SELF EVALUATION CHECKLIST
ISO/IEC 27001:2022

This document is intended to assist you in the identifying your readiness for becoming 3rd party certified to the globally recognized standard ISO/IEC 27001:2022 Information Security Management System (ISMS).

When the checklist has been completed, you may contact us to organise a GAP assessment or get started on your Certification Audit.

Company Name:	
Proposed Scope of Certification:	
Completed by:	

TO BEGIN WITH, PLEASE GIVE THOUGHT TO...

Policy and Leadership

- Do we have a clear and docmen ed Information Security Policy that defines our commitment to protecting our information assets?
- Is our senior management committed to Information Security and actively involved in promoting and supporting the implementation of an ISMS?
- Do we have a designated Information Security Officer or team responsible for managing and implementing the ISMS?

Risk Assessment

- Have we conducted a risk assessment to identify the risks and threats to our information assets?
- Have we identified the impact of potential information security incidents on our business operations and reputation?
- Have we identified the risk owners and their responsibilities for managing risks?
- Do we have a risk treatment plan that outlines the measures to be taken to mitigate identified risks?

ISMS Implementation

- Have we identified the information assets that we need to protect?
- Have we established information security objectives and defined metrics to measure their effectiveness?
- Have we defined roles and responsibilities for all personnel involved in the ISMS implementation?
- Have we established procedures for incident management and reporting?
- Have we established access controls and defined procedures for granting and revoking access to information assets?
- Have we established procedures for managing third-party service providers and their access to our information assets?
- Have we established procedures for managing the physical security of our information assets, including the protection of devices and media containing sensitive information?
- Have we implemented procedures for monitoring and detecting security incidents and breaches?
- Have we established procedures for managing and reporting security incidents and breaches?

ISMS Maintenance

- Do we regularly review and update our Information Security Policy, risk assessments, and risk treatment plan?
- Do we conduct regular internal audits of our ISMS to ensure compliance with ISO 27001 and our own policies and procedures?
- Do we conduct regular management reviews of the ISMS to ensure its effectiveness and suitability for our organization?
- Do we continually improve our ISMS by identifying areas for improvement and implementing corrective actions?

Training and Awareness

- Do we provide regular training and awareness programs to all employees on Information Security policies, procedures, and best practices?
- Do we provide specific training and awareness programs for personnel with access to sensitive information assets?

CHECKLIST ISO/IEC 27001:2022

Next follows the requirements of the standard. You may use the last column to insert your management system documentation reference.

Context of the organization

Requirement	Your organization	Document ref.
4.1 Understanding the organization and its context	☐ External issues have been determined ☐ Internal issues have been determined	
4.2 Understanding the needs and expectations of interested parties	☐ Interested parties relevant to the ISMS identified ☐ All relevant information security requirements of these interested parties identified	
4.3 The organization shall determine the boundaries and applicability of the information security management system to establish its scope.	☐ The internal and external issues ☐ Interested parties needs and expectations ☐ Organisation of activities performed ☐ Services ☐ Third party services ☐ Location ☐ Exclusions from scope have been justified	
4.4 The organization shall establish, implement, maintain and continually improve an ISMS, including the processes and their interactions	☐ The necessary processes and their interactions are included	

Leadership

Requirement	Your organization	Document ref.
5.1 Top management shall demonstrate leadership and commitment with respect to the ISMS	☐ Management provides formal support for the implementation and operation of the ISMS ☐ IS policy and the IS objectives are established ☐ Integration of the ISMS requirements into processes ☐ Communication regarding the ISMS and of conforming to its requirements ☐ Resources are available.	
5.2 ISMS Policy	Our ISMS Policy; ☐ Is appropriate & includes objectives ☐ Includes commitment to requirements ☐ Includes commitment to continual improvement ☐ Is documented ☐ Is communicated ☐ Is available	
5.3 Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated within the organization	Responsibility and authority are assigned for; ☐ Ensuring that the ISMS conforms to the requirements of the standard ☐ Reporting on the performance of the ISMS to top management	

SELF EVALUATION CHECKLIST
ISO/IEC 27001:2022

intertek
Total Quality. Assured.

Planning

Requirement	Your organization	Document ref.
6.1 Actions to address risks and opportunities	**Our organisation has planned;** ☐ The actions necessary to address documented risk and opportunities related to the implementation of the ISMS ☐ How to integrate and implement these actions into the ISMS ☐ How to evaluate these actions **Risk Assessment** ☐ Is defined and documented ☐ Includes business IS requirements ☐ Includes legal and statutory requirements ☐ Includes criteria for risk acceptance and acceptable levels of risk ☐ Identifies organisations risks and risk owner ☐ Identifies impacts on confidentiality, integrity and availability ☐ Risks are analysed and evaluated ☐ Realistic likelihood of IS failures have been studied ☐ Risks have been accepted or mitigated as per defined methodology **Risk Treatment** ☐ Is defined and documented ☐ Risk treatment options are selected ☐ Controls are determined ☐ Includes controls from Annex A and a verification that no necessary controls are omitted **Statement of Applicability** ☐ Is defined and documented ☐ Contains controls and justification of inclusion and exclusion of these ☐ Contains status of selected controls ☐ Contains a formulated risk treatment plan, risk owner and the owner's approval of risk treatment plan and acceptance of residual risk	
6.2 The organization shall establish IS objectives at relevant functions and levels	**Objectives are;** ☐ Consistent with IS Policy ☐ Measurable ☐ Taking IS requirements and results from risk assessment/ treatment into account ☐ Monitored ☐ Communicated ☐ Documented ☐ Planned to be achieved	
6.3 Planning of changes	☐ When need for changes to the ISMS, the changes are carried out in a planned manner	

SELF EVALUATION CHECKLIST
ISO/IEC 27001:2022

intertek
Total Quality. Assured.

Support

Requirement	Your organization	Document ref.
7.1 Resources	☐ Resources needed for establishment, implementation, maintenance and continual improvement are determined and provided	
7.2 Competence	☐ Competency requirements are determined ☐ Management ensures that the competency of persons in scope is appropriate ☐ Documented information as evidence of competence is retained ☐ A training & awareness program is developed	
7.3 Awareness	Persons in scope are aware of; ☐ The IS Policy ☐ Their contribution to the ISMS ☐ The implications of not conforming with the ISMS	
7.4 Communication	☐ The need for internal/external communication has been determined	
7.5 Documented information	Documented information ☐ Has identification and description ☐ Is formally approved ☐ Is available and protected ☐ Is subject to version and change control, review and re-approval	

Operation

Requirement	Your organization	Document ref.
8.1 The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6	☐ Documented information is available to the extent necessary to have confidence that the processes have been carried out as planned ☐ Planned changes are controlled and consequences of unintended changes is reviewed ☐ Externally provided processes, products or services that are relevant to ISMS is controlled.	
8.2 IS risk assessment	☐ Risk assessment is performed at planned intervals ☐ Risk assessment is performed when there are significant changes ☐ Is documented	
8.3 IS risk treatment	☐ Risk treatment plan is implemented ☐ Results are documented	

SELF EVALUATION CHECKLIST
ISO/IEC 27001:2022

intertek
Total Quality. Assured.

Performance evaluation

Requirement	Your organization	Document ref.
9.1 Monitoring, measurement, analysis and evaluation	☐ Process is established ☐ Evidence of results is documented ☐ Performance and effectiveness of the ISMS is evaluated	
9.2 Internal audit	☐ Is conducted at planned intervals ☐ Internal audit programme is established ☐ Evidence of results is documented	
9.3 Management review	☐ Results of management review include decisions related to continual improvement ☐ Results of management review includes needs for changes to the ISMS ☐ Is documented	

Improvement

Requirement	Your organization	Document ref.
10.2 Nonconformity and corrective action	☐ NC's are actioned and corrected ☐ Potential causes to NC's are identified and eliminated ☐ Effectiveness of CA's are evaluated ☐ Are documented	

Mandatory documents & records

Requirement	Your organization
According to ISO 27001, the documented information specified in the next column is required to be produced	☐ Scope of the ISMS (clause 4.3) ☐ IS Policy (5.2) ☐ IS Risk Assessment and Treatment process (6.1.2) ☐ Statement of Applicability (6.1.3) ☐ IS Objectives (6.2) ☐ Risk Assessment and Treatment report (8.2 and 8.3) ☐ Inventory of assets (A.5.9*) ☐ Acceptable use of assets (A.5.10*) ☐ Incident response procedure (A.5.26*) ☐ Statutory, regulatory, and contractual requirements (A.5.31*) ☐ Security operating procedures for IT management (A.5.37*) ☐ Definition of security roles and responsibilities (A.6.2 and A.6.6*) ☐ Definition of security configurations (A.8.9*) ☐ Secure system engineering principles (A.8.27*) *Note: ISO 27001 documents or records required by Annex A controls are mandatory only if there are risks or requirements from interested parties that would demand implementing those controls.
ISO 27001 records that are mandatory	☐ Trainings, skills, experience, and qualifications (Clause 7.2) ☐ Monitoring and measurement results (9.1) ☐ Internal audit program (9.2) ☐ Results of internal audits (9.2) ☐ Results of the management review (9.3) ☐ Results of corrective actions (10.2) ☐ Logs of user activities, exceptions, and security events (A.8.15*) *Note: ISO 27001 documents or records required by Annex A controls are mandatory only if there are risks or requirements from interested parties that would demand implementing those controls.

27001 GAP ANALYSIS
2013 - 2022

intertek
Total Quality. Assured.

Clause	ISO/IEC 27001:2013	ISO/IEC 27001:2022	Change Y/N?
4	Context of the organization		
4.1	**Understanding the organization and its context.** The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.	**Understanding the organization and its context** The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.	N
4.2	**Understanding the needs and expectations of interested parties** The organization shall determine: a. interested parties that are relevant to the information security management system; and b. the requirements of these interested parties relevant to information security	**Understanding the needs and expectations of interested parties** The organization shall determine: a. interested parties that are relevant to the information security management system; b. the relevant requirements of these interested parties; c. which of these requirements will be addressed through the information security management system.	Y
4.3	**Determining the scope of the information security management system** The organization shall determine the boundaries and applicability of the information security management system to establish its scope. When determining this scope, the organization shall consider: a. the external and internal issues referred to in 4.1; b. the requirements referred to in 4.2; and c. interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations. d. The scope shall be available as documented information.	**Determining the scope of the information security management system** The organization shall determine the boundaries and applicability of the information security management system to establish its scope. When determining this scope, the organization shall consider: a. the external and internal issues referred to in 4.1; b. the requirements referred to in 4.2; c. interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations. d. The scope shall be available as documented information.	N
4.4	**Information security management system** The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.	**Information security management system** The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document.	N

27001 GAP ANALYSIS
2013 - 2022

intertek
Total Quality. Assured.

Clause	ISO/IEC 27001:2013	ISO/IEC 27001:2022	Change Y/N?
5	Leadership		
5.1	**Leadership and commitment** Top management shall demonstrate leadership and commitment with respect to the information security management system by: a. ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization; b. ensuring the integration of the information security management system requirements into the organization's processes; c. ensuring that the resources needed for the information security management system are available; d. communicating the importance of effective information security management and of conforming to the information security management system requirements; e. ensuring that the information security management system achieves its intended outcome(s); f. directing and supporting persons to contribute to the effectiveness of the information security management system; g. promoting continual improvement; and h. supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.	**Leadership and commitment** Top management shall demonstrate leadership and commitment with respect to the information security management system by: a. ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization; b. ensuring the integration of the information security management system requirements into the organization's processes; c. ensuring that the resources needed for the information security management system are available; d. communicating the importance of effective information security management and of conforming to the information security management system requirements; e. ensuring that the information security management system achieves its intended outcome(s); f. directing and supporting persons to contribute to the effectiveness of the information security management system; g. promoting continual improvement; and h. supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.	N
5.2	**Policy** Top management shall establish an information security policy that: a. is appropriate to the purpose of the organization; b. includes information security objectives (see 6.2) or provides the framework for setting information security objectives; c. includes a commitment to satisfy applicable requirements related to information security; and d. includes a commitment to continual improvement of the information security management system. The information security policy shall: e. be available as documented information; f. be communicated within the organization; and g. be available to interested parties, as appropriate.	**Policy** Top management shall establish an information security policy that: a. is appropriate to the purpose of the organization; b. includes information security objectives (see 6.2) or provides the framework for setting information security objectives; c. includes a commitment to satisfy applicable requirements related to information security; d. includes a commitment to continual improvement of the information security management system. e. The information security policy shall: f. be available as documented information; g. be communicated within the organization; h. be available to interested parties, as appropriate.	N
5.3	**Organizational roles, responsibilities and authorities** Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated. Top management shall assign the responsibility and authority for: a. ensuring that the information security management system conforms to the requirements of this International Standard; and b. reporting on the performance of the information security management system to top management.	**Organizational roles, responsibilities and authorities** Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated within the organization. Top management shall assign the responsibility and authority for: a. ensuring that the information security management system conforms to the requirements of this document; b. reporting on the performance of the information security management system to top management.	N

27001 GAP ANALYSIS
2013 - 2022

intertek
Total Quality. Assured.

Clause	ISO/IEC 27001:2013	ISO/IEC 27001:2022	Change Y/N?
6	Planning		
6.1 6.1.1	Actions to address risks and opportunities General When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to: a. ensure the information security management system can achieve its intended outcome(s); b. prevent, or reduce, undesired effects; and c. achieve continual improvement. d. The organization shall plan: e. actions to address these risks and opportunities; and f. how to 1. integrate and implement the actions into its information security management system processes; and 2. evaluate the effectiveness of these actions.	General When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to: a. ensure the information security management system can achieve its intended outcome(s); b. prevent, or reduce, undesired effects; c. achieve continual improvement. d. The organization shall plan: e. actions to address these risks and opportunities; and f. how to 1. integrate and implement the actions into its information security management system processes; and 2. evaluate the effectiveness of these actions.	N
6.1.2	Information security risk assessment The organization shall define and apply an information security risk assessment process that: a. establishes and maintains information security risk criteria that include: 1. the risk acceptance criteria; and 2. criteria for performing information security risk assessments; b. ensures that repeated information security risk assessments produce consistent, valid and comparable results; c. identifies the information security risks: 1. apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; an 2. identify the risk owners; d. analyses the information security risks: 1. assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize; 2. assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and 3. determine the levels of risk; e. evaluates the information security risks: 1. compare the results of risk analysis with the risk criteria established in 6.1.2 a); and 2. prioritize the analysed risks for risk treatment. f. The organization shall retain documented information about the information security risk g. assessment process.	Information security risk assessment The organization shall define and apply an information security risk assessment process that: a. establishes and maintains information security risk criteria that include: 1. the risk acceptance criteria; and 2. criteria for performing information security risk assessments; b. ensures that repeated information security risk assessments produce consistent, valid and comparable results; c. identifies the information security risks: 1. apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and 2. identify the risk owners; d. analyses the information security risks: 1. assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize; 2. assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and 3. determine the levels of risk; e. evaluates the information security risks: 1. compare the results of risk analysis with the risk criteria established in 6.1.2 a); and 2. prioritize the analysed risks for risk treatment. f. The organization shall retain documented information about the information security risk g. assessment process.	N

27001 GAP ANALYSIS
2013 - 2022

intertek
Total Quality. Assured.

Clause	ISO/IEC 27001:2013	ISO/IEC 27001:2022	Change Y/N?
6.1.3	Information security risk treatment The organization shall define and apply an information security risk treatment process to: a. select appropriate information security risk treatment options, taking account of the risk b. assessment results; c. determine all controls that are necessary to implement the information security risk treatment option(s) chosen; d. compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted; e. produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A; f. formulate an information security risk treatment plan; and g. obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks. The organization shall retain documented information about the information security risk treatment process.	Information security risk treatment The organization shall define and apply an information security risk treatment process to: a. select appropriate information security risk treatment options, taking account of the risk b. assessment results; c. determine all controls that are necessary to implement the information security risk treatment option(s) chosen; d. compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted; e. produce a Statement of Applicability that contains: – the necessary controls (see 6.1.3 b) and c)); – justification for their inclusion; – whether the necessary controls are implemented or not; and – the justification for excluding any of the Annex A controls. f. formulate an information security risk treatment plan; and g. obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks. The organization shall retain documented information about the information security risk treatment process.	N
6.2	Information security objectives and planning to achieve them The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall: a. be consistent with the information security policy; b. be measurable (if practicable); c. take into account applicable information security requirements, and results from risk assessment and risk treatment; d. be communicated; and e. be updated as appropriate. f. The organization shall retain documented information on the information security objectives. g. When planning how to achieve its information security objectives, the organization shall determine: h. what will be done; i. what resources will be required; j. who will be responsible; k. when it will be completed; and l. how the results will be evaluated.	Information security objectives and planning to achieve them The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall: a. be consistent with the information security policy; b. be measurable (if practicable); c. take into account applicable information security requirements, and results from risk assessment and risk treatment; d. be monitored; e. be communicated; f. be updated as appropriate; g. be available as documented information. The organization shall retain documented information on the information security objectives. When planning how to achieve its information security objectives, the organization shall determine: h. what will be done; i. what resources will be required; j. who will be responsible; k. when it will be completed; and l. how the results will be evaluated.	Y
6.3	NA	Planning of changes When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.	Y

27001 GAP ANALYSIS
2013 - 2022

intertek
Total Quality. Assured.

Clause	ISO/IEC 27001:2013	ISO/IEC 27001:2022	Change Y/N?
7	Support		
7.1	Resources The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.	Resources The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system	N
7.2	Competence The organization shall: a. determine the necessary competence of person(s) doing work under its control that affects its information security performance; b. ensure that these persons are competent on the basis of appropriate education, training, or experience; c. where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and d. retain appropriate documented information as evidence of competence.	Competence The organization shall: a. determine the necessary competence of person(s) doing work under its control that affects its information security performance; b. ensure that these persons are competent on the basis of appropriate education, training, or experience; c. where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and d. retain appropriate documented information as evidence of competence.	N
7.3	Awareness Persons doing work under the organization's control shall be aware of: a. the information security policy; b. their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and c. the implications of not conforming with the information security management system requirements.	Awareness Persons doing work under the organization's control shall be aware of: a. the information security policy; b. their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and c. the implications of not conforming with the information security management system requirements.	N
7.4	Communication The organization shall determine the need for internal and external communications relevant to the information security management system including: a. on what to communicate; b. when to communicate; c. with whom to communicate; d. who shall communicate; and e. the processes by which communication shall be effected.	Communication The organization shall determine the need for internal and external communications relevant to the information security management system including: a. on what to communicate; b. when to communicate; c. with whom to communicate; d. how to communicate	Y

27001 GAP ANALYSIS
2013 - 2022

intertek
Total Quality. Assured.

Clause	ISO/IEC 27001:2013	ISO/IEC 27001:2022	Change Y/N?
7.5 7.5.1	Documented information, General The organization's information security management system shall include: a. documented information required by this International Standard; and b. documented information determined by the organization as being necessary for the effectiveness of the information security management system.	Documented information, General The organization's information security management system shall include: a. documented information required by this International Standard; and b. documented information determined by the organization as being necessary for the effectiveness of the information security management system.	N
7.5.2	Creating and updating When creating and updating documented information the organization shall ensure appropriate: a. identification and description (e.g. a title, date, author, or reference number); b. format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and c. review and approval for suitability and adequacy.	Creating and updating When creating and updating documented information the organization shall ensure appropriate: a. identification and description (e.g. a title, date, author, or reference number); b. format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and c. review and approval for suitability and adequacy.	N
7.5.3	Control of documented information Documented information required by the information security management system and by this International Standard shall be controlled to ensure: a. it is available and suitable for use, where and when it is needed; and b. it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity). For the control of documented information, the organization shall address the following activities, as applicable: c. distribution, access, retrieval and use; d. storage and preservation, including the preservation of legibility; e. control of changes (e.g. version control); and f. retention and disposition. Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.	Control of documented information Documented information required by the information security management system and by this document shall be controlled to ensure: a. it is available and suitable for use, where and when it is needed; and b. it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity). For the control of documented information, the organization shall address the following activities, as applicable: c. distribution, access, retrieval and use; d. storage and preservation, including the preservation of legibility; e. control of changes (e.g. version control); and f. retention and disposition. Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.	N

27001 GAP ANALYSIS
2013 - 2022

intertek
Total Quality. Assured.

Clause	ISO/IEC 27001:2013	ISO/IEC 27001:2022	Change Y/N?
8	Operation		
8.1	**Operational planning and control** The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2. The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned. The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. The organization shall ensure that outsourced processes are determined and controlled.	**Operational planning and control** The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by: — establishing criteria for the processes; — implementing control of the processes in accordance with the criteria. Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned. The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.	Y
8.2	**Information security risk assessment** The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a). The organization shall retain documented information of the results of the information security risk assessments.	**Information security risk assessment** The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a). The organization shall retain documented information of the results of the information security risk assessments.	N
8.3	**Information security risk treatment** The organization shall implement the information security risk treatment plan. The organization shall retain documented information of the results of the information security risk treatment.	**Information security risk treatment** The organization shall implement the information security risk treatment plan. The organization shall retain documented information of the results of the information security risk treatment.	N

27001 GAP ANALYSIS
2013 - 2022

intertek
Total Quality. Assured.

Clause	ISO/IEC 27001:2013	ISO/IEC 27001:2022	Change Y/N?
9	Performance evaluation		
9.1	**Monitoring, measurement, analysis and evaluation** The organization shall determine: a. what needs to be monitored and measured, including information security processes and controls; b. the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;. c. when the monitoring and measuring shall be performed; d. who shall monitor and measure; e. when the results from monitoring and measurement shall be analysed and evaluated; and f. who shall analyse and evaluate these results. The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.	**Monitoring, measurement, analysis and evaluation** The organization shall determine: a. what needs to be monitored and measured, including information security processes and controls; b. the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results. The methods selected should produce comparable and reproducible results to be considered valid; c. when the monitoring and measuring shall be performed; d. who shall monitor and measure; e. when the results from monitoring and measurement shall be analysed and evaluated; f. who shall analyse and evaluate these results. Documented information shall be available as evidence of the results. The organization shall evaluate the information security performance and the effectiveness of the information security management system.	Y
9.2	**Internal audit** The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system: a. conforms to 1. the organization's own requirements for its information security management system; and 2. the requirements of this International Standard; b. is effectively implemented and maintained. The organization shall: c. plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits; d. define the audit criteria and scope for each audit; e. select auditors and conduct audits that ensure objectivity and the impartiality of the audit process; f. ensure that the results of the audits are reported to relevant management; and g. retain documented information as evidence of the audit programme(s) and the audit results.	**9.2.1 General** The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system: a. conforms to 1. the organization's own requirements for its information security management system; 2. the requirements of this document; b. is effectively implemented and maintained. **9.2.2 Internal audit programme** The organization shall plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. When establishing the internal audit programme(s), the organization shall consider the importance of the processes concerned and the results of previous audits. The organization shall: a. define the audit criteria and scope for each audit; b. select auditors and conduct audits that ensure objectivity and the impartiality of the audit process; c. ensure that the results of the audits are reported to relevant management; d. Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.	Y

27001 GAP ANALYSIS
2013 - 2022

intertek
Total Quality. Assured.

Clause	ISO/IEC 27001:2013	ISO/IEC 27001:2022	Change Y/N?
9.3	Management review Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness. The management review shall include consideration of: a. the status of actions from previous management reviews; b. changes in external and internal issues that are relevant to the information security management system; c. feedback on the information security performance, including trends in: 1. nonconformities and corrective actions; 2. monitoring and measurement results; 3. audit results; and 4. fulfilment of information security objectives; d. feedback from interested parties; e. results of risk assessment and status of risk treatment plan; and f. opportunities for continual improvement. The outputs of the management review shall include decisions related to continual improvement. opportunities and any needs for changes to the information security management system. The organization shall retain documented information as evidence of the results of management reviews.	9.3.1 General Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness. 9.3.2 Management review inputs The management review shall include consideration of: a. the status of actions from previous management reviews; b. changes in external and internal issues that are relevant to the information security management system; c. changes in needs and expectations of interested parties that are relevant to the information security management system; d. feedback on the information security performance, including trends in: 1. nonconformities and corrective actions; 2. monitoring and measurement results; 3. audit results; 4. fulfilment of information security objectives; e. feedback from interested parties; f. results of risk assessment and status of risk treatment plan; g. opportunities for continual improvement. 9.3.3 Management review results The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system. Documented information shall be available as evidence of the results of management reviews	Y

27001 GAP ANALYSIS
2013 - 2022

intertek
Total Quality. Assured.

Clause	ISO/IEC 27001:2013	ISO/IEC 27001:2022	Change Y/N?
10	Improvement		
10.1	**Nonconformity and corrective action** When a nonconformity occurs, the organization shall: a. react to the nonconformity, and as applicable: 1. take action to control and correct it; and 2. deal with the consequences; b. evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1. reviewing the nonconformity; 2. determining the causes of the nonconformity; and 3. determining if similar nonconformities exist, or could potentially occur; c. implement any action needed; d. review the effectiveness of any corrective action taken; and e. make changes to the information security management system, if necessary. Corrective actions shall be appropriate to the effects of the nonconformities encountered. The organization shall retain documented information as evidence of: f. the nature of the nonconformities and any subsequent actions taken, and g. the results of any corrective action.	**10.1 Continual improvement** The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.	Y
10.2	**Continual improvement** The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.	**10.2 Nonconformity and corrective action** When a nonconformity occurs, the organization shall: a. react to the nonconformity, and as applicable: 1. take action to control and correct it; 2. deal with the consequences; b. evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1. reviewing the nonconformity; 2. determining the causes of the nonconformity; and 3. determining if similar nonconformities exist, or could potentially occur; c. implement any action needed; d. review the effectiveness of any corrective action taken; and e. make changes to the information security management system, if necessary. Corrective actions shall be appropriate to the effects of the nonconformities encountered. Documented information shall be available as evidence of: f. the nature of the nonconformities and any subsequent actions taken, g. the results of any corrective action.	Y
Annex A			
Annex A	The control objectives and controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2013[1], Clauses 5 to 18 and are to be used in context with Clause 6.1.3.	The information security controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2022[1], Clauses 5 to 8, and shall be used in context with 6.1.3.	See Annex A

27001 GAP ANALYSIS
ANNEX A

intertek
Total Quality. Assured.

Control No.	Control	Applicable	Implementation Status
New Controls			
A.5 Organisational controls			
A.5.7	Threat intelligence -Information relating to information security threats should be collected and analysed to produce threat intelligence.		
A.5.23	Information security for the use of cloud services - Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements		
A.5.30	ICT readiness for business continuity - ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.		
A.7 Physical controls			
A.7.4	Physical security monitoring - Premises should be continuously monitored for unauthorized physical access.		
A.8 Technological controls			
A.8.9	Configuration management - Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.		
A.8.10	Information deletion - Information stored in information systems, devices or in any other storage media should be deleted when no longer required.		
A.8.11	Data masking - Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific, and business requirements, taking applicable legislation into consideration.		
A.8.12	Data leakage prevention - Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.		
A.8.16	Monitoring activities - Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.		
A.8.23	Web filtering - Access to external websites should be managed to reduce exposure to malicious content		
A.8.28	Secure coding - Secure coding principles should be applied to software development.		
Merged Controls			
A.5 Organisational controls			
A.5.1	Policies for information security		
A.5.8	Information security in project management		
A.5.9	Inventory of information and other associated assets		

27001 GAP ANALYSIS
ANNEX A

intertek
Total Quality. Assured.

Control No.	Control	Applicable	Implementation Status
A.5.10	Acceptable use of information and other associated assets		
A.5.14	Information transfer		
A.5.15	Access control		
A.5.17	Authentication information		
A.5.18	Access rights		
A.5.22	Monitoring, review and change management of supplier services		
A.5.29	Information security during disruption		
A.5.31	Legal, statutory, regulatory and contractual requirements		
A.5.36	Compliance with policies, rules and standards for information security		
A.6.8	Information security event reporting		
A.7.2	Physical entry		
A.7.10	Storage media		
A.8.1	User endpoint devices		
A.8.8	Management of technical vulnerabilities		
A.8.15	Logging		
A.8.19	Installation of software on operational systems		
A.8.24	Use of cryptography		
A.8.26	Application security requirements		
A.8.29	Security testing in development and acceptance		
A.8.31	Separation of development, test and production environments		
A.8.32	Change Management		

Renamed controls			
A.5.16	Identity management		
A.5.19	Information security in supplier relationships		
A.5.20	Addressing information security within supplier agreements		
A.5.21	Managing information security in the ICT supply chain		
A.5.24	Information security incident management planning and preparation		

27001 GAP ANALYSIS
ANNEX A

Control No.	Control	Applicable	Implementation Status
A.5.25	Assessment and decision on information security events		
A.5.34	Privacy and protection of PII		
A.6.5	Responsibilities after termination or change of employment		
A.6.7	Remote working		
A.7.1	Physical security perimeters		
A.7.7	Clear desk and clear screen		
A.7.9	Security of assets off-premises		
A.8.14	Redundancy of information processing facilities		
A.8.2	Privileged access rights		
A.8.20	Networks security		
A.8.22	Segregation of networks		
A.8.25	Secure development life cycle		
A.8.27	Secure system architecture and engineering principles		
A.8.33	Test information		
A.8.34	Protection of information systems during audit testing		
A.8.4	Access to source code		
A.8.5	Secure authentication		
A.8.7	Protection against malware		