ISO 27001 : 2013

Annual Surveillance Audit Report for Lynq Limited

Date of Audit:	02/05/2023
Auditor:	David Wilson
Client Reference Number:	38848

Introduction

This report outlines the Citation ISO Certification external audit of your Management System which took place on 02/05/2023and outlines our key findings, recommendations and, where appropriate, nonconformities found. Please read this report carefully prior to contacting Citation ISO Certification for further support and guidance.

This report has been completed by David Wilson (the Citation ISO Certification Auditor) and reviewed by Ellen Folkard (the Citation ISO Certification Reviewer in our Technical Department).

Audit Location:	Lancaster Court 8 Barnes Wallis Road Fareham Hampshire PO15 5TU
Audit Type:	ISO Annual Visit
Standard:	ISO 27001 : 2013

Audit Criteria

An Audit carried out in line with the Citation ISO Certification External Audit Programme against the Management System processes and procedures documented by the Organisation, based on the requirements of the Standard.

Audit Objectives

- To confirm that the requirements of the management system standard are effectively addressed by the Organisation's Management System in accordance with the Audit Criteria.
- To confirm the ability of the Management System to ensure that the Organisation meets applicable statutory, regulatory and contractual requirements and meets its specified objectives.
- To identify areas for potential improvement of the Management System.

Audit Methodology

This Audit has been based on Random Sampling methodology and does not exclude the possibility that other nonconformances may exist.

All identified nonconformances and other recommendations are subject to review and ratification by the Technical Department of Citation ISO Certification.

Nonconformity

During the audit, the Auditor will be reviewing the evidence that you supply to them to assess whether you are following your Management Systems procedures and processes against the requirements of the International Standard.

Should the auditor identify an area of the Management System which does not meet the requirements of the standard and/or your Management System procedures/processes, they may raise a Nonconformity, Observation or Opportunity for Improvement.

Any Major Nonconformities will result in a failed audit grade pending corrective action and the submission of rectification evidence to Citation ISO Certification for review.

Any Minor Nonconformities will result in an audit grade of 'pass subject to rectification'. In this case, we will review your rectification evidence for this Minor Non-conformity at the next Annual Surveillance Audit.

Non-conformities can be defined as:

Major Nonconformity:	A Major Nonconformity usually leads to the break down of the Management System in achieving its intended results. For Major Nonconformities, the Organisation is expected to address this nonconformity using the corrective action process as soon as possible. Records are to be maintained to detail the corrective action taken and its effectiveness to analyse the cause and prevent reoccurrence. Rectification evidence is to be submitted via email to ISOrectifications@citation.co.uk within 60 days of the audit (this audit took place on 02/05/2023).
Minor Nonconformity:	A Minor Nonconformity would be the failure to conform to one of the requirements of the International Standard that is not likely to result in a failure of the management system. It may be a single observed lapse or isolated incident where there is minimal risk of the break down of the Management System. For Minor Nonconformities, the Organisation is expected to address this nonconformance using the nonconformity and corrective action processes as soon as possible. Records are to be maintained to detail the corrective action taken and its effectiveness to analyse the cause and prevent reoccurrence. Citation ISO Certification will review rectification evidence for Minor Nonconformities at the next annual surveillance audit.
Observation:	An Observation is an area of the Management System which could be improved and if not rectified, may result in a Minor Nonconformity in the future if not addressed. For Observations, the Organisation is expected to consider taking action to address the recommendations suggested by the Auditor to aide continual improvement over time.
Opportunity for Improvement:	Opportunities for Improvement are areas of the Management System or the wider operation of the Organisation which the Auditor feels would benefit from additional improvements. Where appropriate, Auditors may provide a number of Opportunities for Improvement which are submitted in the body of the audit report to provide additional assistance and guidance for the Organisation to consider.

Audit Grading

Your audit result can be found at the end of this report. The following actions are required depending on the grade awarded:

PASS	No further action required by the Organisation.
PASS SUBJECT TO RECTIFICATION	Minor Nonconformities have been identified during the audit which are to be rectified prior to the next Citation ISO Certification external audit.
FAIL	Major Nonconformities have been identified during the audit which are to be rectified and evidence submitted to Citation ISO Certification within 60 days of 02/05/2023. Rectification evidence is to be emailed to ISOrectifications@citation.co.uk.

Audit Report Acceptance

You have 30 days from 02/05/2023 to raise any disputes with any of the findings, Nonconformities or other information contained in this report. After 30 days, we will automatically confirm your receipt and acceptance of this report.

If you have a concern or would like any clarification on the content of this report, please contact one of our Technical Liaison Officers who will be happy to assist you.

Support and Assistance

If you have failed your audit and you require any additional assistance or advice and guidance about how to take corrective action to rectify nonconformities, please contact one of our Technical Liaison Officers who will be happy to help you.

	New	Outstanding
Non Compliance - Major	0	0
Non Compliance - QMS to address immediately	0	0
Non Compliance - Minor	0	0
Positive observations	52	

Opening Meeting Attendees	
Name	**Job title**
David Wilson	Auditor
Sarah Paradise-Brown	Chief Operating Officer

Annual Audit Mandatory Topics

Positive observations		
Audit item	**Process audited**	**Evidence findings**
Is the client aware of the Certification Representation Policy and Brand Guidelines?	Certification Representation Policy	This was observed as being followed at the time of this audit.
Are Certification Marks being used correctly?	Certification Marks	This was observed as being followed at the time of this audit.
Is the management system suitable to fulfil relevant statutory, regulatory and contractual requirements and the objectives of the management system?	Statutory, Regulatory and Contractual requirements	This was observed as being followed at the time of this audit.
All subjects from the audit plan and program were evaluated.	Audit plan and programme evaluation	All subjects from the audit plan and programme were evaluated.
Changes in the management system were evaluated?	Changes in the Management System	Changes in the Management System have been evaluated and recorded appropriately.
Corrective actions as a result of nonconformities from the previous audit were evaluated.	Corrective actions from nonconformities from previous audit	All previous nonconformities have been rectified by the Organisation.

ISO 27001:2013 Management System - Section 4 Context of the Organisation

Positive observations		
Audit item	**Process audited**	**Evidence findings**
Context of the Organisation	4.1 Understanding the Organisation 4.2 Understanding the needs and expectations of Interested parties 4.3 Determining the Scope	The Scope of the ISMS remains as defined in the Certificate narrative: **'Developer and systems integrator of manufacturing software and supply chain platforms incorporating the requirements of ISO/IEC 27017:2015 and ISO/IEC 27018:2020'**. This fully covers all required aspects of the Organisation and is suitable for the purposes of certification to BS ISO/IEC 27001:2013. Interested parties have been identified together with their requirements as detailed in the viewed Interested Parties Log held in Atlas ISO. These include: • Certification Body • Employees • Shareholders • Customers • Partners • Sub Contractors. SWOT and PEST analysis has been completed by the Organisation as viewed on registers held within Atlas ISO.

		The Organisation Detailed Information Assets Register was viewed at the time of this audit.
Context of the Organisation	4.4 ISMS System	The ISMS Manual fully meets the requirements of BS ISO/IEC 27001:2013. The ISMS is held within Atlas ISO with changes controlled through the functionality of the platform.

ISO 27001:2013 Management System - Section 5 Leadership

Positive observations		
Audit item	**Process audited**	**Evidence findings**
Leadership	5.1 Leadership and commitment	The significance of the ISMS to the Organisation is demonstrated through the completion and monitoring of the Information Assets Register, the integration of policies included in Annex A and the regular review of operational procedures.
Leadership	5.2 Security Policy A.5.1.1 Policies for Information Security	Viewed the ISMS Policy which is held in the ISMS Manual which was determined to be both current and relevant. This was approved by S.P.B. and defines the Organisation's commitment to determining and fulfilling customer needs and expectations and fulfilling statutory and regulatory requirements. All other ISMS policies are up to date and are reviewed. All policies are made available to staff and acceptance of policies is recorded by the Organisation.
Leadership	5.3 Roles and Responsibilities A.6.1.1 Information Security Roles and Responsibilities	A current Management Structure Chart of the ISMS Committee is included in the ISMS together with the basic responsibilities attached to each role. This was determined to be both current and relevant.

ISO 27001:2013 Management System - Section 6 Planning

Positive observations		
Audit item	**Process audited**	**Evidence findings**
Planning	6.1 Actions to address risk and opportunity 6.2 Security Objectives and control	The Risk Assessments and Risk Treatments as detailed in Annex A have been reviewed and presented clearly and agreed as requiring no action. This has been evidenced through various documents viewed at the time of this audit: • ISMS policies • Business Continuity Plan • Incident Reporting • Asset Register • Organisation's Risk Register • PEST Analysis • SWOT Analysis • Management Review meetings. Objectives have been defined and documented on the viewed Objectives Register as viewed at the time of this audit with 11 identified ISMS Objectives.

ISO 27001:2013 Management System - Section 7 Support

Positive observations		
Audit item	**Process audited**	**Evidence findings**
Support	7.1 Resources	Resources are identified as an integral part of the day-to-day management of operations as well as part of Operational Review meetings.
Support	7.2 Competence 7.3 Awareness A.7.2.2 Information security awareness, education and training	Training records are maintained in accordance with the Organisation's training procedures. Training is held within Atlas (training platform) viewed at the time of this audit that included: Training: Information Security Name: N.P., T.C. & B.G Training: General Data Protection Regulations (GDPR) Name: M.R., A.B. & B.G. Training: Security Training - BSG Name: S.P.B. & D.P.
Support	7.5 Documented Information	All records pertaining to the correct procedures of ISMS were presented at the time of this audit and are retained by the Organisation.

ISO 27001:2013 Management System - Section 8 Operation

Positive observations		
Audit item	**Process audited**	**Evidence findings**
Operation	8.1 Operational Planning and Control 8.2 Information Security Risk Assessment	The Risk Assessments and Risk Treatments as detailed in Annex A have been reviewed and presented clearly and agreed as requiring no action.
Operation	8.3 Information Security Risk Treatment	This has been evidenced through various documents viewed at the time of this audit including the Asset Register, Risk Register, Objectives and ISMS policies and procedures.

ISO 27001:2013 Management System - Section 9 Performance Evaluation

Positive observations		
Audit item	**Process audited**	**Evidence findings**
Performance Evaluation	9.1 Monitoring, measurement, analysis and evaluation 9.2 Internal audit A.12.7 Information Systems Audit Considerations A.18.2.3 Technical Compliance Review	Internal ISMS Audits have been completed during the audit period. The Organisation have detailed Individual Internal Audit reports for the required processes of the Standard. All audits are scheduled using an Internal Audit Schedule as viewed. Individual Audits viewed were completed by M.F. (Business Systems Analyst). These were conducted between September 2022 and March 2023. No significant issues were documented.
Performance Evaluation	9.3 Management Review	A Management Review is held at a minimum of six-monthly intervals with a clear Management Review Agenda being followed. The meeting minutes presented at this audit meet the criteria of the BS ISO/IEC 27001:2013 Standard. Meeting minutes viewed for Management Review meetings held on: • 2nd September 2022 • 4th April 2023.
Performance Evaluation	A.9.3.1 Data Protection	The Organisation is registered under the Data Protection Act 2018. Viewed details by visiting the ICO website that the registration is

	A.18.1.4 Privacy and protection of personally identifiable information	current and as follows: Registration Number: ZA010086 Date Registered: 23 July 2013 Registration Expires: 22 July 2023 Data Controller: Lynq Limited.

ISO 27001:2013 Management System - Section 10 Improvement

Positive observations		
Audit item	**Process audited**	**Evidence findings**
Improvement	10.1 Nonconformity and corrective action	The Organisation records nonconformances on a Nonconformance Log as viewed at the time of this audit. The viewed nonconformances related to ISMS have been documented with the investigation and corrective action taken recorded. There have been eight recordable nonconformances in the audit period dated.
Improvement	10.2 Continual improvement	The Organisation continues to demonstrate improvements to its Management System identified as a result of the findings of Internal Audits, Management Reviews and the continual development of the Organisation's Management System.

ISO 27001:2013 Management System - Statement of Applicability - A.5

Positive observations		
Audit item	**Process audited**	**Evidence findings**
A.5 Information security policies	A.5.1 Management direction for information security	All policies have been reviewed as part of the Management Review and Internal Audit Schedule. Viewed a comprehensive Policy Library of current and applicable policies at the time of this audit.

ISO 27001:2013 Management System - Statement of Applicability - A.6

Positive observations		
Audit item	**Process audited**	**Evidence findings**
A.6 Organisation of information security	A.6.1 Internal organisation	Information Security requirements are controlled by defined responsibilities of the ISMS Committee.
A.6 Organisation of information security	A.6.2 Mobile devices and teleworking	The Organisation only uses Laptops and Mobile Phones for mobile working. All matters of mobile working are addressed by the Organisation following their Remote Access and Mobile Computing Policy, which were viewed at the time of this audit. Laptops are currently encrypted with BitLocker and monitored through Sophos Endpoint Protection and Microsoft Defender with alerts reported to a dedicated email address.

ISO 27001:2013 Management System - Statement of Applicability - A.7

Positive observations		
Audit item	**Process audited**	**Evidence findings**
A.7 Human resource security	A.7.1 Prior to employment A.7.2 During employment	Screening (pre-employment) takes place as required and as per the Organisation's recruitment procedure and is all held in the individual Employment file. As a minimum Proof of eligibility to work is obtained via checking of a Passport/Visa, Employment History and DBS checks. DBS check viewed for C.J. dated 7th April 2021 (001009981174) at the time of this audit. As discussed, Terms and conditions of employment are given to each employee as per HR procedures. Confidentiality Agreements are an inherent part of the recruitment process and are recorded on the viewed Confidentiality Agreement, viewed for P.B. (30th March 2023) and T.C. (30th March 2023) at the time of this audit. Induction checklist viewed at the time of this audit for K.P. (2nd May 2022), V.K. (12th September 2022) and B.B. (10th October 2022).
A.7 Human resource security	A.7.3 Termination and change of employment	Viewed the Organisation's staff termination checklist held at the time of this audit. The checklist viewed includes the following: • Return of Office Keys

		• Return of Company Owned Equipment • Confirm that Confidentiality Agreements remain in force as signed • Confirm that IP and Copyright Rules remain in force as signed • Provide Copy of Employment Contract highlighting Confidentiality Clauses • Termination Payment Arrangements (as per termination letter) • Termination Interview • IT Administration Change Request (Remove Network Access Rights, Diversion of Email). Viewed at the time of this audit: Name: P.H. Date: 12th January 2023 Name: D.G. Date: 29th April 2022 Name: P.V. Date: 29th April 2022

ISO 27001:2013 Management System - Statement of Applicability - A.8

Positive observations		
Audit item	**Process audited**	**Evidence findings**
A.8 Asset management	A.8.1 Responsibility for assets A.8.1.1 Inventory of assets	An inventory of assets is maintained by the ISMS Manager in the form of an Assets Register and Risk Register document, complete with risk values, probability values, Threat Analysis and Treatment Plans. The Organisation's Register viewed was confirmed as current and up to date.
A.8 Asset management	A.8.2 Information classification	Information is classified in terms of its value, sensitivity and criticality to the Organisation as viewed at the time of this audit. This was observed through various documents viewed at the time of this audit.
A.8 Asset management	A.8.3 Media handling A.8.3.1 Management of Removable Media A.8.3.2 Disposal of Media	Removable Media is not permitted with all devices restricted. No confidential material is transferred. All Laptops are protected with encryption (BitLocker) and are controlled through viewed policies throughout the Organisation. The Organisation has not had to destroy any equipment through WEEE, there is an Asset Disposal Log in place if required.

ISO 27001:2013 Management System - Statement of Applicability - A.9

Positive observations		
Audit item	**Process audited**	**Evidence findings**
A.9 Access control	A.9.1 Business requirements of access control A.9.1.1 Access Control Policy	The Organisation reside in a serviced building managed by the Business Centre. Physical controls discussed include: • Main Reception • Keys and Fob controlled access • No server room as the Organisation is 100% cloud supported.
A.9 Access control	A.9.2 User access management A.9.3 User responsibilities	Access is identified by the ISMS Committee and given to staff as part of the Induction/New Starter process. Controls of access are in place throughout the Organisation and satisfy the requirements of the BS EN ISO 27001:2013 Standard. User responsibilities are being followed as per the ISMS system and in particular the Password Control Policy.
A.9 Access control	A.9.4 System and application access control A.9.4.2 Secure Login Procedures A.9.4.3 Password Management System	The Organisation operates a standard network log-on. Each member of staff has a distinct username and password. Login routines are addressed in the Organisation's Access Control and Password Policy. I.P. address connections are typically issued by the system (i.e. DHCP).

		User passwords are a combination of alpha and numeric characters to a defined minimum length and domain passwords. Viewed the Organisation's Password Policy at the time of this audit.
A.9 Access control	A.9.4.5 Access control to program source code	DevOps repositories are used to store and control developer access to program source code generated in the Organisation as applicable to the software being developed.

ISO 27001:2013 Management System - Statement of Applicability - A.10

Positive observations		
Audit item	**Process audited**	**Evidence findings**
A.10 Cryptography	A.10.1 Cryptographic controls	Where required, cryptography is used for connectivity. Cryptographic keys are applied via the software used for generation.

ISO 27001:2013 Management System - Statement of Applicability - A.11

Positive observations		
Audit item	**Process audited**	**Evidence findings**
A.11 Physical and environmental security	A.11.1 Secure areas A.11.1.6 Delivery and Loading Areas	This is not currently applicable. Continuing inapplicability is addressed as a part of the Management Review process
A.11 Physical and environmental security	A.11.2 Equipment A.11.2.2 Supporting Utilities A.11.2.5 Removal of Assets A.11.2.8 Unattended User Equipment A.11.2.9 Clear Desk and Clear Screen Policy	All cloud services are to industry standards and the service provider has contractual responsibility for the maintenance of continuous power supplies and supporting utilities. No property can be removed from the Organisation without express permission unless it is issued equipment. The Organisation ensure that equipment is not left unattended through manually locking work sessions or enforced timeout limits (currently 60 mins). This is set at a more aggressive time-out for developers. A Clear Desk Policy is currently in place with particular care taken that personal data (as defined for GDPR) is not left unattended.

ISO 27001:2013 Management System - Statement of Applicability - A.12

Positive observations		
Audit item	**Process audited**	**Evidence findings**
A.12 Operations security	A.12.1 Operational procedures and responsibilities A.12.1.1 Documented Operations Procedures A.12.1.2 Change Management	Version control has been established and continues to be maintained in accordance with the specifications of the BS EN ISO 27001: 2013 Standard. Many approved documented operational procedures were observed at the time of this audit with full version control. The Organisation has a full change request procedure in place: • Dynamics • Jira. Jira change tickets viewed at the time of this audit: Ref: SLQ-571 Date: 28th April 2023 Ref: SLQ-570 Date: 25th April 2023
A.12 Operations security	A.12.1.4 Separation of Development, Testing & Operational Environment	Separation of development, testing and deployment is clearly identified and controlled through isolated environments.
A.12 Operations security	A.12.2 Protection from malware A.12.3 Backup	Hardware and software firewalls and virus protection programs are run continuously. The logs for these are checked on a regular basis and any

		significant reports are investigated with the use of Intune. The security currently used by the Organisation is Sophos Endpoint Protection and Microsoft Defender.
A.12 Operations security	A.12.4 Logging and monitoring	Certain logs may be monitored through the functionality of Intune with escalation to the ISMS Committee as and when required, e.g. signs off unexpected activity.
A.12 Operations security	A.12.6 Technical vulnerability management	All technical vulnerability issues identified are the responsibility of the ISMS Committee. Pentesting has been completed by the Organisation: Date: 24th April 2023 Results: 4 Medium and 7 Low.
A.12 Operations security	A.12.7.1 Information Systems Audit Control	When applicable, patches to the system are tried and tested before introduction to the main systems.

ISO 27001:2013 Management System - Statement of Applicability - A.13

Positive observations		
Audit item	**Process audited**	**Evidence findings**
A.13 Communications security	A.13.1 Network security management A.13.1.2 Security of network services	IP Address connections are dynamically issued by the system (DHCP) for the Desktops and have password and user name controls for connectivity to other systems and services. No direct (back-end) External customer access is made available to the Organisation's head office system or cloud systems. HTTPS and VPN connections are engaged where required. MFA is used when required.

ISO 27001:2013 Management System - Statement of Applicability - A.14

Positive observations		
Audit item	**Process audited**	**Evidence findings**
A.14 System acquisition, development and maintenance	A.14.1 Security requirements of information systems A.14.1.2 Securing application services on public networks	All information passing over public networks when required is protected from fraudulent activity and unauthorised disclosure and modification.
A.14 System acquisition, development and maintenance	A.14.2 Security in Development and support processes A.14.2.1 Secure Development Policy	A secure development procedure is in place and documented that includes a process for relevant key stages and associated testing and sign-off. Development is tracked through Jira and Azure DevOps. Viewed DevOps at the time of this audit: Date: 29th April 2023 Release No: 27 Pipeline: X10mes-test01-lynqcorp Date: 29th April 2023 Release No: 256 Pipeline: Release-Prod-PlatformPre
A.14 System acquisition, development and maintenance	A.14.3 Test data	The Organisation's test data is protected before use by any application, with 'dummy' data used. The security measures of each system ensure the protection of the data used.

ISO 27001:2013 Management System - Statement of Applicability - A.15

Positive observations		
Audit item	**Process audited**	**Evidence findings**
A.15 Supplier relationships	A.15.1 Information Security in supplier relationships A.15.2 Supplier service delivery management	Confidentiality Agreements are in place with third party service providers as a component of the Contract and/or Service Level Agreement. Viewed the following templates at the time of this audit: • Transfer of License Form • Terms and Conditions Cloud Services • Terms and Conditions Software and Support • Data Processing Agreement Cloud Services • Data Processing Agreement Support and Professional Services.

ISO 27001:2013 Management System - Statement of Applicability - A.16

Positive observations		
Audit item	**Process audited**	**Evidence findings**
A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	All incidents are recorded by the Organisation and reviewed on the Nonconformance Log. There have been eight recordable nonconformances in the audit period dated.

ISO 27001:2013 Management System - Statement of Applicability - A.17

Positive observations		
Audit item	**Process audited**	**Evidence findings**
A.17 Information security aspects of business continuity management	A.17.1 Information security continuity A.6.1.3 Contact with authorities	A Business Continuity Plan document is in place. This includes procedures for the timely restoration of business following interruption or failure of critical business processes. This was last reviewed on the 30th November 2022. Business Continuity Testing scenarios have been completed in the audit period: • Lynq Saas Platform - January & February 2023 • Offices Services (UK) - December 2022.

ISO 27001:2013 Management System - Statement of Applicability - A.18

Positive observations		
Audit item	**Process audited**	**Evidence findings**
A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	The Identification of applicable legislation is monitored on a regular basis through NCSC.
A.18 Compliance	A.18.2 Information security reviews	As discussed, the Organisation’s staff have been required to read the ISMS policies and to acknowledge receipt and understanding.

Closing Meeting Attendees	
Name	**Job title**
David Wilson	Auditor
Sarah Paradise-Brown	Chief Operating Officer

Recommendation	Pass
Auditor’s Name	David Wilson
Auditor’s Signature	

By signing the above, the auditor confirms that the audit objectives have been met.

Recommendation Review	Recommendation confirmed
Reviewer’s Name	Ellen Folkard
Reviewer’s Signature	EFolkard.