Dear ladies and gentleman:

Please

* Give us some specific information for assessment of the complexity of your ISMS because of our requirements from ISO 27006.
* Fill out the column <Customer data> and column the <Customer specifications> regarding the corresponding complexity factor from column <Complexity factor (CF)>.
* Use for your own assessment the content of the column “CF High”, “CF Medium” and “CF Low" in the tables below and
* Send the data sheet together with our “Questionnaire for Offer Preparation and Preparation for a Certification Procedure” (A00F100e) back to TUEV-NORD CERT.

| **CF ID** | **Complexity factor (CF)** | **Customer data** | **Customer specifications** |
| --- | --- | --- | --- |
| 01 | Determine the scope of the information security management system (ISMS).  Keywords: Character of the business, external and internal issues, interested parties, core processes, org units, locations, assets, technology and interfaces performed by the organization, and those that are performed by other organizations.  REF: 27006 IS 9.2.1; 27001.4 | **Scope definition short:** | **Specified scope definition:** |
| 02 | Is the organization equal to the legal entity? REF: 9k 2.2.3; 3.2.1  Please explain the extent of the organization and the relation to the legal entity(s) in case of “no”.  The concept of a organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, association, charity or institution; also parts or combinations of the mentioned above, whether incorporated or not, public or private.  REF: 27006 IS 9.2.1; 27001.4 | **Yes or No?**  **Please select** | **Explanation in case of “No”:** |
| 03 | What is the total number of persons doing work under the legal entity organisation’s control?  REF: 27006 IS 9.2.1; 27001.4 | **0** |  |
| 04 | What is the total number of persons doing work under the organization’s control within the ISMS scope?  Keywords:  - Employees and contractors stuff of the legal entity. - Permanent and temporary employees - Internal and external employees  REF: 27006 IS 9.2.1; 27001.4 Annex B2.1 | **0** |  |
| 04a | Are in the organisation persons who have no direct or no indirect impact to the ISMS?  REF: DAkkS resolution 04 from 2017 | **Yes or No?**  **Please select** | **Explanation in case of “Yes”:** |
| 05 | Please list all your locations (including headquarter) with the corresponding address and the amount of persons doing work at the related site and label each site regarding its "ISMS risk level" which should be composed of the business and the IT perspective. The level of risk should be assessed by a value from [HIGH], [MEDIUM] and [LOW]. There should be an appropriate explanation in case of [HIGH].  Structure: <HQs > ; <Adr1>; <No. Persons>; <Risk Level>;  <Site 1> ; <Adr2>; <No. Persons>; <Risk Level>; <Site 2> ; <Adr3>; <No. Persons>; <Risk Level>; …  OR Reference to attachment.  REF: 27006 IS 9.1.5; 9.2.1; 27001.4 Annex B2.1; |  |  |
| 06 | Do you wish a combined audit (e.g. together with ISO 9001, ISO 20000-1, ISO 22301) or a sector specific extension like ISO 27011, 27017, 27018, ICE 62443 …?  REF: 27006 IS 9.2.1; 27001.4 | **Yes or No?**  **Please select** | **Explanation in case of “Yes”** |
| 07 | Audit form:  Do you wish a multiple-site-sample audit – not a normal audit? (Note: The answer is NO if you have not branch office in your organization)  REF: 27006 IS 9.1.5; 27001.4 | **Yes or No?**  **Please select** | **Explanation in case of “Yes”** |
| 08 | Is there any ISMS documented information that cannot be made available for review by the audit team because it contains confidential or sensitive information?  (Background:  It is required that auditors have access to sensitive information. Access to this information has to be clarified in advance.)  REF: 27006 IS 8.4; 27001.7.5 | **Yes or No?**  **Please select** | **Explanation in case of “Yes”** |

**Factors for adjustment of audit time**

Please change the pre defined values in column customer data and ad your specification.

| **CF ID** | **Complexity  factor (CF)** | **Customer data** | **Customer specifications** | **CF High** | **CF Medium** | **CF Low** |
| --- | --- | --- | --- | --- | --- | --- |
| 09 | Complexity of the ISMS:   How is the complexity of the ISMS? How is the complexity of processes and tasks?  Information security requirements [confidentiality, integrity and availability (CIA)]  Number of critical assets.  Number of processes and services.  REF: 27006 Annex B3.4.a; 27001.4 | **Please select** |  | Complex processes, high number of products and services, many business units included in the scope of certification (ISMS covers highly complex processes or relatively high number or unique activities.)  Higher amount of sensitive or confidential information (e.g. health, personally identifiable information, insurance, or banking) or high availability requirements.  Many critical assets.  More than 2 complex processes with many interfaces and business units involved. | Standard but non-repetitive processes, with high number of products or services.  Higher availability requirements or some sensitive / confidential information.    Some critical assets  2-3 simple business processes with few interfaces and few business units involved. | Standard processes with standard and repetitive tasks; lots of persons doing word under the organization’s control carrying out the same tasks, few products or services.  Only little sensitive or confidential information, low availability requirements.  Few critical assets (in terms of CIA).  Only one key business process with few interfaces and few business units involved. |
| 10 | What are the type(s) of business and regulatory requirements?  REF: 27006 Annex B3.4.b; 27001.4,A18 | **Please select** |  | Organisation works in critical business sectors.   High risk business with (only) limited regulatory requirements. | Organisation has costumers in critical business sectors.  High regulatory requirements. | Organization works in non-critical business sectors and non-regulated sectors  Low risk business without regulatory requirements. |
| 11 | Do you have previously demonstrated the performance of the ISMS?  What is the level of establishment of the MS?  REF: 27006 Annex B3.4.c; 27001.4 | **Please select** |  | No other management system implemented at all, the ISMS is new and not established.  No certification and no recent audits.  ISMS is new and not fully established (e.g. lack of management system specific control mechanisms, immature continual improvement processes, ad hoc process execution). | Some elements of other management systems are implemented, others not.  Recent surveillance audit.  Not certified but partially implemented ISMS. Some management system tools are available and implemented; some continual improvement processes are in place but partially documented. | ISMS is already well established and/or other management systems are in place.  Recently certified.  Not certified but ISMS fully implemented over several audits and improvement cycles, including documented internal audits, management reviews and effective continual improvement systems. |
| 12 | Extent and diversity of technology utilized in the implementation of the various components of the ISMS (e.g. number of different IT platforms, number of segregated networks)    Total number of IT assets (server, network, external interfaces, information systems ...).  Total number of workstations(laptops, PCs, smart phones ...)  REF: 27006 Annex B3.4.d; 27001.A8,A9,A12,A13 | **Please select** |  | High diversity or complexity of IT (e.g. many different segments of networks, types or servers or databases, number of key applications).  # IT Assets >= 5000 OR  # Hardware >= 1000  OR  # Software >= 200 OR  # Networks >= 50 OR # Others >= 500 | Standardized but various IT platforms, servers, operating systems, databases, networks.  # IT Assets < 5000 and >= 500  OR  # Hardware < 1000 and >= 300  OR  # Software < 5000 and >= 50  OR  # Networks < 50 and >= 10  OR  # Others< 500 and >= 50 | Highly standardized environment with low diversity (few IT-platforms, servers, operating systems, databases, networks etc.  # IT Assets < 500 OR  # Hardware < 300 OR  # Software< 50 OR  # Networks < 10 OR  # Others < 50 |
| 13 | What is the extent of outsourcing and third party arrangements used within the scope of the ISMS?  (Background:  Please select one of the options “High”,” Medium” or” Low” and fill out the column “customer specifications”.)  REF: 27006 Annex B3.4.e; 27001.A15,A18 | **Please select** |  | High dependency on outsourcing or suppliers with large impact on important business activities;  OR  Unknown amount or extent of outsourcing;  OR  Several unmanaged outsourcing arrangements. | Several partly managed outsourcing arrangements. | No outsourcing and little dependency on suppliers;  OR  Well-defined, managed and monitored outsourcing arrangements.  Outsourcer has a certified ISMS. Relevant independent assurance reports are available. |
| 14 | What is the extent of information system development?  Total number of IT (software development and maintenance) staff.  REF: 27006 Annex B3.4.f; 27001.A14 | **Please select** |  | Extensive internal software development activities with several ongoing projects for important business purpose.      ------------------------  IT staff >= 100 | Use of standardized software platforms with complex configuration / parameterization.  (Highly) customized software.  Some development activities (in-house or outsourced)  -----------------------  IT staff >= 20 | No in-house system development.  Use of standardized software platforms.  -----------------------  IT staff< 20 |
| 15 | What is the total number of sites and which of these are Disaster Recovery (DR) sites?  (Example: <HQs > ; DR; <Site 1> ; DR; <Site 2> ;  <Site 3> ;  …)  REF: 27006 Annex B3.4.g | **Please select** |  | High availability requirements e.g. 24/7 services.  Several DR sites;  Several Data Centers; | Medium or High availability requirements and no or one alternative DR site. | Low availability requirements and no or one alternative DR site. |
| 16 | Only for surveillance or re-certification audit and only in case of changes of the organization or the Scope:  Is the extent of changes relevant to the ISMS in accordance with notices of changes by the certified client?  (ISO/IEC 17021-1, 8.5.3?)  REF: 27006 Annex B3.4.h | **Please select** |  | Mayor changes in scope or SoA of ISMS, e.g. new processes, new business units, areas, risk assessment management methodology, policies, documentation, risk treatment.  Major changes in the factors above. (B.3.4 a – B.3.4 g) | Minor changes in scope or SoA of ISMS, e.g. some policies, documents, etc.  Minor changed in the factors above (B.3.4.a – B.3.4g) | No changes since last re-certification audit. |

**Additional second level factors for adjustment of additional audit time**

Please change the default specification if you have a different situation in your organization!

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **CF ID** | **Complexity  factor (CF)** | **Reference ISO 27006 or ISO 27001 („Why?“)** | **Customer data** | **Customer specifications** | **CF Very High** | **CF High** | **CF Medium (default)** |
| 17 | What is the complexity of the organization’s network and encryption technology?  REF: 27006 Annex B3.4 | * ISO 27006:2015, Annex B 3.4 Second level factor for additional audit time | **Medium** |  | High modernized network and encryption standards conform to several public standards and requirements (e.g. ETSI standard …). | External / Internet connection with encryption / digital signature / PKI requirements. | External / Internet connection with use of encryption in built-in standard facilities without digital signature / PKI requirements. |
| 18 | Complicated logistics involving more than one building or location on the Scope of the ISMS.  REF: 27006 Annex B3.4 | * ISO 27006:2015, Annex B 3.4 Second level factor for additional audit time | **Medium** |  | Complicated logistics involving several buildings or locations in the scope of the ISMS. | More complex, but easy manageable logistics involving only few buildings. | Simple logistics involving not more than one building. |
| 19 | Staff speaking more than one language or documentation provided in more than one language.  REF: 27006 Annex B3.4 | * ISO 27006:2015, Annex B 3.4 Second level factor for additional audit time. | **Medium** |  | The organisation’s staff is speaking the national language only and/or documents are not provided in English or German. An Interpreter is needed and/or the auditors are not able to work independently. | Organisation’s staff and/or documents are partly in its national language, but also in English or German. | Organisation’s staff and documents are consistently in English or German. No interpreters needed and auditors are able to work independently. |
| 20 | Activities that require visiting temporary or unmanned sites to confirm the activities of the permanent sites whose MS is subject to certification.  REF: 27006 Annex B3.4 | * ISO 27006:2015, Annex B 3.4 Second level factor for additional audit time. | **Medium** |  | It is necessary to visit 5 or more temporary or unmanned sites to confirm activities of permanent sites. | The auditor team requires visiting at least 2 temporary or unmanned sites, but not more than 4. | There is no or only one temporary or unmanned location to visit to confirm the activities of a site. |
| 21 | High number of standards and regulations that apply to the ISMS.  REF: 27006 Annex B3.4 | * ISO 27006:2015, Annex B 3.4 Second level factor for additional audit time. | **Medium** |  | More than 3 standards or regulations apply to the ISMS. | There are up to 2 standards or regulations which apply to the management system. | A Maximum of 1 standard or regulation applies to the ISMS. |

**Additional second level factors for adjustment of less audit time**

Please change the default specification if you have a different situation in your organization!

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **CF ID** | **Complexity  factor (CF)** | **Reference ISO 27006 or ISO 27001 („Why?“)** | **Customer data** | **Customer specifications** | **CF Medium (default)** | **CF Low** | **CF Very Low** |
| 22 | No/Low risk product/processes.  REF: 27006 Annex B3.4 | * ISO 27006:2015, Annex B 3.4 Second level factor for less audit time. | **Medium** |  | No products or processes with low or no risks are in the scope of the management System. | There is exactly 1 process or product which contains no or low risks. | 2 or more no/low risk processes or products apply to the ISMS. |
| 23 | Processes involving a single general activity (e.g. service only).  REF: 27006 Annex B3.4 | * ISO 27006:2015, Annex B 3.4 Second level factor for less audit time. | **Medium** |  | There are no processes which contain only one single activity. | There are exactly 2 processes which depend on single activities. | There are 3 or more processes which can be determined as such with only one single general activity. |
| 24 | High percentage of persons doing work under the organization’s control performing the same tasks.  REF: 27006 Annex B3.4 | * ISO 27006:2015, Annex B 3.4 Second level factor for less audit time. | **Medium** |  | Less than 30% of the staff is performing similar or identical tasks in relation to the total number of persons in scope. | At least 30% of the staff is performing identical tasks. | More than 70% of the whole staff of all persons in scope is doing the same tasks. |
| 25 | Prior knowledge of the organization (e.g. organization has already been certified to another standard by the certification body).  REF: 27006 Annex B3.4 | * ISO 27006:2015, Annex B 3.4 Second level factor for less audit time. | **Medium** |  | There are no other standards which have been certified by the same certification body. | There is one other standard which has been certified by the certification body and moderate knowledge of the organisation exists. | There are 2 or more standards which have been successfully certified by the same certification body and a prior knowledge of the organisation exists. |
| 26 | High client preparedness for certification (e.g. already certified or recognized by another 3rd party scheme).  REF: 27006 Annex B3.4 | * ISO 27006:2015, Annex B 3.4 Second level factor for less audit time. | **Medium** |  | The organisation has no certification from any other 3rd party scheme and is not especially prepared for audit. | The organisation has been certified by a third party scheme and its certification lasts at least 3 years. | The organisation has been certified by a third party scheme and its certification lasts at least 6 years. |
| 27 | High maturity of the management system in place.  REF: 27006 Annex B3.4 | * ISO 27006:2015, Annex B 3.4 Second level factor for less audit time. | **Medium** |  | The organisation has no implemented management systems which are not certified. | A not certified management system is established at least 2 years in the organisation and can be proved by evidence. | A not certified management system is established at least 6 years in the organisation and can be proved by evidence. |

**Additional requirements**

| **CF ID** | **Complexity  factor (CF)** | **Customer data** | **Customer specifications** |
| --- | --- | --- | --- |
| 28 | Is an additional confirmation needed for special interested parties?  (Ex.: TR 3109-6 BSI Erklärung, De-Mail) | **Yes or No?**  **Please select** | **Explanation in case of “Yes”** |