Internal Audit Procedure

Reference: FPD0010A-2022

Version: 1

Owner: Lesley (new) Reeve

First Issued Date: 15/11/2023

Revision Issued Date: 15/11/2023

To outline FISCAL Technologies' Internal Audit process.

Prepared for:
All Employees, select Contractors, Partners and Customers

Prepared by:
James Pobgee

FISCAL Technologies Ltd
448 Basingstoke Road,
Reading, RG2 0LP
Tel: 0845 680 1905

1 CONFIDENTIALITY

Table of Contents

2 DOCUMENT CONTROL

Item	Description
Document Title:	Internal Audit Procedure
Associated Controls:	9.2 9.2.2 B.5.2 B.5.35 B.5.37 B.8.34
Reference ID:	FPD0010A-2022
Version:	1
Status:	Published
Approver:	
Approval Date:	
First Issued Date:	10/11/2023
Revision Issued Date:	15/11/2023
Reference Documents:	Linked Policies: • Information Security Governing Policy Linked Procedures: Linked Records: • ISMS Scope

2.1 DOCUMENT PUBLICATION HISTORY

(All revisions made to this document must be listed in chronological order, with the most recent revision at the bottom)

Version	Date	Author
1	15/11/2023	James Pobgee

3 PURPOSE AND SCOPE

3.1 PURPOSE

This procedure defines the requirements for internal audits of FISCAL's information security management system to determine whether the control objectives, controls, processes, and procedures of the ISMS conform to the requirements of; FISCAL's compliance requirements, relevant legislation, and regulations, the and the organisation's own information security management system, and that these are effectively implemented and maintained and perform as expected.

3.2 SCOPE

This procedure applies to all the information security management system controls relevant to the Internal Audit taking place as detailed in the current scope statement and to all personnel involved in an internal audit.

4 INTERNAL AUDIT PROCEDURE

An internal audit schedule is prepared by the CISO or TISO, or delegate in consultation with the CISO / TISO.

The scheduling of audits will be risk based and shall consider the importance of the activity being audited and previous audit reports.

The information security management system must be audited at least once per year. Certain elements may be audited more frequently if considered necessary, due to levels of risk, previous audit results and recurring issues.

Before audit, areas to be audited will be defined and advised to participants. Previously identified risks will be reviewed, including the verification of actions taken based on previous audits findings and the items to be checked during this audit.

Audits can only be performed by persons who are objective and impartial in relation to the areas being audited.

4.1 SUMMARY AUDIT PROTOCOL

Auditors will generally follow the audit protocol below:

- Audit starts out with a short meeting with management in the area. Purpose, scope and audit approach are discussed.
- The auditor uses the ISMS tool to guide him/her through the audit and to question staff of the information security controls and to obtain evidence.
- The auditor assesses the adequacy or otherwise of the evidence presented and notes same on the audit checklist.
- If the auditor during audit has identified a method of improving a procedure, these ideas should be documented as observations.
- An audit report will then be developed detailing a conclusion, any nonconformity, and observations.

Audit findings shall be discussed with the personnel in the area under audit. Deficiencies, root cause and corrective actions required, together with target dates for implementation, shall be recorded on the Internal Audit Report.

Internal Auditors in conjunction with auditees must monitor and track corrective actions through to closure in line with the agreed time scales.