Audit Report on Lolli's Information Security Management System

Stage 2 Audit

Prepared in Accordance with the

ISO/IEC 27001:2022 (ISO 27001)

Contents

Section I ***3***

AUDIT DETAILS **3**

Introduction 4
Audit Objectives 4
Audit Scope 4
Audit Timing 5
Auditee Representative(s) 5
Audit Team 5
Recommendation 6
Summary of Conformity and Appropriateness 6
Summary of Results 6
ICT Platform(s) Used 7
Effectiveness of ICT Platform(s) Used 7
Audit Activities 8
Audit Tests Performed 9
Types of Findings 10
Key Documents Reviewed 11

Section II ***12***

AUDIT FINDINGS **12**

Information Security Objectives 13
Data Classification and Labelling 15
Endpoint Protections 17
Statement of Applicability 19
Policy Approval Process 20
Master List of Documents 21
Incident Response Root Cause Analysis 21
Asset Disposal Template 22

Section I

AUDIT DETAILS

Introduction

For the initial certification of Lolli Technology Pty Ltd ('Lolli'), a Stage 2 audit was conducted to confirm the organization's conformity for certification of its Information Security Management System (ISMS) in alignment with ISO/IEC 27001:2022 (ISO 27001). The Stage 2 audit included a review of Lolli's implementation of the requirements in Clauses (4) through (10) of the ISO 27001 standard. This encompassed an examination of the documented ISMS, the risk assessment and treatment plan, operational practices, and the controls identified in the Statement of Applicability to determine their alignment with the organization's policies and the standard's requirements.

Audit Objectives

The key objectives of this audit include:

1. Determination of the conformity of Lolli's management system, or parts of it, with audit criteria.
2. Determination of the ability of the management system to ensure Lolli meets applicable statutory, regulatory and contractual requirements.
3. Determination of the effectiveness of the management system to ensure Lolli can reasonably expect to achieve its specified objectives.
4. Determination of the effectiveness of the management system to ensure Lolli has implemented applicable controls and achieved established information security objectives based on the risk assessment.
5. As applicable, identification of opportunities for improvement of the management system.
6. To understand Lolli's organisation to conduct an effective independent audit of their ISMS and its organisational alignment.
7. To challenge the design, implementation and operation of the ISMS system to its defined objectives, the ISO 27001 standard, and internally defined policies and procedures.
8. To provide value-adding feedback to Lolli to support the improvement of their ISMS.
9. To ensure an effective certification decision based on a high-quality audit process that removes any subjectivity or room for dispute in the outcome.

Audit Scope

Legal Entity: Lolli Technology Pty Ltd

Client Scope: The Information Security Management System (ISMS) of Lolli Technology Pty Ltd, supporting the tool for mortgage brokers to connect with their clients, including the development, operation, and support, in accordance with the Statement of Applicability (SoA) and aligned with the control requirements of ISO/IEC 27001:2022.

Facilities:

1. Melbourne Office: 27/360 Collins Street, Melbourne, VIC, 3000, Australia

Audit Timing

Stage 2 Days Planned: 2.8

Stage 2 Days Spent: 2.8

Audit Dates: 11th to 15th June

Auditee Representative(s)

Auditee(s): Damian Brander (Director) and Nick Jones (Digital Producer)

Audit Team

Lead Auditor: Kate Pianta

Audit Team: Steven Cirson

Recommendation

- The management system complies with the requirements of the nominated Standard(s).
- The Lead Auditor recommends that certification be granted.
- The Lead Auditor confirms that sufficient evidence was reviewed to verify the integrity of the management system.

Summary of Conformity and Appropriateness

Statement	Lead Auditor Acknowledgement
The audit was conducted remotely using ICT.	Yes – See 'ICT Platform(s) Used' below.
The ICT used was effective.	Yes – See 'Effectiveness of ICT Platform(s) Used' below.
The audit plan was followed with no deviations.	Yes
There were no significant issues identified that affected the audit.	Yes
There were no significant changes to the management system since the last audit that may impact the audit program.	Yes
Information security risk assessment was assessed and found to be sufficient.	Yes – Risk Assessment completed 24 April 2026.
Internal audit, management review, and corrective review were assessed and found to be sufficient.	Yes – Internal Audit completed 12 December 2025 and Management Review completed 25 September 2025.
The audit scope was deemed appropriate.	Yes
The audit objectives were achieved.	Yes

Summary of Results

Finding Type	Number
Major Non-conformity	0
Minor Non-conformity	3
Opportunity for Improvement	5

ICT Platform(s) Used

Lolli uses the Vanta platform to manage compliance across the business. Leveraging Vanta's auditor function, Sensiba Australia Pty Ltd uses this platform to perform audits across many information security standards, enterprise requirements and regulations.

Effectiveness of ICT Platform(s) Used

Using Vanta to conduct Lolli's ISO 27001 Stage 2 Audit enhanced the effectiveness of the audit process by facilitating an agile, efficient and collaborative audit process between auditors and auditees. Vanta's compliance management software streamlines the documentation, tracking, and reporting of the relevant controls that were required to be tested as part of this audit. This allowed for a smooth and efficient audit, as auditors could easily review the required audit documentation and controls evidence through Vanta's centralised storage repository, as well as maintain clear communication with Lolli through the audit hub.

Audit Activities

The Lolli ISO 27001 Audit Plan was prepared to outline key considerations and plans for conducting the Stage 2 Audit that support the certification decision process with the ISO/IEC 27001:2022 standard.

Sensiba Australia Pty Ltd's ('Sensiba Australia') Stage 2 Audit included a review of Lolli's Information Security Management System (ISMS) and related documentation that supports the Mandatory Requirements of ISO/IEC 27001:2022. This included the following procedures:

- Meeting with management and relevant control owners to perform walkthroughs and observe operational practices related to the ISMS.
- Collecting and evaluating sample evidence to confirm the effective implementation of documented policies, procedures, and controls.
- Reviewing supporting documentation and records that demonstrate how the ISMS has been operationalised across the organisation.
- Assessing whether, based on the above, Lolli's ISMS meets the certification criteria, with all applicable requirements of ISO/IEC 27001:2022 effectively implemented and maintained.

This report was prepared for Lolli's top management to consider any findings, both positive and negative, to guide the continued implementation of the ISMS beyond certification.

The Stage 2 Audit, which was conducted following the issuance of the Stage 1 report, included a review of Lolli's Information Security Management System (ISMS) and related documentation that supports the Mandatory Requirements and Annex A controls of ISO/IEC 27001:2022.

The primary procedures for this audit involved reviewing key documentation supporting Lolli's ISMS, as referenced in the Documents Reviewed section below, as well as reviewing evidence related to the applicable Annex A controls in scope for the audit.

Audit Tests Performed

Sensiba Australia's examination of the controls was performed using the following testing methods, as determined to be most suitable for testing each mandatory requirement and control activity within Lolli's ISMS.

Test Type	Description
Inquiry	Sensiba Australia made inquiries of Lolli personnel to obtain information and representations to determine their knowledge of the control, and to corroborate policy or procedure information.
Observation	Sensiba Australia observed application of the control activities by Lolli personnel.
Inspection	Sensiba Australia inspected among other items, policies, procedures, information logs, source documents, reports, system configurations and audit trails, to determine the design and implementation of the ISMS and related control activities.
Sampling	Sensiba Australia utilised a sampling approach in its audit, reviewing, among other items, policies, procedures, information logs, source documents, reports, system configurations, and audit trails, to evaluate the design and implementation of the ISMS and related control activities

Types of Findings

Finding Type	Description
Major Non-conformity	A major non-conformity is a significant matter that prevents or otherwise impacts Lolli's certification. This may include: • Failure to meet a requirement of the ISO 27001 standard. • Incomplete mandatory documentation. • A major breakdown of a defined policy, process or procedure. • Accumulation of multiple related minor non-conformities, representing a larger, or systemic problem. • Misuse of a certification mark that is misleading. • Minor non-conformities unresolved within an appropriate time period.
Minor Non-conformity	An instance of non-compliance with the established ISMS or the ISO 27001 standard that does not impact the overall effectiveness of the ISMS.
Opportunity for Improvement	Areas where the ISMS and related information security practices could be improved but are not related to non-compliance with the ISMS or ISO 27001 standard.

Key Documents Reviewed

The non-exhaustive list of documents reviewed includes the following. These were determined to be the key documents for the Stage 2 Audit that support the clauses of the ISO/IEC 27001:2022 standard.

ISMS Objectives and Scope:

- 01-ISMS Scope of the ISMS – v2 – dated 27 March 2026
- 10-ISMS Information Security Objectives Plan – v2 - dated 27 March 2026

Information Security Policy:

- Information Security Policy (AUP) – v1 – dated 29 July 2025
- 02-ISMS Information Security Management System (ISMS) Policy – v2 - dated 27 March 2026

Risk Assessment Methodology:

- Risk Management Policy – v2 - dated 27 March 2026

Risk Assessment:

- Risk Assessment - dated 24 April 2026

Risk Treatment Plan:

- Risk Assessment - dated 24 April 2026

Information Security Objectives:

- 10-ISMS Information Security Objectives Plan – v2 - dated 27 March 2026

Statement of Applicability:

- 11-ISMS Statement of Applicability – v2 - dated 27 March 2026

Internal Audit:

- Internal Audit Report - dated 12 December 2025

Management Review:

- Management review meeting minutes - dated 4 December 2025

Corrective and Preventive Actions Plan:

- 09-isms-procedure-for-corrective-action-and-continual-improvement - v2.1 - dated 11 April 2026
- Non_Conformity_Tracking_Updated – dated 24 April 2026

Section II

AUDIT FINDINGS

Information Security Objectives	Ref: #01
Finding Type: Minor Non-conformity	
Finding(s)	The first information security objective speaks to implementing, maintaining, and improving the ISMS; however, the effectiveness measures and timelines only relate to the initial certification being achieved. More specifically, measures and timelines related to the maintenance and improvement of the ISMS after certification have not been defined.
ISO 27001 Reference(s)	**Clause: 6.2** The information security objectives shall: f) be updated as appropriate; When planning how to achieve its information security objectives, the organization shall determine: h) what will be done; k) when it will be completed l) how the results will be evaluated
Document(s) Reviewed	• 10-isms-information-security-objectives-plan (1).pdf - dated 27 Mar 2026, v2.0
Auditee Management Response	
Root Cause Analysis	When establishing the Information Security Objectives Plan, the objectives and their associated effectiveness measures and timelines were carried across from the Vanta pre-populated template, which was oriented towards achieving initial ISO 27001 certification. The measures and timelines needed to maintain and continually improve the ISMS following certification were not added at that time. This was an oversight in working through the pre-populated Vanta templates rather than a deliberate exclusion.
Corrections	We will update the Information Security Objectives Plan (10-ISMS Information Security Objectives Plan) to define effectiveness measures and target timelines for the objectives relating to maintaining and continually improving the ISMS beyond initial certification, so that each objective has a defined measure and review timeframe. **Timeline:** By 2 July 2026
Corrective Actions	To eliminate the root cause and prevent recurrence, we will review the remaining documents adopted from the Vanta pre-populated templates to confirm they have been tailored to Lolli's ongoing operating context rather than only the certification milestone. We will also add a standing review of the information security objectives

	(including their effectiveness measures and timelines) to the management review agenda so they are reassessed and updated as appropriate on an ongoing basis. **Timeline:** By 2 July 2026
Sensiba Australia Response	
Finding Status	Closed
	Comment: Response provided sufficient to close finding. The effectiveness verification will be completed as part of the next audit.

Data Classification and Labelling	**Ref: #02**
Finding Type: Minor Non-conformity	
Finding(s)	The Data Management Policy outlines requirements for labelling confidential, paper-based information, but does not include requirements for electronic information or other data classifications. Additionally, whilst some electronic information was labelled, it was not fully implemented, with documents such as policies and management review minutes not shown to be labelled.
ISO 27001 Reference(s)	**Annex A: 5.13** An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
Document(s) Reviewed	• Data Management Policy - 16 Apr 2026 - V2.0
Auditee Management Response	
Root Cause Analysis	As with the information security objectives, the Data Management Policy was adapted from the Vanta pre-populated template, which addressed the labelling of confidential, paper-based information. Requirements for labelling electronic information and the remaining data classifications were not added when the policy was tailored, and labelling had not yet been fully applied across existing electronic documents such as policies and management review minutes. This was an oversight in working through the pre-populated Vanta templates rather than a deliberate exclusion.
Corrections	We will update the Data Management Policy to define information labelling requirements for electronic information and for all data classifications, in line with the organisation's information classification scheme. We will also apply the appropriate classification labels to the existing electronic documents identified as unlabelled, including policies and management review minutes. **Timeline:** By 2 July 2026
Corrective Actions	To eliminate the root cause and prevent recurrence, we will embed an information classification and labelling check into our document creation and approval workflow, so that new and updated documents (both electronic and paper-based) are classified and labelled in accordance with the classification scheme before they are approved and published. We will also review the remaining policies adopted from the Vanta pre-populated templates to confirm that labelling and

	classification requirements have been tailored to Lolli's operating context. **Timeline:** By 2 July 2026
Sensiba Australia Response	
Finding Status	Closed
	Comment: Response provided sufficient to close finding. The effectiveness verification will be completed as part of the next audit.

Endpoint Protections	Ref: #03
Finding Type: Minor Non-conformity	
Finding(s)	The devices owned by Lolli Technologies do not all adhere to the required security restrictions, with screen locks not enforced on all devices, and antivirus not enforced on one. Additionally, the organisation does not maintain oversight of contractor devices being used to access and interact with Lolli Technologies systems and confidential information.
ISO 27001 Reference(s)	**Annex A: 7.7** Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced. **Annex A: 7.9** Off-site assets shall be protected. **Annex A: 8.1** Information stored on, processed by or accessible via user end point devices shall be protected. **Annex A: 8.7** Protection against malware shall be implemented and supported by appropriate user awareness.
Document(s) Reviewed	• asset-management-policy-bsi - v2 - 29 January 2026 • information-security-policy-bsi - v1 - 29 July 2025 • Computers-2026-06-09-091409.csv
Auditee Management Response	
Root Cause Analysis	The non-conformity arose from two related gaps. For Lolli-owned devices, the required security settings (such as screen lock and antivirus) were applied on a per-device basis rather than being consistently enforced and verified across the fleet, with the result that a small number of devices were missed. For contractor devices, the organisation had not established a mechanism to obtain assurance over, or oversight of, the security configuration of contractor-owned devices used to access Lolli systems and confidential information.
Corrections	For Lolli-owned devices, we will enforce screen locks across all devices and enable antivirus on the device identified as non-compliant, and confirm that every device in the asset inventory meets the required security restrictions. For contractor devices, we will

	require each contractor who accesses Lolli systems or confidential information to sign a statutory declaration confirming their agreement to comply with Lolli's device security requirements, including screen lock, antivirus and related controls. **Timeline:** By 2 July 2026
Corrective Actions	To eliminate the root cause and prevent recurrence: (1) for Lolli-owned devices, we will maintain the required security settings (including screen lock and antivirus) as a standard baseline applied to all devices and verified through periodic compliance checks against the asset inventory; and (2) for contractor devices, we will incorporate the signed statutory declaration into our contractor onboarding process, so that any contractor granted access to Lolli systems or confidential information must agree to and acknowledge the device security requirements before access is provided, with periodic reconfirmation. **Timeline:** By 2 July 2026
Sensiba Australia Response	
Finding Status	Closed
	Comment: Response provided sufficient to close finding. The effectiveness verification will be completed as part of the next audit.

Statement of Applicability	Ref: #04
Finding Type: Opportunity for Improvement	
Finding(s)	The Statement of Applicability (SoA) notes justifications for exclusion of Annex A 7.11 and 7.12 within the implementation details column; however, it also still documents the justification for inclusion for these controls. As such, the organisation should consider revising the SoA to ensure the documentation for these controls is more clear.
ISO 27001 Reference(s)	**Clause: 6.1.3** The organization shall define and apply an information security risk treatment process to: d) 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.
Document(s) Reviewed	• 11-ISMS Statement of Applicability – v2 – 27 March 2026

Policy Approval Process	Ref: #05
Finding Type: Opportunity for Improvement	
Finding(s)	Whilst the security policies have been reviewed and approved, some policies were found to have the same author and approver, such as the following: • 03-ISMS Roles, Responsibilities, and Authorities - dated 16 Apr 2026, v2.0 (authored & approved by Nick Jones) • Third Party Management Policy - dated 16 Apr 2026, v2 (authored & approved by Nick Jones) • 01-ISMS Scope of the ISMS - dated 27 Mar 2026, v2.0 (authored & approved by Damian Brander) Lolli Technologies management should consider ensuring that the author and approver roles are segregated appropriately to enable a more effective review process.
ISO 27001 Reference(s)	**Clause: 7.5.2** When creating and updating documented information the organization shall ensure appropriate: c) review and approval for suitability and adequacy.
Document(s) Reviewed	• Lolli-iso27001_2022-2026-05-06-policy-packet.pdf

Master List of Documents	Ref: #06
Finding Type: Opportunity for Improvement	
Finding(s)	While the policies maintain clear versioning within them, the Master List of Documents document has not been updated to align with recent policy version changes. For example, the 01-ISMS Scope of the ISMS document was last updated 27 Mar 2026 (v2.0), yet the Master List of Documents document shows this aforementioned document as last updated 30 Jul 2025. As such, the organization should consider reviewing the Master List of Documents to ensure it aligns appropriately with the most recent policy versions.
ISO 27001 Reference(s)	**Clause: 7.5.3** For the control of documented information, the organization shall address the following activities, as applicable: e) control of changes (e.g. version control)
Document(s) Reviewed	• 00-isms-master-list-of-documents - dated 8 Aug 2025, v1.0 • Lolli-iso27001_2022-2026-05-06-policy-packet.pdf

Incident Response Root Cause Analysis	Ref: #07
Finding Type: Opportunity for Improvement	
Finding(s)	The organization has an Incident Response Plan that states that root cause analysis "may be performed on all verified P0 security incidents"; however, the organization should consider removing the ambiguity of the wording "may" and expanding to other severities of incidents to ensure consistency.
ISO 27001 Reference(s)	**Annex A: 5.27** Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.
Document(s) Reviewed	• Incident Response Plan - 8 Aug 2025 - V1.0

Asset Disposal Template	**Ref: #08**
Finding Type: Opportunity for Improvement	
Finding(s)	Whilst the Asset Disposal Form documents details related to the disposal method, e.g. donation, dumped, etc., and asset details, it does not document details related to the wiping of sensitive information prior to disposal. As such, the organisation should consider further revisions to the template to ensure details surrounding confidential information being erased are captured to improve alignment with processes and traceability of disposals.
ISO 27001 Reference(s)	**Annex A: 7.14** Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
Document(s) Reviewed	• asset-management-policy-bsi - v2 - 29 January 2026 • asset-disposal-form.pdf