

Updating Transition of ISO/IEC 27001:2013 to ISO/IEC 27001:2022

Cập nhật thông tin Chuyển đổi ISO/IEC 27001:2013 sang ISO/IEC 27001:2022

BSI please to inform that we have received accreditation from the following Accreditation Bodies for ISO/IEC 27001:2022: ISMS-AC, ANAB and RvA.

BSI vui mừng báo cáo rằng chúng ta đã nhận được sự công nhận cho tiêu chuẩn sau: ISO/IEC 27001:2022 từ các Cơ quan Công nhận ISMS-AC, ANAB và RvA.

Transition Plan / Kế hoạch chuyển đổi:

ISO/IEC 27001:2022 Transition Plan has been updated to provides details of the transition arrangements to ISO/IEC 27001:2022 following IAF mandatory document, IAF MD26. There is no change to the overall transition timeline, however the timeline for the start of initial and recertification audits has been updated.

Kế hoạch chuyển đổi ISO/IEC 27001:2022 đã được cập nhật để cung cấp thông tin chi tiết về các thỏa thuận chuyển đổi theo tài liệu bắt buộc của IAF, IAF MD26. Không có thay đổi nào đối với tiến trình chuyển đổi tổng thể, tuy nhiên, đối với đánh giá chứng nhận mới/lần đầu và đánh giá tái cấp chứng nhận có cập nhật lại thời hạn.

Overview of Transition Timeline/ Tổng quan về Thời hạn chuyển đổi:

Based on a transition period of 3 years, the expiry dates on certificates issued following initial certification or recertification referencing ISO/IEC 27001:2013 shall not exceed the published end of transition date (i.e. 3 years from the date of the standard being published). Based on the current information, the following is a summary of the arrangements:

Căn cứ trên thời gian chuyển đổi là 3 năm, ngày hết hạn của các chứng nhận được cấp khi chứng nhận lần đầu hoặc tái chứng nhận sử dụng phiên bản ISO/IEC 27001:2013 sẽ không vượt quá ngày kết thúc chuyển đổi đã công bố (nghĩa là 3 năm kể từ ngày tiêu chuẩn được công bố). Dựa trên thông tin hiện tại, sau đây là tóm tắt về các thỏa thuận:

- **All ISO/IEC 27001:2013 accredited certificates shall expire or be withdrawn no later than 31st October 2025 (the end of the transition period).**

Tất cả các chứng nhận có ISO/IEC 27001:2013 công nhận sẽ hết hạn hoặc bị thu hồi chậm nhất vào ngày 31 tháng 10 năm 2025 (kết thúc giai đoạn chuyển đổi).

- **From 1st May 2024, all initial and recertification audits shall be conducted using ISO/IEC 27001:2022.**

Từ ngày 1 tháng 5 năm 2024, tất cả các cuộc đánh giá chứng nhận mới/lần đầu và đánh giá tái cấp chứng nhận sẽ được thực hiện theo tiêu chuẩn ISO/IEC 27001:2022.

Key Changes of ISO/IEC 27001:2022 based on the Harmonized Structure**Những thay đổi chính của ISO/IEC 27001:2022 dựa trên cấu trúc hài hòa**

ISO/IEC 27001:2022 is not a fully revised edition. Its main changes include, but are not limited to:

ISO/IEC 27001:2022 không phải là phiên bản sửa đổi đầy đủ. Những thay đổi chính bao gồm, nhưng không giới hạn ở:

- Annex A references to the information security controls in ISO/IEC 27002:2022, which includes the information of control title and control;
Phụ lục A tham chiếu đến các biện pháp kiểm soát an toàn thông tin trong ISO/IEC 27002:2022, bao gồm thông tin về tiêu đề kiểm soát và biện pháp kiểm soát;
- Adding a new requirement, clause 4.2 c) to determine which of the interested parties will be addressed in the ISMS;
Bổ sung một yêu cầu mới, điều 4.2 c) nhằm xác định những bên quan tâm nào sẽ được giải quyết trong HTQL ATTT;
- Requirement to include processes needed and their interactions in clause 4.4;
Yêu cầu bao gồm các quá trình cần thiết và tương tác của chúng trong điều 4.4;
- The notes of Clause 6.1.3 c) are revised editorially, including deleting the control objectives and using "information security control" to replace "control";
Các ghi chú của điều 6.1.3 c) được sửa đổi biên tập, bao gồm loại bỏ các mục tiêu kiểm soát và sử dụng "biện pháp kiểm soát an toàn thông tin" để thay thế "biện pháp kiểm soát";
- The wording of Clause 6.1.3 d) is re-organized to remove the potential ambiguity;
Từ ngữ của Điều 6.1.3 d) được tổ chức lại để loại bỏ sự mơ hồ tiềm ẩn;
- The requirement for information security objectives to be monitored in clause 6.2.d);
Yêu cầu đối với giám sát các mục tiêu an toàn thông tin được tại khoản 6.2.d);
- Adding a new subclause 6.3-Planning for changes, which defines that any changes to the ISMS shall be carried out by the organization in a planned manner;
Bổ sung một điều khoản con mới 6.3-Lập kế hoạch cho các thay đổi, trong đó xác định rằng bất kỳ thay đổi nào đối với HTQL ATTT sẽ được tổ chức thực hiện một cách có kế hoạch;
- The consistency in the verb used in connection with documented information, for example, using "Documented information shall be available as evidence of XXX" in Clause 9.1, 9.2.2, 9.3.3 and 10.2;
Tính nhất quán trong động từ được sử dụng liên quan đến thông tin dạng văn bản, ví dụ: sử dụng "Thông tin dạng văn bản sẽ có sẵn làm bằng chứng của XXX" trong điều 9.1, 9.2.2, 9.3.3 và 10.2;
- Clause 8.1 requires planning of processes by determining criteria for the processes to meet requirements of clause 6 and to implement and control them according to those criteria;
Điều 8.1 yêu cầu lập kế hoạch các quy trình bằng cách xác định các tiêu chí để các quá

trình đáp ứng các yêu cầu của điều 6 và thực hiện cũng như kiểm soát chúng theo các tiêu chí đó;

- Using “externally provided process, products or services” to replace “outsourced processes” in Clause 8.1 and deleting the term-“outsource”;

Sử dụng “quá trình, sản phẩm hoặc dịch vụ do bên ngoài cung cấp” để thay thế “quá trình thuê ngoài” tại Điều 8.1 và loại bỏ thuật ngữ “thuê ngoài”;

- Naming and reordering and the subclauses in Clause 9.2-Internal audit and 9.3-Management review;

Đặt tên và sắp xếp lại các điều khoản trong Điều 9.2- Đánh giá nội bộ và 9.3- Xem xét của lãnh đạo;

- Exchanging the order of the two subclauses in Clause 10-Improvement;

Hoán đổi thứ tự của hai điều khoản nhỏ tại Điều 10-Cải tiến;

- Updating the edition of the related documents listed in Bibliography, such as ISO/IEC 27002 and ISO31000;

Cập nhật phiên bản của các tài liệu liên quan được liệt kê trong Thư mục tham khảo, ví dụ như ISO/IEC 27002 và ISO 31000;

- Some deviations in ISO/IEC 27001:2013 to the High Level Structure, identical core text, common terms and core definitions of MSS are revised to keep consistent with the Harmonized Structure for MSS, for example, Clause 6.2 d).

Một số sai lệch trong ISO/IEC 27001:2013 đối với Cấu trúc cấp cao, văn bản cốt lõi giống hệt nhau, các thuật ngữ chung và định nghĩa cốt lõi của MSS được sửa đổi để phù hợp với Cấu trúc hài hòa cho Nhiều tiêu chuẩn hệ thống quản lý, ví dụ, Điều 6.2 d).