



Certification Application

Scoping Questionnaire

Esqb_lac

Please complete this questionnaire as accurately as possible as it forms the basis for the time allocated to each stage of the certification audit.

This questionnaire must be completed/provided by an authorized representative of the organization seeking to be certified. Completion of this questionnaire prior to engaging with a certification body is a requirement of ISO/IEC 17021-1:2015.

Starting page 7, there are included additional questionnaire for ISO 27701, ISO 22301, ISO 9001 and ISO 14001 certifications as well as for Kanta Certification. In case you are not pursuing these certifications, the questions can be left open and unanswered.

If unsure, please reach out to our contacts who can provide illustrative examples for assistance:

Primary point of contact:

KPMG IT Certification sertifiointi@kpmg.fi

ISO Certifications:

Kaleva Piha

ISO Certification Services Lead

kaleva.piha@kpmg.fi

+358 50 439 8255

Kanta Certifications & Findata security audit:

Lauri Kaipainen

Cyber Security Services

lauri.kaipainen@kpmg.fi

+358 20 767 2412

AmI_r_arBcr_gjq

☐ New certification

☐ Change to existing certification, certification number:

1.1 Name of organization to be certified (legal entity), including Company ID or similar

1.2 Primary address (incl. country) of the entity to be certified

1.3 Name and contact details of primary contact for certification

Name:

Position:

Email:

Phone:

1.4 Billing address

1.5 Other related entities (e.g. subsidiaries in scope)

2.1 Intended use case for the certification

2.2 Other relevant certifications held (e.g. ISAE 3402 / 3000, ISO certificate, PCI DSS, national security certifications) or ongoing ISO audits

2.3 Does KPMG currently provide you any other services? (If yes, please provide an overview of these services)

2.4 Have you had any external consultants or similar consultancy advice to support the Management System implementation? (If yes, please provide the name of the service provider)

2.5 Are there any specific language requirements? (If yes, please detail the language(s) and whether it's a preference or requirement)

2.6 Preferred timeline of the certification

K_I_eckcIrQwqrckQamncBcr_gjq

3.1 Certification being currently pursued:

- | | | |
|--|------------------------------------|---|
| ☐ ISO 27001 | ☐ ISO 22301 | ☐ ISO 27018 |
| ☐ ISO 27701 | ☐ ISO 14001 | ☐ Findata security audit |
| ☐ ISO 9001 | ☐ ISO 27017 | ☐ Kanta Certification |
| ☐ ISO 42001 | | |
| ☐ Other certificate, please describe below: | | |

3.2 Draft Scope statement (initial scoping)

3.3 Describe the nature of the business processes and tasks which are within and related to the scope of the Management System, including their overall complexity^(a)

^(a) Example:

Click the icon on the right to open the dropdown list

3.4 Number of individuals working at the organization within the scope of the Management System^(b)

^(b) This is defined within as "the total number of persons doing work under the organization's control for all shifts within the scope of the certification". This may include, but not limited to, the following:

- Senior Management;
- Management system responsible team;
- Staff maintaining systems and locations within scope;
- Service/product affecting staff (such as customer service, sales etc.); and
- Support staff (such as Human Resources, Finance, Facilities etc.)

3.5 Key products and services within scope

3.6 Operations and business processes within scope, including business sector that the scope of the certification will operate in

3.7 High-level description of technical systems in scope (e.g. used cloud solutions, on-premise solutions, complexity of the systems and environments in scope)

3.8 Regulatory and compliance frameworks (including legal obligations) that are relevant to the scope of your Management System

3.9 For the people in scope of the certification, do you operate shift working or in unusual working patterns?

3.10 Are there temporary sites part of the Management System and in scope? (If yes, please provide details on the nature and operations performed in these sites)

GQM 055. /Acprgdga_rgm l ?bbgrgm l _jOscqrgrm lq

4.1 For the data and processes including services in scope of the certification, are you acting as PII Controller? (If yes, please provide description on the data types you are acting as in Controller role)

4.2 For the data and processes including services in scope of the certification, are you acting as PII Processor? (If yes, please provide description on the data types you are acting as in Processor role)

GQM 001. /Acprgdga_rgm l ?bbgrgm l _jOscqrgrm lq

5.1 Third party involvement in business continuity (If yes, describe the role of the service providers)

5.2 Approximate number of critical activities identified by the business impact analysis

5.3 Approximate number of incident management plans

5.4 Approximate number of business continuity plans

6.1 NACE / TOL 2008 code for QMS^(c)

^(c) NACE codes (Nomenclature of Economic Activities) is the European statistical classification of economic activities. To find your organizations NACE code, please review your company Standard Industrial Classification information, or search the relevant code through the following sites:

Standard Industrial Classification TOL 2008: <https://www.stat.fi/en/luokitukset/toimiala/>

Complete list of all NACE Code: <https://nacev2.com/en>

6.2 Risk category for QMS^(d)

Click the icon on the right to open the dropdown list

^(d) According to IAF MD 5:2019 the following risk categories shall be considered:

High risk: Where failure of the product or service causes economic catastrophe or puts life at risk. Examples include but are not limited to: Food; pharmaceuticals; aircraft; shipbuilding; load bearing components and structures; complex construction activity; electrical and gas equipment; medical and health services; fishing; nuclear fuel; chemicals, chemical products and fibres

Medium risk: Where failure of the product or service could cause injury or illness. Examples include but are not limited to: Non load bearing components and structures; simple construction activities; basic metals and fabricated products; non-metallic products; furniture; optical equipment; leisure and personal services.

Low risk: Where failure of the product or service is unlikely to cause injury or illness. Examples include but are not limited to: Textiles and clothing; pulp, paper and paper products; publishing; office services; education; retailing, hotels and restaurants.

7.1 Complexity category for EMS^(e)

Click the icon on the right to open the dropdown list

^(e) According to IAF MD 5:2019 the following complexity categories shall be considered:

High: environmental aspects with significant nature and gravity (typically manufacturing or processing type organizations with significant impacts in several of the environmental aspects);

Medium: environmental aspects with medium nature and gravity (typically manufacturing organizations with significant impacts in some of the environmental aspects);

Low: environmental aspects with low nature and gravity (typically organizations of an assembly type environment with few significant aspects);

Limited: environmental aspects with limited nature and gravity (typically organizations of an office type environment);

Special: these require additional and unique consideration at the audit planning stage.

ISO 42001 Certification Additional Questions

8.1 AIMS roles for maintaining the Artificial Intelligence Management System^(e):

- | | |
|--------------------------------------|---|
| ☐ AI Producer | ☐ AI Provider |
| ☐ AI User | ☐ Multiple AI roles / Combination of the roles |

^(e) **AI Provider:** Focus on creating and supplying AI components/models

AI Producer: Focus on integrating these components to build a complete system

AI User: Focuses on operating and controlling the system

I_r_Acprgdga_rgmI?bbgrgmI_jOscqrgrgmIq

If your application is related to Kanta Certification, please include System Description (Järjestelmälomake) to this application as required by THL (Finnish Institute for Health and Welfare):

[Link to System Description \(In Finnish\)](#)

[Link to regulatory requirements set by THL \(In Finnish\)](#)