APPROVAL SHEET
PROCEDURE
INFORMATION SECURITY MANAGEMENT SYSTEM CERTIFICATION

PT. TÜV NORD Indonesia
PS - TNI – 001 Rev.05

Created : 20-06-2016	Checked: 20-06-2016	Approved : 20-06-2016
Indah Lestari	Karlina Bone	Leopold Hutapea

REVISION SHEET

No.	Part No.	Revision Note	Revision No.	Revision Date
1.	All	Refer to Management System Certification Procedure (Adjusting standard ISO/IEC 17021 Part 1 – 2015)	04	05-01-2016
2.	5	Update new standard ISO/IEC 27006:2015	05	20-06-2016
3.	6.3, 6.4, 6.12	Completed the sentences	05	20-06-2016

Table of Contents

1.	**Purpose**
	Procedure PS-TNI-001 describes the roles, responsibilities and processes in a certification body **by ISO 17021 and ISO 27006** involved in the certification of information security management systems (ISMS).
2.	**Scope**
	This procedure applies to PT. TÜV NORD Indonesia and its auditors.
3.	**Definitions**
	Audit Stage 1: On-site or off-site assessment of the readiness for certification of a company's information security management system and planning of audit stage 2. This includes the review of information security management system documentation. An on-site assessment may not be needed as an exception **.**
	Audit Stage 2: On-site assessment of establishment, implementation and effectiveness of a information security management system with respect to the issue of a certificate.
	Completion of audit: Last day of audit stage 2, typically the day of the final closing meeting.
	Surveillance Audit: Periodical (yearly, optionally half-yearly), post-certification on-site audit of information security management system implementation and effectiveness in representative areas and functions covered by the scope of the information security management system of the organization at defined intervals with respect to the maintenance of a certificate.
	Re-Certification Audit: Review of overall information security management system implementation and effectiveness in the organization with respect to new issue of the certificate.
	Extension Audit: Evaluation of information security management system implementation and effectiveness in additional or changed areas or sites of the scope, or after removal

of parts of the scope with respect to changes of the scope of a certificate.

Short-notice Audit:

Audits of certified clients at short notice to investigate complaints, or in response to changes, or as follow up on suspended clients.

Nonconformity:

Non-fulfilment with respect to the certification requirements.

a) The effectiveness of correction and corrective actions, for all nonconformities that represent
   - a failure to fulfil one or more requirements of the information security management system standard, or
   - a situation that raises significant doubt about the ability of the management system to achieve its intended outputs.

   have to be reviewed, accepted and verified prior to the release of the audit file.

b) For any other nonconformities the auditor reviews and accepts the client`s planned corrections and corrective actions prior to the release of the audit procedure; the verification is performed in the following scheduled audit (e.g. surveillance).

The verification may be satisfied by presenting personalized evidence or on a follow-up visit.

Follow-up Audit:

On-site assessment of the implementation and effectiveness of corrections and corrective actions for nonconformities issued during the audit.

Evaluation of documentary evidence:

Off-site assessment of the implementation and effectiveness of corrections and corrective actions for nonconformities issued during the audit.

Correction:

Action to eliminate a detected nonconformity.

Corrective Action:

Action to eliminate the cause of a detected nonconformity.

Audit day:

An audit day basically comprises 8 hours (net). Where it seems useful, a 10 hours audit day might be accepted by the appointed person.

Appointed Person:

Competence Personnel who are appointed to perform certain, defined tasks on behalf of Head of Certification Body

4. Responsibilities

4.1 Head of Certification Body

With respect to the scope of this procedure, the Head of the Certification Body is ultimately responsible for :

- select and appoint auditors, senior auditors and appointed persons,
- review and approval of certification files and by involving competent auditors if necessary. These auditors shall not have been part of the certification process activities,
- awarding the certificate.

The Head of the Certification Body is authorized to delegate responsibilities for areas covered by a particular management system standard whenever applicable.

Certain tasks from the certification process can be performed in the offices**.**

4.2 QM Manager / Management Representative

The QM manager is the Management Representative of PT. TÜV NORD Indonesia

4.3 Auditors

Auditors are responsible for the proper conduct of the certification process in line with this procedure and other relevant KAN regulations.

within the audit team, the lead auditor has the following additional responsibilities :

- drafting of an audit plan and report for the Audit Stage 1 including assessment of the ISMS documentation,
- drafting of the audit plan and the report for the Audit Stage 2 in consultation with the audit team,
- assigning audit responsibilities during the audit,
- documentation of audit findings and any nonconformities in consultation with the audit team,
- recommendation for issue / maintenance of the certificate or required corrective action and its scope, or decision to terminate an audit,
- determination of scope of the management system in agreement with customer,
- submission of the complete certification documents to the certification body in good time for release.

Within the context of the competent certification decision lead auditors permanently employed at PT. TÜV NORD Indonesia who are not involved in the audit procedure can be included in the review and release process.

4.3.1 Technical Experts

Technical experts can be employed to complete competence requirements for an audit team. They always act under the direction of an auditor and do not contribute to audit time.

4.4 Sales

- After receive an inquiry from the applicant, sales team is requesting the applicant to fill in Questionnaire/Application form. Sales team shall guide the client thus all the crucial information which are used to determine the audit days, audit scope, *etc.* are completed.
- The employees of the Sales department handle cost calculation of orders, the formulation of the offer and conclusion of contract as well as the implementation of the certification procedure in terms of the PT. TÜV NORD Indonesia system. Sales Department need to prepare A Team & Effort Approval (preliminary) before they make quotation.
- They have responsible to follow up and monitor the Questionnaire, A-team preliminary, Quotation (offer) and Contract for Certification to Client.
- Sales Department file Original Record of Contract for Certification, A-team preliminary, Quotation and Questionnaire in the server and notify administration support team once updated.

After scheduled, the sales team shall ensure that all preliminary documents needed prior to audit must be submitted by the client to administration support team.

4.5 Administration

The employees of the administration maintain and update the auditors and experts record.

They prepare the issue of the certificates and send them to the customers. They file the certification records**.**

They monitor and organise the performance of the Certification, Surveillance and Re-certification audits on behalf of the certification body management

5. Reference

a) Manual Mutu
b) ISO/IEC 17021 Part 1 : 2015, Conformity assessment – Requirements for bodies providing audit and certification of management system
c) ISO 9001 : 2015; Quality Management Systems – Fundamentals and Vocabulary
d) DPLS 12 Rev 1 , Persyaratan Tambahan Bagi Lembaga Sertifikasi Sistem Manajemen Kemanan Informasi
e) ISO/IEC 27006:2015, Information Technology – Security Techniques – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems
f) ISO/IEC 27001:2013, Information Technology – Security Techniques – Information Security Management Systems – Requirements

6. Procedure

The process is initiated when an applicant makes an inquiry or an order received through sales activities. The applicant is informed of the basic certification process

6.1 Customer Inquiry / Drafting of Offer

Refer to Management System Certification Procedure PMLF-TNI-02

The questionnaire shall be completed by the applicant to define the ISMS scopes against all applicable certification requirements. PT. TÜV NORD Indonesia conduct a review of the questionnaire and supplementary information for certification before proceeding with the audit. Based on this review, PT. TÜV NORD Indonesia takes in account the clients ISMS complexity and make the selection of the audit team regarding to clients specific needs (sector specific; diversity of technology, skills and experience of auditors) for the certification decision.

6.2 Audit Preparation

Refer to Management System Certification Procedure PMLF-TNI-02

The necessary knowledge and skills of the audit team leader and auditors may be supplemented by technical experts, translators and interpreters who shall operate under the direction of an auditor. Where translators or interpreters are used, they are to be selected such that they do not unduly influence the audit. Auditors-in-training may be included in the audit team as participants, provided an auditor is appointed as an evaluator. The evaluator shall be competent to take over the duties and have final responsibility for the activities and findings of the auditor-in-training.

6.3 Audit Stage 1

Refer to Management System Certification Procedure PMLF-TNI-02

The result of document review using form **Review of Document (FS-TNI-007)** and the report of stage 1 using form **Certification Report Stage** 1 (**FS-TNI-008)**

Audit stage 1 is to provide a focus for planning the stage 2 audit by gaining an understanding of the ISMS in the context of the client organization's ISMS policy and objectives, and, in particular, of the client organization's state of preparedness for the audit. *The client organization's has been operated through at least one management review and one internal ISMS audit covering the scope of certification*.

The audit team shall audit the ISMS of the client covered by the defined scope and ensure that the client's information security risk assessment and risk treatment properly reflects its activities and extends to the boundaries of its activities as defined in the scope of certification. The confirmation is needed to

reflect the client's scope of their ISMS and Statement of Applicability.

Audit stage 1 should not be restricted to the document review. The lead auditor shall agree with the client organization when and where the document review is conducted. In every case, the document review shall be completed prior to the commencement of the stage 2 audit

The following documents shall be available for the stage 1 audit:

a) Documented statements of the ISMS policy and objectives;

b) The scope of the ISMS;

c) Procedures and controls in support of the ISMS;

d) A description of the risk assessment methodology;

e) The information security risk assessment process;

f) The information security risk treatment process;

g) Documented procedures needed by the organization to ensure the effective planning, operation and control of its information security processes and describe how to measure the effectiveness of controls;

h) Records required by this International Standard and

i) The Statement of Applicability (at least one Statement of Applicability per scope of certification)

6.4 Audit planning

Refer to Management System Certification Procedure PMLF-TNI-02

The audit plan for ISMS audits take the determined information security controls into account.
The use of network-assisted (e.g. teleconferencing, web meeting, interactive web-based communications and remote electronic access to the ISMS documentation and/or ISMS processes) as auditing techniques shall be taken into consideration in the audit plan (e.g. video conferences) that will be utilized during the audit, as appropriate. *The audit objectives include the determination of the effectiveness of the management system to ensure that the client, based on the risk assessment, has implemented applicable controls and achieved the established information security objectives.*

6.5 Audit Stage 2

6.5.1 General

Refer to Management System Certification Procedure PMLF-TNI-02

The audit team has to ensure that the client demontrate the internal ISMS audit are scheduled and the programme and procedure are operational and can be shown to be operational.

The audit shall focus on the client organization's

a) Assessment of information security related risks, and that the assessments produce comparable and reproducible results;

b) ISMS documentation
   1) Documented statements of the ISMS policy and objectives;
   2) The scope of the ISMS;
   3) Procedures and controls in support of the ISMS;
   4) A description of the risk assessment methodology;
   5) The risk assessment report;
   6) The risk treatment plan;
   7) Documented procedures needed by the organization to ensure the effective planning, operation and
   8) Control of its information security processes and describe how to measure the effectiveness of controls;
   9) Records required by this International Standard and
   10) The Statement of Applicability.

c) Selection of control objectives and controls based on the risk assessment and risk treatment processes;

d) Reviews of the effectiveness of the ISMS and measurements of the effectiveness of the information security controls, reporting and reviewing against the ISMS objectives;

e) Internal ISMS audits and management reviews;

f) Management responsibility for the information security policy;

g) Correspondence between the selected and implemented controls, the Statement of Applicability, and the results of the risk assessment and risk treatment process, and the ISMS policy and objectives;

h) Implementation of controls, taking into account the organization's measurements of effectiveness of controls [see d) above], to determine whether controls are implemented and effective to achieve the stated objectives;

i) Programmes, processes, procedures, records, internal audits, and reviews of the ISMS effectiveness to ensure that these are traceable to management decisions and the ISMS policy and objectives.

6.5.2 Specific elements of the ISMS audit

Specific elements of the ISMS audit are maintaining procedures for the identification, examination and evaluation of information security related threats to assets, vulnerabilities and impacts on the client organization. The audit team shall

a) Require the client organization to demonstrate that the analysis of security related threats is relevant and adequate for the operation of the client organization;
NOTE The client organization is responsible for defining criteria by which information security related risks of the client organization are identified as significant, and to develop procedure(s) for doing this.

b) Establish whether the client organization's procedures for the identification, examination and evaluation of information security related threats to assets, vulnerabilities and impacts and the results of their application are consistent with the client organization's policy, objectives and targets.

The audit team shall also establish whether the procedures employed in analysis of significance are sound and properly implemented. If an information security related threat to assets, a vulnerability, or an impact on the client organization is identified as being significant, it shall be managed within the ISMS.

6.5.3 Legal and Regulatory Compliance

The maintenance and evaluation of legal and regulatory compliance is the responsibility of the client organization. The team audit shall restrict itself to checks and samples in order to establish confidence that the ISMS functions in this regard. The The team audit shall verify that the client organization has a management system to achieve legal and regulatory compliance applicable to the information security risks and impacts.

6.5.4 Integration of ISMS documentation with that for other management systems

The client organization can combine the documentation for ISMS and other management systems (such as quality, health and safety, and environment) as long as the ISMS can be clearly identified together with the appropriate interfaces to the other systems

6.5.5 Combining management system audits

The ISMS audit can be combined with audits of other management systems. This combination is possible provided it can be demonstrated that the audit satisfies all requirements for certification of the ISMS. All the elements important to an ISMS shall appear clearly, and be readily identifiable, in the audit reports.

The quality of the audit shall not be adversely affected by the combination of the audits.

6.6 Audit Findings

Refer to Management System Certification Procedure PMLF-TNI-02

The audit report is prepared based on the audit findings. The audit report of stage 2 using form **Audit Report** (**FS-TNI-009**). Nonconformities and opportunities for improvement are documented in the audit report. *Nonconformities are written in* ***Nonconformities Report*** *(***FMLF-TNI-002**).

6.7 Certificate Issue and Surveillance

6.7.1 Certificate Issue

Refer to Procedure PMLF-TNI-02 Management System Certification

A review of the certification file could be by veto person to assist Head of Certification Body make a certification decision. Veto person is auditor/technical expert or competence personnel but different personnels from those who carried out the audits.

If Head of Certification Body as Lead Auditor or Auditor, Head of Certification Body must appointed competence personnel to make the certification decision.

Head of Certification shall ensure at least one Person as veto person has the technical competence of the technical area of the audit. If veto person haven't the technical competence of the technical area of the audit, the veto person could be made by 3 (three) auditors that none of them carried out the audit .

If the review is positive, the Head of Certification Body Release the Certification File.

6.7.2 Certificates

In general, the validity of the certificate does not exceed three years from the issue date. Expiry of validity depends on the date of certificate decision. The effective date on certification shall not be before the date of the certification decision.

For the client organization and each of its information systems covered by the certification, these certificate shall identify the scope of the certification granted and the ISMS standard ISO/IEC 27001 to which the ISMS is certified. In addition, the certificate shall include a reference to the specific version of the Statement of Applicability. A change to the Statement of Applicability which does not change the coverage of the controls of the scope of certification need not require an update of the certificate.

One single certificate shall be issued with the name and address of the central office of the organization. A list of all the sites to which the certificate relates shall be issued, either on the certificate itself or in an appendix.

6.7.3 Surveillance Audit

Refer to Procedure PMLF-TNI-02 Management System Certification

At least the following points must be taken into consideration during a surveillance audit:

a) The system maintenance elements which are internal ISMS audit, management review and preventive and corrective action;

b) Communications from external parties as required by the ISMS standard ISO/IEC 27001 and other documents required for certification;

c) Changes to the documented system;

d) Areas subject to change;

e) Selected elements of ISO/IEC 27001;

f) Other selected areas as appropriate.

As a minimum, surveillance shall review the following:

a) The effectiveness of the ISMS with regard to achieving the objectives of the client organization's information security policy;

b) The functioning of procedures for the periodic evaluation and review of compliance with relevant information security legislation and regulations;

c) Action taken on nonconformities identified during the last audit.

The following issues shall be covered the points required for surveillance:

a) Adapt its surveillance programme to the information security issues related threats to assets, vulnerabilities and impacts on to the client organization and justify this programme.

b) The surveillance programme and specific dates for visits may be agreed with the certified client organization.

c) Surveillance audits may be combined with audits of other management systems. The reporting shall clearly indicate the aspects relevant to each management system.

d) Supervise the appropriate use of the certificate

During surveillance audits, the records of appeals and complaints , where any nonconformity or failure to meet the requirements of certification is revealed, that the client organization has investigated its own ISMS and procedures and taken appropriate corrective action.

6.8	**Suspend and withdrawn of Certificate**
	Refer to Procedure PMLF-TNI-02 Management System Certification
6.9	**Re-Certification audit**
	Refer to Procedure PMLF-TNI-02 Management System Certification The time allowed to implement corrective action shall be consistent with the severity of the nonconformity and the associated information security risk.
6.10	**Expanding / Reduction audit**
	Refer to Procedure PMLF-TNI-02 Management System Certification
6.11	**Transfer of certificates from other Certification Bodies**
	Refer to Procedure PMLF-TNI-02 Management System Certification
6.12	**Multiple sites**
	Client has a number of sites meeting the criteria from a) to c) below, PT. TÜV NORD Indonesia may consider using a sample-based approach to multiple-site certification audit: a) all sites are operating under the same ISMS, which is centrally administered and audited and subject to central management review; b) all sites are included within the client organization's internal ISMS audit programme; c) all sites are included within the client organisation's ISMS management review programme. PT. TÜV NORD Indonesia wishing to use a sample-based approach to ensure the following below: a) The initial contract review identifies, to the greatest extent possible, the difference between sites such that an adequate level of sampling is determined. b) A representative number of sites have been sampled by the certification body, taking into account

1) the results of internal audits of head office and the sites,
2) the results of management review,
3) variations in the size of the sites,
4) variations in the business purpose of the sites,
5) complexity of the ISMS,
6) complexity of the information systems at the different sites,
7) variations in working practices,
8) variations in activities undertaken,
9) potential interaction with critical information systems or information systems processing sensitive information,
10) any differing legal requirements
11) *geographical and cultural aspects;*
12) *risk situation of the sites;*
13) *information security incidents at the specific sites.*

c) A representative sample is selected from all sites within the scope of the client organization's ISMS; this selection shall be based upon judgmental choice to reflect the factors presented in item b) above as well as a random element.

d) Every site included in the ISMS which is subject to significant risks is audited by the certification body prior to certification.

e) The audit programme has been designed in the light of the above requirements and covers representative samples of the scope of the ISMS certification within the three years period.

In the case of a nonconformity being observed, either at the head office or at a single site, the corrective action procedure applies to the head office and all sites covered by the certificate.

6.13	**Special Audit**
6.13.1	**Extension to Scope Audit** PT. TÜV NORD Indonesia responses to an application for extension to the scope of a certification already granted, undertake a review of the application and determine any audit activities necessary to decide whether or not the extension may be granted. This may be conducted in conjunction with a surveillance audit.
6.13.2	**Special Cases** The activities necessary to perform special audits shall be subject to special provision if a client of certified ISMS makes major modifications to its system or if other changes take place which could affect the basis of its certification.
6.13.3	**Short-Notice Audits** Short-notoce audits necessary to conducted audits of certified clients at short notice to investigate complaints, or in response to changes, or as follow up on suspended clients .
6.14	**Audit Time**
	Describe on procedure PS-TNI-003
6.15	**Operational Control**
	Certification activities for branch offices are limited only as sales department (see point 4.4).

7. Applicable Documents	
	Questionnaire to Assist Preparation for an ISMS Certification
	Offer (Quotation)
	Contract for The Certification of Management System
	A Team and Effort Approval
	Audit Schedule
	Review of Documents
	Certification Audit Report stage – 1

	Audit Report
	Release of Audit Documentation
	Auditor Note
	Non Conformity Report
	Certificate Draft
	Sub Order (If External audit and/or Expert are involved)

A1 Effort for certification/ surveillance/ re-certification audits
"Employees" as referenced in the auditor time chart (see ACE) refers to all individuals whose work activities relate to the scope of the ISMS. The total number of employees for all shifts is the starting point for determination of audit time.
The effective number of employees includes non-permanent (seasonal, temporary, and subcontracted) staff that will be present at the time of the audit. A certification body should agree with the organization to be audited the timing of the audit which will best demonstrate the full scope of the organization. The consideration could include season, month, day/date and shift as appropriate.
Part-time employees should be treated as full-time-equivalent employees. This determination will depend upon the number of hours worked as compared with a full-time employee.
"Auditor time" includes the time spent by an auditor or audit team in stage 1 audit, stage 2 audit and planning (including off-site document review, if appropriate); interfacing with organization, personnel, records, documentation and process; and report writing. The "Auditor time" involved in such planning and report writing combined can not reduce the total on-site "auditor time" to less than 70 % of the time shown in the auditor time chart. Where additional time is required for planning and/or report writing, this will not be justification for reducing on-site auditor time. Auditor travel time is not included in this calculation, and is additional to the Auditor time referenced in the chart.
Remote Audits (CAAT; Computer Assisted Audit Techniques)
If CAAT such as interactive web-based collaboration, web meetings, teleconferences and/or electronic verification of the organization's processes are utilized to interface with the organization, these activities shall be identified in the audit plan, and may be considered as partially contributing to the total "on-site auditor time". CAAT activities are only up to 30 % of the planned on-site auditor time allowed. On-site auditor time refers to the on-site auditor time allocated for individual sites. Electronic audits of remote sites are considered to be remote audits, even if the electronic audits are physically carried out on the organization's premises
Locations / sites
A temporary site is a location other than the sites/locations identified in the certification document where activities, within the scope of certification, are implemented for a defined period of time. These sites could range from major project management sites to minor service/installation sites. The need to visit such sites and the extent of sampling should be based on an evaluation of the risks of the failure of a product or service to meet needs/expectations due to system nonconformity. The sample of sites selected should represent the range of the organization's competency needs and service variations having given consideration to sizes and types of activities, and the various stages of projects in progress.

A2 Requirements for audit stage 1

According to Section 9.2.3.1.1 of ISO 17021 it is recommended that at least parts of the Stage 1 audit should be performed at the client's location. The Stage 1 audit can also take place at the auditor's office, if this is permissible according to the classification described below. The classification is implemented in the calculation THE ISMS OF SCOPE COMPLEXITY.

Review:

The following are used as **evaluation criteria**:

- Size of company
- Company structure
- Complexity
- Product/ Service risk

Note: In justified individual cases, also classification as **High** by the auditor/ certification body.

In the **evaluation** a difference is made between A (Low, Medium) and B (High).

	Classification	
Evaluation criteria	A	B
Size of company (#employees & contracted staff)	Low, Medium	High
Company structure (#sites)	Low, Medium	High
Complexity (#users or #clients or #servers or #application development & maintenance staff)	Low, Medium	High
Product/Service risks (encryptionor legal compliance or sector specific risk)	Low, Medium	High

The Stage 1 on-site audit is required:

- The Stage 1 audit always takes place at the client's premises if the product/ service risk is classified as B (High).
- The Stage 1 audit takes place at the client's premises if the product/ service risk is classified as A (Low, Medium), but two further evaluation criteria are classified as B.

The duration of the Stage 1 audit is at least 0.5 days and as maximum of 50 % of the total audit time.

The total duration of the Stage 1 and Stage 2 audits is calculated on the basis of the auditor time charts.

The Stage 2 audit can be performed directly following the Stage 1 audit if required on condition that the client was made aware in advance of the consequences if weaknesses occur in the Stage 1 audit (possible categorization of the weaknesses as nonconformities in the Stage 2 audit or interruption of the audit).