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? ______________________________

Number of employees at the following locations:			
Research / Development / Design			
Production			
Administration			
Quality/Testing			
Maintenance			
Marketing			
HRD			
IT			

- 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)

  ☐ not yet decided

- Scope of The Information Security Management System
- Complexity of The ISMS Scope

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
- Which of 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	

Please also answer the questions in Annex 1, Annex 2, Annex 3 and attach all documents required in the Annex.

Signed by:

____________________ ____________________

Place/Date Stamp/Signature

ANNEX 1 – GENERAL QUESTIONS

Please answer the following questions before the commencement of the certification audit. The questions serve as a guideline for the successful preparation of the audit. You may add any remarks to the questions as you see fit.

Please submit additional documents to those questions marked either by ➢ or which are written in *italics*. If not already enclosed with the attachments, please also submit a current organisation chart and an overview over the most important processes in your company.

The successful evaluation of this questionnaire is a pre-requisite for the certification assessment in your company.

■ Have the information security policy and detailed, measurable information security objectives been defined?

yes □ no □ partially □

■ Are customer requirements researched, established and implemented??

yes □ no □ partially □

■ Have the authorities and responsibilities within your organisation been defined and documented?

yes □ no □ partially □

■ Has internal communication between the different functions of your organisation been defined, documented and established?

yes □ no □ partially □

➢ *Has the Information Security Management system been defined in a manual?*

yes □ no □ partially □

➢ *Is the control of documents and data described in a procedure?*

yes □ no □ partially □

➢ *Is the control of quality records described in a procedure?*

yes □ no □ partially □

■ Has a management review been conducted, and have the resulting tasks been implemented?

yes □ no □ partially □

■ Have training needs been determined? Have the required training measures been implemented and reviewed for effectiveness?

yes □ no □ partially □

■ Have the resources required for customer satisfaction and process implementation and improvement been determined and provided?

yes □ no □ partially □

■ Have external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system been determined?

yes □ no □ partially □

➢ *Has the organization retain documented information about the information security risk assessment process?*

yes □ no □ partially □

➢ *Has the organization retain documented information about the information security risk treatment process?*

yes □ no □ partially □

➢ *Has the organization determine A Statement Applicability ?*

yes □ no □ partially □

■ Have the organization plan, implement and control the processes needed to meet information security requirements?

yes □ no □ partially □

➢ *Has the organization retain documented information of the results of the information security risk treatment*?

yes □ no □ partially □

➢ *Has the organization retain documented information of the results of the information security risk assessments*?

yes □ no □ partially □

➢ *Are internal quality audits described in a procedure?*

yes □ no □ partially □

➢ *Is the control of nonconformities described in a procedure?*

yes □ no □ partially □

■ Is there a system to establish, implement, maintain and continually improve an information security management system in accordance with the requirements of standard?

yes □ no □ partially □

➢ *Has the organization retain appropriate documented information as evidence of the monitoring on and measurement results?*

yes □ no □ partially □

➢ *Are corrective actions described in a procedure?*

yes □ no □ partially □

➢ *Are preventive actions described in a procedure?*

yes □ no □ partially □

ANNEX 2 – 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.

Total number of sites		Average size of sites		□ Interested in Multisite/Sampling Certification □ Not interested in Multisite/Sampling Certification		
Head Office	Size of Site 1	Size of Site 2	Size of Site 3	Size of Site 4	Size of Site 5	Size of Site 6
Location	Location	Location	Location	Location	Location	Location

- Shall all locations / sites/ branches listed on page 1 of this questionnaire be included in the certification?

yes □ no □ partially □

- Do all locations / sites/ branches use identical or comparable production processes?

yes □ no □ partially □

- Do all locations / sites/ branches use the same or comparable raw materials or production materials?

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 □

- Is there a common management review for all locations / sites/ branches?

yes □ no □ partially □

- Does all management personnel involved in the environmental management system have identical access and authority at all locations / sites/ branches?

yes □ no □ Pa rtially □

ANNEX 3 – CRITERIA FOR ISMS SCOPE COMPLEXITY

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

Customer data	Customer description	Complexity factor	Category			Significance
			High	Medium	Low	
		# of employees + contractor staff	>= 1.000	>= 200	< 200	* Scale of ISMS implementation * Management information system * Production management-related systems * Sales /distribution/ general service-related systems * Information technology/information services and related systems * Construction/ship-building/plant engineering-related systems
		# of users	>= 1.000.000	>= 200.000	< 200.000	* Financial systems * Governments, schools, medicals/hospitals systems
		# of sites	>= 5	>= 2	<=1	* Scale of ISMS implementation * Physical and environmental security (ISO 27001 A.9)
		# of servers	>= 100	>= 10	< 10	* Scale of ISMS implementation * Physical and environmental security (ISO 27001 A.9) * Telecommunications and operation management (ISO 27001 A.10) * Access control (ISO 27001 A.11)
		# of workstations + PC + laptops	>= 300	>= 50	< 50	* Access control (ISO 27001 A.11)
		# of application development and maintenance staff	>= 100	>= 20	< 20	* Information systems acquisition, development and maintenance (ISO 27001 A.12)
		Network & encryption technology	External / Internet connection with encryption / digital signature / PKI requirements	External / Internet connection with use of encryption in built-in standard facilities without digital signature / PKI requirements	External / Internet connection without encryption / digital signature / PKI requirements	* Telecommunications and operation management (ISO 27001 A.10) * Access control (ISO 27001 A.11)

Customer data	Customer description	Complexity factor	Category			Significance
			High	Medium	Low	
		Significance in legal compliance	Incompliance leads to possible prosecution	Incompliance leads to significant financial penalty or goodwill damage	Incompliance leads to insignificant financial penalty or goodwill damage	* Laws and guidelines (ISO 27001 A.15)
		Applicability of sector-specific risk	Sector-specific law and regulation applies	No applicable sector-specific law and regulation, but significant sector-specific risk applies	No applicable sector-specific law and regulation and no applicable sector-specific risk applies	* Scale of ISMS implementation * Laws and guidelines (ISO/IEC 27001:2005, A. 15)

Evaluation by the Certification Body

1. **Company details complete?**

   ○ yes ○ no ○ Remarks / additionally required information:

   ____

   ____

   ____

2. **Attached documents complete?**

   ○ yes ○ no ○ Remarks / additionally required information:

   ____

   ____

   ____

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

   ○ yes ○ no ○ Remarks / additionally required information:

   ____

   ____

   ____

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

Jakarta,___________________________ ___________________________

Place / Date *Auditor Signature*