|  |  |
| --- | --- |
| **Registered name:** |       |

|  |
| --- |
| **REFERENCES STANDARDS** |
| **[ ]  ISO/IEC 27001** | **[ ]  ISO/IEC 27017** | **[ ]  ISO/IEC 27018** | **[ ]**       |
| **Datacenter where the servers that manage the service are located / Sites where critical assets are located****for the purpose of certification of the processes managed.** |
|  | **Name / Provider** | **Address** | **Activities** | **Certification**(ISO/IEC 27001-27017-27018, ANSI/TIA942, ecc.) |
|  |       |       |       |  |
|  |       |       |       |  |
|  |       |       |       |  |
|  |       |       |       |  |
|  |       |       |       |  |
| Note:  |

|  |
| --- |
| **With reference to the required scope of certification, please put an X to make a choice for the following factors.****Only one choice for each factor is required.** |
| **FACTORS RELATED TO BUSINESS AND ORGANIZATION** | **Answer****X** |
| ***Factor 1: type(s) of business and regulatory requirements.*** |
| **1** | Organization works in non-critical business sectors (low risk business sector) and non-regulated. Only little sensitive or confidential information.(Critical business sectors are sectors that may affect critical public services that will cause risk to health, security, economy, image and government ability to function that may have a very large negative impact to the country: e.g. nuclear sector, chemical and pharmaceutical sector, electrical, gas and water sector, telecoms sector, transport and logistic sector, aerospace sector, railway sector, banking, finance, assurance sector, public administration sector, healthcare sector). |       |
| **2** | Organization works in non-critical business sectors (low risk business sector) with high (specific) regulatory requirements. Sensitive or confidential information. |       |
| **3** | Organization works in critical business sectors (high risk business sector). Higher amount of sensitive or confidential information.  |       |
| ***Factor 2: complexity of the ISMS - processes and tasks.*** |
| **1** | Few critical assets (in terms of confidentiality, integrity, availability). Only one key business process with few interfaces and business units involved. |       |
| **2** | Some critical assets (in terms of confidentiality, integrity, availability). Some key complex processes (2 or 3) with few interfaces and business units involved. |       |
| **3** | Many critical assets (in terms of confidentiality, integrity, availability). More than 3 key complex processes with many interfaces and business units involved. |       |
| ***Factor 3: Level of establishment of the MS.*** |
| **1** | ISMS fully implemented over several years. Internal audits, management reviews and effective continual improvement activities well established. |       |
| **2** | ISMS fully implemented ISMS over some months. Internal audits, management reviews and effective continual improvement activities carried out once. |       |
| **3** | No other management system implemented at all, the ISMS is new and not completely established.(e.g. lack of management system specific control mechanisms implemented, immature continual improvement processes, ad hoc process execution. Limited number of records) |       |

|  |  |
| --- | --- |
| **FACTORS RELATED TO IT ENVIRONMENT** | **Answer****X** |
| ***Factor 4: IT infrastructure complexity.*** |
| **1** | Few and/or highly standardized IT platforms, servers, operating systems, databases, networks, etc. |       |
| **2** | Several and/or different IT platforms, servers, operating systems, databases, networks |       |
| **3** | Few and/or highly standardized IT platforms, servers, operating systems, databases, networks, etc. |       |
| ***Factor 5: Dependency on outsourcing and suppliers, including cloud services.*** |
| **1** | Little or no dependency on outsourcing or critical suppliers. |       |
| **2** | Some dependency on outsourcing or suppliers, related to some but not all important business activities. |       |
| **3** | High dependency on outsourcing or suppliers, large impact on important business activities. |       |
| ***Factor 6: Information System development.*** |
| **1** | None or a very limited in-house systems/applications development. Use of standardized software platforms. |       |
| **2** | Some in-house or outsourced systems/applications development for some important business purposes. Use of standardized software platforms with complex configuration/parameterization. |       |
| **3** | Extensive in-house or outsourced systems/applications development for important business purposes. |       |
|  |
| **OTHER FACTORS** | **Risposta X** |
| **Factor 7**: Complicated logistics involving more than one location (e.g. different data centers, different disaster recovery sites, operational sites, temporary sites etc.). |       |
| **Factor 8**: Staff speaking different languages and documentation provided in more than languages (interpreter required or preventing individual auditors from working independently etc.). |       |
| **Factor 9**: Activities that require visiting temporary sites to confirm the activities of the permanent sites(s) whose management system is subject to certification. |       |
| **Factor 10**: High number of standards and regulations that apply to the ISMS. |       |
| **Factor 11**: Low risk processes or involving a single general activity (e.g. one simple service). |       |
| **Factor 12**: High percentage of persons in the scope of the management system performing the same tasks. |       |
| **Factor 13**: High percentage of persons in the scope of the management system with registered competencies in the field of information security management (e.g. professional certifications). |       |
| **Factor 14**: Renewal of the certification and a high maturity of the management system (any non conformity in the last three years). |       |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** |       | **Signature:** |       |