|  |  |  |  |
| --- | --- | --- | --- |
|  | **Factors** | **Situation** | |
| a1) | Complexity of the ISMS: • Information security requirements [confidentiality,integrity and availability, (CIA)] | |  |  | | --- | --- | | Only little sensitive or confidential information, low availability requirements |  | | Higher availability requirements or some sensitive / confidential information |  | | Higher amount of sensitive or confidential information (e.g. health, personally identifiable information, insurance, banking) or high availability requirements |  | | |
| a2) | • number of critical assets | |  |  | | --- | --- | | Few critical assets (in terms of CIA) |  | | Some critical assets |  | | Many critical assets |  | | |
| a3) | • number of processes and services | |  |  | | --- | --- | | Only one key business process with few interfaces and few business units involved |  | | 2–3 simple business processes with few interfaces and few business units involved |  | | More than 2 complex processes with many interfaces and business units involved |  | | |
| b) | 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 |  | | |
| c) | Previously demonstrated performance of the ISMS | |  |  | | --- | --- | | Recently certified |  | | Recent surveillance audit |  | | No certification and no recent audits |  | | Not certified but ISMS fully implemented over several audit and improvement cycles, including documented internal audits, management reviews and effective continual improvement system |  | | 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 new and not fully established (e.g. lack of management system specific control mechanisms, immature continual improvement processes, ad hoc process execution) |  | | |
| d) | 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 |  | | Several partly managed outsourcing arrangements |  | | |
| e) | Extent of outsourcing and third party arrangements used within the scope of the ISMS | |  |  | | --- | --- | | No outsourcing and little dependency on suppliers |  | | Several partly managed outsourcing arrangements |  | | Well-defined, managed and monitored outsourcing arrangements |  | | Unknown amount or extent of outsourcing |  | | Outsourcer has a certified ISMS |  | | Several unmanaged outsourcing arrangements |  | | Relevant independent assurance reports are available |  | | |
| f) | Extent of information system development | |  |  | | --- | --- | | No in-house system development |  | | Use of standardized software platforms with complex configuration/ parameterization |  | | Extensive internal software development activities with several ongoing projects for important business purpose |  | | Use of standardized software platforms |  | | (Highly) customized software |  | | Some development activities (in-house or outsourced) |  | | |
| g) | 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 |  | | |
| h) | 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. |  | | Major changes in scope or SoA of ISMS, e.g. new processes, new business units, areas, risk assessment management methodology, policies, documentation, risk treatment |  | | Minor changes in the factors above |  | | Major changes in the factors above |  | | |
| i) | Are there any ISMS related information (such as ISMS records or information about design and effectiveness of controls) that cannot be made available for review by the audit team because it contains confidential or sensitive information?  InterCert will determine whether the ISMS can be adequately audited in the absence of such information. If InterCert concludes that it is not possible to adequately audit the ISMS without reviewing the identified confidential or sensitive information, it will advise the client that the certification audit cannot take place until appropriate access arrangements are granted. | Yes |  |
| No |  |
|  | **NOTES** | text | |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Località e Data |  | Timbro e firma del legale rappresentante |