametrisation of systems.

Information security has become more important in nuclear safety. Electrical I&C equipment is being replaced by manufacturers' solutions that incorporate more information technology. Information security shall be ensured for equipment incorporating information technology at all stages of the plant's life cycle, from design to construction and further from commissioning to decommissioning. When making individual modifications or major improvements during operation, the security significance of the equipment shall be taken into account and, on the other hand, its potential significance in relation to the original design criteria shall be understood. The necessary information security management methods are different at different stages of the life cycle and, when entering a new stage, due account shall be taken in advance of any changes that may be required to the management methods.

Access to electrical and I&C rooms shall be controlled in such a way that only the persons concerned have access to these rooms and that visits can be traced. According to requirement 403b, changes in software, parameters and databases of systems and equipment shall be traceable. Tracing does not necessarily imply a technical solution, which, especially in the case of older equipment, would not necessarily be possible.

The installation of unauthorised devices and software shall be prevented in accordance with requirements 403 and 403a. The installation of devices and possible software related to the maintenance, testing or calibration of the system or device is in principle permitted at the agreed time.

The equipment and systems of the nuclear facility and the security surveillance systems and the emergency preparedness communication systems shall be protected in accordance with the level of the information security zones and the security zones required by YVL A.11. As regards the zones, their safety significance in view of plant safety and controlled communication between the zones shall be taken into account.

Networked equipment covers all devices that are connected to other devices by means of a network or cable that can be used for communication. The related cabling and communications shall be protected against unauthorised actions.

The necessary management methods to protect the various systems and the information contained in the information system shall be assessed in accordance with requirements 314–316a. Regardless of the risk assessment, requirement 404 requires the protection of certain systems, but does not specify the level of protection.

In addition to these, requirements 405–406b explicitly require certain protections in addition to other management methods. IAEA guide NSS-17 requires systems to be divided into security zones. Several models, as the one mentioned above, have five zones. Guide YVL A.12 does not lay down requirements for the division of systems into different zones and, as a result, for the number of zones. However, in the case of two systems, data transfer is restricted in the same way as in the IAEA zone model.

The protection system shall be separated from the other I&C systems, the same as the I&C architecture from the administrative information systems. The separation shall take place by implementing unidirectional data transfer so that data transfer is blocked by a separator physically enforcing unidirectional communication, such as a data diode. A software-based arrangement of unidirectional data transfer shall not be considered sufficient. For the other zones, requirement 405a requires the best possible separation that can be achieved in practice. Although no zoning is required in Guide YVL A.12, it is, however, in practice one good way to implement the division of systems into smaller and more manageable sub-entities. However, information security zoning shall not be confused with the above-mentioned security zones required by Section 4 of STUK Regulation Y/3/2020.

The physical and logical separation of the networks and the monitoring of the communication taking place in the networks shall be implemented as well as is practically achievable, while taking the security significance and the technical limitations of the I&C systems into consideration. In the case of the I&C systems, the network separation rules and communication control restrictions usually come from the supplier of the I&C system platform, in which case the networks shall be designed in accordance with these rules and restrictions.

No physical possibility shall exist for the establishment of a data transfer connection to the software-based systems important to the safety of a nuclear facility from outside the system. Requirement 5206 of Guide YVL B.1 prohibits wireless connections in safety functions.

According to requirement 406, the possibility of an individual person installing a malicious functionality in several redundant devices or systems shall be restricted. The requirement shall be observed both in the design and technical implementation of the system and in the administrative procedures during use. It is worth noting that it is precisely a question of restricting the possibility, not of prohibiting it. Also here, the selected I&C system platforms may offer built-in functionalities or, correspondingly, make it difficult to meet the requirement.

Requirement 406b requires the detection of the disabling of a protection function or the installing of a malicious function. The I&C system platforms used in the higher safety classes typically include appropriate self-diagnostics. In addition, periodic tests may, depending on their scope, detect abnormal functioning of the protection functions.

Information security shall be ensured during all stages of the system's life cycle. The licensee shall also pay attention to proactive information security and to the collection and exploitation of operating experience. The systems and their interconnections shall be designed so that only those functions that are necessary for the performance of operations in question are available. Requirement 404b requires a reassessment of the information security requirements at the plant and system level in connection with plant modifications. Although a minor modification may not necessarily require a new plan for principles, a reassessment of the information security requirements shall be carried out in any case.

3.2.1 Section 4.4 Management of information security events

It shall be possible to monitor information security events, such as logins, communication and data transfer, and save related data. In addition, the information security management system shall describe the procedures for identifying, investigating and processing information security events.

Procedures shall be put in place for reporting information security deviations. In accordance with requirement 417, STUK shall be notified without delay of any information security deviations that are significant in view of safety. Requirement 327 specifies that when assessing deviations, special attention shall be paid to repeated observations and deviations. The root causes of such observations and deviations shall be evaluated, and any corrective and preventive actions shall be implemented in a manner that makes it possible to bring repeated deviations under control.

Procedures shall be put in place for reporting information security deviations. STUK shall be informed of information security deviations that have taken place and of possible threats, events and phenomena. Any deviations significant in view of safety shall be reported without delay.

3.2.2 Section 4.5 Access control

Access control shall have related management principles. The purpose of regular review of access rights is to keep access rights up-to-date, documented and correct in terms of tasks. This is particularly emphasised when work tasks change or a person leaves the organisation. Administrator privileges of different systems shall be limited to the minimum number of persons by applying the “need to know” principle, which is commonly used in the security arrangements. Access shall only be granted when it is required to perform work tasks. The password policy of access rights shall be specified, and it shall take into account the technological constraints of different systems and devices, including the length of the password. Further instructions can be found, for example, in the Vahti Guide.

With regard to external resources, secure data processing refers to the security of equipment, the control of access rights and instructions on operating procedures and the control of compliance with them.

3.2.3 Section 4.6 Information security testing of systems

Section 4.6 of the YVL Guide requires that advanced testing methods be used to test networked systems that are important for information security. Examples of advanced testing systems can be found in IAEA guide NSS 17. When designing information security testing, attention shall be paid to comprehensive factory testing, as on-site testing can be very limited or pose a significant risk to individuals or the plant.

The information security of the systems related to the supervision of security arrangements shall be tested. Information security testing can also be performed during the drills arranged to demonstrate the effectiveness of security arrangements pursuant to Guide YVL A.11.

The qualification and testing of I&C system platforms, electrical and I&C equipment and systems shall also take into account the testing of information security. Advanced testing methods shall be used to test networked systems that are important for information security.

If new and old systems are combined, it is important to assess the information security of the combination.

3.3 Chapter 5 Documents to be submitted for regulatory oversight by the Radiation and Nuclear Safety Authority

The regulatory oversight procedures of the Radiation and Nuclear Safety Authority targeting the licensee's information security management system are presented in Chapter 5. This chapter presents the documents to be submitted to STUK at the various stages of the life cycle of a nuclear facility, STUK statements and inspections and other forms of supervision.

In the construction licence phase, the information security requirements, system-level information security plans and system design requirements, including a description of the connections between the systems, among others shall be submitted. According to requirement 608 of YVL B.1, it shall be possible to make the requirement specifications of systems on the basis of the construction licence phase documentation. Not all system-specific requirements have necessarily been established yet, but the system requirements derived from the upper level should be. The construction licence application may explain in more detail in which areas the requirements may be deficient.

4 International provisions concerning the scope of the Guide

"IAEA NSS 17 Computer Security at Nuclear Facilities (TechDoc)" is the most significant reference. Guide YVL A.12 takes into account the procedures set out therein.

The preparation of the Guide has taken into account the standards in the ISO/IEC 27000 series and in the IEC 62443 series.

Other noteworthy standards:

- IEC 62645:2014 Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems
- IEC 62859:2016 Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity.

5 Impacts of the Tepco Fukushima Dai-ichi accident

Guide YVL A.12 was first published in 2013 after the Fukushima accident, so the requirements have been taken into account from the outset.

6 Needs for changes taken into account in the revision

No significant changes have been made to the level of requirements of Guide YVL A.12. The changes are related to the clarification of the Guide. The administrative burden has been reduced by transferring information security-related requirements from guides YVL B.1 and YVL E.7 to Guide YVL A.12. Thus, information security-related requirements have been centralised in Guide A.12. Clarification has been done both linguistically and by dividing items containing several requirements into their own requirements.

New or significantly changed requirements include requirement 415a, which requires drill as in Guide YVL A.11, and requirement 417a, which specifies when STUK shall be notified of events.

Chapter 5, Documents to be submitted for regulatory oversight by STUK, has in practice been rewritten. The administrative burden has been significantly reduced by reducing the number of documents to be submitted to STUK. In addition, the documents of the construction licence and operating licence phase have taken into account the changes made to Guide YVL B.1.

The previous version (2013) of the Guide included the separate section “Procurement, development and maintenance of systems related to information security” which has been deleted because similar requirements have been included in other sections. Also the section “Management and control of communications and operation” has been deleted from the updated Guide.

The clarified and more unambiguous Guide YVL A.12 eliminates ambiguities and, thereby, contributes to facilitating the operations of licensees and inspection activities of the authority.