This applies only to Organizations / Companies which apply for certification to ISO/IEC 27001 and/or ISO/IECE 27701 Standard.

Please fill-in the following information. **For sections 1 to 7 check the description (a, b or c) which best describes your organization. In case of multiple sites, which have significant differences between them, please fill in a separate Annex D form for each different site.**

**Keep in mind that for ISO/IEC 27701 you must have a valid / active ISO 27001 certificate and if not, you have to apply for both standards.**

**The application is for:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ISO/IEC 27001  (skip to page two (2)) | ... | Combined ISO/IEC 27001&27701 | ... | ISO/IEC 277011),2) | ... |

**1)In this case**

|  |  |  |  |
| --- | --- | --- | --- |
| You have an active / valid ISO/IEC 27001 certificate issued by Q-CERT | ... | You have an active / valid ISO/IEC 27001 certificate issued by another accredited CB | ... |

**For ISO/IEC 27701:**

**a) You act as a (for guidance see attached F-2108 ANNEX C) :**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Processor | ... | Controller | ... | Processor & Controller | ... |

**b) Activity scope if different from ISO/IEC 27001 (must be within the boundaries of ISO/IEC 27001 scope)**

|  |
| --- |
| Describe: |

**c) Number of sites if less from those stated for ISO/IEC 27001 (location(s) / address(es) / building(s)):**

|  |
| --- |
| Describe: |

**d) The extent to which the main activity of the Organization requires PII processing:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rarely | ... | Occasionally | ... | Systematically | ... |

**e) The extent to which the main activity of the Organization entails the processing of sensitive PII:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rarely | ... | Occasionally | ... | Systematically | ... |

**f) Percentage of distinct business processes which entail PII processing:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| < 30% | ... | 30-70% | ... | >70% | ... |

**g) PII data are transferred / “exported” to other Organizations that operate under a different PII Legal Framework:**

|  |  |  |  |
| --- | --- | --- | --- |
| Yes | ... | No | ... |

|  |  |
| --- | --- |
| **h) ISO/IEC 27001 Last audit date(s) (if applicable):** |  |

**2)Important Note:**

If applying for ISO/IEC 27701 and you are certified for ISO/IEC 27001 by another CB, you must also complete the rest of the questionnaire of this ANNEX.

|  |  |  |
| --- | --- | --- |
| Factors related to business and organization (other than IT)  *(Required information for both standards)* | | |
| 1. Complexity of the ISMS (e.g. criticality of information, risk situation of the ISMS, etc.) | | Check |
| a) | 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 | ... |
| b) | Higher availability requirements or some sensitive / confidential information  Some critical assets  2-3 simple business processes with few interfaces and few business units involved | ... |
| c) | 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 | ... |
| 1. The type(s) of business performed within scope of the ISMS | | |
| a) | Low risk business without regulatory requirements | ... |
| b) | High regulatory requirements | ... |
| c) | High risk business with (only) limited regulatory requirements | ... |
| Factors related to IT environment | | |
| 1. 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) | | |
| a) | Highly standardized environment with low diversity (few IT platforms, servers, operating systems, databases, networks, etc.) | ... |
| b) | Standardized but diverse IT platforms, servers, operating systems, databases, networks | ... |
| c) | High diversity or complexity of IT (e.g. many different segments of networks, types of servers or databases, number of key applications) | ... |
| 1. Extent of outsourcing and third party arrangements used within the scope of the ISMS | | |
| a) | 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 | ... |
| b) | Several partly managed outsourcing arrangements | ... |
| c) | 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 | ... |
| 1. Extent of information system development | | |
| a) | No in-house system development  Use of standardized software platforms | ... |
| b) | Use of standardized software plat- forms with complex configuration / parameterization  (Highly) customized software  Some development activities (in-house or outsourced) | ... |
| c) | Extensive internal software development activities with several ongoing projects for important business purpose | ... |
| Multi-site Information | | |
| 1. Number of sites and number of Disaster Recovery (DR) sites | | |
| a) | Low availability requirements and no or one alternative DR site | ... |
| b) | Medium or High availability requirements and no or one alternative DR site | ... |
| c) | High availability requirements e.g. 24/7 services  Several alternative DR sites  Several Data Centers | ... |
| Other | | |
| 1. Document other significant information / particularities which might affect the Certification | | |
| ... | | |

Instructions:

* This form is always to be send along with Organization Profile (F-2503 form)