|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Client: |  | | | |  |
| Lead Auditor: | -/- | | | Certificate no.: | -/- |
| Auditor (Expert): | -/- | | | |  |
| Audit Representative: |  | | | Audit Date: | -/- |
| Certification Audit | | 1. Surveillance Audit | 2. Surveillance Audit | | Recertification Audit |
| Pre Audit | | Post implementation Audit | Extension Audit | |  |
| EN ISO 9001 | | ISO 14001 | OHSAS 18001 | | ISO/IEC 27001:2013 |
| IT security catalogue according to §11 paragraph 1a EnWG on the basis of ISO/IEC 27006 | | | | | |
| Economic sector: | |  | Effective no. of employees: | |  |
| Scope: | | see ODS | see certificates text  no changes | | |

**INFORMATION ABOUT THE COMPANY**

|  |  |  |  |
| --- | --- | --- | --- |
| Address |  | | |
| Phone |  | Fax |  |
| Web |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Function | General Management | | |
| Name |  | | |
| Phone |  | Fax |  |
| e-Mail |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Function | MS-Officer | | |
| Name |  | | |
| Phone |  | Fax |  |
| e-Mail |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Function | Responsible person for offer negotiation | | |
| Name |  | | |
| Phone |  | Fax |  |
| e-Mail |  | | |

##### **Employees**

|  |  |  |  |
| --- | --- | --- | --- |
| Total Number of employees |  | | |
| Number of shifts |  | Employees/Shift |  |
| Effective number of employees |  | | |
| Employees within ISMS Scope |  | | |

##### **Sites**

|  |  |
| --- | --- |
| Number of permanently occupied locations  (Locations staffed at least on regular working days) |  |
| Addresses of permanently occupied locations |  |
|  |
|  |
|  |
| Number of permanently unoccupied locations |  |
| Please summarize by appropriate grouping. When forming groups, the relevance of the locations for the overall network as well as the possibility of remote impact via ICT on this location must be taken into account. | |
| Number of groups |  |
| Name of the formed groups |  |
|  |
|  |
|  |

# **Products / Services/ Businesses**

|  |
| --- |
|  |

## expected scope of certification / certificate text

|  |
| --- |
|  |

## External consultant

|  |  |  |  |
| --- | --- | --- | --- |
| Name |  | | |
| Company |  | | |
| Address |  | | |
| Phone |  | Fax |  |
| e-Mail |  | | |
| Web |  | | |

|  |  |
| --- | --- |
| Notes: |  |
|  | |

## information on it infrastructure, competence of it representatives, specific risks RELATED TO DATA PROTECTION PRIVACY, SPECIFIC CLAIMS DUE TO LEGAL AND REGULATORY REQUIREMENTS.

|  |
| --- |
| Assets in the scope of the ISMS are the information processed in the processes of the AIM. In addition, the use of IT services is within the scope.  Number of server systems:  Operating systems of the server:  Number of clients:  Operating systems of the clients:  Used databases:  Used software products:  IT / DC locations:  Service provider for the IT operation:  Additional: |

**Calculation of complexity**

Please mark the applicable category recognizably.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Low** | **Medium** | **High** |
| **Complexity of the ISMS:** | • 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 | • Higher availability requirements  or some sensitive / confidential  information  • Some critical assets  • 2–3 simple business processes  with few interfaces and few business units involved. | • Higher amount of sensitive or confidential  information (e.g. health,  personally identifiable information,  insurance, banking) or high availability  requirements  • Many critical assets  • More than 2 complex processes  with many interfaces and business units involved. |
| **The 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 but 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** | • 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 certified ISMS  • 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 |
| **Number of sites and number 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 site | • 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** | • 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 |

# **Does your company have ISMS-related information that you cannot make available to the team of auditors, e.g. due to confidentiality?**

No

Yes

# If yes, please describe what information is involved and give a reason.

|  |
| --- |
|  |

**To be filled in for multiple locations:**

Ensure and consider the following points for sampling at multiple sites:

|  |  |  |
| --- | --- | --- |
| Fulfilled | Yes | No |
| All sites are subject to the same ISMS, which is centrally managed and audited |  |  |
| All sites are part of the internal ISMS audit program |  |  |
| All locations ae included in the client's ISMS Management Review Program |  |  |
| The group formation is plausible |  |  |
| Results of the internal audits at all locations |  |  |
| Results of the management review |  |  |
| Size of the locations |  |  |
| Different business purposes of the sites |  |  |
| Complexity of the ISMS at the sites |  |  |
| Different performance of work |  |  |
| Different performance of activities |  |  |
| Different interpretation and implementation of controls |  |  |
| Interacting with critical information systems or processing sensitive information systems with sensitive information |  |  |
| Deviating legal requirements |  |  |
| Geographical and cultural aspects |  |  |
| Risk situation of the locations |  |  |
| Information security incidents at the sites |  |  |

**FOR THE ACCURACY OF THE INFORMATION**

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Name |  | Date |