About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe’s citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe’s critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Dr. M.A.C. Dekker, Dimitra Liveri

Contact

For contacting the authors please use cloud.security@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

Acknowledgements

This work has been done in collaboration with CNIT (under the ENISA tender F-COD-13-C24), and in particular with the experts Maria-Cristina Brugnoli, Federico Morabito, Emiliano Casalicchio, and Giuseppe Bianchi.

We are grateful for the good collaboration with the EC, which allowed ENISA to effectively support the implementation of the EU cloud strategy. We are grateful for the continuous feedback, guidance and suggestions from the members of the C-SIG group on Cloud Certification, chaired by the EC: http://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-certification-schemes

We also thank the experts of the ENISA Cloud Security and Resilience expert group who provided useful comments and feedback on earlier drafts of this document: https://resilience.enisa.europa.eu/cloud-security-and-resilience

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2014

Reproduction is authorised provided the source is acknowledged.
Executive Summary

The EU’s cloud strategy, published in 2012, contains several key actions. Key action 1 called “Cutting through the Jungle of Standards” addresses, among other things cloud standards and cloud certification schemes. Specifically about certification it says the EC will:

“Work with the support of ENISA and other relevant bodies to assist the development of EU-wide voluntary certification schemes in the area of cloud computing (including as regards data protection) and establish a list of such schemes by 2014.”

The EC set up working groups of experts from industry, industry associations and other interested stakeholders to discuss and agree on which steps to take in this direction. One of the working groups, the Cloud Select Industry Group on Certification Schemes, focuses on certification schemes. At the end of 2013 ENISA, in collaboration and agreement with the EC and the members of this working group, published a short paper about certification in the cloud strategy. That paper provides a description of the problem and it motivates the development of two specific tools for EU cloud customers:

- **CCSL - Cloud Certification Schemes List**: CCSL is a list of (existing) certification schemes, relevant for cloud computing customers. CCSL provide potential customers with an overview of objective characteristics per scheme, to help them understand how the scheme works and if it is appropriate for their setting. CCSL was already implemented as an online tool and published in spring 2014. CCSL is being improved continuously and updated by ENISA and stakeholders from industry and public sector.

- **CCSM - Cloud Certification Schemes Metaframework**: CCSM is a metaframework of existing certification schemes, which maps detailed security requirements used in the public sector to security objectives in existing cloud certification schemes. The goal of CCSM is to provide more transparency and help customers in the public sector with their procurement of cloud computing services.

This document provides the background to the first version (version 1.0) of CCSM. The scope in this version is restricted to generic network and information security requirements. This version of CCSM contains: 27 security objectives, a mapping to the ISO27001 certification scheme, and the ISO27018 standard (as first examples), an overview of 29 relevant documents with NIS requirements from 11 countries (United Kingdom, Italy, Netherlands, Spain, Sweden, Germany, Finland, Austria, Slovakia, Greece, Denmark).

This version of CCSM will be implemented as an online web-based tool at the end of 2014. In the future we aim to expand the scope of CCSM and include NIS requirements from other countries, NIS requirements specific for personal data protection (and thus integrate CCSM with the output of the Cloud computing Data Protection Code of Conduct).
Contents

1 Introduction .................................................................................................................. 1
2 Terminology .................................................................................................................. 2
3 Framework setup ......................................................................................................... 3
   3.1 Mapping mechanism ............................................................................................... 3
   3.2 Public sector NIS requirements relevant for cloud procurement ......................... 4
4 Security Objectives .................................................................................................... 7
   SO 01 - Information security policy ............................................................................. 7
   SO 02 - Risk management .......................................................................................... 7
   SO 03 - Security roles ............................................................................................... 7
   SO 04 - Security in Supplier relationships ................................................................ 8
   SO 05 - Background checks ..................................................................................... 8
   SO 06 - Security knowledge and training .................................................................. 8
   SO 07 - Personnel changes ....................................................................................... 9
   SO 08 - Physical and environmental security ............................................................ 9
   SO 09 - Security of supporting utilities ..................................................................... 9
   SO 10 - Access control to network and information systems .................................... 10
   SO 11 - Integrity of network and information systems ............................................. 10
   SO 12 - Operating procedures .................................................................................. 10
   SO 13 - Change management .................................................................................... 11
   SO 14 - Asset management ....................................................................................... 11
   SO 15 – Security incident detection and response .................................................... 11
   SO 16 – Security incident reporting ......................................................................... 12
   SO 17 – Business continuity ..................................................................................... 12
   SO 18 - Disaster recovery capabilities ...................................................................... 12
   SO 19 - Monitoring and logging policies .................................................................... 13
   SO 20 - System tests .................................................................................................. 13
   SO 21 - Security assessments ..................................................................................... 13
   SO 22 – Checking compliance .................................................................................. 14
   SO 23 - Cloud data security ....................................................................................... 14
   SO 24 - Cloud interface security ............................................................................... 14
   SO 25 - Cloud software security ............................................................................... 14
   SO 26 - Cloud interoperability and portability ............................................................ 15
   SO 27 - Cloud monitoring and log access ................................................................... 15

Annex A: Mapping security objectives to public procurement requirements .............. 16

Annex B: Public sector NIS requirements ................................................................. 24

B.1 United Kingdom ........................................................................................................ 24
   B.1.1 Document UK.1: Contractual process ............................................................... 24
   B.1.2 Document UK.2: PSN compliance - Public Service Network Program Version 4.1 25
   B.1.3 Document UK.3: IA Requirements for Cloud Services for PSN Accreditation .... 25
   B.1.4 Document UK.4: Security requirements for list X contractors - April 2014 ....... 26
B.1.5 Document UK.5: Implementing the Cloud Security Principles .................................................. 26

B.2 Italy ........................................................................................................................................... 27
B.2.1 Document IT.1: Caratterizzazione dei sistemi cloud per la pubblica amministrazione ......................... 27
B.2.2 Document IT.2: Technical specifications regarding security of computer applications in the Executive and the Legislative Assembly of the Emilia-Romagna .......................................................................... 29
B.2.3 Document IT.3: Cloud Computing: How to Protect Your Data without Falling From a Cloud - A Mini- Vademecum for Businesses and Public Bodies .................................................................................. 29

B.3 Netherlands ............................................................................................................................... 30
B.3.1 Document NL.1: Law - for security requirements for special information VIRBI 2013 .................. 30
B.3.2 Document NL.2: ICT security for web applications (national and decentralized government) ........ 31
B.3.3 Document NL.3: Baseline Regional Water information Strategic and Tactical standards ............... 31

B.4 Spain ........................................................................................................................................ 32
B.4.2 Document ES.2: National security scheme for eGovernment (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.) .. 33
B.4.3 Document ES.3: Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal ................. 33
B.4.4 Document ES.4: Ley 34/2002, de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI) (Service providers regulations law) ...................................................... 34

B.5 Sweden .................................................................................................................................... 34
B.5.1 Document SW.1: Vägledning –informationssäkerhet i upphandling Informationssäkerhet i upphandling av system, outsourcing och moln tjänster .................................................. 34
B.5.2 Document SW.2: Cloud services and the Personal Data Act ........................................................ 36
B.5.3 Document SW.3: “Kontorsstöd som molntjänst” (Cloud services for office automation) ............ 36

B.6 Germany ................................................................................................................................... 37
B.6.1 Document DE.1: Cloud-fahrplan für die öffentliche verwaltung ................................................ 37

B.7 Finland ..................................................................................................................................... 40
B.7.1 Document FI.1: KATAKRI, National Security Auditing Criteria .................................................. 40
B.7.2 Document FI.2: VAHTI, Government Information Security Guideline ........................................ 42

B.8 Austria ...................................................................................................................................... 43

B.9 Slovakia .................................................................................................................................... 45

B.10 Greece ................................................................................................................................... 46
B.10.1 Document GR.1 Central Computational Infrastructures IS SA - Node G-Cloud GSIS Tender .......... 47
B.10.2 Document GR.2 “Regulation on the Protection and Privacy Electronic Communications”, 2011. .. 49
B.10.3 Document GR.3: 2013 “Regulation for the Safety and Integrity Network and Electronic Communications Services” ................................................................. 50

B.11 Denmark ................................................................................................................................ 51
B.11.1 Document DK.1: Cloud computing and the legal framework - Guidance on legislative requirement and the contractual environment related to cloud computing .................................................. 51
B.11.2 Document DK.2: Informationssikkerhedspolitik for organisationer ............................ 52
1 Introduction

This document contains the first version of the Cloud Certification Schemes Metaframework (CCSM), a mapping from network and security (NIS) requirements from across the EU’s public sector to existing cloud certification schemes. The goal of CCSM is to provide a tool for experts in the public sector when procuring cloud services. For background about CCSM we refer the reader to the executive summary and the vision for CCSM contained in a short paper about certification in the cloud strategy.

CCSM consists of three main parts:

● An overview of public sector documents with relevant NIS requirements from across the EU. For each country and each document we derive a list of (numbered) NIS requirements. See Annex B.

● A layer of security objectives, which address most of the NIS requirements and a mapping from these security objectives to existing certification schemes. See Section 3. We also point the reader to similar security objectives in national documents. This map is in Annex A.

Target audience

CCSM is targeted at experts in the public sector involved with procurement of cloud computing services. Also experts in the cloud sector might find this Annex A and B useful as it provides an grouping and overview of relevant public sector requirements across a number of EU countries.

Policy Context: the European Cloud Strategy

In 2012, the European Commission published its cloud computing strategy, called "Unleashing the potential of cloud computing in Europe". The EU cloud strategy is designed to support the uptake of cloud computing across the EU. It centres around three key actions:

1. Standardization and certification of cloud services.
2. Safe and fair contract terms and SLAs, and a
3. Setting up a European cloud partnership to promote cloud computing adoption in the EU.

The EU Cloud strategy and the vision produced by the European Cloud Partnership both stress the importance of facilitating the adoption of cloud computing by SMEs, because they stand to gain most from cloud computing and they are an important driver for innovation and growth in the EU.

The commissioner of the EU’s Digital Agenda, Miss Kroes, said explicitly: “These issues [blocking adoption of cloud computing] are particularly troublesome for smaller companies, which stand to benefit the most from the Cloud, but do not have a lot of spending power, nor resources for individual negotiations with Cloud suppliers”.

ENISA has supported several actions under the EU cloud strategy: ENISA participated in the working group on cloud standardisation led by ETSI. ENISA has worked with the EC and industry to create a list of cloud certification schemes (CCSL). This document describes CCSM, an extension of CCSL. ENISA also contributes to a working group which aims to clarify and harmonize Cloud SLAs.

---

2 Terminology

To avoid confusion, we first explain the terminology used in this document (see Figure 1 below):

- **Security requirements**: Customers have *security requirements*. In the procurement phase customers usually check which security requirements are met by the security objectives of the provider. This process is often referred to as *due-diligence*.

- **Security objectives**: Providers have several *security objectives*. Objectives are high-level goals and usually do not include much detail about technical details. For example, an uptime of 99.9%, or “customer data cannot be accessed by unauthorized personnel”. Security objectives are sometimes grouped in *‘security domains’* (e.g. “software security”).

- **Security measures**: Providers have *security measures* in place, to reach the security objectives. Security measures are often called ‘controls’.

We give a simple example of this terminology (see figure below):

*A customer’s requirement is to have 99% uptime, during working hours.*

*The security objective of the provider is to have 99.9% availability and a recovery time objective of 10 minutes. This objective is specified in SLAs with customers. An SLA is typically composed of several SLO’s.*

*In terms of security measures (or controls), the provider has a business continuity plan, i.e. one or more procedures to deal with the impact of disasters. The provider also synchronizes data across multiple datacenters to deal with (regional) natural disasters affecting one datacenter at the time, and the provider has a 24/7 incident response team.*
3 Framework setup

The CCSM framework is essentially a mapping from NIS requirements used in procurement in the public sector, to the relevant parts in cloud certification schemes. In this section we explain how CSSM is derived and how it works.

3.1 Mapping mechanism

CCSM uses an abstraction/mapping layer of security objectives, which are high-level, in the sense that they are technology-neutral and scheme/standard neutral. The overall idea of CCSM is depicted in the diagram below (see Figure 2): By analysing documents from across the EU we derive a list of common security objectives (in the center of the diagram). The security objectives are then mapped to the relevant parts in existing certification schemes (at the bottom).

The goal of the mapping is to allow experts in the public sector to understand more easily if their NIS requirements are covered by existing cloud certification schemes, and if so, in which parts (paragraphs, sections, chapters, ...) of the relevant documents (standards, frameworks, etc) underlying the certification scheme. This would speed up their due-diligence when procuring.

This document also provides an overview of NIS requirements applicable to cloud computing procurement in the public sector, which in itself may be useful to experts in the field (see below).
3.2 Public sector NIS requirements relevant for cloud procurement

The main structure of CCSM is a set of security objectives. The CCSM security objectives are listed in the next section. The security objectives were derived in two steps:

1. By using a public survey to get from the relevant people (CIO’s, architects, project managers, etc) in the public sector a high-level idea of the NIS requirements relevant for cloud services procurement. We give some details about the survey in this section.

2. Subsequently we went into more detail by looking at national documents containing detailed security requirements. We derived detailed security objectives, mapping them to these security requirements. The security objectives are listed in the next section. The mapping from security objectives to detailed NIS requirements in national documents is included in Annex XX.

3.2.1 Survey of public sector NIS requirements

19 experts from the public sector answered our survey. The majority of respondents are architects or policy officers (see Figure 3 below):

![Figure 3: Your role in procurement of cloud computing services.](image)

The target audience of the cloud services these experts are procuring is mixed (see Figure 4). Most respondents are involved in procuring cloud services targeted at citizens (in an e-government scenario), internal employees, and also other government agencies.

![Figure 4: Which are the users of the cloud services you are procuring? (multiple answers possible)](image)

We also asked the type of requirements cloud procurement is subject to. This question gave us a general idea about the type of laws, regulations, or guidance taken into account. In most cases there is a national law, with high-level requirements, and guidance.
Two thirds of the experts said that, besides existing national law, guidance, et cetera, they need to specify additional security measures, in tender specifications and/or RFP’s (see Figure 6). This underlines the need for a flexible tool which allows the security experts dealing with cloud procurement to add security requirements ad-hoc, when needed.
3.2.2 Analysing national documents with NIS requirements

As a second step we analysed the detailed NIS requirements which are relevant to cloud service procurement, or more generally ICT service and products procured by government. The goal is to give a concise overview of a relevant document with NIS requirements. On the one hand this overview should be useful in itself, both for cloud providers and for public sector cloud customers. On the other hand this overview is used as a basis for the security objectives in CCSM.

In Annex B we give an overview of 29 relevant documents containing NIS requirements from a subset of 11 countries (United Kingdom, Italy, Netherlands, Spain, Sweden, Germany, Finland, Austria, Slovakia, Greece, Denmark).

Please note that this is not an exhaustive overview. We did not cover all countries and maybe there are other relevant documents in the countries we do cover. We welcome feedback about documents we might have overlooked.

The structure of the annex is as follows: For each country we give an overview of the relevant documents with NIS requirements. Each document is described by the following information/fields/attributes:

- Description: We briefly describe the document, who issued it, its role in procurement.
- Link: We provide where the document is published - or if not public, if/how it can be obtained.
- Application domain: The application domain indicates which the type of services or products to which these requirements apply.
- Tags: Tags like DPSpecific, CloudSpecific, CriticalInfrastructure, etc. indicate roughly the origin of the document. These tags are not mutually exclusive.
- Status: Status describes whether a document is guidance, recommendation, mandatory or to be award criteria.
- NIS requirements: We provide a numbered list of NIS requirements which pertain to the service or products. These requirements are (where needed) summarized for the sake of clarity. In annex A we provide a map from the CCSM security objectives to these numbered NIS requirements.
- Other requirements: We also list any other requirements which cannot be readily translated to NIS requirements, for example when a document places requirements on the procurement process (e.g. “does a risk assessment”) or when requirements are not NIS requirements (e.g. “service should comply with standard X”).
4 Security Objectives

In this section we list high-level security objectives (SO1, SO2, ...) which were derived from NIS requirements present in public sector documents from across the EU. These security objectives provide the mapping layer between public sector requirements and certification schemes.

For each security objective we provide:

- **Description**: Brief description of the security objective.
- **Countries**: List of countries where a similar security objective was found in national documents. Note that in Annex A we provide a more detailed mapping to security requirements.
- **Examples of measures**: Examples, keywords indicating possible security measures which could be implemented to reach the objective. The reason we provide some examples and key words is mainly to clarify, not to prescribe any particular security measures or controls. The security measures needed to reach certain objectives depends on the setting.
- **Certification scheme mapping**: A mapping to existing cloud certification schemes. In this document we only map to ISO27001 as an example. The goal for CCSM is to map to various relevant certification schemes. The other schemes will be mapped in the online tool.

**SO 01 - Information security policy**

**Description**: Cloud provider establishes and maintains an information security policy.

**Countries**: DE, FI, UK, IT, NL, ES, GR. See for a detailed mapping Annex A.

**Examples of security measures**: policy document, main assets and processes, strategic security objectives, etc.

<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO27001, A.5 Information Security policies</td>
<td></td>
</tr>
<tr>
<td>ISO27018, A.5 Information Security policies</td>
<td></td>
</tr>
</tbody>
</table>

**SO 02 - Risk management**

**Description**: Cloud provider establishes and maintains an appropriate governance and risk management framework, to identify and address risks for the security of the cloud services.

**Countries**: FI, UK, IT, ES, GR, SK. See for a detailed mapping Annex A.

**Examples of security measures**: List of threats, risks and assets, GRC tools, RA tools, etc.

<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO27001</td>
<td>ISO27001 is a standard for systems to manage information security. ISO27005 is a standard for risk management.</td>
</tr>
<tr>
<td>ISO27018</td>
<td></td>
</tr>
</tbody>
</table>

**SO 03 - Security roles**

**Description**: Cloud provider assigns appropriate security roles and security responsibilities.
Countries: SW, UK, DK, ES, GR. See for a detailed mapping Annex A.
Examples of security measures: Assigned roles include CSO/CISO, CIO/CTO, DPO, description of responsibilities per role, roles and contact points are communicated across the organisation, etc.

<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO27001, A.6.1 Internal organization</td>
<td></td>
</tr>
<tr>
<td>ISO27018, A.6.1 Internal organization</td>
<td></td>
</tr>
</tbody>
</table>

SO 04 - Security in Supplier relationships

Description: Cloud provider establishes and maintains a policy with security requirements for contracts with suppliers to ensure that dependencies on suppliers do not negatively affect security of the cloud services.
Countries: SW, UK, IT, AT. See for a detailed mapping Annex A.
Examples of security measures: SLAs, security requirements in contracts, outsourcing agreements, procurement rules, etc.

<table>
<thead>
<tr>
<th>Certification schemes mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO27001 A.15.1 Information security in supplier relationships</td>
<td></td>
</tr>
<tr>
<td>ISO27018, A.15.1 Information security in supplier relationships, A.7.1 Disclosure of sub-contracted PII processing, A.10.12 Sub-contracted PII processing</td>
<td></td>
</tr>
</tbody>
</table>

SO 05 - Background checks

Description: Cloud provider performs appropriate background checks on personnel (employees, contractors and third party users) if required for their duties and responsibilities
Countries: DE, SW, UK, IT, NL, DK, ES. See for a detailed mapping Annex A.
Examples of security measures: background checks, checking past jobs, checking professional references, etc.

<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO27001 A.7.1 Human resource security - Prior to employment</td>
<td></td>
</tr>
<tr>
<td>ISO27018 A.7.1 Human resource security - Prior to employment</td>
<td></td>
</tr>
</tbody>
</table>

SO 06 - Security knowledge and training

Description: Cloud provider verifies and ensures that personnel have sufficient security knowledge and that they are provided with regular security training.
Countries: DE, FI, UK, DK, ES. See for a detailed mapping Annex A.
Examples of security measures: Security awareness raising, security education, security training, etc.
<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO27001 A.7.2 Human resource security - During employment</td>
<td></td>
</tr>
<tr>
<td>ISO27018 A.7.2 Human resource security - During employment</td>
<td></td>
</tr>
</tbody>
</table>

**SO 07 - Personnel changes**

**Description:** Cloud provider establishes and maintains an appropriate process for managing changes in personnel or changes in their roles and responsibilities.

**Countries:** NL, ES. See for a detailed mapping Annex A.

*Examples of security measures:* Security in procedures for personnel changes, authorization revocation, account removal, etc.

<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO27001 A.7.3 Human resource security - Termination and change of employment</td>
<td></td>
</tr>
<tr>
<td>ISO27018 A.7.3 Human resource security - Termination and change of employment</td>
<td></td>
</tr>
</tbody>
</table>

**SO 08 - Physical and environmental security**

**Description:** Cloud provider establishes and maintains policies and measures for physical and environmental security of cloud datacenters.

**Countries:** DE, FI, UK, IT, NL, DK, ES, GR. See detailed mapping in Annex A.

*Example of security measures:* physical access controls, alarm systems, environmental controls, automated fire extinguishers, fences, etc.

<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
</table>

**SO 09 - Security of supporting utilities**

**Description:** Cloud provider establishes and maintains appropriate security of supporting utilities (electricity, fuel, etc.).

**Countries:** DE, IT, ES, GR. See for a detailed mapping Annex A.

*Examples of security measures:* Protection of power grid connections, diesel generators, fuel supplies, etc.
**SO 10 - Access control to network and information systems**

**Description:** Cloud provider establishes and maintains appropriate policies and measures for access to cloud resources.

**Countries:** DE, SW, FI, UK, IT, NL, DK, ES, AU, GR, SK. See for a detailed mapping Annex A.

*Examples of security measures:* ID management, authentication, access control, firewalls, network security, etc.

<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO27001 A.9.1 Business requirements of access control, A.9.2 User access management, A.9.3 User responsibilities, A.9.4 System and application access control, A.13.1 Network security management</td>
<td></td>
</tr>
</tbody>
</table>

**SO 11 - Integrity of network and information systems**

**Description:** Cloud provider establishes and maintains the integrity of its own network, platforms and services and protect from viruses, code injections and other malware that can alter the functionality of the systems.

**Countries:** DE, SW, FI, UK, IT, NL, DK, ES, AT, GR, SK. See for a detailed mapping Annex A.

*Examples of security measures:* malware detection, antivirus systems, patch management, etc.

<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO27001 A.12.2 Protection from malware, A.12.5 Control of operational software, A.12.6 Technical vulnerability management. A.13.1 Network security management</td>
<td></td>
</tr>
<tr>
<td>ISO27018 A.12.2 Protection from malware, A.12.5 Control of operational software, A.12.6 Technical vulnerability management. A.13.1 Network security management</td>
<td></td>
</tr>
</tbody>
</table>

**SO 12 - Operating procedures**

**Description:** Cloud provider establishes and maintains procedures for the operation of key network and information systems by personnel.

**Countries:** DE, SW, FI, UK, DK, ES, AU, GR, SK. See for a detailed mapping Annex A.

*Examples of security measures:* manuals, operating procedures, administration procedures (for critical systems), etc.
SO 13 - Change management
Description: Cloud provider establishes and maintains change management procedures for key network and information systems.
Countries: DE, FI, UK, ES, AT, SK. See for a detailed mapping Annex A.
Examples of security measures: change and configuration management processes and procedures, change procedures and tools, patching procedures, etc.

<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 270001 A.12.1 Operational procedures and responsibilities.</td>
<td></td>
</tr>
<tr>
<td>ISO 270018 A.12.1 Operational procedures and responsibilities, A.9.2 Retention period for administrative security policies and guidelines</td>
<td></td>
</tr>
</tbody>
</table>

SO 14 - Asset management
Description: Cloud provider establishes and maintains asset management procedures and configuration controls for key network and information systems.
Countries: NL, DK. See detailed mapping in Annex A.
Examples of security measures: Inventory of critical assets, roles responsible, etc.

<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001 A.8.1 Responsibility for assets</td>
<td></td>
</tr>
<tr>
<td>ISO 27018 A.8.1 Responsibility for assets, A.10.5 Use of unencrypted portable storage media and devices</td>
<td></td>
</tr>
</tbody>
</table>

SO 15 – Security incident detection and response
Description: Cloud provider establishes and maintains procedures for detecting and responding to incidents appropriately.
Countries: DE, FI, UK, IT, DK, NL, AT, ES, GR, SK. See for a detailed mapping Annex A.
Examples of security measures: Procedures for handling incidents, incident response team, Detection tools, anomaly detection, intrusion detection, etc.
SO 16 – Security incident reporting

**Description:** Cloud providers establish and maintain appropriate procedures for reporting and communicating about security incidents.

**Countries:** SW, FI, IT, ES, GR. See for a detailed mapping Annex A.

*Examples of security measures:* Plans for communication with customers, media and/or public, procedures for reporting to authorities, etc.

<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001 A.16.1 Management of information security incidents and improvements</td>
<td></td>
</tr>
<tr>
<td>ISO 27018 A.16.1 Management of information security incidents and improvements</td>
<td></td>
</tr>
</tbody>
</table>

SO 17 – Business continuity

**Description:** Cloud provider establishes and maintains contingency plans and a continuity strategy for ensuring continuity of cloud services.

**Countries:** DE, SW, FI, IT, NL, DK, ES, AT, GR. See for a detailed mapping Annex A.

*Examples of security measures:* Continuity strategy and contingency plans for disasters

<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001 A.17.1 Information security continuity. ISO 27001 A.17.2 Redundancies.</td>
<td></td>
</tr>
</tbody>
</table>

SO 18 - Disaster recovery capabilities

**Description:** Cloud provider establishes and maintains an appropriate disaster recovery capability for restoring cloud services provided in case of natural and/or major disasters.

**Countries:** DE, SW, FI, IT, DK, ES, GR. See for a detailed mapping Annex A.

*Examples of security measures:* Tools and equipment for mitigating and recovering from disasters, etc.
SO 19 - Monitoring and logging policies

**Description:** Cloud provider establishes and maintains systems for monitoring and logging of cloud services.

**Countries:** DE, SW, FI, UK, IT, NL, ES, GR. See for a detailed mapping Annex A.

**Examples of security measures:** Logs of user actions, system transactions, system performance monitors, automated monitoring tools, etc.

<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001 A.17.1 Information security continuity. ISO 27001 A.17.2 Redundancies.</td>
<td></td>
</tr>
<tr>
<td>ISO 27018 A.17 Information security aspects of business continuity management</td>
<td></td>
</tr>
</tbody>
</table>

SO 20 - System tests

**Description:** Cloud provider establishes and maintains appropriate procedures for testing key network and information systems underpinning the cloud services.

**Countries:** FI, UK, IT, GR. See detailed mapping in Annex A.

**Examples of security measures:** Test procedures for changes, automated unit-tests, test environments, etc.

<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001 A.12.4 Logging and monitoring</td>
<td></td>
</tr>
<tr>
<td>ISO 27018 A.12.4 Logging and monitoring</td>
<td></td>
</tr>
</tbody>
</table>

SO 21 - Security assessments

**Description:** Cloud provider establishes and maintains appropriate procedures for performing security assessments of critical assets.

**Countries:** DE, SW, FI, UK, ES, AT, GR, SK. See for a detailed mapping Annex A.

**Examples of security measures:** periodic penetration tests, vulnerability scans, white hat hacking, etc.

<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001 A.18.2 Information security reviews</td>
<td></td>
</tr>
<tr>
<td>ISO 27018 A.18.2 Information security reviews</td>
<td></td>
</tr>
</tbody>
</table>
SO 22 – Checking compliance

**Description:** Cloud provider establishes and maintains a policy for checking compliance to policies and legal requirements.

**Countries:** DE, SW, FI, UK, IT, DK, ES, AT, GR. See for a detailed mapping Annex A.

*Examples of security measures:* Checks against policy, regulations, industry best practices, periodically and after changes, internal audit functions, etc.

<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001 A.18.1 Compliance with legal and contractual requirements.</td>
<td>ISO 27001 follows the Deming cycle (PDCA) which states that all security objectives and policies should be periodically checked.</td>
</tr>
<tr>
<td>ISO 27018 A.18.1 Compliance with legal and contractual requirements, A.10.11 Data processing contract measures, A.1.1 Obligation to co-operate regarding PII principals’ rights</td>
<td></td>
</tr>
</tbody>
</table>

SO 23 - Cloud data security

**Description:** Cloud provider establishes and maintains appropriate mechanisms for the protection of the customer data in the cloud service.

**Countries:** DE, SW, FI, UK, IT, NL, DK, ES, AT, GR, UK. See for a detailed mapping Annex A.

*Examples of security measures:* Access control mechanisms protecting customer data, separation of duties, administration interfaces for customers, encryption and key management, secure deletion, secure disposal of media, etc.

<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27018 A.4.1 Secure erasure of temporary files, A.9.3 PII return, transfer and disposal, A.10.5 Use of unencrypted portable storage media and devices, A.10.6 Encryption of PII transmitted over public data-transmission networks, A.10.13 Access to data on pre-used data storage space, A.10.11 Data processing contract measures</td>
<td>ISO27017 addresses cloud data security in more detail.</td>
</tr>
</tbody>
</table>

SO 24 - Cloud interface security

**Description:** Cloud provider establishes and maintains an appropriate policy for keeping cloud services interfaces secure.

**Countries:** DE, SW, FI, UK, IT, ES, AT, GR, SK. See for a detailed mapping Annex A.

*Examples of security measures:* Protection of customer administration interfaces, SSL/TLS, 2-factor authentication, protection of cloud end-user interfaces (in the case of SaaS), etc.

<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27018 A.10.8 Unique use of user IDs, A.10.9 Records of authorized users, A.10.10 User ID management</td>
<td>ISO27017 addresses cloud data security in more detail.</td>
</tr>
</tbody>
</table>

SO 25 - Cloud software security
**Description:** Cloud provider establishes and maintains a policy for keeping software secure.

**Sources:** DE, SW, FI, UK, IT, NL, DK, ES, AT, GR, SK. See for a detailed mapping Annex A.

*Examples of security measures: secure development lifecycle, patching, security training for software developers, secure software configuration, etc.*

<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO27001 A.14.2 Security in development and support processes, A.18.2 Information security reviews</td>
<td></td>
</tr>
<tr>
<td>ISO27018 A.14.2 Security in development and support processes, A.18.2 Information security reviews</td>
<td></td>
</tr>
</tbody>
</table>

**SO 26 - Cloud interoperability and portability**

**Description:** Cloud provider uses standards which allow customers to interface with other cloud services and/or if needed migrate to other providers offering similar services.

**Countries:** DE, IT, ES, AT. See detailed mapping in Annex A.

*Examples of security measures: export functions and standard data formats for customer data, standard interfaces, etc.*

<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001</td>
<td></td>
</tr>
<tr>
<td>ISO 27018</td>
<td></td>
</tr>
</tbody>
</table>

**SO 27 - Cloud monitoring and log access**

**Description:** Cloud provider provides customers with access to relevant transaction and performance logs so customers can investigate issues or incidents when needed.

**Countries:** SW, UK, ES, GR. See for a detailed mapping Annex A.

*Examples of security measures: Dashboards, transaction logs in standard format, log retrieval functions, etc.*

<table>
<thead>
<tr>
<th>Certification scheme mapping</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001 A.12.4 Logging and monitoring</td>
<td></td>
</tr>
</tbody>
</table>
Annex A: Mapping security objectives to public procurement requirements

The following table shows how security objectives were derived from existing NIS requirements which apply to procurement of ICT and/or cloud services by the public sector in the EU.

NIS requirements are uniquely labelled, referring to documents analyzed. A full overview of these documents, grouped per country, and per document a description and their NIS requirements can be found in Annex B.

To explain the numbering of NIS requirements, take for example DE.2.1: This refers to the second document analysed for Germany (and the first requirement we derived from that document). Details about that document can be found in Annex B, under the heading Germany.

Note that this is a rough mapping to point the reader to similar, related, security requirements in national documents.

<table>
<thead>
<tr>
<th>Security Objective (SO)</th>
<th>Security Requirements</th>
</tr>
</thead>
</table>
| SO01 - Information security policy | • DE.2.1 Implementation of an information security management system  
• FI.1.2 Security policy  
• UK.5.4 Governance  
• IT.1.9 Information security policy  
• NL.2.6 Security Integration  
• ES.2.1 Organization and implementation of the security process  
• ES.2.12 Continuous improvement of the security process (policy)  
• GR.1.10 Security policies and procedures |
| SO02 - Risk management | • FI.1.8 Network security: security of routing according to the risk assessment  
• FI.1.10 Monitoring of network, system, infrastructure according to the risk assessment  
• FI.2.31 Threat scenario modelling and analysis  
• FI.2.32 Risk analysis  
• UK.5.4 Governance  
• UK.5.5 Operational security (vulnerability management)  
• IT.1.27 Resiliency and Impact Analysis  
• ES.2.1 Organization and implementation of the security process  
• GR.1.8 Reporting and monitoring mechanisms  
• GR.2.7 Risk Assessment  
• GR.3.15 Risk Assessment and internal audit  
• SK.1.1. Risk management for information security |
| SO03 - Security roles | • SW.1.1. Roles and responsibilities for data management and information security (contractual agreement between customer and provider)  
• UK.5.4 Governance  
• DK.2.1 Organization and responsibilities  
• ES.2.11 Differentiation in Security roles  
• GR.3.11 Security roles |
| SO04 - Security of third party assets | • SW.1.9 Security of third party  
• UK.5.8 Supply chain security  
• IT.1.24 Security of third party  
• AU. 1.4 Rights management |
| SO05 - Background checks | • DE.2.26 Trustworthy staff  
• SW.1.8 Human resources check  
• UK.5.6 Personnel security  
• IT.1.17 Human resources security  
• NL.1.2 Trust of persons working with special information  
• DK.2.3 User Conduct  
• ES.2.2 Personnel security |
| SO06 - Security knowledge and training | • DE.2.27 Training staff  
• FI.1.5 Security training  
• UK.3.3 Personnel staff training concerning separation issues |
| SO 07 - Personnel changes                                      | • UK.5.6 Personnel security  
|                                                              | • DK.2.3 User Conduct       
|                                                              | • ES.2.2 Personnel security |
| SO 08 - Physical and environmental security                   | • DE.2.2 Physical security  
|                                                              | • FI.1.7 Physical Security  
|                                                              | • FI.1.19 Protection of media storage  
|                                                              | • FI.1.20 Protection of classified information from third-party access  
|                                                              | • UK.5.2 Asset protection and resilience  
|                                                              | • IT.1.16 Physical and environmental security  
|                                                              | • NL.1.1 Management of assets  
|                                                              | • NL.1.3 Physical and environmental security  
|                                                              | • DK.2.2 Classification of systems and data  
|                                                              | • DK.2.4 Physical security  
|                                                              | • ES.2.4 Infrastructure security  
|                                                              | • GR.3.5 Physical security  
| SO 09 - Security of supplies                                 | • DE.2.3 Redundant Key supply components  
|                                                              | • IT.1.28 Security of supplies  
|                                                              | • ES.1.4 Security for subcontracting  
|                                                              | • GR.2.5 Physical security  
|                                                              | • GR.3.7 Power supply  
| SO 10 - Access control to network and information systems     | • DE.2.5 Server security with Technical measures to protect the host  
|                                                              | • DE.2.8 Security measures against malware and network-based attacks  
|                                                              | • DE.2.9 Security measures against DDoS attacks ...  
|                                                              | • DE.2.10 Network security with network segmentation...  
|                                                              | • DE.2.11 Redundant networking of the cloud data centres  
|                                                              | • DE.2.17 Authentication  
|                                                              | • DE.2.18 Role-based access control  
|                                                              | • SW.1.3 Access control to information  
|                                                              | • SW.3.7 Intrusion prevention  
|                                                              | • SW.3.9 Authentication and Access control per user, per group  
|                                                              | • FI.1.8 Network security  
|                                                              | • FI.1.9 Protection of wireless networks with encryption and user Identification  
|                                                              | • FI.1.11 Identification and authentication  
|                                                              | • FI.1.21 Protection of networks from unauthorized devices  
|                                                              | • FI.1.27 Storage of Authentication data not in clear text format  
|                                                              | • FI.1.30 Security mechanisms against the risks of remote working  
|                                                              | • FI.2.3 Strong authentication and access control  
|                                                              | • FI.2.7 Access roles and permissions to logs  
|                                                              | • FI.2.11 Management of password and user accounts  
|                                                              | • FI.2.12 Testing of network security  
|                                                              | • FI.2.27 Network-based security mechanisms  
|                                                              | • UK.3.1 Separation between PSN and non-PSN service environment  
|                                                              | • UK.5.1 Data in transit protection  
|                                                              | • UK.5.2 Asset protection and resilience (Data at rest protection)  
|                                                              | • UK.5.9 Secure consumer management  
|                                                              | • UK.5.10 Identity and authentication  
|                                                              | • UK.5.11 External interface protection  
|                                                              | • UK.5.12 Secure service administration  
|                                                              | • IT.1.8 Control of the access to sensitive information from mobile devices  
|                                                              | • IT.1.15 Identity and authentication for access to app., platforms, networks  
|                                                              | • IT.1.22 Intrusion detection  
|                                                              | • IT.2.2 Authentication  
|                                                              | • IT.2.3 Authorization  
|                                                              | • IT.2.4 Management of users sessions  
|                                                              | • NL.1.4: Access control (procedures and rules)  
|                                                              | • NL.2.4 Identity and access management  
|                                                              | • DK.2.6 Access Control  
|                                                              | • ES.1.1 Authentication  
|                                                              | • ES.2.3 Authorization and access control  
<p>|</p>
<table>
<thead>
<tr>
<th>SO 11 - Integrity of network and information systems</th>
<th>SO 12 - Operating procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>• ES.2.7 Protection of information stored and in transit</td>
<td>• DE.2.5 Server security with Technical measures to protect the host</td>
</tr>
<tr>
<td>• AU.1.4 Rights management</td>
<td>• DE.2.7 Server security with secure basic configuration</td>
</tr>
<tr>
<td>• AU.1.5 Safety of services/Access control</td>
<td>• SW.1.5 Availability and restoration of the service</td>
</tr>
<tr>
<td>• AU.1.9 Network availability</td>
<td>• SW.1.6 Backup</td>
</tr>
<tr>
<td>• GR.1.3 Network security</td>
<td>• SW.3.2 Website for current security levels and procedures</td>
</tr>
<tr>
<td>• GR.1.6 Access control</td>
<td>• SW.3.8 Data and metadata storage, backup and restore</td>
</tr>
<tr>
<td>• GR.2.3. Authentication and Access policy</td>
<td>• FI.1.12 Standard Operational procedures for configuration and installation</td>
</tr>
<tr>
<td>• GR.2.4 Network security</td>
<td>• FI.1.13 Separation of development, testing and production environment</td>
</tr>
<tr>
<td>• GR.3.8 Access control</td>
<td>• FI.1.15 Backup procedures</td>
</tr>
<tr>
<td>• GR.3.12 Management and Network Monitoring</td>
<td>• FI.1.19 Protection of media storage</td>
</tr>
<tr>
<td>• SK.1.5. Access control</td>
<td>• FI.2.18 Standard application security settings and related documentation</td>
</tr>
<tr>
<td></td>
<td>• FI.2.19 Mechanisms for critical security updates and installations of applications and patches</td>
</tr>
<tr>
<td></td>
<td>• FI.2.20 Mechanisms for the applications backup</td>
</tr>
<tr>
<td></td>
<td>• UK.5.2 Asset protection and resilience</td>
</tr>
<tr>
<td></td>
<td>• UK.5.5 Operational security</td>
</tr>
<tr>
<td></td>
<td>• UK.5.7 Secure development</td>
</tr>
<tr>
<td></td>
<td>• DK.2.5 Network and operation management</td>
</tr>
<tr>
<td></td>
<td>• ES.1.7 Data Integrity and Confidentiality</td>
</tr>
<tr>
<td></td>
<td>• ES.2.3 Authorization and access control</td>
</tr>
<tr>
<td></td>
<td>• ES.2.6 Integrity and system update</td>
</tr>
</tbody>
</table>
| SO 13 - Change management | AU.1.6. Integrity  
|                          | GR.1.4 System security  
|                          | SK.1.2. Procedures for protection against malicious code  
|                          | SK.1.8. Software update  
| DE.2.14 Patch and change management  
| FL.1.4 Change management procedure in place for changes related to data processing  
| FL.1.14 Procedures for vulnerabilities of networks and services  
| FL.1.16 Malware detection, prevention and recovery procedures  
| FL.1.29 Recovery procedures from malfunctions, disturbances, attacks  
| FL.2.19 Mechanisms for critical security updates and installations of applications and patches  
| FL.2.21 Processes for application patch management  
| UK.5.5 Operational security (configuration and change management)  
| ES.2.6 Integrity and system update  
| AU.1.15 Patch management  
| SK.1.8. Software update  
| SO 14 - Asset management | NL.1.1 Management of assets  
|                          | DK.2.2 Classification of systems and data  
| SO 15 - Incident detection and response | DE.2.19 Monitoring and Security Incident Management  
| FL.2.23 Processes for Security incidents management  
| FL.2.5 Proper Logs of failures and security incidents and Rich event log data  
| FL.2.9 Periodical monitoring of logs  
| UK.5.5 Operational security (incident management)  
| IT.1.19 Incident detection  
| IT.1.18 Incident management  
| DK.2.8 Management of security incidents in IT area  
| ES.1.8 Incident reporting and handling rules  
| ES.1.9 time to restore rules  
| ES.2.10 Security incidents  
| GR.3.2 Incident management and System recovery reporting  
| GR.3.13 Incident management process security  
| SK.1.6. Monitoring and management of security incidents  
| DE.2.19 Monitoring and Security Incident Management  
| UK.5.5 Operational security (incident management)  
| NL.3.6 Management of technical vulnerabilities  
| ES.1.8 Incident reporting and handling rules  
| ES.2.9 Activity Log  
| ES.2.10 Security incidents  
| AU.1.10 Threat management  
| GR.1.8 Reporting and monitoring mechanisms  
| SO 16 - Incident reporting | SW.1.7 Incident reporting  
| FL.2.5 Proper Logs of failures and security incidents and Rich event log data  
| FL.2.23 Processes for Security incidents management  
| FL.2.24 Communication of Security incidents  
| FL.2.25 Post-analysis of incidents  
| IT.1.20 Incident reporting  
| ES.1.8 Incident reporting and handling rules  
| GR.1.8 Reporting and monitoring mechanisms  
| GR.2.8 Incident analysis and reporting  
| GR.3.2 Incident management and System recovery reporting  
| SO 17 - Service continuity strategy | DE.2.3 Redundant Key supply components  
| DE.2.4 Redundant data centres  
| DE.2.11 Redundant networking of the cloud data centres  
| DE.2.20 Set up and operation of a business continuity management system  
| SW.1.5 Availability and restoration of the service  
| SW.1.10 Business continuity  
| SW.3.6 Business continuity  
| FI.1.3 Business continuity management and plans  
| IT.1.25 Business continuity and disaster recovery plan  
| NL.2.7 Monitoring, auditing and alerting  
| DK.2.9 IT business continuity management  
| ES.1.6 Availability  
| ES.1.9 time to restore rules  |
### SO 18 - Disaster recovery capabilities

- ES.2.13 Business continuity
- AU.1.9 Network availability
- GR.1.5 Backup requirements and disaster recovery features
- GR.3.3 Business Continuity
- FI.1.3 Business continuity management and plans
- IT.1.26 Exercise and operation of contingency plan

### SO 19 - Monitoring and logging policies

- DE.2.4 Redundant data centres
- DE.2.11 Redundant networking of the cloud data centres
- DE.2.20 Set up and operation of a business continuity management system
- SW.1.10 Business continuity
- SW.3.6 Business continuity
- FI.1.3 Business continuity management and plans
- FI.1.29 Recovery procedures from malfunctions, disturbances, attacks
- IT.1.25 Business continuity and disaster recovery plan
- IT.2.10 Data Availability
- DK.1.3 The data controller’s leave of personal data to a data processor
- DK.1.4 Certain critical information
- DK.2.9 IT business continuity management
- ES.1.6 Availability
- ES.1.9 time to restore rules
- ES.2.13 Business continuity
- GR.1.5 Backup requirements and disaster recovery features

### SO 20 - System tests

- FI.2.12 Testing of network security
- UK.5.5 Operational security (configuration and change management)
- IT.1.6 Control and verification of secure mobile code execution
- IT.1.13 Quality and security test of the systems and services
- IT.1.23 Separation between operation and non-operation environments
- GR.1.13 Evaluation and Testing
- GR.2.11 Integrity checks and testing
- GR.3.10 Vulnerability assessment

### SO 21 - Security assessments

- DE.2.24 Audit
- DE.2.25 Security testing
- SW.1.2 Monitoring and assessment of security activities and controls in place
- SW.1.11 Audit
- FI.1.32 Communication of the achieved security objectives at least annually
- FI.2.15 Security audit
- FI.2.17 Security penetration tests
- FI.2.22 Periodical audit of settings affecting security
- UK.3.1 Separation between PSN and non-PSN service environment
- UK.5.3 Separation between consumers
- UK.5.13 Audit information provision to consumers
- ES.4.1. Transparency and obligations to communicate adopted security measures
- AU.1.3 Compliance with data protection regulation (monitoring and audit)
- AU.1.12. Audits
- AU.1.14 Security policy compliance audit/Technical revision
- GR.1.2 Data privacy (auditing)
- GR.2.10 Control policy and audits
- GR.3.4 Testing and control efficiency plans
### SO 22 - Compliance

- DE.1.1 Compliance with Federal Data Protection Act
- DE.1.2 Compliance with laws and regulations for classified information
- DE.2.6 Deploying certified hypervisors
- DE.2.20 Set up and operation of a business continuity management system
- DE.2.24 Audit
- DE.2.28 Data protection and compliance with laws and regulation
- SW.1.1 Request for different levels of protections from the providers
- SW.1.11 Audit
- SW.2.1. Requirements for the users of cloud services for processing of personal data
- SW.3.3 Audit
- FI.1.1 Compliance with legal requirements and security guidelines
- FI.2.1 Compliance with laws, regulations and guidelines
- FI.2.22 Periodical audit of settings affecting security
- UK.2.1 PSN compliance Certificate
- UK.5.2 Asset protection and resilience (Physical location and legal jurisdiction)
- UK.5.7 Secure development
- IT.1.1 Compliance with standards, legal and regulatory obligations
- IT.1.5 Design of applications, platforms, systems compliant with security standards, legal and organizational obligations
- IT.2.1 Compliance with obligations by law force (rule 25 of Annex B of the Legislative Decree no. 196/03)
- DK.1.2 Processing of personal data: caution in using cloud solutions. Be compliant with the DK Act on Processing of Personal Data
- ES.1.5 Data protection and information protection
- AU.1.11 Audits
- GR.1.2 Data privacy (compliance with standards)
- GR.1.7 Legal and regulatory compliance requirements
- GR.1.11 Compliance with standards and interoperability
- GR.3.1 Compliance with standards
- GR.3.14 Business Impact Analysis

### SO 23 - Cloud data security

- DE.1.1 Compliance with Federal Data Protection Act
- DE.1.2 Compliance with laws and regulations for classified information
- DE.2.10 Network security with network segmentation...
- DE.2.15 Data security
- DE.2.16 Encryption and key management
- DE.2.22 Exit agreement with assured formats and retention of logical relations and specifying any associated costs (SaaS)
- SW.1.3 Access control to information
- SW.1.6 Backup
- SW.2.1. Requirements for the users of cloud services (i.e. the controller) for processing of personal data
- SW.3.4 Protection and Encryption (TLS, SMTP, key management)
- SW.3.8 Data and metadata storage, backup and restore
- SW.3.10 Regulatory framework for data
- FI.1.4 Change management procedure in place for changes related to data processing
- FI.1.19 Protection of media storage
- FI.1.20 Protection of classified information from third-party access
- FI.1.22 Marking of classified information
- FI.1.23 Secure delete of classified information
- FI.1.24 Secure electronic transfer of classified information
- FI.1.25 Encryption and key management
- FI.2.2 Encryption
- FI.2.28 Data security (delete policy, data portability, data classification)
### UK.5.1 Data in transit protection
- Ensure data security during transmission.

### UK.5.2 Asset protection and resilience
- Safeguard against physical and cyber threats.

### UK.5.3 Separation between consumers
- Maintain isolation for each consumer's data.

### UK.5.4 Secure consumer management
- Manage consumer access securely.

### UK.5.5 Operational security (proactive monitoring)
- Monitor systems for security breaches.

### UK.5.6 Identity and authentication
- Secure user authentication.

### IT.1.7 Data governance
- Establish policies for data management.

### IT.1.11 Protection and classification of information related to e-commerce transactions
- Classify and protect e-commerce data.

### IT.2.5 Validation of data
- Verify data accuracy and authenticity.

### IT.2.9 Encryption of data at rest and in motion
- Encrypt data to prevent unauthorized access.

### IT.2.10 Data Availability
- Ensure data is accessible when needed.

### NL.3.2 Correct processing in applications: Prevent errors, loss, unauthorized modification or abuse of information in applications
- Ensure proper application processing.

### NL.3.4 Security of file system: accomplish file system security
- Secure file systems.

### NL.3.5 Security in development and support processes: maintaining security of application software and information
- Maintain application security through development and support.

### DK.1.1 No processing of personal data: in this case cloud solution can be applied for processing and storing
- Process personal data securely.

### ES.1.3 Data handling: data management in the cloud, migration of data to the cloud
- Manage data in the cloud securely.

### ES.1.6 Availability
- Ensure data and service availability.

### ES.1.7 Data Integrity and Confidentiality
- Maintain data integrity and confidentiality.

### ES.2.7 Protection of information stored and in transit
- Protect data in storage and transit.

### ES.3.8 Access control
- Control access to data.

### AU.1.1 Data Protection and privacy requirements
- Adhere to data protection regulations.

### AU.1.2 Data location
- Secure data location.

### AU.1.8 Data management
- Manage data effectively.

### GR.1.1 Data Integrity and Confidentaility
- Maintain data integrity.

### GR.1.2 Data privacy
- Protect user privacy.

### GR.2.1 Confidentiality, integrity and availability of data
- Ensure data confidentiality, integrity, and availability.

### GR.2.3 Authentication and Access policies
- Establish authentication and access policies.

### GR.3.8 Access control
- Implement access control measures.

### SK.1.7 Email security
- Secure email communication.

### DE.2.6 Deploying certified hypervisors
- Use certified hypervisors for enhanced security.

### DE.2.7 Server security with secure basic configuration
- Secure server configurations.

### DE.2.10 Network security with network segmentation, secure Remote administration, Encrypted communication
- Secure network communication.

### DE.2.12 Application and Platform Security
- Secure application and platform environments.

### DE.2.13 Automated checking of customer applications vulnerabilities
- Regularly check for vulnerabilities.

### DE.2.17 Authentication
- Implement strong authentication methods.

### DE.2.23 Standard or open interfaces (API and protocols)
- Use standard or open interfaces securely.

### SW.3.2 Website for current security levels and procedures
- Provide current security levels.

### SW.3.4 Protection and Encryption (TLS, SMTP, etc.)
- Use encryption for secure communication.

### FI.1.9 Protection of wireless networks with encryption and user Identification
- Secure wireless networks.

### FI.1.11 Identification and authentication
- Implement secure identification and authentication.

### FI.1.26 Use of known and trustworthy techniques for session management
- Use trusted session management techniques.

### FI.1.27 Storage of Authentication data not in clear text format
- Store authentication data securely.

### FI.1.30 Security mechanisms against the risks of remote working
- Secure remote working environments.

### FI.1.32 Strong authentication and access control
- Implement robust authentication and access control.

### FI.2.3 Strong authentication and access control
- Maintain strong authentication and access control.

### FI.2.6 Common time source synchronizations for logging and events detection
- Use common time source synchronizations.

### FI.2.7 Access roles and permissions to logs
- Implement access controls for logs.

### FI.2.9 Periodical monitoring of logs
- Regularly monitor logs.

### FI.2.10 Security measures in place to prevent session hijacking
- Prevent session hijacking.

### UK.5.3 Separation between consumers
- Protect consumer separation.

### UK.5.5 Operational security (proactive monitoring)
- Monitor and protect operational security.

### UK.5.10 Identity and authentication
- Secure identity and authentication.

### UK.5.11 External interface protection
- Protect external interfaces.

### UK.5.12 Secure service administration
- Secure service administration.

### UK.5.14 Secure use of the service by the consumers
- Ensure secure consumer use.

### IT.1.21 Dedicated interfaces, accesses and tools for audit and monitoring activities
- Use dedicated tools for audit and monitoring.

### ES.1.1 Authentication
- Implement authentication mechanisms.

### ES.1.5 Data protection and information protection
- Protect data and information securely.
<table>
<thead>
<tr>
<th>SO 25 - Cloud software security</th>
<th>SO 26 - Cloud interoperability and portability</th>
<th>SO 27 - Cloud monitoring and log access</th>
</tr>
</thead>
<tbody>
<tr>
<td>• ES.2.5 Security by default</td>
<td>• DE.2.22 Exit agreement with assured formats and retention of logical relations and specifying any associated costs (SaaS)</td>
<td>• SW.1.4 Traceability and logging</td>
</tr>
<tr>
<td>• ES.2.8 Protection from other interconnected information systems</td>
<td>• DE.2.23 Standard or open interfaces (API and protocols)</td>
<td>• UK.5.13 Audit information provision to consumers</td>
</tr>
<tr>
<td>• AU.1.5 Safety of services/Access control</td>
<td>• IT.1.2 Portability and interoperability</td>
<td>• ES.1.2 Traceability</td>
</tr>
<tr>
<td>• AU.1.6. Integrity</td>
<td>• IT.1.3 Migration and reutilization</td>
<td>• ES.4.1 Transparency and obligations to communicate adopted security measures</td>
</tr>
<tr>
<td>• GR.1.6 Access control</td>
<td>• ES.1.3 Data handling: data management in the cloud, migration of data to the cloud</td>
<td>• GR.1.4 System security</td>
</tr>
<tr>
<td>• GR.3.10 Vulnerability assessment</td>
<td>• ES.2.5 Security by default</td>
<td>• GR.1.12 SLA monitoring and cross-checking</td>
</tr>
<tr>
<td>• SK.1.5. Access control</td>
<td>• AU.1.11. Standards compliance</td>
<td></td>
</tr>
</tbody>
</table>
Annex B: Public sector NIS requirements

In this section we analyse existing NIS requirements in the EU member states which apply to cloud services, or more generally ICT service and products procured by government. The goal is to give a concise overview, with relevant links, of documents with NIS requirements.

Note that this is not an exhaustive overview. We welcome feedback about documents we overlooked. Contact us via cloud.security@enisa.europa.eu.

The structure of this section is as follows. For each country we give an overview of the relevant documents with NIS requirements. Each document is described by the following information/fields/attributes:

- **Description**: We briefly describe the document, who issued it, its role in procurement.
- **Link**: We provide where the document is published - or if not public, if/how it can be obtained.
- **Application domain**: The application domain indicates which the type of services or products to which these requirements apply.
- **Tags**: Tags like DPSpecific, CloudSpecific, CriticalInfrastructure, etc. indicate roughly the origin of the document. These tags are not mutually exclusive.
- **Status**: Status describes whether a document is guidance, recommendation, mandatory or to be award criteria.
- **NIS requirements**: We provide a numbered list of NIS requirements which pertain to the service or products. These requirements are (where needed) summarized for the sake of clarity.
- **Other requirements**: We also list any other requirements which cannot be readily translated to NIS requirements, for example when a document places requirements on the procurement process (e.g. “does a risk assessment”) or when requirements are not NIS requirements (e.g. “service should comply with standard X”).

B.1 United Kingdom

The CESG, the UK’s National Technical Authority on Information Assurance published a set of guidance to help public organizations in the secure use of cloud services and to assist the public sector in the application of cloud security principles during the risk assessment and the implementation phase. The guidance is aiming even at publishing general needs in terms of security for the cloud providers wishing to be accredited in the Public Cloud Market, G-Cloud.

In the UK the main relevant documents with NIS requirements are

- UK.1 Contractual process - April 2014
- UK.2 PSN compliance - Public Service Network Program Version 4.1
- UK.3 Information Assurance Requirements for Cloud Services to attain PSN Accreditation
- UK.4 Security requirements for list X contractors - April 2014
- UK.5 Implementing the Cloud Security Principles

B.1.1 Document UK.1: Contractual process

- **Description**: Describes the process the UK government authorities must follow when decide to assign contracts. Specific attention is devoted to SENSITIVE-PERSONAL, SECRET (or above) information. Any contract must comply with the specification contained in this document. The
document refers also data privacy issues and measures.

- **Link/source:**

- **Application domain:** ICT services where processing classified assets/information OFFICIAL-SENSITIVE, SECRET or above.

- **Tags:** Procurement, ClassifiedInformation, CriticalInfrastructure

- **Status:** Mandatory

- **NIS Requirements:**
  - **UK.1.1** the system/service processing classified assets SECRET or above must comply with MODUK DEFCON659 - Security Measures (No public available) or with similar Security Measures standards.
  - **UK.1.2** The contractor of system/service processing classified assets SECRET or above must be accredited in the List X or it must be compliant with all the List X requirements (See Document UK.4)
  - **UK.1.3** Contractors shall apply the requirements of *HMG Baseline Personnel Security Standard (BPSS)* (see Document UK.8) for all individuals having access to OFFICIAL-SENSITIVE information
  - **UK.1.4** Contractor must be compliant with the “Security Conditions - Guidance for UK Contractors on the Protection of UK Assets marked as OFFICIAL-SENSITIVE”

### B.1.2 Document UK.2: PSN compliance - Public Service Network Program Version 4.1

- **Description:** The document specifies obligations for GCN Service Providers, Direct Network Service Providers, PSN Service Providers and PSN Customers.

- **Link:** [https://www.publicservicesnetwork.service.gov.uk/CHttpHandler.ashx?id=801&p=0](https://www.publicservicesnetwork.service.gov.uk/CHttpHandler.ashx?id=801&p=0)

- **Application domain:** Cloud services provided through UK Public Services Network

- **Tags:** Procurement, CriticalInfrastructure, CloudSpecific

- **Status:** Mandatory, Award criteria

- **NIS Requirements:**
  - **UK.2.1** Any G-Cloud Service Provider whom connects to or wishes to offer services across the PSN (Public Services Network) will also require a PSN compliance Certificate before they may connect to the PSN (see Document UK.3)

- **Other Requirements:**

### B.1.3 Document UK.3: IA Requirements for Cloud Services for PSN Accreditation

- **Description:** The document provides a set of control requirements for service provider wishing to supply a service to consumers in both PSN and non-PSN domains using the same service infrastructure.

- **Link:** [https://www.publicservicesnetwork.service.gov.uk/CHttpHandler.ashx?id=884&p=0](https://www.publicservicesnetwork.service.gov.uk/CHttpHandler.ashx?id=884&p=0)

- **Application Domain:** Cloud services provided through UK Public Services Network

- **Tags:** CloudSpecific, Procurement, CriticalInfrastructure

- **Status:** Recommendation, Guidance, Award criteria
● **NIS Requirements:**
  ○ UK.3.1 The service provider shall be required to demonstrate appropriate “separation” between its PSN service environment and its non-PSN service environment.
  ○ UK.3.3 Personnel staff of the service provider has to receive training concerning separation issues.

● **Other Requirements**
  ○ UK.3.2 PSN and Cloud service providers are accredited against CAS(T) or ISO/IEC27001:2005

**B.1.4 Document UK.4: Security requirements for list X contractors - April 2014**

- **Description:** Definition of requirement must be satisfied to join the List-X. Accreditation in List-X is an award criteria and/or an obligation for contractor processing classified information
- **Application domain:** Any service or product
- **Tags:** Procurement
- **Status:** Mandatory, award criteria
- **NIS Requirements:** -
- **Other Requirements:**
  ○ UK.4.1 Contractor Management
  ○ UK.4.2 Access control to contractor infrastructures/premise
  ○ UK.4.3 Contingency plans
  ○ UK.4.4 Oversea promotion, sale, release of defence equipment/technologies
  ○ UK.4.5 Homeworking

**B.1.5 Document UK.5: Implementing the Cloud Security Principles**

- **Description:** the document describes various ways a cloud service can demonstrate how it meets the different Cloud Security Principles. Mechanisms and approaches are even provided together with the level of residual risk that a particular cloud service has depending on the mechanisms used.
- **Application domain:** Cloud services
- **Tags:** CloudSpecific, Procurement
- **Status:** Recommendation, Guidance
- **NIS Requirements:**
  ○ UK.5.1 Data in transit protection
  ○ UK.5.2 Asset protection and resilience
  ○ UK.5.3 Separation between consumers
  ○ UK.5.4 Governance
  ○ UK.5.5 Operational security
Cloud Certification Schemes Metaframework
Version 1.0, November 2014

- UK.5.6 Personnel security
- UK.5.7 Secure development
- UK.5.8 Supply chain security
- UK.5.9 Secure consumer management
- UK.5.10 Identity and authentication
- UK.5.11 External interface protection
- UK.5.12 Secure service administration
- UK.5.13 Audit information provision to consumers
- UK.5.14 Secure use of the service by the consumers

B.2 Italy
The AGID (Agenzia per l’Italia Digitale) is actively working to facilitate the adoption of Cloud Computing in the public administration sector. AGID defines the technical guidelines to characterize cloud systems for the public administration sectors specifying non-functional requirements that must be satisfied by the providers. The AGID documents are intended as guidelines that are not mandatory. Therefore local administration are free to implement their own strategy for cloud computing. In what follow we analysed two main guidelines from the government IT.1 (AGID) and IT.3 (“Garante della Privacy”), and a document from AGID (IT.1) and mandatory technical specification issued by the Regione Emilia Romagna (IT.2).

In Italy the following 3 documents are relevant:
- IT.1 Characterization of cloud systems for the public administration
- IT.2 Technical specifications regarding security of computer applications in the Executive and the Legislative Assembly of the Emilia-Romagna
- IT.3: Cloud Computing: How To Protect Your Data Without Falling From A Cloud - A Mini-Vademecum for Businesses and Public Bodies

B.2.1 Document IT.1: Caratterizzazione dei sistemi cloud per la pubblica amministrazione
- **Description:** the document reports a first set of guidelines for the certification of cloud solutions for the governmental institutions, providing with the technical rules for the qualification of the suppliers and for the certification of services being issued. The document provides a set of requirements related to control areas, which are Compliance, Interoperability, Data Governance, Security, Management, and Resiliency. Note that some requirements listed in the document are taken from the CLOUD CONTROLS MATRIX VERSION 3.0.
- **Link:** [http://www.agid.gov.it/sites/default/files/documentazione/cloud_pa_consultazione_pubblica_v1.0_bozza.pdf](http://www.agid.gov.it/sites/default/files/documentazione/cloud_pa_consultazione_pubblica_v1.0_bozza.pdf)
- **Application Domain:** Cloud Infrastructures, platforms and applications for the Italian government agencies (at central and local level).
- **Tags:** Cloud Specific, Procurement
- **Status:** guidance, recommendations
- **NIS Requirements:**
○ IT.1.1 Compliance of information, objects, installations, systems, applications with standards, legal and regulatory obligations
○ IT.1.2 Portability and interoperability: standard VM images for IaaS (Openstack), open API for PaaS (API RESTful), specification of the programming languages supported for PaaS, open and standard data format, standard systems for authentication for SaaS, use of machine readable SLAs for VMs
○ IT.1.3 Migration and reutilization: exchange of inter-VM cloud (IaaS), persistent and interoperable storage (PaaS), adherence to open standards and source code (SaaS)
○ IT.1.4 Operational procedures for vulnerability of applications, platforms, systems, (patch changes, virus, malware, etc.)
○ IT.1.5 Design of applications, platforms, systems compliant with security standards (e.g. OWASP per web applications), legal and organizational obligations
○ IT.1.6 Control and verification of secure mobile code execution
○ IT.1.7 Data governance: data classification, handling, labelling, retention, dispersion, removal and deletion policy, back-up procedure, mechanisms for prevention of data dispersal
○ IT.1.8 Control of the access to sensitive information from mobile devices (PDA, smartphone, mobile PCs, etc.)
○ IT.1.9 Information security policy
○ IT.1.10 Information integrity: encryption of data at rest and in motion, access control to information, policy for permissions and roles,
○ IT.1.11 Protection and classification of information related to e-commerce transactions
○ IT.1.12 Automatic routines embedded for the control of integrity of information
○ IT.1.13 Quality and security test of the systems and services
○ IT.1.14 Network security: use of secure protocols, identification of the parts of the networks with high level of risks, control of the connections between networks, ad-hoc security mechanisms for wireless networks
○ IT.1.15 Identity and authentication for access to applications, platforms, networks
○ IT.1.16 Physical and environmental security
○ IT.1.17 Human resources security
○ IT.1.18 Incident management
○ IT.1.19 Incident detection
○ IT.1.20 Incident reporting
○ IT.1.21 Dedicated interfaces, accesses and tools for audit and monitoring activities
○ IT.1.22 Intrusion detection: use of log, use of technology location-aware for integrity and authentication
○ IT.1.23 Separation between operation and non-operation (test, development) environments
○ IT.1.24 Security of third party
○ IT.1.25 Business continuity and disaster recovery plan
○ IT.1.26 Exercise and operation of contingency plan
○ IT.1.27 Resiliency and Impact Analysis
○ IT.1.28 Security of supplies
○ IT.1.29 Clock synchronization

B.2.2 Document IT.2: Technical specifications regarding security of computer applications in the Executive and the Legislative Assembly of the Emilia-Romagna

- **Description**: This specification describes the technical and procedural aspects required for the design, development, deployment, testing and management of a secure application. Particular attention is dedicated to web applications, as they are more exposed to threats to their intrinsic characteristic to make available services to a large number, and often undefined users. Moreover the document provides the MINIMAL LAW REQUIREMENTS for external and internal agents suppliers of products or services for government administration

- **Link**: [http://194.242.234.211/documents/10160/2052659/CLOUD+COMPUTING+%E2%80%93+PROTECT+YOUR+DATA+WITHOUT+FALLING+FROM+A+CLOUD.pdf](http://194.242.234.211/documents/10160/2052659/CLOUD+COMPUTING+%E2%80%93+PROTECT+YOUR+DATA+WITHOUT+FALLING+FROM+A+CLOUD.pdf)

- **Application Domain**: Online applications and services processing and storing non-sensitive, sensitive and/or juridical data, for the Local government agencies of the Emilia-Romagna

- **Tags**: Procurement,

- **Status**: mandatory

- **NIS Requirements**:
  ○ IT.2.1 Compliance with obligations by law force (rule 25 of Annex B of the Legislative Decree no. 196/03)
  ○ IT.2.2 Authentication
  ○ IT.2.3 Authorization
  ○ IT.2.4 Management of users sessions
  ○ IT.2.5 Validation of data
  ○ IT.2.6 Error handling
  ○ IT.2.7 Tracking
  ○ IT.2.8 Monitoring
  ○ IT.2.9 Encryption of data at rest and in motion
  ○ IT.2.10 Data Availability

- **Other Requirements**
  ○ IT.2.11 Project Documentation
  ○ IT.2.12 Testing deployment and management

B.2.3 Document IT.3: Cloud Computing: How to Protect Your Data without Falling From a Cloud - A Mini-Vademecum for Businesses and Public Bodies

- **Description**: The document is a guidance to all users (in particular businesses and public administrative bodies) issued in 2013 by the Italian Data Protection Authority “Garante per la protezione dei dati” Agency to providing the description of the major legal, economic and technological issues of the Cloud computing and some practical rules and tips to foster the appropriate use of Cloud computing technologies. It provides the introduction of the basics of Cloud Computing and the legal framework related to data privacy and protection. It then proposes a list of checks for assessing risks, costs, benefits before opting for a given type of cloud and a list of basic checks to be analysed to choose properly the provider. The documents describes some basic questions to be posed and fully analysed by the users of Cloud
Computing before selecting cloud options and initiating the procurement.

- **Link:** [http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1906143](http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1906143)

- **Application domain:** procurement of cloud-systems, data protection

- **Tags:** CloudSpecific, DPspecific

- **Status:** guidance.

- **NIS Requirements:**

- **Other requirements:**
  - IT 3.1. Check list for assessing risks, costs, benefits
  - IT.3.2 Basic checks to choose the provider

### B.3 Netherlands

The Netherlands government (Minister of General Affairs) provides mandatory prescriptions for information security for special information. Cloud computing is considered as one of the available ICT technologies to implement services, therefore there are not specific guidelines for cloud computing. The Dutch National Cyber Security Center provides a set of recommendations for the security of web applications. Such recommendations apply to central government and local governments. Another important Dutch board, the Water Board, emanated Mandatory security measures which should be taken into account to guarantee the minimum security levels to be met by a (local) water authority.

The following 3 documents contain relevant NIS requirements:

- **NL.1 Law - for security requirements for special information VIRBI 2013**

- **NL.2 ICT security guideline for web applications (national government and decentralized government)**

- **NL.3 Baseline information security Public Water Management**

#### B.3.1 Document NL.1: Law - for security requirements for special information VIRBI 2013

- **Description:** This rule with the accompanying notes and annex 1 shall apply to the National Office, which included the ministries of the subordinate departments, companies and institutions. The rule applies to classified information (see article 2). Annex 1: Define Minimum security design principles and requirements. The document specifies both Security Objectives and Related Requirements.

- **Link/source:** [http://wetten.overheid.nl/BWBR0033507/geldigheidsdatum_14-04-2014](http://wetten.overheid.nl/BWBR0033507/geldigheidsdatum_14-04-2014)

- **Application Domain:** ICT system and services processing and storing special (classified) information.

- **Tags:** Procurement, Classified Information

- **Status:** Mandatory

- **NIS Requirements:**
  - NL.1.1 Management of assets: Assets which specific information is processed, must be recorded and assigned
  - NL.1.2 Trust of persons working with special information: confidentiality guidelines of the AIVD (civil sector) and DISS (military sector) should be followed. Termination policy must be considered and implemented
○ NL.1.3 Physical and environmental security
○ NL.1.4: Access control (procedures and rules)
○ NL.1.5: Monitoring of network, systems and applications where information is classified
○ NL.1.6 Transmission of classified information: measure to maintain confidentiality of information must be implemented to support (electronic) transport outside controlled territory

● Other Requirements: -
○ NL.1.7 Preparatory Threats and risk analysis in Lifecycle of ICT facilities: risk and threats analysis are preparatory to the acquisition, development, maintenance and repels of systems processing special information

B.3.2 Document NL.2: ICT security for web applications (national and decentralized government)
● Description: The Directive is based on the Framework for Web applications Security (RBW) published by the NCSC. The framework is based on the concept of layered security.
● Application Domain: Web application
● Tags: Procurement,
● Status: Guidelines, Recommendations
● NIS Requirements:
  ○ NL.2.1 Network security
  ○ NL.2.2 Application Security
  ○ NL.2.3 Platform security
  ○ NL.2.4 Identity and access management
  ○ NL.2.5 Confidentiality and non-repudiation
  ○ NL.2.6 Security Integration
  ○ NL.2.7 Monitoring, auditing and alerting

● Other Requirements: -

B.3.3 Document NL.3: Baseline Regional Water information Strategic and Tactical standards
● Description: The baseline includes measures to mitigate information security risks covered at the Water Boards. The baseline includes some minimum security levels should be met by a water authority. The document does not cover the all the security risk. For risks that are not covered by the baseline the Water Boards will use further management measures
● Link/source: http://www.uvw.nl/download.php?f=5c2d7ab9f43504266becc140c00cf5aa
● Application Domain: ICT systems in water management
● Tags: Procurement, Critical Infrastructures
● Status: Mandatory
● NIS Requirements:
  ○ NL.3.1 Security of Information: Ensure that security is an integral part of information systems.
  ○ NL.3.2 correct processing in applications: Prevent errors, loss, unauthorized modification or abuse of information in applications.
  ○ NL.3.3 Cryptographic controls: Protecting the confidentiality, authenticity or
integrity of information using cryptographic means.
○ NL.3.4 Security of file system: accomplish file system security
○ NL.3.5 Security in development and support processes: maintaining security of application software and information.
○ NL.3.6 Management of technical vulnerabilities: Reduce risks resulting from exploitation of published technical vulnerabilities

B.4 Spain
Spain has a draft legal document on the security for cloud (ES.1). This document provides recommendations on the security requirements that should be taken into account when procuring cloud services in order to meet the guidelines specified by national Cyber security strategy and the National security scheme for eGovernment (ES.2).

In Spain there are 4 documents with relevant NIS requirements:
- ES.2: National security scheme for eGovernment (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.)
- ES.3: Personal Data protection law (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal)
- ES.4: Service providers regulations law (Ley 34/2002, de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI))

- Description: The document “Guia/norma de seguridad de las TIC - Seguiridadad en entornos Cloud” is a draft legal document on the security for cloud. The document includes the security requirements that should be taken into account when procuring cloud services in order to meet demands of the ES Cyber security strategy. The requirements are divided in general security requirements and data protection requirements.
- Application domain: Governmental cloud based services and their procurement
- Tags: CloudSpecific, Procurement, DPSpecific
- Status: Guidance, Recommendations
- NIS Requirements:
  ○ ES.1.1 Authentication
  ○ ES.1.2 Traceability
  ○ ES.1.3 Data handling: data management in the cloud, migration of data to the cloud
  ○ ES.1.4 Security for subcontracting;
  ○ ES.1.5 Data protection and information protection: compliance of the cloud solutions with national laws. Cloud solutions must meet the requirements defined in the Article 12 of the Data Protection Act and Article 82 of RDLOPD.
  ○ ES.1.6 Availability
  ○ ES.1.7 Data Integrity and Confidentiality
○ ES.1.8 Incident reporting and handling rules,
○ ES.1.9 time to restore rules,

● Other Requirements:
  ○ ES.1.8 Risk analysis of the assets
  ○ ES.1.9 Liability and responsibility
  ○ ES.1.10 Fees in cases of incidents or/and changes

B.4.2 Document ES.2: National security scheme for eGovernment (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.)

● Description: The document provides a high level outline of all the security measures that should be taken into account in the use of ICT by Public Administrations. It includes measures related to analysis, prevention, and evaluation. It gives guidelines for the design of security measures/layers and provides minimum security requirements. The document also provides guidelines for the protection of information and the procurement of ICT services/products.


● Application domain: Governmental ICT-based services

● Status: Guidance, Mandatory

● NIS Requirements
  ○ ES.2.1 Organization and implementation of the security process (policy);
  ○ ES.2.2 Personnel security;
  ○ ES.2.3 Authorization and access control;
  ○ ES.2.4 Infrastructure security;
  ○ ES.2.5 Security by default;
  ○ ES.2.6 Integrity and system update;
  ○ ES.2.7 Protection of information stored and in transit;
  ○ ES.2.8 Protection from other interconnected information systems.
  ○ ES.2.9 Activity Log.
  ○ ES.2.10 Security incidents.
  ○ ES.2.11 Differentiation in Security roles
  ○ ES.2.12 Business continuity

● Other Requirements
  ○ ES.2.14 Purchase of products (procurement). Certification of security functionalities is an award criteria

B.4.3 Document ES.3: Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal

● Description: The document is focussed on directives for the protection of personal data. Directions are not strictly related to cloud solutions and/or ICT in general, but to all activities in which data and information protection is to be considered. The document defines principles of data protection in terms of data quality, data ownership (responsible/processor) and management (controller). It defines also rules for the communication data (data transfer from public sources to other sources and access by third parties)

● Link/source: http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf

● Application domain: Public and governmental institutions and services
Cloud Certification Schemes Metaframework
Version 1.0, November 2014

- **Status**: Mandatory
- **NIS Requirements**: -
- **Other Requirements**:
  - ES.3.1. Data ownership and processing: The processor, and may not subcontract with a third party performing services involving the treatment of the data
  - ES.3.2. Data communication and transferability: In case of transfer of data in international context, the information needs to be treated in accordance to the Articles 33 and 34 of the Data Protection Act;

### B.4.4 Document ES.4: Ley 34/2002, de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI) (Service providers regulations law)

- **Description**: LSSI - The document is focussed on the obligations for the services provider established in Spain to communicate the adopted security practices to the customers. The provider must inform its customers about security measures to increase the security of information and of the provision of services, tools for filtering and restricting illicit Internet content, sanctions to users that may incur in the illicit use of the Internet
- **Application domain**: services providers (hosting data in the cloud, internet access)
- **Status**: Mandatory
- **NIS Requirements**:
  - ES.4.1. Transparency and obligations to communicate adopted security measures
- **Other requirements**: -

### B.5 Sweden

The Swedish Civil Contingencies Agency (MSB) has issued a guideline to information security in procurement of IT-systems, outsourcing and cloud services. The guideline (issued in 2013) targets governmental agencies, municipalities, and county councils in support of making their procurement of IT-systems, outsourcing and cloud services more secure. A tender has been launched for the procurement of public cloud services for the office automation of the governmental institutions.

In Sweden there are 3 documents with relevant NIS requirements:
- SW.1: Cloud services and the Personal Data Act SW.1: Vägledning –informationssäkerhet i upphandling Informationssäkerhet i upphandling av system, outsourcing och molntjänster
- SW.2: Cloud services and the Personal Data Act
- SW.3: “Kontorsstöd som molntjänst”, Requirements for the Cloud services tender

#### B.5.1 Document SW.1: Vägledning –informationssäkerhet i upphandling Informationssäkerhet i upphandling av system, outsourcing och molntjänster

- **Description**: The document is a guideline (issued in 2013 by The Swedish Civil Contingencies Agency) for the information security in procurement of IT-systems, outsourcing and cloud services targeting governmental agencies, municipalities, and county councils in support of making their procurement more secure. The document reports an overview of the main security aspects to be addressed in IT procurement (security information strategy, redundancy
and flexibility, security solutions in general, roles and responsibilities, subcontracting, risk of falling into "bad company", Lock-up and transfer of contractual terms to another party, business continuity and disaster recovery, data storing and delete, legal risks) and provides support for the various activities of the procurement process related to information security aspects which require specific consideration such as risk analysis, classification of information, accountability, and monitoring requirements. It concludes suggesting the use of cloud services for an organization with high demands on availability, but where the information is not sensitive in terms of confidentiality, integrity and traceability.

- Link: https://www.msb.se/RibData/Filer/pdf/26589.pdf
- Application domain: procurement of IT systems, outsourcing and cloud-systems
- Tags: CloudSpecific
- Status: guidance.

- NIS Requirements:
  - SW.1.1 Request for different levels of protections from the providers. The supplier should be able to offer a range of different levels of protection, giving the fact that the use of the service may change over time and/or a re-classification of information requirements can occur. To be adherent with ISO standard (ISO / IEC 27001 and 27002) should be included in the requirement specifications (indication, not mandatory).
  - SW.1.2 Monitoring and assessment of the security activities and controls in place
  - SW.1.3 Access control to information
  - SW.1.4 Traceability and logging
  - SW.1.5 Availability and restoration of the service
  - SW.1.6 Backup
  - SW.1.7 Incident reporting
  - SW.1.8 Human resources check
  - SW.1.9 Security of third party
  - SW.1.10 Business continuity
  - SW.1.11 Audit

- Other requirements:
  - SW.1.14. Roles and responsibilities for data management and information security: The relationship between customer and supplier must be based on accepted responsibility model, which reports specific security measures (logging, user management, incident management and business continuity management).
  - SW.1.15 Implementation of process for risk analysis and information classification. The key tools to determine the requirements for IT-related services include risk analysis and information classification because the service must meet the organization's general security principles.
  - SW.1.16 Contractual agreements in general: the requirements in the contractual agreements should cover other than security areas (Roles and responsibilities, handling of personal data and not outside the EEA, use of subcontractors, flexibility and scalability of the services, licenses and intellectual property rights, dispute settlements)
B.5.2 Document SW.2: Cloud services and the Personal Data Act

- **Description**: The document reports an overview of the main checks to be performed by the controller regarding the processing of personal data under the Personal Data Act. Personal data processors are only allowed to process personal data in accordance with instructions from the controller, which must be in compliance with the Personal Data Act and other legislation, such as government agency-specific records statutes and the Public Access to Information and Secrecy Act.
- **Application domain**: cloud services and privacy of personal data
- **Tags**: DPSpecific
- **Status**: guidance, mandatory
- **NIS Requirements**
  - SW.2.1. Requirements for the users of cloud services (i.e. the controller) for processing of personal data: The controller of personal data must carry out legal checks and risk and impact assessment, sign a processor agreements with the cloud provider compliant with the Personal Data Act, assure himself that all the security measures required are in place, ensure that some exemptions are applied in case of processors based in third country outside the EU/EEA.

B.5.3 Document SW.3: “Kontorsstöd som molntjänst” (Cloud services for office automation)

- **Description**: The document is the contractual framework agreement for the procurement of cloud services for the public sector produced by the State Trading Centre (responsible for coordinating the procurement in information technology for public administration). The cloud services of the tender are electronic calendar, Address Book with contacts, Word Processing, spread sheet, Presentation. The documents describe technical requirements, security requirements, contractual clauses, personal data processing obligations, etc.
- **Link**: [http://www.avropa.se/PageFiles/23990/ffu.pdf](http://www.avropa.se/PageFiles/23990/ffu.pdf)
- **Application domain**: cloud services
- **Tags**: CloudSpecific
- **Status**: mandatory
- **NIS Requirements**:
  - SW.3.1. Compliance with PDA
  - SW.3.2. Website for current security levels and procedures. The bidder shall specify the address to website (URL) where the security levels and security practices for cloud service exist.
  - SW.3.3 Audit: The service should be revised according to the SSAE 16 Type 2 and / or ISAE 3402\textsuperscript{nd} audit report
  - SW.3.4 Protection and Encryption (TLS, SMTP, etc.)
  - SW.3.5 Protection from spam, malware, virus
  - SW.3.6 Business continuity
  - SW.3.7 Intrusion prevention
  - SW.3.8 Data and metadata storage, backup and restore
  - SW.3.9 Authentication and Access control per user, per group
  - SW.3.10 Regulatory framework to prevent files from being shared outside the
organization and in the internet.

- SW.3.11 Tracing, Logging and monitoring of login, email, access control changes, read or changed data
- SW.3.12 Synchronization of password and accounts based on TLS

**Other Requirements:**
- SW.3.13 List of compatible browsers for cloud services
- SW.3.14 OSs specification for the client-side apps
- SW.3.15 Request for Import/export functions without manual data processing
- SW.3.16 Request for APIs (for creating address books, for migration of e-mail lists, for migration of calendar data, to update the calendar data, for creating/updating/downloading files, to update the access control information files, to retrieve authentication information files, to update the access control information, to retrieve authentication information)
- SW.3.17 Request of export functions for the users settings, preferences, filters for email, templates, signatures
- SW.3.18 Contractual agreements in general (other than security areas): Roles and responsibilities, handling of personal data and not outside the EEA, use of subcontractors, flexibility and scalability of the services, licenses and intellectual property rights, dispute settlements

### B.6 Germany

The Fraunhofer Fokus published a Cloud Roadmap for federal institutions that covers more than only security issues, focused mainly on the migration of IT services to Cloud. The BSI published a guideline with the minimum requirements for Information security in Cloud Computing, to help the Cloud Providers to adequately implement security measures. Recently the BSI delivered some control modules of the IT Grundschutz Certificate (in a pre-release version) specifically related to the Cloud (cloud management, cloud adoption, cloud storage, web services).

In Germany there are main 2 documents with relevant NIS requirements:
- DE.1: Cloud-fahrplan für die öffentliche verwaltung
- DE.2: Security Recommendations for Cloud Computing Providers, white paper BSI

#### B.6.1 Document DE.1: Cloud-fahrplan für die öffentliche verwaltung

**Description:** The document published by the Fraunhofer Institute FOKUS is a road map to help federal institutions in the migration of IT services to Cloud. The document reports an overview of the main aspects to be addressed in the migration of IT services to Cloud: security and privacy issues (data locations, Multi-Tenancy, access right management, data deletion, availability), specific risks of the Cloud model, dependence to providers, legal issues. The document provides then an overview of the aspects to be considered in a procurement action that are relevant to the specific case of the migration of IT services to the Cloud: preliminary checks, needs analysis and assessment of the requirements for the services migrated to the Cloud, risk analysis (BSI-Standard 100-3, ISO standards 31000, ENISA report), set-up of an appropriate tender procedure, award and contractual clauses, migration.

**Link:** [http://www.oeffentliche-it.de/documents/18/21941/Cloud-](http://www.oeffentliche-it.de/documents/18/21941/Cloud-
Fahrplan+oeffentliche+Verwaltung

- **Application domain**: procurement of IT systems, cloud systems
- **Tags**: CloudSpecific
- **Status**: guidance.
- **NIS Requirements**
  - DE.1.1 Compliance with Federal Data Protection Act (BDSG), if personal data are processed or stored in the Cloud (each state has different data protection laws).
  - DE.1.2 Compliance with laws and regulations for classified information (“General Administrative Regulation of the Federal Ministry of the Interior to the material and organizational protection of classified information (VS statement - VSA)”).

- **Other requirements**:  
  - DE.1.3 Architectural requirements for implementing and operating large IT-systems and infrastructures. For example, compliance with SAGA, that is a compilation of references to specifications and methods for software systems of public administration (http://www.cio.bund.de/Web/DE/Architekturen-und-Standards/SAGA/saga_node.html)


- **Description**: The document published by BSI defines the minimum requirements for Information security in Cloud Computing, collected through joint discussion between providers and users. The purpose of the paper is to give a guideline for the Cloud Providers to adequately implement security and for the users to properly ask the security measures of the providers. The focus of the document is on security issues in the cloud-based processing of information with a normal to high protection requirement, e.g. confidential company and personal data worthy of protection. The paper provides an overview of the main Cloud Computing areas in which security should be implemented, differentiating the security measures indicated for private and public clouds.

- **Link**:  

- **Application domain**: procurement of IT systems, cloud systems
- **Tags**: CloudSpecific
- **Status**: guidance.
- **NIS Requirements**.
  - DE.2.1 Implementation of an information security management system (recommended ISO 27001/2 or, preferably, the BSI standard 100-2/IT-Grundschutz methodology)
  - DE.2.2 Physical security
  - DE.2.3 Redundant Key supply components
  - DE.2.4 Redundant data centres for high availability protection requirement
  - DE.2.5 Server security with Technical measures to protect the host (host firewalls, regular integrity checks, host-based intrusion detection systems)
o DE.2.6 Deploying certified hypervisors (Common Criteria EAL 4 at least)
o DE.2.7 Server security with secure basic configuration for the host
o DE.2.8 Security measures against malware and network-based attacks
o DE.2.9 Security measures against DDoS attacks for high availability protection requirement
o DE.2.10 Network security with network segmentation, Remote administration via a secure communication channel (e.g. SSH, TLS/SSL, IPSec, VPN), Encrypted communication between user and provider, between cloud computing locations, with third party providers
o DE.2.11 Redundant networking of the cloud data centres for high availability protection requirement
o DE.2.12 Application and Platform Security (security in the SW development life cycle process, Securely isolated applications and Guidelines for customers to create secure applications for PaaS, compliance of SW with OWASP)
o DE.2.13 Automated checking of customer applications for application vulnerabilities for high availability protection requirement (PaaS)
o DE.2.14 Patch and change management
o DE.2.15 Data security (data security in the life cycle, isolation, backup and deletion policy)
o DE.2.16 Encryption and key management
o DE.2.17 Authentication
o DE.2.18 Role-based access control
o DE.2.19 Monitoring and Security Incident Management
o DE.2.20 Set up and operation of a business continuity management system. Compliance with BS 25999 or BSI standard 100-4 for high availability protection requirement is required
o DE.2.22 Exit agreement with assured formats and retention of all logical relations and specifying any associated costs (SaaS)
o DE.2.23 Standard or open interfaces (API and protocols)
o DE.2.24 Audit (transparency about security measures, changes to the IT security management system, security incidents, the results of IS reviews and penetration tests)
o DE.2.25 Security testing (penetration test, security reviews)
o DE.2.26 Trustworthy staff
o DE.2.27 Training staff
o DE.2.28 Data protection and compliance with laws and regulation

**Other requirements:**
o DE.2.29 Defined procedural model for all IT processes (e.g. as per ITIL, COBIT)
o DE.2.30 Adequate organizational structure for information security (including named contact persons to answer customers’ security questions)
o DE.2.31 Interfaces to monitor the service quality specified in their agreement
o DE.2.32 Legal and ownership structure and decision-making powers of the cloud provider
o DE.2.33 Contractual agreement for Transparency on governmental intervention or viewing rights, on any legally definable third party rights to view data and on any obligations that the cloud service provider has to check stored data at any potential location
o DE.2.34 Contractual agreement for Transparency on datacenters location where are processed data, subcontractors, etc.
o DE.2.35 Security SLAs
o DE.2.29 Certification in compliance with ISO 27001 based on IT-Grundschutz, ISO 27001 or other established standard (recommended)

B.7 Finland

Central government imposes obligations to the private organizations to implement and maintain administrative and technical information security policy. The documents more relevant for the procurement of cloud services are the KATAKRI guideline, which defines national security auditing criteria for services processing classified governmental data and the VAHTI guide that reports the security requirements to be follower for applications development. The “Guideline for technical ICT environment security”\(^5\) has a section dedicated to the procurement of cloud services, where the main advantages and disadvantages of the cloud models are surveyed.

In Finland there are 2 documents with relevant NIS requirements:
- FI.1: KATAKRI, Kansallinen turvallisuusauditointikriteeristö, National Security Auditing Criteria
- FI.2: VAHTI, Valtionhallinnon tietoturvaohje, Government Information Security Guideline

B.7.1 Document FI.1: KATAKRI, National Security Auditing Criteria
- **Description:** The KATAKRI document defines national security auditing criteria for services that are procured from private sector for processing of classified government data and to be followed when an authority conducts an audit to verify their security level. The document is applied for information whose confidentiality, integrity and usability shall be protected, including the sensitive information of companies (business secrets regarding product development, for example) and the protected or classified information of the authorities. The criteria are divided into four main areas: administrative security (security management), personnel security physical security and information security. The information security assurance provides the minimum requirements for information whose confidentiality, integrity and usability shall be protected. The information assurance criteria have been divided into Data Communications Security, Security of Information Systems, Security of Information, Security of Information Handling, specifying requirements for the base level (IV/RESTRICTED), for the increased level (III/CONFIDENTIAL), for the high level (II/SECRET) and finally, general recommendations for the industry

\(^5\) [http://www.vm.fi/vm/fi/04_julkaisut ja asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20121122Teknis/name.jsp](http://www.vm.fi/vm/fi/04_julkaisut ja asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20121122Teknis/name.jsp)
- Application domain: procurement of IT systems,
- Tags: CriticalInfrastructur
- Status: guidance.
- **NIS Requirements.**
  o FI.1.1 Compliance with legal requirements and security guidelines
  o FI.1.2 Security policy covering premises security, information assurance and personnel security
  o FI.1.3 Business continuity management and plans
  o FI.1.4 Change management procedure in place for changes related to data processing
  o FI.1.5 Security training, increasing security awareness and know how
  o FI.1.6 Guidelines for recruitment procedures and during employment considering the security
  o FI.1.7 Physical Security (area, structures, Technical Security Systems)
  o FI.1.8 Network security: Protection of management connections, Private network for internal network, Identification of special features of IPv6, Security of routing according to the risk assessment
  o FI.1.9 Protection of wireless networks with encryption and user Identification
  o FI.1.10 Monitoring of network, system, infrastructure according to the risk assessment
  o FI.1.11 Identification and authentication
  o FI.1.12 Standard Operational procedures for configuration and installation
  o FI.1.13 Separation of development, testing and production environment
  o FI.1.14 Procedures for vulnerabilities of networks and services
  o FI.1.15 Backup procedures
  o FI.1.16 Malware detection, prevention and recovery procedures
  o FI.1.17 Logging for detection of security breaches
  o FI.1.18 Separation for classified information through user permission definitions and handling
  o FI.1.19 Protection of media storage
  o FI.1.20 Protection of classified information from third-party access
  o FI.1.21 Protection of networks from unauthorized devices
  o FI.1.22 Marking of classified information
  o FI.1.23 Secure delete of classified information
  o FI.1.24 Secure electronic transfer of classified information
  o FI.1.25 Encryption and key management
  o FI.1.26 Use of known and trustworthy techniques for session management
  o FI.1.27 Storage of Authentication data (like passwords, fingerprints etc.) not in clear test format
  o FI.1.28 Trusted and authorized sources for the code
  o FI.1.29 Recovery procedures from malfunctions, disturbances, attacks,
  o FI.1.30 Security mechanisms against the risks of remote working
- **Other requirements:**
B.7.2 Document FI.2: VAHTI, Government Information Security Guideline

- **Description:** The document VAHTI (“Valtionhallinnon tietoturvaohje”, “Government Information Security Guideline” in English) is a guide for the governmental organizations that reports the security requirements expected to be considered in the software and application development and used in defining procurement requirement specifications for tenders related to customized applications and services, comprising as an extension the SaaS services. The document provides an overview of the main issues related to the Clouds and that have to preliminary verified before choosing the providers and the solutions, which are mainly support for the data and application portability, Backup of encrypted data, Backup of data on different providers, Transparency of security measures implemented, Transparency of the Data location, encryption and key management, Auditing and test of the provider.

- **Application domain:** procurement of IT systems, cloud systems
- **Tags:** CriticalInfrastructure
- **Status:** guidance.

- **NIS Requirements.** The document defines security requirements to be followed in the whole applications development cycle (Feasibility Study, Requirement Specifications, design, Implementation, Testing, Maintenance, disposal) to ensure information security.
  - FI.2.1 Compliance with laws, regulations and guidelines
  - FI.2.2 Encryption
  - FI.2.3 Strong authentication and access control
  - FI.2.4 Design and implementation of mechanisms for application exception and error handling notifications
  - FI.2.5 Proper Logs of failures and security incidents and Rich event log data
  - FI.2.6 Common time source synchronizations for logging and events detection
  - FI.2.7 Access roles and permissions to logs
  - FI.2.8 Enhanced security measures for logs (check-sum, encryption, etc.)
  - FI.2.9 Periodical monitoring of logs
  - FI.2.10 Security measures in place to prevent session hijacking
  - FI.2.11 Management of password and user accounts
  - FI.2.12 Testing of network security
  - FI.2.13 Code reviews for the security of critical parts
  - FI.2.14 Integration of automated testing tools
  - FI.2.15 Security audit
  - FI.2.16 Security mechanisms for inspection
  - FI.2.17 Security penetration tests
  - FI.2.18 Standard application security settings and related documentation
  - FI.2.19 Mechanisms for critical security updates and installations of applications and patches
  - FI.2.20 Mechanisms for the applications backup
o  FI.2.21 Processes for application patch management
o  FI.2.22 Periodical audit of settings affecting security
o  FI.2.23 Processes for Security incidents management
o  FI.2.24 Communication of Security incidents
o  FI.2.25 Post-analysis of incidents
o  FI.2.26 Backup and recovery procedures
o  FI.2.27 Network-based security mechanisms
o  FI.2.28 Data security (delete policy, data portability, data classification)

• Other requirements:
  o  FI.2.29 Definition of the scope of the application and criticality and of the related security requirements
  o  FI.2.30 Business impact analysis
  o  FI.2.31 Threat scenario modelling and analysis
  o  FI.2.32 Risk analysis
  o  FI.2.33 Documentation of the expected operating environment for the correct use of applications

B.8 Austria
Austria has been quite active in the implementation of cloud computing services for the public. In 2011, for example the EDM (Environment Data Management) system has been realised under the coordination of the Ministry of life and Environment. Following this first experience, in 2012, an ad hoc cloud strategy for the public service been defined (see document AU.1), providing the specific criteria for the procurement of cloud computing services by public administration.

• Description: The Cloud strategy provides information necessary for strategic decisions on cloud computing. The document defines the criteria based on which public administration should procure cloud services and also defines the decision making process and the proposed cloud solutions that can be followed. It also provides basic information about cloud computing (concepts, models, impact, benefits, market conditions, opportunities and risks, etc.) as well as potential applications for traditional data center, and examples and processes for migration (a 5-stage process provides insights and guidelines on how to introduce cloud computing for public services). Specifically, the document describes the requirements that the users (internal ICT service public administration) will have to take into account while procuring cloud based system and services.
• Link: https://www.sicherheitshandbuch.gv.at/downloads/Cloud.pdf
• Application domain: Cloud procurement
• Tags: CloudSpecific
• Status: Guidance.
• NIS Requirements
  o  AU.1.1 Data Protection and privacy requirements. The provider is obliged to comply with the national data protection law. In particular compliance with data security
measures according to § 14 DSG\(^6\) (e.g. protection against accidental and illegal destruction, loss or unauthorized access to the data, logging of requests) and data secrecy will have to be addressed.

- **AU.1.2. Data location.** Data should be stored/located should be only within the European Economic Area (§ 12 DSG\(^7\)). Otherwise, a request for authorization should be addressed to the Data Protection Commission.

- **AU.1.3 Compliance with data protection regulation.** Monitoring and audit mechanism to be used by the CSP (e.g. for the traceability features and/or system performance evaluation tasks) will have to be compliant with the data protection regulation.

- **AU.1.4 Rights management.** The system should allow secure identification of clients (as well as the administrators of the CSP and particularly the protection of privileged user profiles of the CSP). The connectivity to a local IDM (Identity Management) customer should be ensured. However, the ID and rights management could be located at a third party.

- **AU.1.5 Safety of services/Access control:** the system should ensure secure access to services and secure identification of clients and administrators of the CSP.

- **AU.1.6. Integrity.** The CSP should ensure that software integrity, configuration integrity and message integrity are all addressed.

- **AU.1.7 Security requirements:** compliance with privacy laws, audit compliance to the privacy and data protection laws, privacy breach, information security, confidentiality, integrity, availability, authenticity are satisfied.

- **AU.1.8 Data management.** The CSP should ensure that security aspects related to data management are addressed, and in particular data access (who has access, deletion and inspection liability) data protection and management (including data location, retention policy (data location), data destruction).

- **AU.1.9 Network availability.** In this case related security measures may vary from service to service. They should however include logical protection measures such as access rights, as well as technical measures such as redundancy or protection against targeted sabotage attempts by third parties.

- **AU.1.10 Threat management.** The system should ensure effective security measures in order to monitor manage and recover the system. Specific segregation of responsibilities for accessing, processing, managing and assessing the threat. Structure process should be earlier defined and responsibilities in order to better manage security incidents.

- **AU.1.11. Standards compliance.** In the provisioning of cloud services, a number of standards (e.g., SAML, SPML, XACML, LIAF) should be supported by the CSP in addition to other that currently are already supported by most of providers but not focussed on cloud computing issues (ISO2700X, BSI Baseline Protection, BASEL III)

- **AU.1.12. Audits.** The system should provide features/functionalities in order to allow

---

regular audits (accesses, access profile, etc.).
  ○ AU.1.13. Control and Monitoring of services. Functionalities that include starting, stop and restarting as well as functionalities in order to raise the efficiency/performance.
  ○ AU.1.14 Security policy compliance audit/Technical revision: the customer should be able to access the required information (e.g. log files) and in general all the information related to the implementation of security policy and security policy compliance
  ○ AU.1.15 Patch management. Fast and standardized roll out patches by unified infrastructure.

● Other requirements:
  ○ AU.1.16. Organisational requirements. In the selection of the CSP, a key aspect will be analysis of the "cloud-ability" of IT applications. In particular, from organizational perspective, the following aspects have to be considered: Continuity of business operations, information security, risk tolerance (resilience), interdependence of IT applications, and migration cost and efforts. AU.1.17 System performance: Massive scalability and resources management

B.9 Slovakia
The Slovak Republic is quite active in the promotion and adoption of innovative technologies in the public sector. For example, the Information Society Section of the Ministry of Finance of the Slovak Republic has been actively participating in the preparation of the 2014-2020 programming period as the sponsor responsible for compliance with the ex-ante conditionality Digital Growth and Next Generation Access. For what specifically concerns cloud computing and governmental services, the Slovak Republic the Ministry of Finance has issued a (decree), effective from March 2014, with the objective of legislating the use of information systems in the public administration. The law also provides specific instructions about cloud computing services.

● Description: The decree provides instructions about standards, formats and general rules to be followed in the use of information system by and for public administration. Specifically the decree details the technical standards related to technical resources, network infrastructure and software resources (including for interconnection, access to electronic services, webservices, data integration, accessibility and functionality, network infrastructure, middleware and data, architecture management), technical security (eGovernment services relating to the data registers, dials and application software, project management standards relating to the procedures and conditions related to the formation and development of information systems in public administration), and finally standards related to cloud computing and the use of cloud services related to hardware and software resources.
  ● Application domain: procurement and use of ICT service and systems
● **Tags:** SecurityPolicy
● **Status:** Mandatory (Law)
● **NIS requirements:**
  o SK.1.1. Risk management for information security (regular collection of data related to risks), and procedures for identification, analysis and monitoring of risks.
  o SK.1.2. Procedures for protection against malicious code
  o SK.1.3. Network security: firewalls, establishment of a “secure area”, back-up mechanism and physical storage of back-up mechanism facilities. Maintenance, storage and recording of public IT systems and components.
  o SK.1.4. Periodic vulnerability assessment
  o SK.1.5. Access control
  o SK.1.6. Monitoring and management of security incidents (instructions for the development of an “internal act”)
  o SK.1.7. Email security. Support for protected transmission of data over the cryptographic protocol SSL at least version 3.0 or TLS to ensure the transmission of electronic email messages
  o SK.1.8. Software update

● **Other requirements**
  o SK.1.9. Standards for identity federation protocol (for both the provider and the user). Security Assertion Mark-up Language (SAML) version 2.0 according to the Advancement of Structured Information Standards (OASIS)
  o SK.1.10. Web accessibility standards, visual layout, components and functionalities of websites.
  o SK.1.11. Network protocols (IPv6)
  o SK.1.12. Formats. File formats (audio, video, graphics files etc.), compression formats (.zip, .tar, etc.), email and web domain formats.
  o SK.1.13. Standards for third party involvement

**B.10 Greece**

Greece has not defined a specific national cloud strategy, but has launched a number of actions to support the implementation of cloud in the public sector (currently cloud services are provided in the Greek academic community by GRNET). In 2011 an important tender (see document GR.1) has been launched for the provisioning of cloud computing services and infrastructures for the public sector. Alongside a number of regulatory initiatives (GR.2 and GR.3) has been realised to regulate electronic and network communications in the public sector.

In Greece there are 3 documents with relevant NIS requirements:

● GR.1: “Central Computational Infrastructures IS SA - Node G-Cloud GSIS”, a GovCloud tender launched by the KTPAE (Information Society SA) in 2011.
● GR.3: 2013 “Regulation for the Safety and Integrity Network and Electronic Communications Services”, produced by the Assurance Authority for Confidentiality of Communications
B.10.1 Document GR.1 Central Computational Infrastructures IS SA - Node G-Cloud GSIS Tender

- **Description** The document is related to a tender launched in 2011 as an open international competition for the procurement of Governmental cloud services. The project is called “Central Computational Infrastructures IS SA - Node G-Cloud GSIS” and forms part of the strategic plan of the government to provide e-government services to citizens. The contracting authority is the KTPAE (Information Society SA), the public organization that is in charge of the cloud services to be procured. The aim is the creation of cloud based public data centers for providing computing, network and storage power to public administration. The tender also includes the supply of equipment, standard software and applications as well as all the activities, works and services required for the installation and commissioning of complete technical and operational functioning of the computing data centers, with final aim of building a national provider that will offer private and public cloud services.

- **Link:** http://www.ktpae.gr/index.php?option=com_ktpconsultations&task=Details&id=125&Itemid=23

- **Application domain:** Governmental cloud

- **Tags:** CloudSpecific

- **Status:** Mandatory/Award criteria (Tender specification)

- **NIS Requirements:**
  - **GR.1.1 Data Protection.** The most important requirement is related to the confidentiality and integrity of data of classified information of the users/customers that are stored or transferred in the infrastructure. This requirement is considered as a “high priority” so that the design of the different components of the systems and the overall system infrastructure will have to be driven having in consideration this specific requirement. The design phase should take carefully into account the isolation mechanisms for the execution environments of the different users, for the storage centers and for the connecting networks so that desired levels of confidentiality and integrity are achieved.
  - **GR.1.2 Data privacy.** Privacy and secrecy of classified information transferred through the cloud, confidentiality of communications (backup mechanisms, auditing, and compliance with specific standards if needed).
  - **GR.1.3 Network security:** isolations, firewalls, load balancing etc.- for both the creation of the CSP and the creation of the users interfaces
  - **GR.1.4 System security (high availability, scalability, backup and storage features, asset and configuration management, SLA management and monitoring):** Specific security requirements for platforms, software and applications of the system in order to ensure the infrastructure of the data center, ensure the integrity and availability of the infrastructure.
  - **GR.1.5 Backup requirements (resilience and redundancy) and disaster recovery features**
  - **GR.1.6 Access control.** Authentication and authorization: need for a single point of
authentication and authorization.

- **GR.1.7** Legal and regulatory compliance requirements. Security requirements will have to fulfil and be based on the national policy background.

- **GR.1.8** Reporting and monitoring mechanisms. Tools for reporting incidents and malfunctioning, features to allow/support the definition of incident, or about the non-availability for the different components of the system, threat, risk and vulnerability analysis, threat management plan.

- **GR.1.9** Audit and traceability. Auditing is another requirement that should be taken into account in level of user, action, service, session and system so that there is traceability when and where needed.

- **GR.1.10** Security policies and procedures: Information security policies information security procedures reports, security metrics, and certification. Also includes risk assessment, impact assessment. KPI and metrics (related to availability, system performance, etc.) will be used to test the system once implemented.

- **GR.1.11** Compliance with standards and interoperability. The system will have to be compliant with the major international standards (e.g. analysis of the deviation from the ISO 27K1 is required) to ensure interoperability.

- **GR.1.12** SLA monitoring and cross-checking

- **GR.1.13** Evaluation and Testing: before the final implementation of the cloud infrastructure a pilot phase with ad hoc performance testing will have realised by the providers. On-site knowledge transfer during pilot phase will have to be ensured as well. Testing and staging requirements, vulnerability check will have to be ensured.

**Other requirements:**

- **GR.1.14** Architectural requirements (virtualization, application hosting, storage and networks virtualization. virtual DBS, G2G, intercloud capabilities open architecture) including infrastructure and hardware specifications/needs.

- **GR.1.15** Service oriented implementation: the final goal would be the creation of a public service catalogue, which will comply with standard models of service offerings. The reasons behind this approach is that the quality of the service will be certified and because this way continuous improvement is achieved.

- **GR.1.16** User interface. A user friendly process of authentication, certification, authorization and confirmation will have to be implemented.

- **GR.1.17** Flexibility, stability, openness. The system should be designed as a simple and ensure also to ensure portability and interoperability in a reliable way. It should also be based on open architecture solutions. The infrastructure will have to be flexible and open enough in order to ensure further/additional developments. Abstraction levels will need to be included in the design phase so that future extensions can be done. Also provisions in case of scaling up or scaling down.

- **GR.1.18** Quality of services/products. Products (machines) and services to be delivered will have to be of high quality (e.g. in terms of performance, also enabling high computational capacities) and business continuity (24/7 availability and continuity of the requested service). Demand based architecture, optimization of resources.
○ GR.1.19 Environmental impact. The solution to be developed will have to ensure low environmental impact.
○ GR.1.20 Training services: before the launch of the cloud infrastructure ad hoc training services will have to be organised by the cloud provider.


- **Description:** The regulation has been produced by The ASSURANCE AUTHORITY CONFIDENTIALITY OF COMMUNICATIONS (ADAE) in 2011, following the need to harmonise and integrate national rules to ensure the privacy of communications. The regulation applies to a wide variety of telecommunication technologies and services (mobile, satellite, radio, etc.) and provides guidelines for privacy provision of networks and services of electronic communications. Specifically it aims at defining general requirements and policies for the protection, security and privacy of communications. The security procedures provided in the regulation are to be used and define actions for employees, partners, users and subscribers, and others responsible for the implementation of the systems and system operations as well. The document remains at a high level, indicating the actions and activities that will have to be managed through a specific process and the obligations of the responsible person. The appropriate procedures and the specific security mechanisms (e.g. for creation, certification, management, storage, etc.) have to be implemented by the responsible person in accordance with standard and internationally recognised security principles (but not specifically indicated in the document). The document finally provides details about the control and audits to be performed by ADAE.

- **Application domain:** ICT systems, Critical Infrastructures, electronic communication services
- **Tags:** DP Specific, Procurement
- **Status:** Guidance, recommendations

- **NIS Requirements:**
  ○ GR.2.1. Confidentiality, integrity and availability of data (architectural level). Methods for creating, collecting, storing and managing data together with measures to ensure integrity, confidentiality and availability of the data. Rules and obligations to prevent abuse exercise of rights, and in parallel requirements and security measures to ensure confidentiality of communications.
  ○ GR.2.3. Authentication and Access policies
  ○ GR.2.4 Network security to follow the principle of international and widely accepted standards.
  ○ GR.2.5 Physical security (as part of the Network security regulation)
  ○ GR.2.6. Policies against malware.
  ○ GR.2.11 Integrity checks and testing.
  ○ GR.2.12 Encryptions systems must be applied, and based on the results of the risk assessment (see GR.2.7)
  ○ GR.2.7 Risk Assessment methodologies (following international practices) to be performed periodically.
GR.2.8 Incident analysis and reporting: Details, causes (both technical and organisational) have to be investigated and effects to be determined.

GR.2.10 Control policy and audits. Activity has to be performed on the basis of the specific stages of preparation, conduct, results and corrective control actions to be defined by the responsible person.

B.10.3 Document GR.3: 2013 “Regulation for the Safety and Integrity Network and Electronic Communications Services”

- Description: The document has been produced by the Greek authority for privacy, the ADAE (Assurance Authority for Confidentiality of Communications) in 2013 and provides guidelines for the security and integrity of networks and services of electronic communications. The document aims to define the technical and organisation measures to be taken into account while providing “communication network services available to the public”. The aim is to define the “technical and organisation measures for risk management, (while risks are considered in terms of secure networks), prevent and minimise incidents, preserve the integrity of their networks to ensure continuity of services. The document does not define specific technical requirements for the implementation of public network services, but is rather is focused onto the obligations that the provider will have to fulfil, in particular in terms of data ownership issues and responsibilities and system recovery.


- Application domain: ICT systems, Critical Infrastructures, network and electronic communication services

- Tags: Procurement

- Status: Guidance, recommendations

- NIS Requirements:
  - GR.3.1 Compliance with standards or specifications adopted at Community level, (European Organization Standards Board). In absence of such standard the provider will refer to the ISO and the International Electro technical Commission (IEC).
  - GR.3.2 Incident management and System recovery reporting
  - GR.3.3 Business Continuity
  - GR.3.4 Testing and control efficiency plans: scheduled exercises (tests), technical controls penetration (penetrations tests)
  - GR.3.5 Physical security to prevent unauthorized access and protection from natural disasters
  - GR.3.6 Redundancy: backup solutions, to be implemented in relation to the criticality (as from the results of the Evaluation Risk)
  - GR.3.7 Power supply: The provider must ensure the protection of CMS interruptions or disturbances of the public power supply network to ensure uninterrupted operation of these assets.
  - GR.3.8 Access control: mechanisms for logical access control (username and password).
  - GR.3.9 Security Perimeter Network. The provider is required to implement logical
separation of the network from external networks and has been divided into security zones or subnets defining security zones.

- GR.3.10 Vulnerability assessment to evaluate security weaknesses (periodically)
- GR.3.11 Security roles
- GR.3.12 Management and Network Monitoring to control the traffic on the network and identify early increase traffic, while ensuring the performance optimization network.
- GR.3.13 Incident management process security, to be designed by the provider and activated immediately in each case security incident.
- GR.3.14 Business Impact Analysis to be provided periodically (includes changes in the legislative framework - at both national and Community level - the results of inspections, and any other relevant information for the security of the system.
- GR.3.15 Risk Assessment and internal audit (for network integrity): internal reliability, security and resilience of the network as well as external threats (including unpredictable events as natural disasters, accidents, etc.). Vulnerabilities and weaknesses of resources shall also be identified.
- GR.3.16 Control and monitoring procedures to measure the Security and Integrity Networks and Services (include the Preparation of control, the Conduct of monitoring, and the Results of control).

**B.11 Denmark**

It has been decided that all government bodies in Denmark must adhere to IEC/ISO 27001:2013. Danish government does not see cloud services separate from other outsourced ICT services and therefore does not expect to develop a dedicated cloud strategy; hence the guidelines for security and supplier management covers all outsourced ICT services. In Denmark there are two documents with relevant NIS requirements:

- **DK.1**: Cloud computing and the legal framework - Guidance on legislative requirement and the contractual environment related to cloud computing.
- **DK.2** “Informationssikkerhedspolitik for <organisation>” (Security guide for organization)

**B.11.1 Document DK.1: Cloud computing and the legal framework - Guidance on legislative requirement and the contractual environment related to cloud computing.**

- **Description**: The Agency for Digitisation, in cooperation with Kammeradvokaten, the legal adviser to the Danish Government, prepared this guidance for the purpose of reviewing matters, which both the customer (e.g. a public authority) and the supplier of the cloud solution should consider and be aware of when forming a contract regarding cloud computing. This guidance specifies the requirements for personal data handling and how to apply the “The Danish Act on Processing of Personal Data” to the cloud context. Moreover the guidance put in evidence the constraints imposed by other DK acts on the use of cloud solutions. In the specific: The Bookkeeping Act (Bogføringsloven), The Audit Act (Regnskabsloven), The Archive Act (Arkivloven).

- **Link**: [http://digitaliser.dk/resource/2368677](http://digitaliser.dk/resource/2368677)
- **Application domain**: Cloud computing
Cloud Certification Schemes Metaframework

Version 1.0, November 2014

- **Tags:** CloudSpecific, LegalRequirements, DPA
- **Status:** Guidance
- **NIS Requirements:**
  - DK.1.1 No processing of personal data: in this case cloud solution can be applied for processing and storing.
  - DK.1.2 Processing of personal data: caution in using cloud solutions. Be compliant with the DK Act on Processing of Personal Data.
  - DK.1.3 The data controller’s leave of personal data to a data processor (cloud supplier). The data controller is always responsible of data processing. Both public and private data controller and data processor must implement the necessary technical and organisational security measures against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, abuse or other processing in violation of section 41, 3 of the Act on Processing of Personal Data.
  - DK.1.4 Critical information. Precautions must be taken to ensure that the data can be disposed of or destroyed in the event of war or other such events (the Act on Processing of Personal Data section 41, nr 4. Information from the Civil Register (“CPR-registret”), central tax registers and other special registers, in general must not be transferred to a data processor outside Denmark.

- **Other requirements:**
  - DK.1.5 The risk assessment may be done based on a standard for data security such as ISO/IEC 27001 or DS 484, which is the common governmental standard for data security.

**B.11.2 Document DK.2: Informationssikkerhedspolitik for organisationer**

- **Description:** This document is a guideline for organizations to help them define security policies.
  - **Link:** [http://digitaliser.dk/resource/20002](http://digitaliser.dk/resource/20002)
- **Application domain:** ICT systems
- **Tags:** SecurityPolicy
- **Status:** Guidance
- **NIS Requirements:**
  - DK.2.1 Organization and responsibilities
  - DK.2.2 Classification of systems and data
  - DK.2.3 User Conduct
  - DK.2.4 Physical security
  - DK.2.5 Network and operation management
  - DK.2.6 Access Control
  - DK.2.7 The acquisition, development and maintenance of IT systems
  - DK.2.8 Management of security incidents in IT area
  - DK.2.9 IT business continuity management

- **Other Requirements:**
  - DK.2.10 Compliance with statutory requirements