KOMPLEYE

Office Address
12110 Sunset Hills Road, Suite 600
Reston VA 20190

Mailing Address
9893 Georgetown Pike #186
Great Falls, VA 22066

Telephone: (571)-830-5140
E-mail: info@kompleye.com
Website: www.kompleye.com

TRANSITION PLAN FROM ISO/IEC 27001:2013 TO ISO/IEC 27001:2022

Issuance Date: August 10, 2023

Aimed at: Companies holding or interested in KOMPLEYE certification - Information Security Management Systems according to the ISO/IEC 27001:2013 and ISO 27001:2022 standards.

Through this communication, KOMPLEYE announces the transition plan it has established for the ISO/IEC 27001:2013 standard to the new version ISO/IEC 27001:2022.

1 APPROVAL OF THE NEW ISO/IEC 27001:2022 STANDARD

On October 25, 2022, the new version of the international standard ISO/IEC 27001:2022 "Information security, cybersecurity, and privacy protection - Information Security Management Systems - Requirements" was published. This document provides the requirements for establishing, implementing, maintaining, and continually improving an information security system and replaces ISO/IEC 27001:2013.

On the other hand, on February 15, 2023, 2022, the International Accreditation Forum - IAF published the mandatory document IAF MD 26:2022 "TRANSITION REQUIREMENTS FOR ISO/IEC 27001:2022", which establishes a transition period of three (3) years ending on October 31, 2025.

2 MAIN CHANGES OF THE ISO/IEC 27001:2022 STANDARD COMPARED TO ISO/IEC 27001:2013 STANDARD

Compared with ISO/IEC 27001:2013, the main changes of ISO/IEC 27001:2022 include, but are not limited to:

- In requirement 4.2, literal c is included to identify which requirements will be addressed through the management of the information security system.
- In requirement 4.4, the words in bold are included: The organization shall establish, implement, maintain, and continually improve an information security management system, **including the necessary processes and their interactions**, in accordance with the requirements of this document.
- A note regarding the interpretation of the word "business" is included in 5.1 "Leadership and Commitment":
    - Reference to "business" in this document can be interpreted broadly to refer to those activities that are core to the purposes of the organization's existence.
- The notes of Clause 6.1.3 c) are revised editorially, including deleting the control objectives and using “information security control” to replace “control”.
- The wording of Clause 6.1.3 d) is re-organized to remove potential ambiguity.

KOMPLEYE

Office Address
12110 Sunset Hills Road, Suite 600
Reston VA 20190

Mailing Address
9893 Georgetown Pike #186
Great Falls, VA 22066

Telephone: (571)-830-5140
E-mail: info@kompleye.com
Website: www.kompleye.com

- In requirement 6.2 "Information Security Objectives and Planning to Achieve Them", literals d and g are included as requirements:
    - d) Be monitored
    - g) Be available as documented information.
- Requirement 6.3 "Planning of Changes" was included as a new requirement.
- In requirement 7.4 "Communication", literals d and e were eliminated:
    - d) who shall communicate; and
    - e) the processes by which communication shall be effected.

  Establishing a new literal d) How to communicate
- In requirement 8.1 "Operational planning and control", two bullets are included with mechanisms for the implementation of the provisions of clause 6, which indicate:
    - establish criteria for the processes;
    - implement the control of processes in accordance with the criteria.

  The use of "externally provided processes, products or services" is included to replace "outsourced processes" in clause 8.1 and the term "outsource" is deleted.
- Requirement 9.2 Internal Audit has been divided into 9.2.1: General and 9.2.2: Internal audit program. However, the requirements remain the same.
- In the requirement 9.3 "Management review", the following numerals 9.3.1, 9.3.2 and 9.3.3 are included; this information was previously included in requirement 9.3. In numeral 9.3.2, the following literal was included:
    - c) changes in the needs and expectations of interested parties that are relevant to the information security management system.
- The name of Annex A (Normative) Control objectives and reference controls is changed to Annex A (Normative) "Information security controls reference". In addition, the controls are aligned with ISO/IEC 27002:2022.
- In Annex A (Normative), the number of controls in ISO/IEC 27002:2022 decreased from 114 controls in 14 domains to 93 controls in 4 sections (themes).
- For the controls in ISO/IEC 27002:2022, 11 of these are new, 24 were merged from existing controls and 58 were updated. Additionally, the structure of the controls was revised, introducing the "attribute" and "purpose" for each control and eliminating the use of "objective" for a group of controls.

3 TRANSITION OF CURRENT CERTIFICATES GRANTED WITH THE ISO/IEC 27001:2013 STANDARD

KOMPLEYE has established a transition period of three (3) years from the publication date of ISO/IEC 27001:2022 (October, 2022), therefore, ISO/IEC 27001:2013 certificates will not be valid after October 31, 2025.

4 RECOMMENDATIONS FOR ORGANIZATIONS WITH CERTIFICATION OF THEIR SECURITY MANAGEMENT SYSTEM TO THE ISO/IEC 27001:2013 STANDARD

For organizations holding KOMPLEYE certification of their information security management system with the ISO/IEC 27001:2013 standard, it is recommended to keep in mind the following guidelines to successfully update the management system and thus their certification:

KOMPLEYE

Office Address
12110 Sunset Hills Road, Suite 600
Reston VA 20190

Mailing Address
9893 Georgetown Pike #186
Great Falls, VA 22066

Telephone: (571)-830-5140
E-mail: info@kompleye.com
Website: www.kompleye.com

- Know the requirements and concepts of the revised ISO/IEC 27001:2022 standard.
- Identify organizational gaps that need to be addressed to meet the new or modified requirements.
- Update the risk treatment plan.
- Implement, review, and verify the effectiveness of the new risk treatment plan.
- Update the statement of applicability (SoA).
- Update the management system to meet the revised requirements and provide verification of effectiveness.
- Provide appropriate training and knowledge to all parties that have an impact on the organization's effectiveness and performance, on the new requirements and on the expected outcome of their implementation.
- Schedule, plan, and execute the internal audit to the management system, considering the requirements of the standard in general, as well as new and modified requirements.
- Define and implement the pertinent corrections and corrective actions.
- Perform the review of the management system by the top management of the organization.
- Define and develop a transition plan for updating the management system and certification to the new requirements, including activities, responsible persons in the organization, key issues, required resources and implementation schedule.
- Periodically verify the progress and effectiveness of the transition plan.
- Coordinate and confirm with KOMPLEYE the development of the transition audit.

5 OPTIONS FOR PERFORMING THE ISO/IEC 27001:2022 CERTIFICATION UPGRADE AUDIT

KOMPLEYE offers its clients certified with ISO/IEC 27001:2013 the transition to ISO/IEC 27001:2022, starting July 1, 2023 and presents the following options for its realization:

Option 1: Update the certification to the new version of ISO/IEC 27001:2022 certificate at the recertification audit within the period corresponding to the organization's current certification cycle and up to three (3) months before the deadline for the transition.

Due date: 31 de Julio 2025.
Option 2: Update the certification by early renewal to ISO/IEC 27001:2022 prior to the next expiration date of your certificate and up to three (34) months before the deadline for the transition.

Due date: 31 de Julio 2025.

In all cases KOMPLEYE will increase the audit time by a minimum 0.5 days, therefore, the audit plan will include this additional time on a one-time basis. No additional charges will be applied

KOMPLEYE

Office Address
12110 Sunset Hills Road, Suite 600
Reston VA 20190

Mailing Address
9893 Georgetown Pike #186
Great Falls, VA 22066

Telephone: (571)-830-5140
E-mail: info@kompleye.com
Website: www.kompleye.com

Once the transition audit has been performed, with satisfactory results and in accordance with the provisions of the KP-CP-008-EN Certification Process, the certificate shall be updated with the 2022 version of the standard, without modifying the dates of the certification cycle.

Option 3: Update the certification with the new version ISO/IEC 27001:2022 in a surveillance audit, within the period corresponding to the organization's current certification cycle and up to three (3) months before the deadline for the transition. For this Alternative, Kompleye will include the assessment of conformity to the new and modified requirements of ISO/IEC 27001:2022.

Due date: 31 de Julio 2025.

In this case, KOMPLEYE will increase the audit time by a minimum of 1 day, therefore, the audit plan will include this additional time on a one-time basis. No additional charges will be applied.

Option 4: Update the certification through an independent audit (extraordinary) maintaining the current certification cycle, i.e. in an additional audit to those established in the certification cycle.

The duration of the audit to be performed under Option 4 will be determined by taking as a starting point the calculation of the time corresponding to a surveillance audit and will be increased by 1 day. No additional charges will be applied.

Once the transition audit has been performed, with satisfactory results and in accordance with the provisions of the KP-CP-008-EN Certification Process, the certificate shall be updated with the 2022 version of the standard, without modifying the dates of the certification cycle.

OPTION 5: Transition in a "separate audit" performed only for the purpose of a transition to ISO 27001: 2022.

The duration of the audit to be performed under Option 5 will be 1 day, during this day only the new or revised requirements will be reviewed. This option will not change the time required for the other audits within the certification cycle.

Once the transition audit has been performed, with satisfactory results and in accordance with the provisions of the KP-CP-008-EN Certification Process, the certificate shall be updated with the 2022 version of the standard, without modifying the dates of the certification cycle.

6 ASPECTS TO BE CONSIDERED BY KOMPLEYE DURING THE TRANSITION AUDIT

The transition audit shall include, among others, the following aspects:

- The gap analysis of ISO/IEC 27001:2022, as well as the need for changes to the client's ISMS.
- Verification that relevant personnel are competent for ISO/IEC 27001:2022 and transition process.
- Document review to confirm whether or not clients are competent for ISO/IEC 27001:2022

KOMPLEYE

Office Address
12110 Sunset Hills Road, Suite 600
Reston VA 20190

Mailing Address
9893 Georgetown Pike #186
Great Falls, VA 22066

Telephone: (571)-830-5140
E-mail: info@kompleye.com
Website: www.kompleye.com

- The updating of the statement of applicability (SoA).
- If applicable, the updating of the risk treatment plan.
- The implementation and effectiveness of the new or changed information security controls chosen by the clients.

Kompleye will be able to perform the transition audit remotely if it ensures that the transition audit objectives are met.

7 SUSPENDED MANAGEMENT SYSTEM CERTIFICATES

In the event that the KOMPLEYE certificate for the ISO/IEC 27001:2013 information security management system is suspended during the term of the transition plan, the certification holder may request the reactivation audit with the corresponding surveillance audit and the certification transition audit together, taking as a starting point the calculation of the time corresponding to a surveillance audit and increased by 1 days If the suspension occurs at the second surveillance audit and the reactivation audit is scheduled to be performed close to the expiration date of the certificate, the case will be reviewed on a case-by-case basis by the Kompleye CEO.

8 REVISED ISO 27001:2022 CERTIFICATES

As with any audit, non-conformities identified during a transition audit will require a corrective action to be submitted and approved. An updated ISO 27001:2022 certification will be issued following corrective action approval.

Updated ISO 27001:2022 certificate issuance and validity will be as follows:

- Surveillance Audit– The organization’s existing ‘Expiration Date’ will be maintained.
- Renewal – A new ‘Expiration Date’ will be issued for the renewed 3-year period.
- Independent audit – The organization’s existing ‘Expiration Date’ will be maintained.

Kompleye will update the certification documents and database for the certified clients if their ISMS meets the requirements of ISO/IEC 27001:2022.

If certified clients do not successfully complete the transition assessment before the related due date listed in clause 3, the expiration date of their accreditation to ISO/IEC 27001:2013 shall be no later than the end of the transition period.

When the certification document is updated because the client successfully completed only the transition audit, the expiration of its current certification cycle will not be changed.

9 OTHER GUIDELINES ESTABLISHED BY KOMPLEYE

KOMPLEYE

Office Address
12110 Sunset Hills Road, Suite 600
Reston VA 20190

Mailing Address
9893 Georgetown Pike #186
Great Falls, VA 22066

Telephone: (571)-830-5140
E-mail: info@kompleye.com
Website: www.kompleye.com

- KOMPLEYE will continue to accept applications for certification and issue new certificates to 27001:2013 until April 30 25, 2024. All initial (new) certification and recertification audits will be to the ISO 27001:2022 after this date.
- All transition audits shall be completed by July 31, 2025.
- The transition audit will not only rely on the document review, but additionally on the review of the information security technological controls.
- Recertification audits entering the restoration process shall have completed all pending activities including decision making and ratification by KOMPLEYE before October 31, 2025.
- The expiration date of ISO/IEC 27001:2022 certifications issued during the transition period shall be 2025/10/31 to correspond to the end of the transition period.
- The certificates of the organizations that do not comply with the established deadlines to update to the new version of ISO/IEC 27001:2022 shall expire or be withdrawn and a new certification process will have to be started. See: Kompleye » Kompleye Accreditation Information.
- These certificates will initially be issued without accreditation logo, once ANAB confirms the transition of Kompleye's accreditation to ISO/IEC 27001:2022, the certificates will be updated with the respective accreditation logo symbol.

Kind regards,

Mery Carolina Hidalgo A.

Mery Carolina Hidalgo Alférez
ISO Lead
M: (+57) 317 636 8618
carolina@kompleye.com