



INDEPENDENT PRESS STANDARDS ORGANISATION C.I.C.

ISO27001:2013 REMOTE AUDIT REPORT

| | |
|--|---|
| Client Name (As per the Certificate): | Independent Press Standards Organisation C.I.C. |
| Certificate Scope: | Independent Regulator for the Paper and Magazine Industry in the UK |
| Certificate Expiry Date: | 6 th September 2025 |
| Certificate Number: | ISM7799303 |
| Certification Date: | 21 st September 2018 |
| Next Audit Due: | September 2024 |

| | | | |
|-----------------------------------|---|--------------------------|-------|
| Audit Date(s): | 30 th November 2023 | | |
| Time Started: | 10:00 | Time Left Client: | 15:00 |
| Business Contact Name: | Tonia Milton | | |
| Business Contact Details: | Tel: 0300 123 2220 Email: tonia.milton@ipso.co.uk | | |
| Address for Site of Audit: | Gate House 1 Farringdon Street London EC4M 7LG | | |
| Auditor Name(s): | Chris Sheppard | | |

| | | | |
|--|---|----------------|---------------------|
| I confirm that the information in this report is correct and I am happy with the content and conduct of the work carried out and the findings recorded by my appointed Auditor. | | | |
| Client Lead A: | Tonia Milton | Signed: | <i>Tonia Milton</i> |
| Position A: | Head of Systems and Information Security | Dated: | Nov 30, 2023 |
| Notes: | Independent Press Standards Organisation C.I.C. have a fully robust Information Security Management System that meets all the requirements of ISO27001:2013. There were zero non-conformances raised during this audit, with no observations noted. | | |

| | | | | |
|-----------------------------|------------------------------------|---|--|-------------|
| 1 | 2 | 3 | 4 | 5 |
| Unqualified PASS | PASS with Rectification | Probationary PASS with Rectification and Re-inspection within 6 months | Certificate Suspension Subject to Re-inspection within 3 months | FAIL |

INTRODUCTION:

This document has been prepared for you in order to establish your level of compliance against the ISO 27001:2013 Standard. The body of the audit report will contain questions that your auditor will have asked during their visit along with the findings as a result. The identified non-conformances and observations are summarised in the "Report Summary" at the end of this document.

METHOD OF AUDIT:

This audit was conducted remotely; therefore certain assumptions may have been made.

A full analysis of a selection of your operating processes took place against the requirements of the ISO 27001:2013 Standard to prepare this Audit Report, detailing all areas of compliance and non-compliance. This has been obtained through interview, witnessed evidence, sample auditing and site tour.

NB: It may not be possible to identify all existing non-conformances within the organisation as we carry out sample audits.

Based on the auditor's findings, this report has been compiled at the conclusion of the audit and your auditor will have discussed the actions you must address in order to maintain your certification.

AUDIT SUMMARY:

Grade 1 Pass (Full Pass):

Independent Press Standards Organisation C.I.C. has a fully effective management system that meets all of the requirements.

ISO 27001:2013 AUDIT REPORT

REPORT LEGEND:

| | |
|--------------|--|
| PASS | Your Organisation meets the requirements of this section |
| N/A | This section is currently not applicable to your Organisation |
| OBS | Observation |
| MINOR | Minor non-conformance |
| MAJOR | Major non-conformance |

CATEGORISATION OF MAJOR AND MINOR NON-CONFORMANCES AND OBSERVATIONS FOR IMPROVEMENT

Major Non-Conformance – Where you have not complied with a whole clause or sub-clause of the Standard OR the non-conformance has the potential to have a major impact on the organisation. Examples of a Major Non-Conformance include no evidence of Management Review, no evidence of any actions to address risk etc.

Minor Non-Conformance – Where you do not meet some requirements of a whole clause or sub-clause of the Standard but do meets others. Examples of a minor non-conformance could include carrying out the management reviews but not covering all of the review inputs or you have addressed risk and opportunities but not evaluated the effectiveness of the actions taken.

Observations for Improvement – These are areas where your auditor has identified an area of possible improvement within your management system. You should consider these items (usually as part of your management review process) and record your decision as to whether you wish to address such actions.

Categorisation of your pass grade: -

Grade 1: You have no Major or Minor Non-Conformances and your system is fully established and running.

4. Context of the Organisation

4.1 Understanding the Organisation and its context

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|--|----------------------------------|---|-----------|
| 1 | Has the Organisation determined external and internal issues that could affect its ISMS and its ability to achieve compliance to their ISMS and the ISO 27001:2013 Standard? | P | The Scope of the Information Security Management System, (ISMS), confirms that the external and internal issues have been determined and have been documented in the Scope section of the ISMS Manual, (section 5, page 4). | N/A |

4.2 Understanding the needs and expectations of interested parties

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|--|----------------------------------|--|-----------|
| 1 | Has the Organisation determined interested parties relevant to their ISMS? | P | Interested Parties, relevant to the Information Security Management System, have been defined & documented in the Scope. | N/A |
| 2 | Has the Organisation determined the requirements of these interested parties relevant to their ISMS? NB: These may be legal, regulatory or contractual. | P | The requirements of the interested parties, have noted above, have been identified & as noted above. | N/A |

4.3 Determining the scope of the information security management system

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|--|----------------------------------|--|-----------|
| 1 | Has the Organisation determined the scope of the ISMS taking into account the external and internal issues referred to in 4.1, the requirements within 4.2 and the activities of the organisation? | P | The scope has been determined, taking into account the external & internal issues along with the requirements of interested parties, as documented in the Scope. | N/A |

Report Body

4.3 Determining the scope of the information security management system

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|--|----------------------------------|--|-----------|
| 2 | Has this determined scope been documented? | P | The scope has been documented, as noted above, this was evidenced during this audit & found to be in good order. | N/A |

4.4 Information Security Management System

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|---|----------------------------------|--|-----------|
| 1 | Has the organisation established, implemented, maintained and continually improved an ISMS in line with the requirements of ISO 27001:2013? | P | The ISMS has been fully established, implemented, maintained and approved and evidenced during this audit. | N/A |

5. Leadership

5.1 Leadership and commitment

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|---|----------------------------------|---|-----------|
| 1 | Has top management established (i) ISMS objectives and (ii) an ISMS Policy compatible with the strategic direction of the organisation? | P | The organisation has established ISMS Objectives and an Information Security Policy based on the strategic direction of the Organisation. | N/A |
| 2 | Has top management ensured the integration of its ISMS requirements into their organisation's processes? | P | Procedures defined by the organisation have been implemented into the processes of the organisation. | N/A |
| 3 | Are there adequate resources available for the operation of the ISMS? | P | The organisation has ensured that adequate resource is available in order to manage the ISMS. | N/A |

Report Body

5.1 Leadership and commitment

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|---|----------------------------------|---|-----------|
| 4 | Have top management communicated the importance of the effective implementation and management of the ISMS to all interested parties? | P | The principles of the information Security Policy have been communicated to all employees and other interested parties. All employees are aware of the potential consequences of departure from specified operating procedures. | N/A |
| 5 | How do top management ensure that the ISMS achieve its intended outcomes? | P | The organisation has ensured that control methods are in place to achieve the intended outcomes of the ISMS, through the establishment of policies as defined within the Statement of Applicability. | N/A |
| 6 | How does top management direct and support people to contribute to the effectiveness of the ISMS? | P | The organisation has ensured that people are encouraged to contribute to the ISMS through risk assessment & risk treatment. | N/A |
| 7 | How does top management promote continual improvement throughout the organisation? | P | Top management promote continual improvement by establishing and implementing improvement actions at management review. | N/A |
| 8 | How does top management support other management roles as applicable to their individual areas of responsibility? | P | Roles and responsibilities are clearly defined within the Management Responsibilities chart; these are communicated to all staff members. | N/A |

5.2 Policy

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|--|----------------------------------|---|-----------|
| 1 | Has an ISMS Policy been established that; <ul style="list-style-type: none"> • Is appropriate to the purpose of the organisation • Includes ISMS objectives • Includes a commitment to satisfy requirements of the ISMS • Includes a commitment to continual improvement | P | An Information Security Policy has been established & documented; this was evidenced during this audit & found to be in good order. | N/A |

Report Body

5.2 Policy

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|---|----------------------------------|---|-----------|
| 2 | Is / has the ISMS Policy; <ul style="list-style-type: none">• Been documented• Been communicated within the organisation• Available to interested parties | P | An Information Security Policy has been documented and is available to interested parties upon request. | N/A |

5.3 Master roles, responsibilities and authorities

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|---|----------------------------------|--|-----------|
| 1 | Has top management assigned responsibility and authority for roles relevant to information security and communicated them? | P | Yes, the organisation has ensured that responsibilities and authorities within the ISMS have been defined & have been communicated to all staff. | N/A |
| 2 | Has responsibility and authority been assigned to ensure the ISMS conforms to the requirements of ISO 27001:2013? | P | Yes, an ISMS manager has been appointed & assigned responsibility and authority for ensuring the ISMS meets the requirements of ISO 27001:2013 | N/A |
| 3 | Has responsibility and authority been assigned for the reporting on the performance of the ISMS and reporting this to top management? | P | Yes, an ISMS manager has been appointed & assigned responsibility and authority for reporting on the performance of the ISMS. | N/A |

Report Body

6. Planning

6.1 Actions to address risk and opportunities

6.1.1 General

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|--|----------------------------------|--|-----------|
| 1 | Taking into account section 4.1 and 4.2 has planning taken place to determine the risks and opportunities to be addressed in order to ensure the ISMS achieves its intended outcome, prevent or mitigate unwanted effects and achieve continual improvement? | P | Actions to address risks and opportunities have been documented onto the Risk Register. | N/A |
| 2 | How has the organisation planned the actions required to address these risks and opportunities? | P | Actions to address risk are planned and documented as stated above. | N/A |
| 3 | How does the organisation plan to integrate and implement the actions into the ISMS and evaluate the effectiveness of their implementation? | P | Actions to address risk have been implemented into working practice through training and where necessary written into documented procedures. | N/A |

6.1.2 Information security risk assessment

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|--|----------------------------------|--|-----------|
| 1 | Has a risk assessment process been established to identify and maintain the risk acceptance criteria and method for performing risk assessments? | P | Risk analysis, risk acceptance criteria and methods for performing risk assessment have been documented within the Risk Register. This was evidenced during this audit & demonstrates compliance with this clause. | N/A |
| 2 | Do the risk assessments ensure that the results are consistent, valid and comparable? | P | Risk assessments undertaken have been consistent, valid and comparable to the previous risk assessments. The results of risk assessments appear on the Master Risk Register; these were evidenced during this audit & were found to be in good order. | N/A |

Report Body

6.1.2 Information security risk assessment

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|---|----------------------------------|---|-----------|
| 3 | Do the risk assessments identify risks associated with the loss of confidentiality, integrity and availability of information covered within the scope of the certification as well as the owners of that risk? | P | Risk assessments have covered loss of confidentiality, integrity and availability of information. | N/A |
| 4 | Do the risk assessments analyse the potential consequences, likelihood and severity should a risk materialise? | P | Risk assessments carried out have addressed potential consequences, likelihood and severity if the event that they materialise. | N/A |
| 5 | Have the risks been evaluated against the risk criteria in section 6.1.2 (1) and have they been prioritised for treatment? | P | Risk treatment has been prioritised based on the severity of the risk. | N/A |
| 6 | Is there documented evidence to record information about the ISMS risk assessment process? | P | Risk Assessments have been documented as was evidenced during this audit, along with treatment plans. The results of risk assessments have been added to the Risk Register. | N/A |

6.1.3 Information security risk treatment

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|--|----------------------------------|---|-----------|
| 1 | Has the organisation defined and applied a risk treatment process, taking into account the risk assessment results? | P | Risk treatment has been defined and applied in line with the planned actions as documented in the Master Risk Register. | N/A |
| 2 | Has the organisation identified all controls necessary to implement the ISMS risk treatment? | P | All controls have been identified by the organisation, as noted within the Statement of Applicability & demonstrates compliance with this clause. | N/A |
| 3 | Has the organisation compared the controls identified above with the control in the Statement of Applicability to ensure that no controls have been overlooked? | P | A Statement of Applicability has been completed which documents all of the controls applicable to the ISMS. | N/A |
| 4 | Has the organisation produced a Statement of Applicability that contains the necessary justification for inclusion and exclusion as appropriate and the necessary controls required? | P | A Statement of Applicability has been completed; all clauses within Annex A that are not applicable have been noted & justified appropriately. | N/A |

Report Body

6.1.3 Information security risk treatment

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|--|----------------------------------|---|-----------|
| 5 | Has an ISMS treatment plan been formulated? | P | A risk treatment plan has been formulated against the results of analysis against the Statement of Applicability and the Risk Register. | N/A |
| 6 | Has approval been obtained from the risk owners in respect to the information security risk treatment process? | P | The risk owners have approved all actions formulated in the risk treatment process. | N/A |
| 7 | Is there documented evidence available for the risk treatment process? | P | The Risk Register, Risk Assessments & the Statement of Applicability, are available as documented evidence of risk. | N/A |

6.2 Information security objectives and planning

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|---|----------------------------------|--|-----------|
| 1 | Has the organisation established ISMS objectives at relevant functions and levels that are; <ul style="list-style-type: none"> • Consistent with the ISMS policy • Measurable • Applicable to ISMS requirements and take into account risk assessment results and the risk treatment plans • Communicated • Updated periodically as appropriate? | P | ISMS objectives have been established & documented in the Objectives Register, (ISMS03) ; they were evidenced during this audit & demonstrate compliance with this clause. | N/A |
| 2 | Have the above objectives been documented? | P | ISMS Objectives have been documented in the Objectives and KPIs Register , as noted above. | N/A |
| 3 | Has a plan to achieve these objectives been formulated that; <ul style="list-style-type: none"> • Determines what shall be done • Determines the resources required • Determines who will be responsible • Determines time scales for completion • Determines how the results will be evaluated? | P | Objectives have been defined as noted above & meet all of the requirements of this clause. | N/A |

Report Body

7. Support

7.1 Resources

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|--|----------------------------------|---|-----------|
| 1 | Has the organisation determined and provided resources necessary for the establishment, implementation, maintenance and continual improvement of the ISMS? | P | Human and physical resource has been provided as required for the establishment and implementation of the ISMS. | N/A |

7.2 Competence

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|---|----------------------------------|--|-----------|
| 1 | Has the organisation determined the competency requirements for people under its control who affect the ISMS? | P | Competency requirements are established through Job descriptions & the establishment of a Staff Training Log | N/A |
| 2 | Are these people competent based on appropriate education, training or experience? | P | Job descriptions, as noted above, establish the competency requirements for each role within the organisation. | N/A |
| 3 | Where competency is not at the desired level are actions taken to acquire the necessary competence and to evaluate those actions taken? | P | Additional training is provided where there is a lack of competence and records retained. | N/A |
| 4 | Has documented evidence of the above been recorded and retained? | P | Documented evidence of training & competencies are noted in the Staff Training Log; this was viewed during this audit & found to be in good order. | N/A |

Report Body

7.3 Awareness

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|---|----------------------------------|---|-----------|
| 1 | Persons doing work under the organisations control must be aware of; <ul style="list-style-type: none">• the ISMS Policy• their contribution to the effectiveness of the ISMS including the benefits of improved ISMS performance• the implications of not conforming with the ISMS requirements. | P | The Information Security Policy has been communicated to all staff as part of the induction process. The organisation ensures they are aware of their contribution to the effectiveness of the ISMS and the implications of not conforming to its requirements. | N/A |

7.4 Communication

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|---|----------------------------------|---|-----------|
| 1 | In relation to internal and external communication relevant to the ISMS, has the organisation determined; <ul style="list-style-type: none">• what to communicate• when to communicate• with whom to communicate• who shall communicate• the process by which communication is affected | P | Items to be communicated and the method by which they are communicated is determined by the ISMS manager. | N/A |

7.5 Documented information

7.5.1 General

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|---|----------------------------------|---|-----------|
| 1 | Does the organisations ISMS include documented information required by the ISO 27001:2013 Standard? | P | All documentation pertaining to the ISMS is in place & meets all the requirements required by the Standard. | N/A |
| 2 | Do the organisations ISMS include other documented information necessary in order for the ISMS to be effective? | P | All other documents required for the effective implementation of the ISMS are in place. | N/A |

Report Body

7.5.2 Creating & Updating

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|--|----------------------------------|---|-----------|
| 1 | <p>Has the organisation ensured all documents are;</p> <ul style="list-style-type: none"> • identifiable and descriptive (e.g., title, date, author, reference etc) • appropriately formatted for use (e.g., language, software version, paper, electronic etc) • reviewed and approved for suitability and adequacy? | P | All documents and records viewed at this audit were suitably identified through the document names. Documents are electronic & all documents have been reviewed for suitability by the Information Security Manager | N/A |

7.5.3 Control of documented information

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|--|----------------------------------|--|-----------|
| 1 | Are all documents required by the ISMS controlled and available and suitable for use where and when it is needed? | P | All documents are available at the point of use; this was demonstrated through the documents viewed during this assessment. Documented Information is controlled through the implementation of a Master Document List & are additionally controlled at document level. | N/A |
| 2 | Are all documents required by the ISMS adequately protected from loss of confidentiality, improper use or loss of integrity? | P | Documents are protected through permission settings, to Google Drive, restricting editable access only to those who are authorised. | N/A |
| 3 | <p>As part of the document control process has the organisation taken into account;</p> <ul style="list-style-type: none"> • the distribution, access, retrieval and use • storage and preservation (including legibility) • control of changes • retention and disposition? | P | As noted above; all documents are controlled, thus demonstrating compliance with the requirements of this clause. | N/A |
| 4 | Are documents of external origin, necessary to form part of the planning and operation of the ISMS, identified and controlled as appropriate? | P | Documents of an external origin are controlled in line with internal documents and are subject to regular review to ensure they are up to date and relevant | N/A |

8. Operation

8.1 Operational planning and control

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|---|----------------------------------|--|-----------|
| 1 | Has the organisation planned, implemented and controlled the processes needed to meet information security requirements? | P | All actions planned as a result of the risk assessment process have been implemented and controlled. Work processes have been adopted, controlled and reviewed to ensure that they meet the ISMS requirements. | N/A |
| 2 | Has the organisation implemented plans to achieve ISMS objectives? | P | Specific Information Security Objectives have been established as noted in section 6.2 of this report. | N/A |
| 3 | Has the organisation retained documented information in order to be confident that processes have been carried out as planned? | P | Records have been established to demonstrate that processes have been carried out as planned. | N/A |
| 4 | Has the organisation controlled planned changes and reviewed the consequences of unintentional changes, as well as taking action to mitigate any adverse effects of unintentional change? | P | Planned and unplanned changes have been reviewed at Management Review to ensure that there is no adverse impact on the ISMS. | N/A |
| 5 | Has the organisation ensured that any outsourced processes are determined and controlled? | P | Outsourced processes are controlled through 3 rd Party Supplier Agreements | N/A |

8.2 Information security risk assessment

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|---|----------------------------------|---|-----------|
| 1 | Has the organisation performed information security risk assessments at planned intervals and when significant changes occur? | P | ISMS risk assessments have been performed at planned intervals and when significant changes occur. These were viewed during this assessment as noted previously in this report. | N/A |
| 2 | Has the organisation retained documented evidence of the results of the information security risk assessments? | P | Documented risk assessments are in place, as noted previously in this report. The Master Risk Register has been implemented to demonstrate compliance. | N/A |

Report Body

8.3 Information security risk treatment

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|--|----------------------------------|---|-----------|
| 1 | Has the organisation implemented the security risk treatment plan? | P | As noted previously in this report, Risk Assessments have been defined & fully implemented. Evidence of this was viewed at this audit. | N/A |
| 2 | Has the organisation retained documented evidence of the results of the information security risk treatment? | P | Risk Assessment Records have been produced to demonstrate evidence of security risk treatment. Assessments were viewed during this audit & demonstrate compliance with this clause. The organisation has implemented a Business Continuity Plan, (ISMS08), this was evidenced during this audit & found to be in good order. | N/A |

9. Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|--|----------------------------------|---|-----------|
| 1 | Has the organisation evaluated the performance of the ISMS by determining; <ul style="list-style-type: none"> • what is to be monitored and measured, including processes and controls • the method for monitoring, measurement, analysis and evaluation to ensure valid results • when monitoring and measurement should be performed • who shall carry out monitoring and measurement? • when results should be analysed and evaluated • who is responsible for analysis and evaluation? | P | The Organisation have monitored and measured their performance against the risk treatment plan and the Statement of Applicability. | N/A |
| 2 | Has the organisation retained documented information to provide evidence of the above? | P | Records have been produced to provide evidence of the monitoring and measurement that has taken place. These are in the form of Management Review Meeting Minutes & Internal Audit Reports. | N/A |

Report Body

9.2 Internal Audit

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|---|----------------------------------|---|-----------|
| 1 | Has the organisation conducted internal audits at planned intervals that ensures the ISMS conforms to the organisations and the ISO 27001:2013 requirements? | P | Internal audits have been conducted covering all of the requirements of the standard, in line with the schedule. | N/A |
| 2 | Has the internal audit process been effectively implemented and maintained? | P | The internal audit schedule has been effectively maintained by the organisation. | N/A |
| 3 | Has the organisation planned, established and maintained an audit programme to include the frequency, methods, responsibilities, planning requirements and reporting? | P | The internal audit plan has been established & covers the elements required by this clause. | N/A |
| 4 | Does the audit programme take into consideration the importance of the processes concerned and the results of previous audits? | P | Internal audits take into account the importance of the process & the results of previous audits. | N/A |
| 5 | Has the audit criteria and scope been defined for each audit? | P | The audit report defines the audit criteria and scope for each audit | N/A |
| 6 | Have the auditors been selected to ensure objectivity and impartiality of the audit process? | P | Internal auditors are independent of the process being audited. | N/A |
| 7 | Have the results of the audit been reported to relevant management? | P | Internal audits carried are presented as input to the management review process. | N/A |
| 8 | Is there documented evidence of the audit programme and audit results? | P | The Internal Audits provide documented evidence of internal audit results. Internal audits have been conducted against the clauses within ISO27001:2013 & the organisation's Statement of Applicability. Internal audit reports were evidenced during this audit & were found to be in good order. | N/A |

Report Body

9.3 Management review

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|--|----------------------------------|--|-----------|
| 1 | Has top management carried out a review of the ISMS at planned intervals to ensure its continued suitability, adequacy and effectiveness? | P | Management Review Meetings have been carried out at quarterly intervals to ensure compliance with this . clause. | N/A |
| 2 | Has the management review taken into consideration; <ul style="list-style-type: none"> • the status of actions from previous management reviews • changes in external and internal issues relevant to the ISMS • feedback on the performance of the ISMS including NCR's and corrective actions, monitoring and measurement results, audit results and fulfilment of information security objectives. • feedback from interested parties • results of risk assessments and status of risk treatment plans • opportunities for continual improvement? | P | Management reviews follow an established agenda that covers all of the elements required by this clause. | N/A |
| 3 | Do the outputs of the management review include decisions related to continual improvement opportunities and the need for change to the ISMS? | P | Management reviews include decisions related to continual improvement opportunities and the need for change to the ISMS. | N/A |
| 4 | Has the organisation established documented evidence of the results of the management review process? | P | <p>Management Reviews are conducted on a monthly basis; the following</p> <p>The following Meeting minutes were evidenced during this audit & were found to be in good order:</p> <ul style="list-style-type: none"> • 18th May 2023 • 23rd November 2023 <p>In addition, an annual review of the ISMS was conducted on 23rd November 2023; minutes of this review was evidenced & found to be in good order.</p> | N/A |

Report Body

10. Improvement

10.1 non-conformity and corrective actions

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|---|----------------------------------|--|-----------|
| 1 | In the event of a non-conformity, has the organisation taken action to control and correct it and deal with the consequences? | P | The organisation has established a procedure for reporting information security events. | N/A |
| 2 | Has the organisation evaluated the need to eliminate the causes of the non-conformity to ensure that it does not recur or occur elsewhere by; <ul style="list-style-type: none">• reviewing the non-conformity• determining the cause• determining whether similar non-conformities exist or could potentially occur? | P | Root cause analysis is carried out as part of the investigative process of non-conformances or security incidents, as appropriate. | N/A |
| 3 | Has the organisation implemented any action needed? | N/A | There have been no non-conformances raised against the ISMS during the current audit period. | N/A |
| 4 | Has the effectiveness of any corrective action been reviewed? | N/A | There have been no non-conformances raised against the ISMS during the current audit period. | N/A |
| 5 | Has the organisation made changes to the ISMS, as a result of a non-conformance, where necessary? | N/A | Changes to the Management System have not been required as a result of non-conformance. | N/A |
| 6 | Are the corrective actions appropriate to the effects of the non-conformity? | N/A | There have been no non-conformances raised against the ISMS during the current audit period. | N/A |
| 7 | Has the organisation established documented information as evidence of the occurrence, investigation and actions taken as a result of a non-conformance? | N/A | There have been no non-conformances raised against the ISMS during the current audit period. | N/A |
| 8 | Has the organisation established documented information as evidence of the results of any corrective action? | N/A | There have been no non-conformances raised against the ISMS during the current audit period. | N/A |

Report Body

10.2 Continual improvement

| | QUESTION | STATUS P-PASS, F-FAIL, n/a | EVIDENCE AUDITED / FINDINGS | NCR TABLE |
|---|--|----------------------------------|---|-----------|
| 1 | Has the organisation continually improved the suitability, adequacy and effectiveness of the ISMS? | P | Continual improvement has been evidenced by way of implementation of the management review, internal audit, and risk treatment processes. | N/A |

Report Summary

MAJOR NON-CONFORMANCE SUMMARY

| Clause(s) | Nature of Non-Conformance | Agreed Actions to Remedy | Responsibility |
|-----------|---------------------------|--------------------------|----------------|
| | NONE | | |

The items above **MUST** be rectified prior to obtaining and retaining certification. You will not achieve certification unless evidence of the rectification of the non-conformances above are provided to your certification auditor.

MINOR NON-CONFORMANCE SUMMARY

| Clause(s) | Nature of Non-Conformance | Agreed Actions to Remedy | Responsibility |
|-----------|---------------------------|--------------------------|----------------|
| | NONE | | |

The items above **MUST** be rectified prior to your annual external audit by CQS. Your grade of pass will depend on you rectifying these points.

Opportunities for Improvement Summary

| Clause(s) | Nature of Observation | Agreed Actions to Remedy (if required) | Responsibility |
|-----------|-----------------------|--|----------------|
| | NONE | | |

The items above should be considered prior to your annual external audit by CQS.






Independent Press Standards Organisation - ISO 27001_2013 Remote Audit Report 30112023 CS

Final Audit Report

2023-11-30

| | |
|-----------------|---|
| Created: | 2023-11-30 |
| By: | Audits Department (audits@cqsltd.com) |
| Status: | Signed |
| Transaction ID: | CBJCHBCAABAAQGGJut87AcdOwP1LklinSSVxssXe-x4be |

"Independent Press Standards Organisation - ISO 27001_2013 Remote Audit Report 30112023 CS" History

-  Document created by Audits Department (audits@cqsltd.com)
2023-11-30 - 2:28:55 PM GMT- IP address: 86.146.122.47
-  Document emailed to Tonia Milton (tonia.milton@ipso.co.uk) for signature
2023-11-30 - 2:46:50 PM GMT
-  Email viewed by Tonia Milton (tonia.milton@ipso.co.uk)
2023-11-30 - 3:32:32 PM GMT- IP address: 20.0.41.83
-  Document e-signed by Tonia Milton (tonia.milton@ipso.co.uk)
Signature Date: 2023-11-30 - 3:33:48 PM GMT - Time Source: server- IP address: 20.0.41.83
-  Agreement completed.
2023-11-30 - 3:33:48 PM GMT