



International Association for Assessment Board Inc. (IAAB)

IAAB Guideline for CB Assessment of Security and resilience - Business continuity management systems based on ISO/IEC 17021-1 & 6 for ISO 22301 Standard

IAAB GDCB – 8: 2024, Issue 1

TABLE OF CONTENTS

0.	Introduction	3
1.	Scope	3
2.	Normative References	3
3.	Terms and Definitions	3
4.	Principles.....	4
5.	General Requirements.....	4
6.	Structural Requirements.....	4
7.	Resource Requirements.....	4
8.	Information Requirements	5
9.	Process requirements.....	6
10.	Management system requirements.....	8
	Annexure 01: Technical Sector.....	8
	Annexure 02: Required types of knowledge and skills for personnel involved with ISO 22301 certification activities	11
	Annexure 03: Required types of Qualification and Work experience and skills for personnel involved with ISO 22301 certification activities	12
	Annexure 04: Requirements for Audit Man-Day for Stage 1, Stage 2, Surveillance, Recertification audit.....	12
	Annexure 05: Integrated audit or combined audit.....	13
	Annexure 06: Other country Audit	13

Application of ISO/IEC 17021-1 based on ISO 22301 standard

0. INTRODUCTION

ISO/IEC 17021-1 is an International Standard

- that sets out the general requirements for bodies operating audit and certification of organizations' management systems.
- this document aims to guide certification bodies (CBs) in the consistent application of ISO/IEC 17021-1 & 6 for the accreditation of organizations that provide audit and certification services in accordance with ISO 22301.

1. SCOPE

This document specifies normative criteria for CBs auditing and certifying organizations' business continuity management systems to ISO 22301, in addition to the requirements contained in ISO/IEC 17021-1 & 6.

2. NORMATIVE REFERENCES

The following normative references applies:

- The normative references given in ISO/IEC 17021-1 & 6 and the following apply.
- ISO 22301* Security and resilience - Business continuity management systems - Requirements

*Note: Standard version refers to the latest version

3. TERMS AND DEFINITIONS

Terms and Definitions refers to ISO 22300 - Security and resilience – vocabulary.

Abbreviation used in this document:

Certification Body	CB
Business continuity management systems	BCMS
Technical Expert	TE
Team Leader	TL

4. PRINCIPLES

4.1	General	No additional requirements for ISO/IEC 17021-1 & 6.
4.2	Impartiality	No additional requirements for ISO/IEC 17021-1 & 6.
4.3	Competence	No additional requirements for ISO/IEC 17021-1 & 6.
4.4	Responsibility	CB requires to comply with the statutory and regulatory requirements applicable business continuity management systems.
4.5	Openness	No additional requirements for ISO/IEC 17021-1 & 6.
4.6	Confidentiality	No additional requirements for ISO/IEC 17021-1 & 6.
4.7	Responsiveness to Complaints	No additional requirements for ISO/IEC 17021-1 & 6.
4.8	Risk-based Approach	No additional requirements for ISO/IEC 17021-1 & 6.

5. GENERAL REQUIREMENTS:

5.1	Legal and Contractual Matters	The CB shall establish appropriate agreements with their clients to release audit report & relevant information to concern regulators or authority, incase required by them.
5.2	Management of Impartiality	No additional requirements for ISO/IEC 17021-1 & 6.
5.3	Liability and Financing	No additional requirements for ISO/IEC 17021-1 & 6.

6. STRUCTURAL REQUIREMENTS

6.1	Organization Structure and Top Management	No additional requirements for ISO/IEC 17021-1 & 6.
6.2	Operational Control	No additional requirements for ISO/IEC 17021-1 & 6.

7. RESOURCEREQUIREMENTS

7.1	Competence of Personnel	CB shall have competent personal having knowledge ISO 22301. All personnel involved in ISO 22301 certification Audit process shall meet the competency requirements of Annexure 2 & 3
7.2	Personnel Involved in the Certification Activities	Application reviewer Application reviewer shall meet the competency requirements of Annexure 2 & 3 Application reviewer may be certification decision personal if he/she compliance the requirement of Personnel making the certification decision as per Annexure 2. Auditor Each auditor shall have demonstrated competence as defined in Annexure 2 & 3.

		The CB shall use competent auditors for each business sector refer to Annexure 1 for conducting audit. Auditor experience The auditor shall comply with the following criteria, which shall be demonstrated in audits under guidance and supervision: a) Has gained experience in the entire process of auditing Compliance management systems, including review of documentation, implementation audit and audit reporting. b) Has gained experience by participating as a trainee in a minimum of two audits or total of at least 5 man-days audit for initial ISO 22301 Audit or surveillance audit / re-certification audit program. Audit team leaders: Shall fulfill the following: a) Has experienced as an audit team leader role under the supervision of a qualified team leader for at least Five audits or at least 10 man-days audit for initial ISO 22301 Audit or surveillance audit / re-certification audit program. Technical Expert (TE) Shall fulfill the following: Has minimum three years relevant experience in field of Compliance management systems. Personnel making the certification decision The CB shall ensure that personnel (group or individual) making the certification decision fulfil the competence in Annexure 2. This does not mean that each individual in the group needs to comply with all requirements, but the group as a whole shall meet all the requirements. When the certification decision is made by an individual, the individual shall meet all the requirements.
7.3	Use of Individual External Auditors and External Technical Experts	No additional requirements for ISO/IEC 17021-1 & 6.
7.4	Personnel Records	No additional requirements for ISO/IEC 17021-1 & 6.
7.5	Outsourcing	No additional requirements for ISO/IEC 17021-1 & 6.

8. INFORMATION REQUIREMENTS

8.1	Public Information	CB shall provide the information about the list of Certified clients, suspended clients, or withdrawn & cancelled clients to the public without the request or to the Regulatory Authority when demanded.
8.2	Certification Documents	The CB shall precisely document - Name of the organization - Location(s) - the scope of certification - issue date - date of surveillance audit - expiry date

		- in case of any modification in certification mention the modification, date shall be mentioned.
8.3	Reference to Certification and Use of Marks	No additional requirements for ISO/IEC 17021-1 & 6.
8.4	Confidentiality	No additional requirements for ISO/IEC 17021-1 & 6.
8.5	Information Exchange Between a CB and its Clients	In case of CB merged or sold to another CB or Suspension or Cancel the accreditation this relevant information shall be informed to the certified clients & information shall be made publicly available.

9. PROCESS REQUIREMENTS

9.1	PROCESS REQUIREMENTS	Outsourced process: CB shall verify the applicants outsourced process for compliance person / organization where applicable. Determining audit time: Annexure 4 provides a starting point for estimating the audit time of an initial certification audit (Stage 1 + Stage 2). Audit time is dependent on factors such as the audit scope, objectives, and specific regulatory requirements to be audited, as well on the range, class and complexity, and the size and complexity of the organization. When CBs are planning audits, sufficient time shall be allowed for the audit team to determine the conformity status of the client organization's compliance management system with respect to the relevant regulatory requirements. Note: Time required to audit national or regional regulatory requirements and dossier reviews shall be additional and justified, so as not to diminish the audit of the BCMS. Multi-site sampling Annexure 1 applicable for the multi-site
9.2	Planning Audits	The audit team shall have the competence for the Technical Area (Annexure 2 in conjunction with relevant knowledge and skills as defined in Annexure 3) for the scope of audit.
9.3	Initial Certification	Stage 1 The stage 1 can be performed on-site or Virtual audits can also be performed with justifications
	Conducting Audits	Identifying and recording audit findings Examples of major nonconformities which require the acceptance, and the verification of the effectiveness of correction and corrective actions are as follows:

9.4		a) failure to fully address applicable requirements and implement an entire process for BCMS b) failure to implement applicable requirements for BCMS c) failure to implement appropriate correction and corrective action d) deviations with the regulatory requirements e) repeated nonconformities from previous audits
9.5	Certification Decision	No additional requirements for ISO/IEC 17021-1 & 6.
	Transfer of certification	When transferring certification from one certification body to another certification body, the accepting certification body shall have a process for obtaining sufficient information to take a decision on certification. Consideration of documents related to sufficient information are not limited to the below documents: 1. Client's filled Application Form 2. Client's Stage-1, Stage-2 Audit, surveillance audit and recertification reports, which are applicable. 3. Correction & Corrective Actions Report filled by Client 4. Decision of Certification Grant 5. Certificate Copy 6. A Copy of Signed Client Agreement with Certification Body. 7. Any Complaint from Client/Stakeholder.
9.6	Maintaining Certification	Surveillance: the surveillance programme shall include a review of actions taken for notification of adverse events, advisory notices in addition to the compliance BCMS requirements. Surveillance frequency: CB shall conduct surveillance audit within 12 & 24 months of initial audit. Short notice audit: Short notice or unannounced audits may be required in case of: a) scope of certification indicates a possible significant deficiency in the BCMS. b) significant changes occur due to regulations, or any factor known to the CB, and which could affect the compliance with the regulatory requirements c) when required by legal requirements under public law or by the relevant Regulatory Authority The following are examples of such changes for considering a short notice or unannounced audit: a) BCMS – impact and changes: b) new ownership c) new regulations d) new processes, process changes e) Request from Client or AB. An unannounced or short-notice audit may also be necessary if the CB has justifiable concerns about implementation of corrective actions or compliance with standard and regulatory requirements.

		CB shall inform to the client about the short notice audit and shall be documented. CB shall make an agreement with client for witness audit which will be witnessed AB or IAAB or both assessors.
9.7	Appeals	No additional requirements for ISO/IEC 17021-1 & 6
9.8	Complaints	No additional requirements for ISO/IEC 17021-1 & 6
9.9	Client Records	No additional requirements for ISO/IEC 17021-1 & 6

10. MANAGEMENT SYSTEM REQUIREMENTS

10.1	Option A:	General Management System Requirements
10.1.1	General	No additional requirements for ISO/IEC 17021-1 & 6.
10.1.2	Management system manual	No additional requirements for ISO/IEC 17021-1 & 6.
10.1.3	Control of documents	No additional requirements for ISO/IEC 17021-1 & 6.
10.1.4	Control of records	No additional requirements for ISO/IEC 17021-1 & 6.
10.1.5	Internal audits	No additional requirements for ISO/IEC 17021-1 & 6.
10.1.6	Management review	No additional requirements for ISO/IEC 17021-1 & 6.
10.1.7	Corrective actions	No additional requirements for ISO/IEC 17021-1 & 6.
10.2	Option B:	No additional requirements for ISO/IEC 17021-1 & 6.
10.2.1	General	No additional requirements for ISO/IEC 17021-1 & 6.
10.2.2	Scope	No additional requirements for ISO/IEC 17021-1 & 6.
10.2.3	Management review	No additional requirements for ISO/IEC 17021-1 & 6.

Annexure 01: Technical Sector for business continuity management systems (BCMS)

Three primary complexity categories of compliance risks based on the nature and severity of an organization that fundamentally affect the auditor time.

These are:

- **High** – organizations operations with significant nature and severity (typically the construction industry, heavy manufacturing or processing type organizations),
- **Medium** – organizations operations with medium nature and severity (typically light manufacturing organizations with some significant risks), and
- **Low** – organizations operations with low nature and severity (typically small organizations).

Business Sector	Complexity category
• mining and quarrying • manufacture of coke and refined petroleum products • oil and gas extraction • pulping part of paper manufacturing including paper recycling processing • oil refining • chemicals (including pesticides, fabrication of batteries and accumulators), and pharmaceuticals • gas production, storage and distribution • electricity generation and distribution • nuclear • storage of large quantities of hazardous material • non-metallic processing and products covering ceramics, concrete, cement, lime, plaster, etc. • primary productions of metals • hot and cold forming and metal fabrication • manufacturing and assembly of metal structures • shipyards (depending on the activities could be medium) • aerospace industry • automotive industry • manufacturing of weapons and explosives • recycling of hazardous waste • hazardous and non-hazardous waste processing e.g. incineration etc. effluent and sewerage processing • industrial and civil construction and demolition (including building completion with electrical, hydraulic and air conditioning installation activities) • slaughter houses • transport and distribution of dangerous goods (by land, air and water) • defense activities/crisis management • telecommunications • healthcare/hospitals/veterinary/social works • corporate activities and management, HQ and management of holding companies • public administration, local authorities • financial institutions, advertising agency	High
• aquaculture (breeding, rearing, and harvesting of plants and animals in • all types of water environments) • fishing (offshore fishing is high) • farming/forestry (depending on the activities could be high) • food, beverage and tobacco – processing • textiles and clothing except for dyeing • leather and leather product except for tanning	Medium

• manufacturing of wood and wooden products including manufacturing of boards, treatment/impregnation of wood • paper production and paper products excluding pulping • non-metallic processing and products covering glass, ceramics, clay, etc. • general mechanical engineering assembly • manufacturing of metallic products • surface and other chemically based treatment for metal fabricated products excluding primary production and for general mechanical engineering (depending on the treatment and the size of the component could be high) • production of bare printed circuit boards for electronics industry • rubber and plastic injection molding, forming and assembly • electrical and electronic equipment assembly • manufacturing of transport equipment and their repairs - road, rail and air (depending on the size of the equipment, could be high) • recycling, composting, landfill (of non-hazardous waste) • water abstraction, purification and distribution including river management (note commercial effluent treatment is graded as high) • fossil fuel wholesale and retail (depending on the amount of fuel, could be high) • transport of passengers (by air, land and sea) • transport and distribution of non-dangerous goods (by land, air and water) • research & development in natural and technical sciences (depending on the business sector could be high). Technical testing and laboratories • hotels, leisure services and personal services excludes restaurants • education services (depending on the object of teaching activities could be high or low) • manufacturing of fiberglass • dyeing of textiles and clothing • tanning of leather and leather products • fishing (offshore, coastal dredging and diving)	
• wholesale and retail (depending on the product, could be medium or high, e.g. fuel) • general business services include industrial cleaning, hygiene cleaning & dry cleaning. • engineering services (could be medium depending on type of services) • post office services • restaurants • commercial estate agency, estate management	Low

Additional Manday Consideration:

In case of high-risk CB should calculate additional man days if needed based on the complexity / legal requirements and calculated effective number of personnel.

Effective Number of Personnel

The effective number of personnel consists of all personnel (permanent, temporary, and part-time) involved within the scope of certification including those working on each shift.

When included within the scope of certification, it shall also include non-permanent (e.g. contractors) personnel.

Calculation of the Effective Number of Personnel

The effective number of personnel as defined above is used as a basis for the calculation of audit time of

management systems of BCMS.

Considerations for determining the effective number of employees include

- part-time personnel and employees partially in scope,
- those working on shifts, administrative and
- all categories of office staff,
- similar or repetitive processes.

In case of seasonal trainings and operations the calculation of the effective number of personnel shall be based on the personnel typically present in peak season operations.

Part time personnel and employees partially in scope dependent upon the hours worked, part time personnel numbers and employees partially in scope may be reduced or increased and converted to an equivalent number of full-time personnel.

{e.g. 50 part time employee working 4 hours/day equates to 25 full time employees (FTE)}

The justification to determine the effective number of personnel shall maintain the record by CB.

Multi-site Organization

A multi-site organization does not need to be a distinct legal entity, but all sites must:

- Have a legal or contractual link with the central function.
- Operate under a unified management system that is established, monitored, and audited by the central function.

The central function has the authority to enforce corrective actions at any site when necessary.

Where applicable, this requirement should be formally documented in an agreement between the central function and the sites.

Eligibility of a multi-site organization for certification

- The organization shall have a single management system.
- The organization shall identify its central function.
- The central function is part of the organization and shall not be subcontracted to an external organization.
- The central function shall have organizational authority to define, establish and maintain the single management system.
- The organization's single management system shall be subject to a centralized management review.
- All sites shall be subject to the organization's internal audit programme.
- The central function shall be responsible for ensuring that data is collected and analyzed from all sites and shall be able to demonstrate its authority and ability to initiate organizational change as required in regard, but not limited, to:
 - (i) system documentation and system changes;
 - (ii) management review;
 - (iii) complaints;
 - (iv) evaluation of corrective actions;
 - (v) internal audit planning and evaluation of the results; and
 - (vi) statutory and regulatory requirements pertaining to the applicable standard(s).

Methodology for auditing of a multi-site organization using site sampling

- Sampling of a set of sites is permitted where the sites are each performing very similar

processes/activities.

- Not all organizations fulfilling the definition of “multi-site organization” will be eligible for sampling
- The sample shall be partly selective based on the factors set out below and partly random, and shall result in a representative range of different sites being selected, ensuring all processes covered by the scope of certification will be audited as per the below table:

Number of Sites	Sample size
2-5	02
6-10	04
11-20	06
21-50	08
51-100	10
101-200	15
201-500	20
500 - 1000	30
Above 1000	Based on calculation

Note: CB may increase or decrease the sample size along with the justification. But CB shall cover “Core area / activities of scope” in selected samples. Record of justification of sample size shall be maintained.

Annexure 2: Required types of knowledge and skills for personnel involved with ISO 22301 certification activities

The following table specifies the type of knowledge and skills that an CB shall define for specific functions.

Knowledge and skills	Certification Body functions			
	Application Reviewer	Auditor and Audit team leader	Technical Expert	Reviewing audit reports and making certification decisions
Knowledge of business management practices of business continuity management systems		X	X	
Knowledge of audit principles, practices and techniques related to business continuity management systems		X	X	X
Knowledge of ISO 22301 standard & normative documents related to business continuity management systems	X	X		X
Knowledge of certification body's processes related to business continuity management systems	X	X		X
Knowledge of client's business sector related business continuity management systems	X	X	X	X
Knowledge of client products, processes and organization related to business continuity management systems	X	X	X	
Language skills appropriate to all levels within the client organization		X		
Note-taking and report-writing skills		X		
Presentation skills		X		

Annexure 3: Required types of Qualification and Work experience and Skills for personnel involved with ISO 22301 certification activities

Qualification and Work experience	Certification functions				
	Application reviewer	Auditor	Audit team leader (TL)	Technical Expert	Report reviewer Certification decision maker
Education (i.e. Graduate or equal qualification)	X	X	X		X
Work experience (Minimum 3 years) TL have minimum 4 years		X	X	X	
Certificate of ISO 22301 Lead Auditor Course		X	X		
Industry specific knowledge (as per applicable)		X	X	X	X
Assessment experience on ISO 22301 standard		X	X		

Annexure 4: Requirements for Audit Man-Day for Stage 1, Stage 2, Surveillance, Recertification audit

Effective number of employees	Stage 1 Audit Man-day	Stage 2 Audit Man-day	Surveillance 1 Audit Man-day	Surveillance 2 Audit Man-day	Recertification Audit Man-day
1-10	0.5	1	0.5	0.5	1
11-20	1	1.5	1	1	1.5
21-50	1.5	2.5	1.5	1.5	2.5
51-100	2	3	2	2	3
101-250	3	5	3	3	5
251-500	4	6	4	4	6
501- 1000	5	7	5	5	7

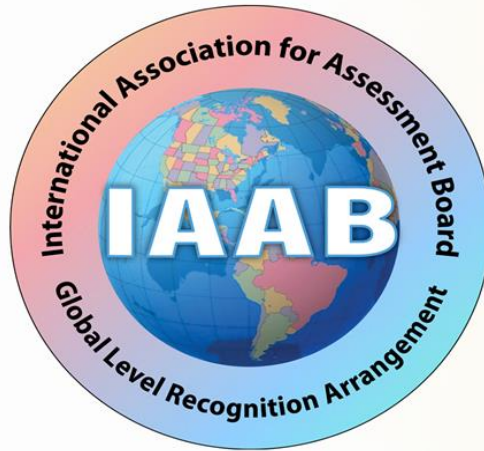
Note: CB may add additional man-days for high & medium complexity business sectors.

Annexure 5: Integrated audit or combined audit

ISO 22301 audit can combine / Integrated audit with other management system, CB can add the Audit time for 30-50% as per applicable, justification required for added audit time. In case CB reduce the audit time, CB show the valid justification with Man-day calculation for audit time reduction. CB shall maintain the record for Audit time calculation.

Annexure 6: Other country Audit

- A. CB shall make risk assessment before conduct audit other country then CB resident country, CB shall cover in Risk assessment include, but are not limited to economic, sociology, working environment, security of assessment team, language interpreter, Religion and Other relevant factors. Records of risk assessment shall be maintained.
- B. CB shall make risk assessment before conduct audit more than 1 country then CB resident country, CB shall cover in Risk assessment include, but are not limited to economic, sociology, working environment, security of assessment team, language interpreter, Religion and Other relevant factors. Records of risk assessment shall be maintained.
- C. CB may take interpreter for language support.



FURTHER INFORMATION

**For further information
on this document
contact:**

Secretariat:
IAAB Corporate Secretary

Email:
Contact@IAAB.US

