China ISO/IEC ISO27701 (Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines)

Contents

Revision History

Rev No	Revision Date	Author	Approved by	Page No	Sec. No	Brief Description of Change
1.0	Aug.08 2019	Rose PAN	Leon Zhang			Initial

Related Documents

Document Number	Title
ISO/IEC 27018:2014	Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC 27006	Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
PP114	ISO 27001 (Information Security Management System) Scheme Manual
GP027	Conducting a BSI Assessment
GP035	Staff Competency & the Competency Code System
GP047	Certificate Decision Policy

1 Scope

This manual defines activities in relation to ISO27701 Certification Scheme based on "ISO27701 Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines" to enable consistent delivery of the scheme. This manual should be read in conjunction with the ISO 27001 Scheme Manual.

2 Legally Enforceable Agreement with Client

The standard BSI Assurance Ltd Conditions of Contract is applied..

3 Legal and Regulatory Requirements of the Scheme

All applicable local national and ratified International laws and regulations in relation to ISO 27001 scheme activities applied.

4 Scheme Description

In order to meet Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines, this certification scheme with ISO/IEC 27701has been developed by BSI.

ISO/IEC 27001 is used in conjunction with ISO/IEC 27701to ensure that clients establish and implement a robust management system to protect general personal information

5 Accreditation & Impartiality Requirements

5.1 Accreditation

BSI is the scheme owner of ISO/IEC 27701 certification globally, as a non-accredited scheme.

5.2 Impartiality

The requirements of PP114 ISO 27001 Scheme Manual, 5.2 apply.

6 Competence Requirements

Staff Competency & the Competency Code System GP035

Code System Best Fit GP011

Function	Code	Remark
Sales	C305	Including understanding of audit time calculation approach defined in this manual.

Function	Code	Remark
Planner	C350	Including understanding of audit team competence defined in this manual and the requirements to ISO/IEC 27701 certificate.
Audit Team	P27701	Having training for ISO/IEC 27701,hold P27001 or P10012
Certification Reviewer	C104	Hold C104 and P27701 code

7 Licence Coding

Certificate Number Prefix	Description
GPIP	P27701 Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

8 Assessment Time Determination

8.1 Number of persons doing work under the organization's control

The total number of relevant persons doing work for providing Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines within the scope of certification is the starting point for determination of audit time..

8.2 Audit time calculation

The ISO/IEC 27701 audit time is calculated in addition to the ISO/IEC 27001 on-site audit time. Normal rounding rules for each country applies, but the minimum additional audit time should be 1 day.

The standard calculation of ISO/IEC 27001 audit time for multi-site client is applied and then the additional ISO/IEC 27701 audit time is calculated based on ISO/IEC 27001 on-site audit time by adding **50%** percentage to the ISO/IEC 27001 audit time. The multisites sampling methodology for ISO/IEC 27701 assessment is applicable along with ISO/IEC 27001.

Justification for determination of audit time must be recorded and sufficient audit time must be provided to the audit team.

For clients who already have ISO/IEC 27001 certification, Stage 1 audit may not be required.

There are two possible scenarios below that will decide if a Stage 1 is required.

a) Where an existing ISO/IEC 27001 scope has covered activities/processes to protect PII , additional ISO/IEC 27701 audit time is calculated as relevant incremental percentage (see Table A) of Stage 2 on-site audit time. (e.g. ISO/IEC 27001 Stage 2 on-site audit time x 50%)

b) Where existing ISO/IEC 27001 scope has not covered activities/processes to protect PII

Additional audit time to extend ISO/IEC 27001 scope to include activities/processes to protect PII, including a Stage 1

Additional ISO/IEC 27701 audit time is calculated as (Stage 1 + Stage 2 on-site audit time for ISO/IEC 27001) x relevant incremental percentage (see Table A)

c) The audit time of surveillance for ISO/IEC 27701 is calculated based on ISO/IEC 27001 on-site surveillance audit time by using Table A above, and it is about 1/3 of initial certification audit. (e.g. surveillance on-site audit time for ISO/IEC 27001 x 50%)

d) The audit time of re-certification for ISO/IEC 27701 is calculated based on ISO/IEC 27001 onsite re-certification audit time by using Table A above, and it is about 2/3 of the initial audit. (e.g. re-certification on-site audit time for ISO/IEC 27001 x 50%)

Table A Calculation of Audit time for PII protection audit time

Role	ISO 27001	ISO27018	BS10012	ISO27701 quotation
Controller	Y	N	N	50%
Processor	Y	N	N	35%
Controller	Y	Y	N	20%
Processor	Y	Y	N	15%
Controller	Y	Y	Y	10%
Processor	Y	Y	Y	7%

Y means certified, N means not certified.

9 Certification Processes

Process	Remark
Application to Signed Agreement	Refer to section 9.1
Transfer	Refer to section 9.2
Scope Extension & Reduction	Refer to section 9.3
Multi-site certification	Refer to section 9.4
Assessment Planning	Refer to section 9.5

Process	Remark
Assessment Delivery	Refer to section 9.6
Nonconformity Management	Refer to section 9.7
Certification Decision	Refer to section 9.8
External Database Management	NA

9.1 Application to Signed Agreement

The standard BSI application procedure applies. In addition, it shall be requested the applicant to provide the following necessary information for ISO/IEC 27701 certification as follow.

a) The desired scope of the certification, indicating association with scope of ISO/IEC 27001

b) The type of cloud service (IaaS, PaaS, SaaS or other types of service provider) and providing single nation service or multinational services

c) Legal, Statutory, Regulatory and Contractual Requirements

d) Size of organization, number of cloud services within the desired scope e) Local activities

9.2 Transfer

The procedure of "GP031 Transfer of Certification to BSI" applies for both Global (nonaccreditation) and Japan (JIPDEC accreditation) .

9.3 Scope Extension & Reduction

The procedure of "PP114 ISO 27001 Scheme Manual", section 9.3 applies.

9.4 Multi-site certification

The procedure of "PP114 ISO 27001 Scheme Manual", section 9.4 applies.

9.5 Assessment Planning

The requirements of ISO 27001 Scheme Manual, section 9.5 apply. In addition, the following requirements apply.

The ISO/IEC 27701 audits shall be planned in conjunction with ISO 27001 audits.

For clients who already have ISO/IEC 27001 certification with requisite scope for ISO/IEC 27701, the stage 1 audit shall not be required. In this case an Extension to Scope audit to add ISO/IEC 27701 shall be conducted by a special audit.

9.5.1 Audit team and team competence

An audit team may consist of one ISMS assessor holding P27701 for all types of audits including initial certification audits, surveillance audits and re-certification audits. The team leader must ensure that

the cloud-specific implementation guidance and additional controls of ISO/IEC 27701 shall be covered by ISMS assessor holding P27701.

9.6 Assessment Delivery

The standard procedure of "PP114 ISO 27001 Scheme Manual" applies. In addition, the following requirements apply.

9.6.1 Audit report

The standard audit reporting process for ISO/IEC 27001 applies and the audit report for ISO/IEC 27701 is integrated within the ISO/IEC 27001 audit report if the ISO/IEC 27701 audit is conducted in conjunction with ISO/IEC 27001 audit.

Where standalone audit is conducted to add ISO/IEC 27701certification to existing ISO/IEC 27001 certification, the audit report is prepared solely for ISO/IEC 27701.

In addition to the standard ISO/IEC 27001 audit report, the audit report for ISO/IEC 27701 shall include the following.

a) Scope of the audit must refer to the protection of generally personal information as well as the information and processes covered by the ISMS

b) Summary of the audit undertaken and audit findings with regards to the requirements of ISO/IEC 27701

c) Any nonconformities identified against the requirements of ISO/IEC 27701 during the audit

d) For initial certification and recertification audits, recommendation for ISO/IEC 27701 certification or further audit as appropriate

e) For surveillance audit, confirmation that the client continues to satisfy the requirements of ISO/IEC 27701

9.7 Nonconformity Management

The requirements of ISO 27001 Scheme Manual, section 9.7 apply. In addition, the following requirements apply.

Where major nonconformity is raised against the requirement of ISO/IEC 27701, both of ISO/IEC 279151 and ISO/IEC 27001 certificates must be held until verifying effectiveness of correction and corrective actions for major nonconformity.

9.8 Certification Decision

In addition to the ISO/IEC 27001 certificate, the non-accredited ISO/IEC 27701 certificate is issued to the organizations that have demonstrated compliance to all relevant requirements to ISO/IEC 27001 and ISO/IEC 27701.

The ISO/IEC 27701 certificate is usually valid for 3 years and will have the same expiry date for ISO/IEC 27001 certificate. Where adding ISO/IEC 27701 to existing ISO/IEC 27001 certification, the ISO/IEC 27701 certificate will be issued with the same expiry date on ISO/IEC 27001 certificate.

The certificate will contain the following details in addition to the standard ISO/IEC 27001 certificate:

a) Certificate number with prefix GPIP;

b) The scope of activities including version of the Statement of Applicability and the reference of the certificate number of the relevant ISO/IEC 27001 certification.

10 Expected Outcomes

N/A