Văn phòng Công nhận Chất lượng/ *Bureau of Accreditation*
HỆ THỐNG CÔNG NHẬN TỔ CHỨC CHỨNG NHẬN VIỆT NAM
VIETNAM CERTIFICATION ACCREDITATION SCHEME
--- VICAS ---
70 Tran Hung Dao, Hanoi; Tel: (+84 24) 37911555; Email: vpcongnhan@boa.gov.vn; Http://www.boa.gov.vn

QUY ĐỊNH RIÊNG CÔNG NHẬN TỔ CHỨC CHỨNG NHẬN ISMS

SPECIFIC REQUIREMENTS FOR ACCREDITATION OF CB OPERATING ISMS CERTIFICATION

Mã số/ *Code*: ARC.19

Lần ban hành/ *Issue number*: 1.25

Ngày ban hành/ *Issue date:* 09/01/2025

1. Mục đích

Tài liệu này nêu yêu cầu cụ thể cho việc công nhận tổ chức chứng nhận hệ thống quản lý an toàn thông tin.

1. Purpose

This document sets up the specicfic requirements for accreditation of information security management systems certification bodies.

2. Tài liệu liên quan

ISO/IEC 17021-1: 2015 Đánh giá sự phù hợp – Yêu cầu cho tổ chức đánh giá và chứng nhận hệ thống quản lý – Phần 1: Yêu cầu.

ISO/IEC 27006-1: 2024 An toàn thông tin, an ninh mạng và bảo vệ quyền riêng tư - Yêu cầu đối với các tổ chức cung cấp dịch vụ đánh giá và chứng nhận hệ thống quản lý an toàn thông tin.

IAF MD17: 2023 Quy định bắt buộc áp dụng của IAF về việc chứng kiến trong công nhận tổ chức chứng nhận hệ thống quản lý.

2. Referrence

ISO/IEC 17021-1: 2015 Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 1: Requirements

ISO/IEC 27006-1: 2024 Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems

IAF MD17: 2023 Witnessing activities for the accreditation of management systems certification bodies.

3. Yêu cầu về khách hàng của tổ chức chứng nhận

Tổ chức chứng nhận (TCCN) phải hoàn thành quá trình chứng nhận cho ít nhất 01 khách hàng.

3. Requirements regarding clients of certification body

The certification body (CB) shall complete the certification process for at least 01 client.

4. Yêu cầu về năng lực chuyên gia của TCCN

Chuyên gia đánh giá phải có trình độ đại học trở lên.

4. Requirements regarding competence of CB's auditor and technical experts

Auditors shall be at least university graduate.

5. Chuẩn mực đánh giá công nhận

5. Assessment criteria

Chuẩn mực công nhận/ *Accreditation criteria:*

ISO/IEC 17021-1: 2015	Đánh giá sự phù hợp – Yêu cầu cho tổ chức đánh giá và chứng nhận hệ thống quản lý/ *Conformity assessment – Requirements for bodies providing audit and certification of management systems.*
ISO/IEC 27006-1: 2024	An toàn thông tin, an ninh mạng và bảo vệ quyền riêng tư - Yêu cầu đối với các tổ chức cung cấp dịch vụ đánh giá và chứng nhận hệ thống quản lý an toàn thông tin/ *Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems.*
IAF MD 1	Chứng nhận các tổ chức có nhiều địa điểm dựa trên việc chọn mẫu/ *Certification of Multiple Sites Based on Sampling.*
IAF MD 2	Chuyển giao chứng nhận Hệ thống quản lý được công nhận giữa các tổ chức chứng nhận/ *Transfer of Accredited Certification of Management Systems.*
IAF MD 4	Áp dụng kỹ thuật ICT trong đánh giá/ *The use of ICT in auditing.*
IAF MD 11	Áp dụng ISO/IEC 17021 trong đánh giá tích hợp hệ thống quản lý/ *Application of ISO/IEC 17021 for Audits of Integrated Management Systems.*

IAF MD 28	Công bố và cập nhật thông tin trên cơ sở dữ liệu của IAF/ *Upload and Maintenance of Data on IAF Database.*

Chuẩn mực chứng nhận/ *Certification criteria:*

ISO/IEC 27001: 2022	An toàn thông tin, an ninh mạng và bảo vệ quyền riêng tư - Hệ thống quản lý an toàn thông tin - Yêu cầu/ *Information security, cybersecurity and privacy protection - Information security management systems - Requirements*

6. Yêu cầu về chứng kiến

Khi đánh giá chứng kiến, đoàn đánh giá công nhận phải có năng lực kỹ thuật về hệ thống quản lý an toàn thông tin.

Một số lĩnh vực sau đây được xem là có mức độ rủi ro cao về khía cạnh an toàn thông tin, nghĩa là sẽ gây ra thiệt hại lớn hoặc tác động nghiêm trọng khi xảy ra sự cố mất an toàn thông tin:

- Lĩnh vực quốc phòng, an ninh;
- Lĩnh vực tài chính, ngân hàng và bảo hiểm;
- Lĩnh vực hành chính công;
- Lĩnh vực năng lượng hạt nhân.

6.1 Chứng kiến khi đánh giá công nhận lần đầu

Nếu ít nhất 01 cuộc chứng kiến được thực hiện đối với các ngành nghề, lĩnh vực rủi ro cao nói trên, TCCN có thể được cấp phạm vi công nhận không giới hạn (nghĩa là bao gồm tất cả các ngành nghề, lĩnh vực của xã hội).

Nếu không có cuộc chứng kiến nào được thực hiện đối với các ngành nghề, lĩnh vực rủi ro cao nói trên, TCCN chỉ có thể được cấp phạm vi công nhận giới hạn (nghĩa là bao gồm tất cả các ngành nghề, lĩnh vực của xã hội ngoại trừ các ngành nghề, lĩnh vực rủi ro cao nói trên).

Phải chứng kiến ít nhất một cuộc đánh giá chứng nhận lần đầu (gồm cả giai đoạn 1 và giai đoạn 2). Trong trường hợp TCCN không có khách hàng mới, có thể chứng kiến một cuộc đánh giá chứng nhận lại, hoặc hai cuộc đánh giá giám sát bao quát các quá trình chính.

6.3 Chứng kiến để duy trì công nhận

Trong một chu kỳ công nhận (5 năm kể từ khi công nhận có hiệu lực), phải chứng kiến mỗi năm một cuộc đánh giá ISMS.

6. Requirements for witnessing

In witnessing assessment, the assessment team shall have technical competence related to information security management system.

In terms of information security, the following sectors are considered to have a high level of risk due to the great damage or serious impact in case of an information security incident:

- Defense and security sectors;
- Finance, banking and insurance sectors;
- Public administration sector;
- Nuclear fuel sector.

6.1 Witnessing for initial assessment

If at least one witnessing is conducted for the high-risk economic activities, the CB can be granted an unlimited scope of accreditation which covers all economic activities.

If no witnessing is conducted for the high-risk economic activities, the CB can only be granted a limited scope of accreditation which covers all economic activities except for the aforementioned ones.

At least one initial audit (both stage 1 and stage 2) shall be witnessed. If CB does not have any new clients, it is possible to witness one renewal or two surveillances which cover the key processes.

6.3 Witnessing for maintaining of accreditation

During the accreditation cycle (5 years since the effective date of accreditation), at least one ISMS witnessing shall be conducted annually.

Để duy trì phạm vi công nhận không giới hạn, trong một chu kỳ công nhận phải chứng kiến ít nhất 01 cuộc đối với các ngành nghề, lĩnh vực rủi ro cao.

Trong một chu kỳ công nhận cần chứng kiến:

- Các chuyên gia đánh giá khác nhau;
- Các khách hàng khác nhau;
- Các loại hình đánh giá khác nhau.
-

To maintain an unlimited scope of accreditation, in an accreditation cycle, at least one witnessing shall be conducted for the high-risk economic activities

In the accreditation cycle, it is necessary to witness:

- Different auditors;
- Different audited clients;
- Different type of audit.
-

7. Xác định thời lượng đánh giá công nhận

7. Determination of assessment duration

Hoạt động đánh giá/ *Assessment activities*	Thời lượng/ *Duration*
Xem xét tài liệu (đối với công nhận lần đầu, chuyển đổi tiêu chuẩn)/ *Document review (applicable for initial assessment, transition to new assessment standard)*	1 MD
Đánh giá tại văn phòng/ *Office assessment*:	
• Đối với đánh giá công nhận lần đầu/ *Initial assessment*	3 MD
• Đối với đánh giá giám sát/ *Surveillance assessment*	1 MD
• Đối với đánh giá công nhận lại/ *Reaccreditation assessment*	2 MD
• Đối với đánh giá mở rộng/ *Extension assessment*	1 MD
• Đối với đánh giá tại các địa điểm khác ngoài trụ sở chính của TCCN (nếu có)/ *Assessment at sites of CB other than the main site (if any)*	1 MD mỗi địa điểm/*each site*
• Giảm thời lượng đánh giá trong các trường hợp đánh giá kết hợp các hệ thống (giảm không quá)/ *Reduction of assessment duration in case of integrated assessment (reduction shall not exceed)*	30% tổng thời lượng đánh giá *30% of total assessment time*
Đánh giá chứng kiến/ *Witnessing assessment*	Theo thời lượng cuộc đánh giá được chứng kiến *According to the duration of the audit witnessed*
Thẩm xét hồ sơ trong đánh giá công nhận lần đầu/ *Reviewing of initial assessment records*	1 MD
Thẩm xét hồ sơ khác/ *Reviewing of other assessment records*	0.5 MD
Ghi chú/ *Note:* MD (Manday) – ngày công đánh giá	

8. Phạm vi công nhận

BoA cấp công nhận cho các tổ chức chứng nhận theo phạm vi dưới đây:

8. Scopes of accreditation

BoA grants accreditation for CBs according to the following scopes:

8.1 Phạm vi công nhận giới hạn

8.1 Limited scope of accreditation

Chứng nhận Hệ thống quản lý An toàn thông tin theo tiêu chuẩn ISO/IEC 27001:2022 với phạm vi chứng nhận không bao gồm các lĩnh vực sau/ *Certification of Information Security Management System according to ISO/IEC 27001:2022 with the scope of certification excluding the following sectors*:

- Lĩnh vực quốc phòng, an ninh/ *Defense and security sectors*;
- Lĩnh vực tài chính, ngân hàng và bảo hiểm/ *Finance, banking and insurance sectors*;
- Lĩnh vực hành chính công/ *Public administration sector*;
- Lĩnh vực năng lượng hạt nhân/ *Nuclear fuel sector*.

8.2 Phạm vi công nhận không giới hạn **8.1 Unlimited scope of accreditation**

Chứng nhận Hệ thống quản lý An toàn thông tin theo tiêu chuẩn ISO/IEC 27001:2022/ *Certification of Information Security Management System according to ISO/IEC 27001:2022.*