|  |
| --- |
| **By fax to: +xxx (xxx)xxx xxxx, or by e-mail to: xxx.xxx@xx.tuv.com** |
| **[Local Office]** |

|  |
| --- |
| **Registered office (head office)** |
| **Company name** |  |
| **Address** |  |
| **Postal code, city** |  |
| **Managing director**Last name, first name |  |

|  |
| --- |
| **Primary contact** |
| **Last name, first name** |  |
| **Position** |  | **Phone** |  |
| **E-mail** |  | **Fax** |  |
| **Website:** |  |

|  |
| --- |
| **Responsible contact person** **IT security or information security officer** |
| **Last name, first name** |  |
| **Position** |  | **Phone** |  |
| **E-mail** |  | **Fax** |  |

|  |
| --- |
| **Please mark required standards** (please add standard if not listed) |
| **[ ]**  | **ISO/IEC 27001** | **[ ]**  | **ISO 22301** | **[ ]**  |  |
| **[ ]**  | **ISO/IEC 27001 + ISO/IEC 27017** | **[ ]**  | **ISO/IEC 20000-1** | **[ ]**  |  |
| **[ ]**  | **ISO/IEC 27001 + ISO/IEC 27017 + ISO/IEC 27018** | **[ ]**  | **Other: (please specify)** | **[ ]**  | **Other: (please specify)** |

|  |
| --- |
| **Type of Company** (please send the respective proof) |
| **[ ]**  | **Sole Proprietorship** |
| **[ ]**  | **Limited liability company** |
| **[ ]**  | **Partnership** |
| **[ ]**  | **Others (please specify)** |

|  |
| --- |
| **Multi-site certification within the group with legally independent companies** |
| Certification requirements for multi-site procedures are specified in ISO 17021, IAF MD 1 and in the OFFICIAL NOTICE on the inadmissibility of "matrix certifications" of the Deutsche Akkreditie-rungsstelle GmbH (DAkkS).According to the information in the official notification of the DAkkS, an organisation with several legal entities has to prove the eligibility for a multi-site certification by proving the access rights of the contracting party (certificate holder) to one of the possibilities mentioned in the following table. Please enter the name(s) of the legal entity(ies) in the table on the following page and tick the respective applicable characteristic.Please include the relevant evidence (official certificates, documents, certified by a notary public if necessary, signed by the company management in the case of internal documents) together with this questionnaire.**Please note that any site intended to be included within the multi-site must meet one of the 3 criteria noted in the table** **Please contact us if you have any questions. Thank you** |

|  |  |
| --- | --- |
|  | **Multi-site certification** **with legally independent companies** |
|  |  | **or** | **or** |
|  | **Has an interest equal to the majority of the voting rights** | **is a shareholder with an arbitrary share and has the right to appoint or dismiss the executive bodies of the company**  | **due to a concluded control agreement, profit transfer agreement** |
|  | The status of 'sister company' within the same group does not in itself meet any of the above conditions with respect to other affiliates |
| **Location Name and address** |  |
|  | **[ ]**  | **[ ]**  | **[ ]**  |
|  | **[ ]**  | **[ ]**  | **[ ]**  |
|  | **[ ]**  | **[ ]**  | **[ ]**  |
|  | **[ ]**  | **[ ]**  | **[ ]**  |
|  | **[ ]**  | **[ ]**  | **[ ]**  |
|  | **[ ]**  | **[ ]**  | **[ ]**  |
|  | **[ ]**  | **[ ]**  | **[ ]**  |
|  | **[ ]**  | **[ ]**  | **[ ]**  |
|  | **[ ]**  | **[ ]**  | **[ ]**  |
|  | **[ ]**  | **[ ]**  | **[ ]**  |
|  | **[ ]**  | **[ ]**  | **[ ]**  |

|  |
| --- |
| **Questions for combined audits only** (e.g. ISO 27001 + ISO 20000-1) |
| Combined audits may only be carried out simultaneously if the following aspects of the combined standards (e.g., ISO 27001 + ISO 20000-1) are integrated and/or their implementation is combined:  |
| Management review covering the entire organizational planning and strategy: | **[ ]**  |
| An integrated approach to internal audits: | **[ ]**  |
| An integrated approach to policy and objectives: | **[ ]**  |
| An integrated approach for the system processes: | **[ ]**  |
| The highest possible integrated system documentation including work instructions: | **[ ]**  |
| An integrated approach for improvement: | **[ ]**  |
| An integrated approach for planning, including risk management measures: | **[ ]**  |
| Unified occupational status (system officer) and responsibilities: | **[ ]**  |

|  |
| --- |
| **With which standard(s) should the audit be combined?**Please list the relevant standards. |
|  |

|  |
| --- |
| **What is the required scope (wording) of the certificate?**Please provide a brief description of the company's purpose and primary fields of activity (products and services) |
|  |
| (E.g., manufacture and sale of XXX products, as well as assembly and consultancy services in the field of YYY) |

|  |  |  |
| --- | --- | --- |
| **Is your company responsible for Design?** | **[ ]** yes | **[ ]** no |
| **Did your company receive consultancy (or in-house training) to provide support for the development or implementation of the management system?** | **[ ]** yes | **[ ]** no |
| If yes, please name the consultant/consultancy/Company that has provided the in-house training. |  |
| **Are there outsourced processes (e.g., purchasing, sales, manufacturing processes)?** | **[ ]** yes | **[ ]** no |
| **If yes, which ones?** |  |

|  |
| --- |
| **Are there any information security relevant operational records that should not be viewed during the audit? If so, please specify:** |
| **Record name (if there is not enough space, please use back or additional sheet)** |  |

|  |  |
| --- | --- |
| **Number of employees in total:** |  |
|  | **ISO/IEC 27001** | **ISO/IEC 20000-1** | **ISO 22301** | **Other standard (please specify)** |
| **Total number of employees within the scope of the requested standard:** |  |  |  |  |

|  |  |
| --- | --- |
| **Desired audit date Stage1 and Stage2 (KW):** |  |
| **Date and signature for the correctness of the information** |  |
| **Reviewed by TÜV Rheinland employees** |  |
| **Spoken to (name of the customer)** |  |
| **The following information is necessary to make a reliable calculation for an ISO/IEC 27001-certification.** |
|  | Category |
| Low | normal | High |
| **Complexity of the ISMS**1. Information security requirements (confidentiality, Integrity, and availability) 2. Quantity of critical assets3. Quantity of processes and services | 1. Only little sensitive or confidential information, low availability requirements2. Few critical assets (in terms of confidentiality, Integrity, and availability) 3. Only one key-business-process with few interfaces and few business units involved | 1. Higher availability requirements or some sensitive/confidential information2. Some critical assets3. 2 – 3 simple business processes with few interfaces and few business units involved | 1. Higher amount of sensitive or confidential information (e.g., health, personal identifiable information, insurance, banking) or high availability requirements 2. Many critical assets3. More than 2 complex processes with many interfaces and business units involved |
| **Type(s) of business performed within scope of the ISMS** | - Low risk business without regulatory requirements | - High regulatory requirements | - High risk business with (only) limited regulatory requirements |
| **Previously demonstrated performance of the ISMS** | - Recently certified - Not certified but ISMS fully implemented over several audit and improvement cycles, including documented internal audits, management reviews and effective continual improvement system | - Recent surveillance audit- Not certified part partially implemented ISMS: Some management system tools are available and implemented; some continual improvement processes are in place but partially documented | - 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) |
| **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)** | - Highly standardized environment with low diversity (few IT-platforms, servers, operating systems, databases, networks, etc.) | - Standardized but diverse IT platforms, servers, operating systems, databases, networks | - High diversity or complexity of IT (e.g., many different segments of networks, types of servers or databases, number of key applications) |
| **Extent of outsourcing and third-party arrangements used within the scope of the ISMS** | - no outsourcing and little dependency on suppliers, or- Well-defined, managed and monitored outsourcing arrangements- Outsourcer has a ISO 27001-certificate'- Relevant independent assurance reports are available | - Several partly managed outsourcing arrangements | - 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 |
| **Extent of information system development** | - No in-house system development- Use of standardized software platforms | - Use of standardized software platforms with complex configuration/parameterization- (Highly) customized software- Some development activities (in-house or outsourced) | - Extensive internal software development activities with several ongoing projects for important business purpose |

|  | Category |
| --- | --- |
| Low | normal | High |
| **Quantity of sites and quantity of Disaster Recovery (DR) sites** | - Low availability requirements and no or one alternative DR site | - Medium or High availability requirements and no or one alternative DR sites | - High availability requirements e.g., 24/7 services- several alternative DR sites- several Data Centers |
| **For surveillance or re-certification audit: The amount and extent of change relevant to the ISMS in accordance with ISO/IEC 17021-1; 8.5.3** | - No changes since last re-certification audit | - Minor changes in scope or SoA of ISMS, e.g., some policies, documents, etc.- Minor changes in the factors above | - Major 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 |

|  |
| --- |
| **Do you exclude any standard chapters or controls (e.g., from Annex A of ISO/IEC 27001) due to non-applicability?** |
| **Control designations (if there is not enough space, please use back or additional sheet)** |  |

|  |
| --- |
| **The following information is necessary to make a reliable calculation for an ISO/IEC 20000-1 and/or ISO 22301 certification.** |
|  | Category |
| Low | Normal | High |
| Complexity of business processes, activities and logistics that take place within the scope of the management system. | - few sensitive or confidential information, only a low availability requirement- a few critical assets (in terms of confidentiality, integrity, availability)- only one main business process with few interfaces and few connected business units | - higher demands on the availability or on the sensitivity or confidentiality of the information- some critical assets (in terms of confidentiality, integrity, availability)- two to three main business processes with few interfaces and few connected business units | - high demands on the sensitivity and confidentiality of information (e.g. patient data, bank data, insurance data, etc.) or on the availability- many critical assets (in terms of confidentiality, integrity, availability)- more than two main business processes with many interfaces and connected company departments |
| Degree of dependence on other parties, such as suppliers, internal groups or customers, who act as suppliers and are involved in the provision/provision of services. | - no outsourcing and only few suppliers- Well defined, managed and monitored outsourcing/supplier SLA's- Suppliers have a relevant ISO certificate- relevant independent evidence is available | - There are several managed outsourcing/supplier SLA's | - High dependence on outsourced services or suppliers, which has a high impact on the business model- The number or scope of the outsourced processes is not known- several unmanaged outsourcing/supplier SLA's |
| Degree of legal and regulatory requirements affecting the management system. (e.g. multi-jurisdiction, intellectual property rights, data protection, food, pharmaceuticals, aerospace, nuclear power) | - Business model with few legal risks or regulations | - High legal requirements and regulations for the business model(e.g., medical services/products) | - Risky business model with high legal requirements and regulations for the business model(e.g., investment banks with a high number of regulations to be complied with...) |
| Number of changes to the management system and services. | - No changes have been made since the last audit | - Slight changes were made to the scope (e.g., documents were added or changed...)- This is an initial certification (ISO/IEC 20000-1, ISO 22301) | - There have been far-reaching changes in scope (e.g., new processes, new business areas, risk analysis has changed, risk treatment has changed, etc.) |
| Degree of diversity of activities carried out in different shifts and/or temporary locations. | No differences in the activities of the different shifts and/or sites | Only few differences in the activities of the different shifts and/or sites | Large differences in the activities of the different shifts and/or locations |
| Complexity of language differences between different sites, e.g., staff speaks more than one language (requires translator or blocks individual auditors from working independently). | No language differences within the scope | Only few, manageable language differences within the scope (no translator required) | Large language differences within the scope (translator is required) |

|  |  |
| --- | --- |
| **Are there special legal requirements for your company?** **If yes, which ones?** |  |

**Questions in case of multiple sites:**

|  |
| --- |
| **Sites** |
| **Number of physical sites to be certified in total** (Please fill in page X for each location) |  |
| **Number of virtual sites (e.g., permanent project groups that are not assigned to a physical location) to be certified in total** (Please fill in page X for each location) |  |
| **Please describe the type of virtual locations:** |  |

|  |
| --- |
| **Multi-site certification is only possible if the following points apply** (Please confirm by clicking) |
| **[ ]**  | A centrally controlled management system | **[ ]**  | Centralized (legal, contractual, regulatory) cut-through clause into all sites |
| **[ ]**  | A centralized management system representative | **[ ]**  | A centralized assessment of all internal audits |
| **[ ]**  | Similar products/processes/services at all Sites or consecutive products/processes/services at all Sites  |

**Please fill in theses information separately for each site** (duplicate per each site)**.**

|  |
| --- |
| **Registered office** |
| **Company name** |  |
| **Address** |  |
| **Postal code, city** |  |

|  |
| --- |
| **Type of site** |
| **Head office** (e.g.: Top-Management, HR, Administration …) | **[ ]**  |
| **Service or supporting site** (e.g., Administration, Research, Logistic, Purchasing, Sales…) | **[ ]**  |
| **Virtual site** | **[ ]**  |
| **Main processes at this site** (please give a short description) |  |
| **Are the following functions also performed at this location?** (Please mark as appropriate) |
| (Information is necessary to make decisions about possible reductions/increases) | Yes, also for other sites | Yes, only for this site | No |
| The following processes are being audited at another location: |  |  |  |
|  | Information security policy | **[ ]**  | **[ ]**  | **[ ]**  |
|  | Information security management system planning | **[ ]**  | **[ ]**  | **[ ]**  |
|  | Organizational roles, Responsibility, and authorities | **[ ]**  | **[ ]**  | **[ ]**  |
| Document management | **[ ]**  | **[ ]**  | **[ ]**  |
| Personnel management | **[ ]**  | **[ ]**  | **[ ]**  |
| Procurement | **[ ]**  | **[ ]**  | **[ ]**  |
| Risk management | **[ ]**  | **[ ]**  | **[ ]**  |
| Development activities | **[ ]**  | **[ ]**  | **[ ]**  |
|  | **Low** | **Mid** | **High** |
| Relevance and risk of the site for the management system | **[ ]** (e.g., sales office) | **[ ]**  | **[ ]** (e.g., data center location) |
| Justification (in case of "Low" or "High”): |  |

|  |  |  |
| --- | --- | --- |
| **Existing system certifications at the location** | **Certification body** | **Valid until**  |
| **[ ]  ISO 9001** |  |  |
| **[ ]  ISO 14001** |  |  |
| **[ ]  IATF 16949** |  |  |
| **[ ]  ISO/IEC 27001** |  |  |
| **[ ]  ISO/IEC 20000-1** |  |  |
| **[ ]  ISO 22301** |  |  |
| **[ ]  ISO 45001** |  |  |
| **[ ]**  |  |  |
| Please attach copies of current certificates. |

|  |  |
| --- | --- |
| **Total number of employees at the site** |  |
| **Of which in the scope (information required):** |
|  | ISO/IEC 27001 | ISO/IEC 20000-1 | ISO 22301 | Other standard (please specify) |
| Full-Time (100%) |  |  |  |  |
| Half-Time (50%) |  |  |  |  |
| Less than half time (25% or less) |  |  |  |  |

|  |
| --- |
| **Do you have shift work? If yes, please indicate:** |
| **Number of shifts** |  |
| **If applicable, times of the shift change** |  |