Questionnaire to prepare for a Certification Audit for Information Security Management Sytem (ISMS)

1 Purpose

With the help of this questionnaire you can provide a detailed description of your company.

The questionnaire will be used by the certification body to establish whether the prerequisites of a certification audit have been fulfilled. It is either filled in by the company and/or completed by the auditors during the stage 1 audit.

1.1 Company Data

Please enclose company brochure.

Company _____

Address _____

_____

Contact Person _____

QM Representative _____

Telephone _____ Extension _____

Fax _____ Email _____

1.2 Company Structure

Legal Form _____

Multi sites certification? _____

List or name of sites: _____

_____

_____

Industrial Sector _____

Main Products/Services _____

_____

_____

Shift Operation? _____

_____

_____

Temporary sites (i.e installation sites, project locations etc.) :

_____

_____

_____

Number of employees at the following locations:		Shift 1	Shift 2	Shift 3
Research / Development / Design				
Production				
Administration				
Quality/Testing				
Maintenance				
Marketing				
HRD				
IT				
......				
Total				

- an organisational chart of the entire company or the organisational units to be audited has been attached ☐ yes ☐ no

- Have you received consultancy services? ☐ yes ☐ no

    If **yes**, by whom? _____

- Is the Information Security Management System integrated in an existing management system?

    If **yes**, in which? _____

- Is there ☐ a separate manual for the Information Security Management System

    ☐ an integrated management manual for all systems (QMS,EMS and ISMS)?

- Is there a group wide manual? ☐ yes ☐ no ☐ not applicable

- Have the manuals of the subsidiaries been derived from the group manual?
    ☐ yes ☐ no ☐ not applicable

- What type of audit are you interested in?

    ☐ a certification audit according to ISO 27001 : 2013

    ☐ a certification audit of an integrated management system (QMS,EMS & ISMS)

    ☐ a certification audit of combined with audit of other management system (QMS&EMS)

    ☐ not yet decided

- Scope of The Information Security Management System

    _____

    _____

- Total site Number : .... Sites

    ☐ Interested in Multisite/Sampling Certification
    ☐ Not interested in Multisite/Sampling Certification

Which organisational units are to be certified?　　　　**Organisational Unit**

☐　Entire company including all locations and branches

☐　Entire company except the following organisational units/locations/branches

☐　Only the following organisational unit(s):

For how long has the ISMS been practised?

Please state your requirements for the certification date?

- ▪ Do you request a pre-audit?　　　☐ yes　　　☐ no

- ▪ Please submit the documents listed below are already on hand?

Document Type	Remarks (e.g. document title, revision etc..)
Management review report	
Internal audit report	
Information Security policy	
Information Security objectives	
Information Security planning	
Quality manual	
Statement of Applicability	

Please also answer the questions in Annex 1 and Annex 2,

Signed by:

_____　　　　_____
　　　　　Place/Date　　　　　　　　　　　　　　　　Stamp/Signature

	QUESTIONNAIRE TO ASSIST PREPARATION FOR AN ISMS CERTIFICATION	Form Title : FS-TNI-001 Revision No. : 02 Effective Date : 07.09.2016 Page : 4 of 7

PT. TÜV NORD Indonesia

ANNEX 1 – MULTISITE CERTIFICATION

The following questions only need to be answered if your management system covers several locations, sites or branches which should be covered by the certification:

The completion of these questions allows us to determine whether the multi-site certification procedure may be used for the audit.

List of Site	Total Employees In Scope	Location
Head Office		
Site 1		
Site 2		
Site 3		
Site 4		
Etc...		

▪ Shall all locations / sites/ branches listed above of this questionnaire be included in the certification?

yes ☐   no ☐   partially ☐

▪ Do all locations / sites/ branches operating under the same ISMS, which is centrally administered and audited and subject to central management review?

Yes ☐   no ☐   partially ☐

▪ Have all locations / sites/ branches been subject to a complete internal audit, and are the results of these audits available?

yes ☐   no ☐   partially ☐

▪ Are there any differing legal requirements for all locations / sites/ branches?

yes ☐   no ☐   partially ☐

▪ Are there any variation of design & operation of controls and activities undertaken for all locations / sites/ branches?

yes ☐   no ☐   partially ☐

▪ Is there potential interaction with critical information system or information system processing sensitive information for all locations / sites/ branches?

yes ☐   no ☐   partially ☐

	QUESTIONNAIRE TO ASSIST PREPARATION FOR AN ISMS CERTIFICATION	Form Title : FS-TNI-001 Revision No. : 02 Effective Date : 07.09.2016 Page : 5 of 7

PT. TÜV NORD Indonesia

ANNEX 2 – ISMS SCOPE COMPLEXITY

Please answer the customer data and customer description on the table below to classify the ISMS scope complexity.

Customer data (H / M / L)	Customer description	Complexity factor	Category		
			High (H)	**Medium (M)**	**Low (L)**
		# of sites (head and branch offices)	>= 5	>= 2	<=1
		Complexity of the ISMS (Processes and tasks)	Complex processes; many business units included in scope; (high number of products and services)	Standard but non-repetitive processes; (high number of products and services)	Standard processes with standard and repetitive tasks; (few products and services)
		The type(s) of business and regulatory .	High risk business with (only) limited regulatory requirements. Organisation works in critical business sectors.	High regulatory requirements. Organisation has costumers in critical business sectors.	Low risk business without regulatory requirements.
		Previously demonstrated performance of the ISMS.	No other MS implemented at all, ISMS is new and not established	Some elements of other MS are implemented, others not	ISMS is already is well established and/or other MS are in place.
		IT infrastructure complexity: # of IT Assets (server, workstations, PCs, network, external interfaces, smartphones, ...)	Few or high standardized IT platforms, servers, OSs', databases, networks, … >5000	Several different IT platforms, servers, OSs', databases, networks, … >500	Many different IT platforms, servers, OSs', databases, networks, … >50
		Extent of outsourcing and third party arrangements. (including Cloudservice)	High dependency on outsourcing or suppliers with large impact on important business activities; or unknown amount or	Several partly managed outsourcing arrangements.	No outsourcing and little dependency on suppliers; or well-defined, managed and monitored out-sourcing ar-rangements.

Customer data (H / M / L)	Customer description	Complexity factor	Category		
			High (H)	Medium (M)	Low (L)
			extent of outsourcing; or several unmanaged outsourcing arrangements.		Outsourcer has a certified ISMS. Relevant inde-pendent assur-ance reports are available.
		Information System developement	Extensive in-house or outsourced system and application development for important business purposes	Some in-house or outsourced system and application development für some important business purposes	None or very limited in-house system and application development
		Total number of sites and number of Disaster Recovery sites	High availability requirements e.g. 24/z services.	Medium or High availability requirements and no or one DR site	Low availability requirements and no or one alernative DR site.
		For survailance or re-certification audit and only in case of changes of the organization or the Scope: Is the extent of changes relevant to the ISMS iin accordance with notices changes by the certified client?	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 scope or SoA of ISMS, e.g. some policies, documents, etc.	No changes since last (Re)-certification audit.

Evaluation by the Certification Body

1. Company details complete?

Ο yes　Ο no　Ο Remarks / additionally required information:

_____

_____

_____

2. Attached documents complete?

Ο yes　Ο no　Ο Remarks / additionally required information:

_____

_____

_____

3. Implementation and application of the management system sufficient?
(Based on the results of the details given in the annex)

Ο yes　Ο no　Ο Remarks / additionally required information:

_____

_____

_____

4. In case of multisite certification
Number of sample site need to be audited: _____ sites

Jakarta, _____　　　_____

　　　　　Place / Date　　　　　　　　Auditor / Head of CB Signature