



CERTIFICATE OF REGISTRATION

INTERCERT hereby certifies that the Information Security Management System of

Neofin Global Inc.

919 North Market Street, Suite 950, City of Wilmington, County of New Castle, Zip Code 19801, State of Delaware, United States

Has been successfully assessed as per the requirements of

ISO/IEC 27001:2022

For the scope of

Design, Development, Maintenance, Technical Support, Sales and Marketing of Neofin Core: Lending Automation SaaS Platform.

SOA Version -1.0


Initial Certification Date : April 02, 2025
Certificate Issue Date : April 02, 2025
Next Surveillance Date : April 01, 2026
Recertification Date : April 01, 2028

This Certificate is valid from April 02, 2025 to April 01, 2026.

Registration Number: ICI-IS-2504007


Issued on behalf of InterCert
Head - Certifications




	INTERCERT INC.	Doc No	IC.F.21C.02
	Stage-1 ISMS Audit Report	Rev Dt.	12.03.2023

Date of the Stage-1 Audit	17-03-2025
Name of the Organization	Neofin Global Inc.
Client Location/Site Address	919 North Market Street, Suite 950, City of Wilmington, County of New Castle, Zip Code 19801, State of Delaware, United States


Scope	"Design, Development, Maintenance, Technical Support, Sales and Marketing of Neofin Core: Lending Automation SaaS Platform."
Audit Criteria	To evaluate the client's documented system, location & site-specific conditions and gather other details through discussions with the client's personnel to determine the organization's readiness for the Stage 2 Audit for Certification
Applicable Legal, Statutory & Regulatory, and contractual requirements and its compliance	Verified company registration certificate no. File Number: 6781670 Address: 919 North Market Street, Suite 950, City of Wilmington, County of New Castle, Zip Code 19801, State of Delaware, United States Dated: 05-06-2022
Are Calculated man days ok or any changes is required?	No changes are required.
Are there any changes in no. of employees as calculated from application?	No
Any additional Information regarding change since application	No
Internal Audit (One complete cycle of internal audit and action plan for nonconformity identified during internal audit)	Yes, Internal Audit was conducted on 06-01-2025.
Management Review Meeting & its output	MRM was conducted on 06-01-2025.

	INTERCERT INC.	Doc No	IC.F.21C.02
	Stage-1 ISMS Audit Report	Rev Dt.	12.03.2023

Stage-1 Audit	
4.1-Context of Organization - (Internal and External) Related to Information Security Management System	Verified organization's brochures & website along with Context of the Organization on the Sprinto compliance automation tool.
4.2-Identification of Interested Parties and their Needs and Expectations Related to Information Security Management System	All the parties that have an interest in the organization's needs and expectations have been identified by the Management. Protection of client information, protecting the organization's proprietary information and intellectual property rights are addressed on the Sprinto compliance automation tool.
4.3 & 4.4 Establishment of Information Security Management System and Interaction of Processes & Applicability of Scope of the Information Security Management System	Verified scope of ISMS on the Sprinto compliance automation tool and its boundaries are clearly defined with respect to ISMS standard.
5.1 Demonstration of Top Management for Leadership and Commitment w.r.t. ISMS	Top management has clearly defined roles and responsibilities for the Information Security Officer. Verified the same on Sprinto compliance automation tool.
5.2 ISMS Policy	Verified Information Security Policy in the Sprinto compliance automation tool.
5.3 Organizational Roles & Responsibility (For ISMS)	The organization chart is evident. Verified Roles and Responsibilities.
6.1.1 & 6.1.2 General-Establishment of Risk Identification Criterion & Identification of Risk and Opportunities	The Risk Management Policy has been documented and confirmed using the Sprinto compliance automation tool.
6.1.3 ISMS Risk Treatment and the operational control established over them	Information Security Risk Assessment process is established within its Procedure for Risk Management Policy. SOA Detail: NEOF/CISO/SOA/001 Dated: 11-12-2024
6.2- Establishment of ISMS Objectives and Action Plan for achieving these Objectives	Information Security Policy defines objectives, framework, and plans for ISMS. Verified on the Sprinto compliance automation tool.

	INTERCERT INC.	Doc No	IC.F.21C.02
	Stage-1 ISMS Audit Report	Rev Dt.	12.03.2023

6.3 Planning of Changes to ISMS	Organization has established a Change Management Policy to carry out the ISMS changes in a planned manner.
7.1 Determination of Appropriate Resources needed for Effective Implementation, maintenance, and Continual Improvement of ISMS	Organization has allocated sufficient resources for effective implementation, maintenance, and continual improvement of ISMS. Information Security Officer roles and responsibilities verified on the Sprinto compliance automation tool.
7.2 & 7.3 Competence, Training and Awareness of Employees w.r.t. ISMS	ISMS training material verified on the Sprinto compliance automation tool.
7.4 Communication (Internal & External) relevant to Information Security Management System	Communication hierarchy documented as per organization structure on the Sprinto compliance automation tool.
7.5(7.5.1, 7.5.2 & 7.5.3) - Establishment of System of Documented Information (Creating & Updating and Control of Documented Information)	Systematic maintenance documented information observed on the Sprinto compliance automation tool.
8.1 Operational Planning and Control	Verified Information Security Policy. Action plans are available for ISMS Objectives and Risk Management.
8.2 & 8.3 Risk Assessment and Risk Treatment in accordance with 6.1	Review frequency as per the Risk Assessment and Treatment Procedure is defined. Risk Treatment plan verified. Risk assessment and Risk treatment review carried out as per the Risk Management Policy.
9.1. Monitoring, Measuring, Analysis, and Performance Evaluation of ISMS	Organization utilizes Sprinto as a continual compliance automation tool.
9.2 Internal Audit	Verified Internal Audit Assessment on the Sprinto compliance automation tool evidenced as of 06-01-2025.
9.3 Management Review Meeting	Verified MRM was done on 06-01-2025 and its frequency is every twelve months. MRM Output is documented.
10.1 Continual Improvement	Organization utilizes Sprinto as a continual compliance automation tool.
10.2 Non-Conformity and Corrective Action	


	INTERCERT INC.	Doc No	IC.F.21C.02
	Stage-1 ISMS Audit Report	Rev Dt.	12.03.2023

**Recommendation for Stage-2 Audit: I have checked, examined, discussed, and confirm the following:
Mark "X" where applicable.**


Sl.	Validation of Critical Points	Yes	No	Not Applicable	Comment of the Auditor
1	Relevance of the ISMS documentation with activities of the client	X			
2	Scope applied are justified with the present activities of the Clients	X			
3	Does the organization have availed Exclusions?	X			
4	Are Exclusion justified?	X			
5	Temporary Site?			X	
6	will it require Considerable Travel Time to visit site			X	
7	is there any Seasonality Factor		X		
8	Suitability of Audit Timing (Activities at Site)	X			
9	Process and element of the ISO 27001 in Stage-1 audit addressed?	X			

Sign Off:	
INTERCERT Report Submission	Client Acceptance for Report
Name of Auditor: Anupam Saha	Name: Oleksandr Kshutashvili
Signature:	Signature:


-----X End of Report X-----

	INTERCERT INC.	Doc No	IC.F.22C.02
	Stage-2 ISMS Audit Report	Rev Dt.	12.03.2023


Client Reg. No.	ICI-IS-2504007 Dated- 02-04-2025		
Date of the Stage-2 Audit	26-03-2025		
Name of the Organization	Neofin Global Inc.		
Client Location/Site Address	919 North Market Street, Suite 950, City of Wilmington, County of New Castle, Zip Code 19801, State of Delaware, United States		
Number of audit man days	11 Days		
Audit Criteria	ISO 27001:2022 standards requirements with Annexure A, Client ISMS Manual and Procedure, SOA & Applicable Statutory & Regulatory requirements.		
Standard	ISO 27001:2022		
Audit Objective	<ul style="list-style-type: none">Ensure that the clients’ management system documentation meets the requirements of the standard/specification.To confirm that the client organization adheres to its own policies, objectives, and procedure and all the requirements of the ISMS standard and other normative documents.To verify the implementation of the Information Security Management System as per the Standards Requirement, verification of records for the conformity of the implementation.		
Client Contact Person Name	Oleksandr Kshutashvili	Designation: CTO	
Auditor Name	Anupam Saha	Role: Lead Auditor	
Technical Expert Name	Anuja Patil	Role: Audit Team Member	
Scope of Certification	“Design, Development, Maintenance, Technical Support, Sales and Marketing of Neofin Core: Lending Automation SaaS Platform.” SOA Detail: NEOF/CISO/SOA/001 Dated: 11-12-2024		
Applicable Legal, statutory & regulatory requirements and other requirements.	IT Act, no other requirements are applicable related to their services.		
Stage-1 Audit Status	Recommended for Stage 2 audit.		
Stage-1 Audit NCR status	Previous Audit findings verified and found closed.		
Any Difference between certification audit agreement/Plan and Stage-2 certification audit finding (Related to Scope of certification or any other relevant matters)	No		

	INTERCERT INC.	Doc No	IC.F.22C.02
	Stage-2 ISMS Audit Report	Rev Dt.	12.03.2023


Have previous issues been addressed appropriately	Yes
Has there been any significant changes to the company	No

	INTERCERT INC.	Doc No	IC.F.22C.02
	Stage-2 ISMS Audit Report	Rev Dt.	12.03.2023

Stage-2 Audit	
4.1-Context of Organization - (Internal and External) Related to Information Security Management System	Verified organization's brochures & website along with Context of the Organization on the Sprinto compliance automation tool.
4.2-Identification of Interested Parties and their Needs and Expectations Related to Information Security Management System	All the parties that have an interest in the organization's needs and expectations have been identified by the Management. Protection of client information, protecting the organization's proprietary information and intellectual property rights are addressed on the Sprinto compliance automation tool.
4.3 & 4.4 Establishment of Information Security Management System and Interaction of Processes & Applicability of Scope of the Information Security Management System	Verified scope of ISMS on the Sprinto compliance automation tool and its boundaries are clearly defined with respect to ISMS standard.
5.1 Demonstration of Top Management for Leadership and Commitment w.r.t. ISMS	Top management has clearly defined roles and responsibilities for Information Security Officer. Verified the same on Sprinto compliance automation tool.
5.2 ISMS Policy	Verified Information Security Policy in the Sprinto compliance automation tool.
5.3 Organizational Roles & Responsibility (For ISMS)	The organization chart is evident. Verified Roles and Responsibilities.
6.1.1 & 6.1.2 General-Establishment of Risk Identification Criterion & Identification of Risk and Opportunities	Risk Management Policy is documented and verified on the Sprinto compliance automation tool
6.1.3 ISMS Risk Treatment and the operational control established over them	<p>The Information Security Risk Assessment process is established within Risk Management Policy.</p> <p>The risk register during the observation period has been verified on the Sprinto compliance automation tool. Observed 48 identified risks along with required mitigation controls and measures.</p> <p>SOA Detail: NEOF/CISO/SOA/001 Dated: 11-12-2024</p>

	INTERCERT INC.	Doc No	IC.F.22C.02
	Stage-2 ISMS Audit Report	Rev Dt.	12.03.2023


6.2- Establishment of ISMS Objectives and Action Plan for achieving these Objectives	Information Security Policy defines objectives, framework, and plans for ISMS. Verified on the Sprinto compliance automation tool.
6.3 Planning of Changes to ISMS	Organization has established Change Management Policy to carry out the ISMS changes in a planned manner.
7.1 Determination of Appropriate Resources needed for Effective Implementation, maintenance, and Continual Improvement of ISMS	Organization has allocated sufficient resources for effective implementation, maintenance, and continual improvement of ISMS. Information Security Officer roles and responsibilities verified on the Sprinto compliance automation tool.
7.2 & 7.3 Competence, Training and Awareness of Employees w.r.t. ISMS	ISMS training material verified on the Sprinto compliance automation tool.
7.4 Communication (Internal & External) relevant to Information Security Management System	Communication hierarchy documented as per organization structure on the Sprinto compliance automation tool.
7.5(7.5.1, 7.5.2 & 7.5.3) - Establishment of System of Documented Information (Creating & Updating and Control of Documented Information)	Systematic maintenance documented information observed on the Sprinto compliance automation tool.
8.1 Operational Planning and Control	Verified Information Security Policy. Action plans are available for ISMS Objectives and Risk Management.
8.2 & 8.3 Risk Assessment and Risk Treatment in accordance with 6.1	Review frequency as per the Risk Assessment and Treatment Procedure is defined. Risk Treatment plan verified. Risk assessment and Risk treatment review carried out as per the Risk Management Policy.
9.1. Monitoring, Measuring, Analysis, and Performance Evaluation of ISMS	Organization utilizes Sprinto as a continual compliance automation tool.
9.2 Internal Audit	Verified Internal Audit Assessment on the Sprinto compliance automation tool evidenced as of 06-01-2025.
9.3 Management Review Meeting	Verified MRM was done on 06-01-2025 and its frequency is every twelve months. MRM Output is documented.
10.1 Continual Improvement	Organization utilizes Sprinto as a continual compliance automation tool.
10.2 Non-Conformity and Corrective Action	The dashboard is 100% complete for the entity with no major observations, but with 01 failing check, 02 critical checks and 02 due checks pending. Checks are in progress and will be delivered by Sprinto as per SLA.

	INTERCERT INC.	Doc No	IC.F.22C.02
	Stage-2 ISMS Audit Report	Rev Dt.	12.03.2023


Annex A Control Objectives - Record objective evidence to confirm the effectiveness of the controls or if the control objective is deemed not applicable provide the detailed justification for this:

A.5.1	Policies for information security	Verified Information Security Policy document on the Sprinto compliance automation tool. Policy is reviewed and communicated regularly.
A.5.2	Information security roles and responsibilities	
A.5.3	Segregation of duties	Verified Information Security Roles and Responsibilities in ISMS Information Security Roles and Responsibilities document.
A.5.4	Management responsibilities	Verified Information Security Roles and Responsibilities on the Sprinto compliance automation tool.
A.5.5	Contact with authorities	Information Security Officer verified on the Sprinto compliance automation tool.
A.5.6	Contact with special interest groups	
A.5.7	Threat intelligence	Evidenced within the Information Security Policy of the organization.
A.5.8	Information security in project management	Verified Threat Intelligence procedure in Sprinto compliance automation tool.
A.5.9	Inventory of information and other associated assets	Verified the information security awareness training material given to all employees at the time of induction and training records for the same.
A.5.10	Acceptable use of information and other associated assets	Inspected training log for Tamo Kifshidze conducted on 02-12-2024.
A.5.11	Return of assets	Assets associated with information and information processing facilities identified and verified.
A.5.12	Classification of information	Verified Organizational Assets Responsibility through Asset register verified asset handling procedure.
A.5.13	Labelling of information	Verified Data Classification Policy in Sprinto compliance automation tool.
A.5.14	Information transfer	Network Diagram verified on the Sprinto compliance automation tool.
A.5.15	Access control	Access Control Policy and Procedure verified. Verified access logs for employee Sergey Batan with updated AWS User.
A.5.16	Identity management	
A.5.17	Authentication information	Users of AWS, GCP, GitHub and Google Workspace. Users have been updated throughout the observation period.
A.5.18	Access rights	


05 users of AWS.
04 users of GCP.
09 users of GitHub.
24 users of Google Workspace.

	INTERCERT INC.	Doc No	IC.F.22C.02
	Stage-2 ISMS Audit Report	Rev Dt.	12.03.2023


A.5.19	Information security in supplier relationships	Vendor Management Policy and Procedure evidenced on the Sprinto compliance automation tool and risk related to suppliers identified and evaluated in Risk Register. Verified Security within supplier agreement by verifying Non-Disclosure Agreement.
A.5.20	Addressing information security within supplier agreements	
A.5.21	Managing information security in the information and communication technology (ICT) supply chain	
A.5.22	Monitoring, review, and change management of supplier services	
A.5.23	Information security for use of cloud services	Organization uses AWS cloud services. All ISMS relevant controls are in place.
A.5.24	Information security incident management planning and preparation	Verified Incident Management Policy and Procedure on the Sprinto compliance automation tool. Verified Incident register. 10 Incidents recorded throughout observation period. All incidents have a severity level identified, reporting dates captured and closed with closing dates and closing notes by the responsible Incident Manager.
A.5.25	Assessment and decision on information security events	
A.5.26	Response to information security incidents	
A.5.27	Learning from information security incidents	
A.5.28	Collection of evidence	
A.5.29	Information security during disruption	Business Continuity Plan and Business Continuity Policy & Disaster Recovery Policy verified, documented on the Sprinto compliance automation tool.
A.5.30	ICT readiness for business continuity	
A.5.31	Legal, statutory, regulatory, and contractual requirements	Verified the Legal and Contractual Requirements Register for the Legal, statutory, regulatory, and contractual requirements. Verified the Company Legal Documents- File Number: 6781670
A.5.32	Intellectual property rights	
A.5.33	Protection of records	
A.5.34	Privacy and protection of personal identifiable information (PII)	Verified Compliance Policy & Procedure document on the Sprinto compliance automation tool. Organization has implemented procedures to protect records. Independent review through Certification Body – INTERCERT Technical review done continuously by Sprinto compliance automation tool.
A.5.35	Independent review of information security	
A.5.36	Compliance with policies, rules, and standards for information security	
A.5.37	Documented operating procedures	

	INTERCERT INC.	Doc No	IC.F.22C.02
	Stage-2 ISMS Audit Report	Rev Dt.	12.03.2023

A.6.1	Screening	Employee details and induction process followed.
A.6.2	Terms and conditions of employment	Verified Human Resource processes for employee Tamo Kifshidze whose Employment Start Date: 02-12-2024 Policy Acknowledgement Date: 02-12-2024
A.6.3	Information security awareness, education and training	
A.6.4	Disciplinary process	
A.6.5	Responsibilities after termination or change of employment	
A.6.6	Confidentiality or non-disclosure agreements	Verified Information Security Awareness Training logs.
A.6.7	Remote working	
A.6.8	Information security event reporting	In the non-disclosure agreement, verified the formal and communicated disciplinary process.
A.7.1	Physical security perimeters	Verified employees and contractors are aware of and fulfil their information security responsibilities.
A.7.2	Physical entry	
A.7.3	Securing offices, rooms, and facilities	
A.7.4	Physical security monitoring	
A.7.5	Protecting against physical and environmental threats	
A.7.6	Working in secure areas	
A.7.7	Clear desk and clear screen	
A.7.8	Equipment siting and protection	
A.7.9	Security of assets off-premises	
A.7.10	Storage media	
A.7.11	Supporting utilities	
A.7.12	Cabling security	
A.7.13	Equipment maintenance	
A.7.14	Secure disposal or re-use of equipment	
A.8.1	User end point devices	Physical Security Policy and Physical & Environmental Security Procedure evidenced.
A.8.2	Privileged access rights	
A.8.3	Information access restriction	
A.8.4	Access to source code	
A.8.5	Secure authentication	Power and telecommunications cabling carrying data or supporting information services protected from interception, interference, or damage.
A.8.6	Capacity management	A Clear Desk Policy for papers and removable storage media and a Clear Screen Policy for information processing facilities adopted and evidenced within Physical & Environmental Security Procedure.
		Verified the Media Disposal Policy.
		Access Control Policy and Procedure verified. Organization has adopted a role-based access control system on need-to-know basis. Access provisioning logs are verified.
		Verified the access control matrix on user and project level on the Sprinto compliance automation tool.
		Capacity Management Procedure evidenced within Operation Security Policy and Procedure through the Sprinto compliance automation tool.

	INTERCERT INC.	Doc No	IC.F.22C.02
	Stage-2 ISMS Audit Report	Rev Dt.	12.03.2023

A.8.7	Protection against malware	Antivirus installed on all devices.
A.8.8	Management of technical vulnerabilities	
A.8.9	Configuration management	Data Backup Policy verified.
A.8.10	Information deletion	Event Logging is done – verified.
A.8.11	Data masking	Verified the protection of log information.
A.8.12	Data leakage prevention	Vulnerability Management Policy is evidenced.
A.8.13	Information backup	
A.8.14	Redundancy of information processing facilities	Unauthorized installation of software is not allowed - verified.
A.8.15	Logging	Critical data systems protected from public internet access.
A.8.16	Monitoring activities	
A.8.17	Clock synchronization	Communications & Network Security Policy verified on the Sprinto compliance automation tool.
A.8.19	Installation of software on operational systems	
A.8.20	Networks security	Verified Network diagram.
A.8.21	Security of network services	
A.8.22	Segregation of networks	Verified Web Filtering procedure.
A.8.23	Web filtering	
A.8.24	Use of cryptography	Verified Encryption Policy in Sprinto compliance automation tool.
A.8.25	Secure development life cycle	Verified Database encryption status document evaluated as of 09-03-2025.
A.8.26	Application security requirements	
A.8.27	Secure system architecture and engineering principles	Software Development Life Cycle practised and evidenced on the Sprinto compliance automation tool.
A.8.28	Secure coding	
A.8.29	Security testing in development and acceptance	Secure systems engineering practiced and evidenced on the Sprinto compliance automation tool.
A.8.30	Outsourced development	
A.8.31	Separation of development, test and production environments	Verified Change Management Policy and Change Management repositories in Sprinto compliance automation tool.
A.8.32	Change management	
A.8.33	Test information	
A.8.34	Protection of information systems during audit testing	

	INTERCERT INC.	Doc No	IC.F.22C.02
	Stage-2 ISMS Audit Report	Rev Dt.	12.03.2023

Evidence:

Fig 1: Legal Document

State of Delaware
Secretary of State
Division of Corporations
Delivered 09:07 AM 05/06/2022
FILED 09:07 AM 05/06/2022
SR 20221817334 - File Number 6781670

CERTIFICATE OF INCORPORATION
OF
NEOFIN GLOBAL INC.

ARTICLE I

The name of the corporation is NeoFin Global Inc. (the “*Corporation*”).

ARTICLE II

The address of the Corporation’s registered office in the state of Delaware is 919 North Market Street, Suite 950 in the City of Wilmington, County of New Castle, Zip Code 19801. The name of its registered agent at such address is Incorp Services, Inc.

ARTICLE III

The purpose of the Corporation is to engage in any lawful act or activity for which corporations may be organized under the Delaware General Corporation Law.

ARTICLE IV

The aggregate number of shares which the Corporation shall have authority to issue is Ten Million (10,000,000) shares of capital stock all of which shall be designated “*Common Stock*” and have a par value of \$0.00001 per share.

ARTICLE V

The business and affairs of the Corporation shall be managed by or under the direction of the Board of Directors. Elections of directors need not be by written ballot unless otherwise provided in the Bylaws of the Corporation. In furtherance of and not in limitation of the powers conferred by the laws of the state of Delaware, the Board of Directors of the Corporation is expressly authorized to make, amend or repeal Bylaws of the Corporation.

Distributions by the Corporation may be made without regard to “preferential dividends arrears amount” or any “preferential rights,” as such terms may be used in Section 500 of the California Corporations Code.

ARTICLE VI

To the fullest extent permitted by the Delaware General Corporation Law, as the same exists or as may hereafter be amended, a director of the Corporation shall not be personally liable to the Corporation or its stockholders for monetary damages for breach of fiduciary duty as a director.


	INTERCERT INC.	Doc No	IC.F.22C.02
	Stage-2 ISMS Audit Report	Rev Dt.	12.03.2023

Fig 2: SOA

Domain 1 ORGANIZATIONAL CONTROLS	A51 A52 A53 A54 A55 A56 A57 A58 A59 A60 A61 A62 A63 A64 A65 A66 A67 A68 A69 A70 A71 A72 A73 A74 A75 A76 A77 A78 A79 A80 A81 A82 A83 A84 A85 A86 A87 A88 A89 A90 A91 A92 A93 A94 A95 A96 A97 A98 A99 A100 A101 A102 A103 A104 A105 A106 A107 A108 A109 A110 A111 A112 A113 A114 A115 A116 A117 A118 A119 A120 A121 A122 A123 A124 A125 A126 A127 A128 A129 A130 A131 A132 A133 A134 A135 A136 A137
Domain 2 PEOPLE CONTROLS	A51 A52 A53 A54 A55 A56 A57 A58 A59 A60 A61 A62 A63 A64 A65 A66 A67 A68 A69 A70 A71 A72 A73 A74 A75 A76 A77 A78 A79 A80 A81 A82 A83 A84 A85 A86 A87 A88 A89 A90 A91 A92 A93 A94 A95 A96 A97 A98 A99 A100 A101 A102 A103 A104 A105 A106 A107 A108 A109 A110 A111 A112 A113 A114 A115 A116 A117 A118 A119 A120 A121 A122 A123 A124 A125 A126 A127 A128 A129 A130 A131 A132 A133 A134 A135 A136 A137
Domain 3 PHYSICAL CONTROLS	A71 A72 A73 A74 A75 A76 A77 A78 A79 A80 A81 A82 A83 A84 A85 A86 A87 A88 A89 A90 A91 A92 A93 A94 A95 A96 A97 A98 A99 A100 A101 A102 A103 A104 A105 A106 A107 A108 A109 A110 A111 A112 A113 A114 A115 A116 A117 A118 A119 A120 A121 A122 A123 A124 A125 A126 A127 A128 A129 A130 A131 A132 A133 A134 A135 A136 A137
Domain 4 TECHNOLOGICAL CONTROLS	A51 A52 A53 A54 A55 A56 A57 A58 A59 A60 A61 A62 A63 A64 A65 A66 A67 A68 A69 A70 A71 A72 A73 A74 A75 A76 A77 A78 A79 A80 A81 A82 A83 A84 A85 A86 A87 A88 A89 A90 A91 A92 A93 A94 A95 A96 A97 A98 A99 A100 A101 A102 A103 A104 A105 A106 A107 A108 A109 A110 A111 A112 A113 A114 A115 A116 A117 A118 A119 A120 A121 A122 A123 A124 A125 A126 A127 A128 A129 A130 A131 A132 A133 A134 A135 A136 A137
Mapping key:	
1	Applicable, implemented and measured by this organization
2	Applicable, implemented locally and measured by another corporate organization
3	Applicable, but implemented and measured by another corporate organization
4	Not Applicable: No business conducted for this objective

Fig 3: Sprinto Dashboard

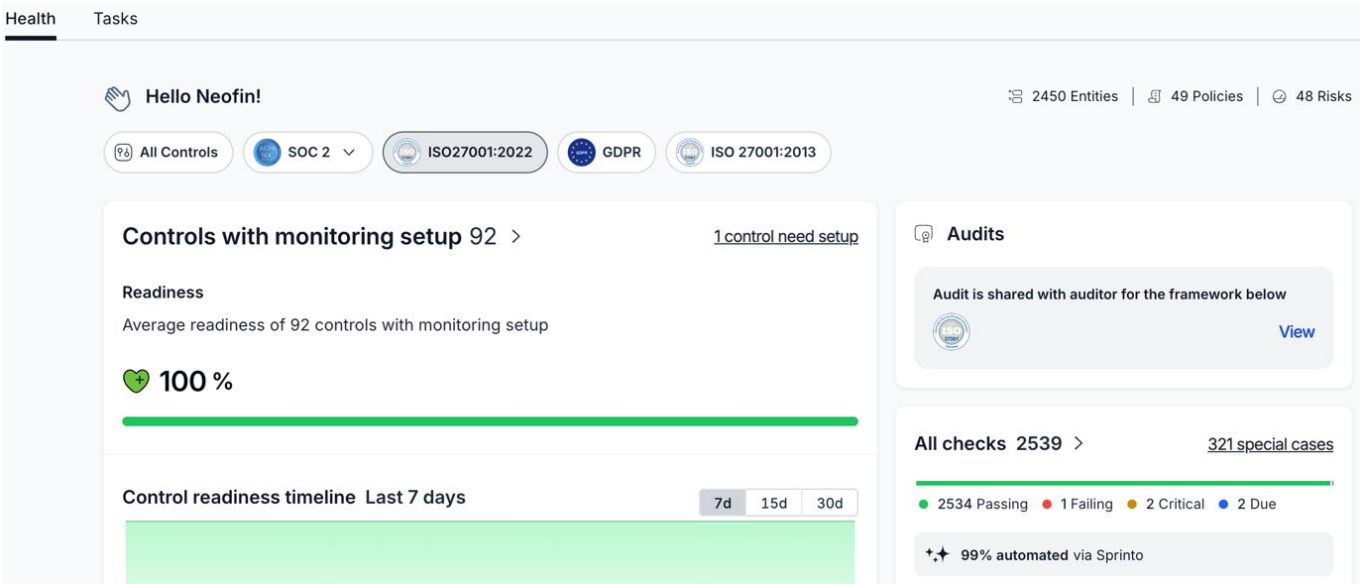


Fig 4: Organization Structure

Reportee	Manager	Assigned Roles
Olena Myronenko (olena@neofin.global)	Svitlanka Sergiichuk (svitlanka@neofin.global)	Director - Sales
Sergey Batan (s.batan@neofin.global)	Oleksandr Kshutashvili (oleksandr@neofin.global)	DevOps Architect
Anton Makushchenko (makushchenko@neofin.global)	Oleksandr Kshutashvili (oleksandr@neofin.global)	Software Engineer
Ruslan Volkhov (ruslan@neofin.global)	Oleksandr Kshutashvili (oleksandr@neofin.global)	Software Engineer
klemen Klemen Kostomaj (klemen@neofin.global)	Oleksandr Kshutashvili (oleksandr@neofin.global)	Lead Designer
Alena Molochaeva (design@neofin.global)	Svitlanka Sergiichuk (svitlanka@neofin.global)	Web Designer
Artemii Lipatiev (a.lipatiev@neofin.global)	Oleksandr Kshutashvili (oleksandr@neofin.global)	Product Manager
Prem Kumar (prem@neofin.global)	Oleksandr Kshutashvili (oleksandr@neofin.global)	Software Engineer
Tamo Kifshidze (tamo@neofin.global)	Oleksandr Kshutashvili (oleksandr@neofin.global)	Product Manager
Bohdan Havryshchuk (bohdan@neofin.global)	Oleksandr Kshutashvili (oleksandr@neofin.global)	Software Engineer
Ira Osypenko (ira@neofin.global)	Oleksandr Kshutashvili (oleksandr@neofin.global)	Product Manager
Iryna Gryshyna (legal@neofin.global)	Svitlanka Sergiichuk (svitlanka@neofin.global)	Finance Controller
Yuliana K (yuliana@neofin.global)	Svitlanka Sergiichuk (svitlanka@neofin.global)	Finance Controller
Ludmila Kovalska (l.kovalska@neofin.global)	Oleksandr Kshutashvili (oleksandr@neofin.global)	Product Manager
Andriy Pivnenko (finance@neofin.global)	Svitlanka Sergiichuk (svitlanka@neofin.global)	Finance Controller
Vitalii Mykhailiuk (vitalii@neofin.global)	Oleksandr Kshutashvili (oleksandr@neofin.global)	Software Engineer
Maxim Slobodyanyuk (max@neofin.global)	Maxim Slobodyanyuk (max@neofin.global)	CEO
Oleksandr Kshutashvili (oleksandr@neofin.global)	Oleksandr Kshutashvili (oleksandr@neofin.global)	CTO
Svitlanka Sergiichuk (svitlanka@neofin.global)	Svitlanka Sergiichuk (svitlanka@neofin.global)	CEO


	INTERCERT INC.	Doc No	IC.F.22C.02
	Stage-2 ISMS Audit Report	Rev Dt.	12.03.2023

Fig 5: Training Logs

Staff member	Employment Start Date	Employment Status	Infosec training date
Vitalii Mykhailiuk (vitalii@neofin.global)	01-Oct-24	New	22-Oct-24
klemen Klemen Kostomaj (klemen@neofin.global)	01-Nov-24	New	28-Nov-24
Ira Osypenko (ira@neofin.global)	01-Nov-24	New	06-Nov-24
Yuliana K (yuliana@neofin.global)	20-Nov-24	New	05-Dec-24
Tamo Kifshidze (tamo@neofin.global)	02-Dec-24	New	02-Dec-24
Ruslan Volkhov (ruslan@neofin.global)	03-Feb-25	Old	14-Feb-25

Fig 6: List of Staff devices

User	Device	Hard Disk encrypted?	Reported On
Bohdan Havryshchuk (bohdan@neofin.global)	MacBook-Pro-Bohdan.local (macOS 13.0.1)	Yes	15-Mar-24
Prem Kumar (prem@neofin.global)	stroke-RAVEN-SE-R (Ubuntu 20.04.5)	No	15-Mar-24
Oleksandr Kshutashvili (oleksandr@neofin.global)	Macintosh.local (macOS 15.4.0)	No	09-Mar-25
Andriy Pivnenko (finance@neofin.global)	MacBook-Air-Kateryna.local (macOS 11.3.1)	Yes	15-Mar-24
Andriy Pivnenko (finance@neofin.global)	Svitlanas-MacBook-Air.local (macOS 13.2.1)	Yes	09-Mar-25
Tamo Kifshidze (tamo@neofin.global)	Tamo (Microsoft Windows 11 Home 10.0.22631)	No	02-Dec-24
Ira Osypenko (ira@neofin.global)	MacBook-Pro-Ira.local (macOS 15.2.0)	Yes	08-Mar-25

Fig 7: List of critical system users of AWS

AWS User	Has access to AWS console?	User type	Staff Member	AWS access level
s.batan@neofin.global	Yes	IAM User	Sergey Batan (s.batan@neofin.global)	Admin neofinusercore
bohdan@neofin.global	Yes	IAM User	Bohdan Havryshchuk (bohdan@neofin.global)	Admin
pulumi_user	No	IAM User		S3_full_access
S3_user	No	IAM User		S3_full_access
phonxis	Yes	IAM User	Anton Makushchenko (makushchenko@neofin.global)	Admin


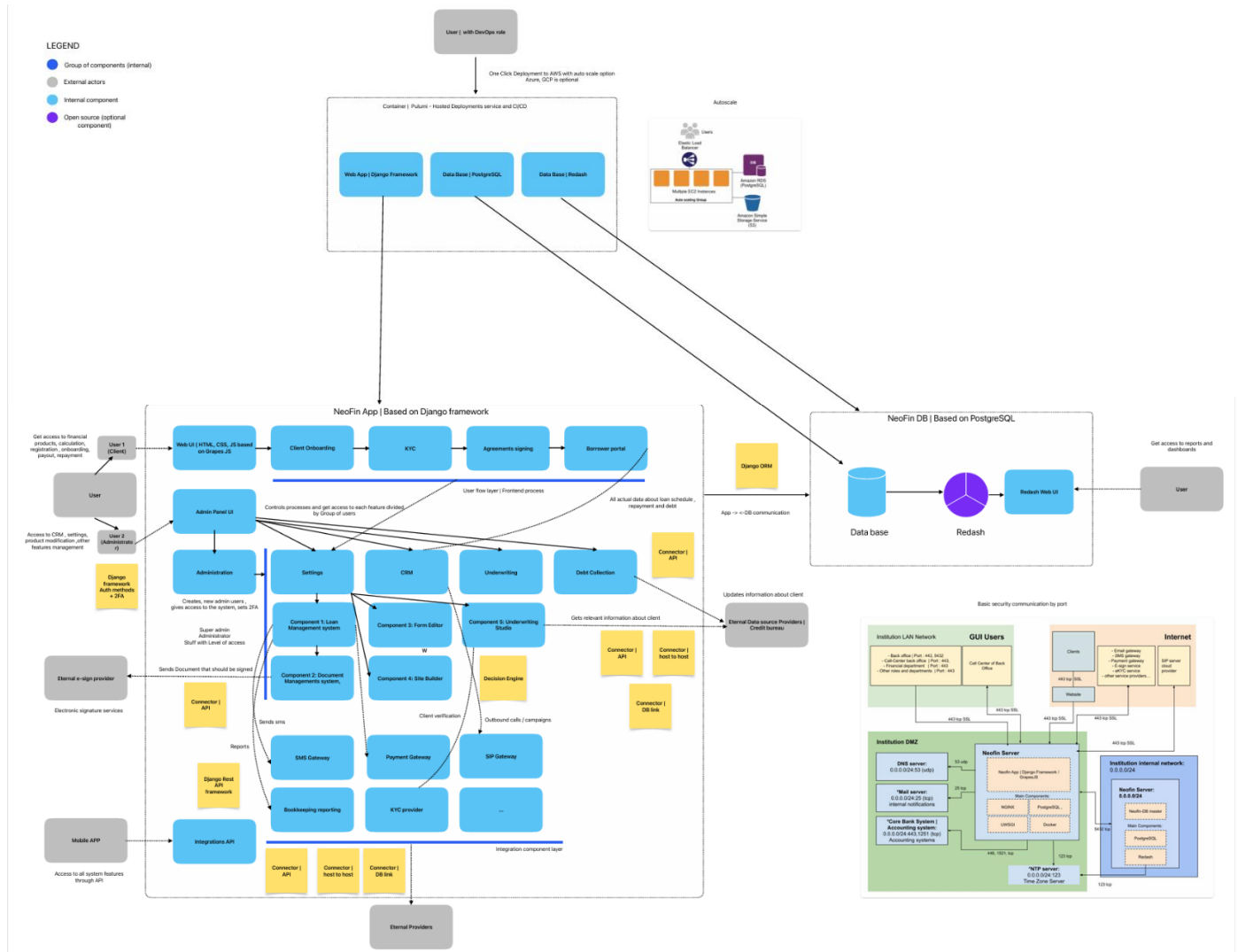

	<h1>INTERCERT INC.</h1>	Doc No	IC.F.22C.02
	<h2>Stage-2 ISMS Audit Report</h2>	Rev Dt.	12.03.2023

Fig 8: System Flow Diagram



	INTERCERT INC.	Doc No	IC.F.22C.02
	Stage-2 ISMS Audit Report	Rev Dt.	12.03.2023

A. Summary of the Audit

ISMS is in place and implemented using compliance automation tool, Sprinto. All technical controls are maintained as a continual check on the tool, administrative controls are presented for validation and are due for checks in a timely manner – has been witnessed in the SOA. Sprinto tool is in compliance as per the presented system flow. Recommended for certification based on intent and audit evidence.

B. Recommendation:

<input checked="" type="checkbox"/>	Issuance of Certificate
<input type="checkbox"/>	Refusal of the Certification
<input type="checkbox"/>	Follow Up audit
<input type="checkbox"/>	Other (if any):

C. Reason:

<input checked="" type="checkbox"/>	The system complies with the requirements of the reference standard: Congratulations, on the basis of the above summary, Lead Auditor is pleased to put forward a recommendation for the issuance of a Certificate.
<input type="checkbox"/>	The system complies with the requirements of the reference standard with exception of minor NC: Congratulations, Lead Auditor is pleased to put forward a recommendation for of Organization upon off-site verification of closure of all issues, the NC closure need to be submitted along with the Corrective Action Plan and objective evidence with 15 days from the stage-II audit but not later than 60 days from the date of Stage-II audit. If all non-conformances are not closed within 60 days, a full reassessment may be conducted.
<input type="checkbox"/>	Evidence of major non-conformities: Organization is not recommended for Certification. A follow-up assessment will be scheduled to allow for on-site verification and closure of all issues within 60 days from the date of Stage-II audit. If all nonconformances are not closed within 60 days, a full reassessment may be conducted.
<input type="checkbox"/>	Not Recommended: Organization is not recommended for certification, a Stage-II audit will be required. To progress your application for registration, please respond to each non-conformance, with a plan showing proposed actions, timescales and responsibilities for resolution. The organization should consider the root cause of the non-conformance and the potential for related issues in other parts of your system.
	Proposed Audit Date for Surveillance/Re-Certification Audit (04/2026)

On behalf of the Certification Body		Name of the organization: Neofin Global Inc.	
M/s INTERCERT INC. Stamp and Sign: Name of the auditor: - Anupam Saha (LEAD AUDITOR) Date of Audit: - 26-03-2025	Name:	Oleksandr Kshutashvili	Stamp:
	Designation:	CTO	
	Date of Audit: -	26-03-2025	
	Stage of Audit: -	Stage 2	Signature: -

-----X End of Report X-----



NEOFIN GLOBAL INC.

SOC 2 REPORT

FOR

**Neofin – A Cloud-Hosted
Software Application**

**TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON
CONTROLS RELEVANT TO SECURITY, CONFIDENTIALITY & AVAILABILITY**

13th March 2024 - 13th March 2025

Attestation and Compliance Services

CertPro

This report is intended solely for use by the management of NeoFin Global Inc. user entities of NeoFin Global Inc.'s services, and other parties who have sufficient knowledge and understanding of NeoFin Global Inc.'s services covered by this report (each referred to herein as a "specified user").

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against CertPro and the service auditor as a result of such access. Further, CertPro and the service auditor do not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

SECTION 1	INDEPENDENT SERVICE AUDITOR'S REPORT	1
SECTION 2	MANAGEMENT'S ASSERTION	5
SECTION 3	DESCRIPTION OF THE SYSTEM	8
SECTION 4	TESTING MATRICES26

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Board of Directors
NeoFin Global Inc.

Scope

We have examined the accompanying "Description of Neofin, a cloud-hosted software application" provided by NeoFin Global Inc. throughout the period 13 March 2024 to 13 March 2025 (the description) and the suitability of the design and operating effectiveness of controls to meet NeoFin Global Inc.'s service commitments and system requirements based on the criteria for Security, Confidentiality, Availability, Processing Integrity, and Privacy set forth in TSP Section 100 Principles and Criteria, Trust Services Principles and Criteria for Security, Confidentiality, and Availability (applicable trust services criteria) throughout the period 13 March 2024 to 13 March 2025.

NeoFin Global Inc. uses Amazon Web Services Inc. (AWS), a subservice organization, to provide cloud Software-As-A-Service (SaaS), Google Cloud Platform Inc. (GCP), a subservice organization, to provide cloud Software-As-A-Service (SaaS), Microsoft Azure, a cloud computing service operated by Microsoft for application management, GitHub, a cloud computing service operated by GitHub Inc. (GitHub), a subservice organization, to provide and host the GitHub application, and Google Workspace, a collection of cloud computing, productivity and collaboration tools, software, and products such as Gmail, Calendar, Drive, Docs, Sheets, Slides, Meet, and many more. The description presents NeoFin Global Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of NeoFin Global Inc.'s controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description presents NeoFin Global Inc.'s controls, the applicable trust services criteria, and the types of complementary user entity controls assumed in the design of NeoFin Global Inc.'s controls. The description does not disclose the actual controls at the user entity organizations. Our examination did not include the services provided by the user entity organizations and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

NeoFin Global Inc. has provided the accompanying assertion titled "NeoFin Global Inc.'s Management Assertion throughout the period 13 March 2024 to 13 March 2025" about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet NeoFin Global Inc.'s service commitments and system requirements based on the applicable trust services criteria. NeoFin Global Inc. is responsible for: (1) preparing the description and assertion; (2) the completeness, accuracy and method of presentation of the description and assertion; (3) providing the services covered by the description; (4) identifying the risks that would prevent the applicable trust services criteria from being met; (5) specifying the controls that meet NeoFin Global Inc.'s service commitments and system requirements based on the applicable trust services criteria and stating them in the description; (6) designing, implementing, maintaining and documenting controls to meet NeoFin Global Inc.'s service commitments and system requirements based on the applicable trust services criteria stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in NeoFin Global Inc.'s assertion and on the suitability of the design and operating

effectiveness of the controls to provide reasonable assurance that the service organizations commitments and system requirements were met based on applicable trust services criteria. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is fairly presented based on the description criteria and (2) the controls were suitably designed to provide reasonable assurance that the service organization's commitments and system requirements would be achieved if controls operated effectively based on the applicable trust services criteria (3) the controls operated effectively to provide reasonable assurance that the service organization's commitments and system requirements were achieved based on the applicable trust services criteria throughout the period 13 March 2024 to 13 March 2025.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to provide reasonable assurance that the service organization's commitments and system requirements meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the service organization's commitments and system requirements based on the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the description. We believe that the evidence obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of users and may not therefore include every aspect of the system that each individual user may consider important to its own particular needs. Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria.

Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Description of tests of controls

In Section III, the specific controls tested and the nature and timing, and results of those tests are listed in the accompanying description of Criteria, Controls, Tests and Results of Tests (Description of Tests and Results).

Opinion

In our opinion, in all material respects, based on the description criteria described in NeoFin Global Inc.'s assertion and the applicable trust services criteria:

- a. The description fairly presents Neofin, a cloud-hosted software application provided by NeoFin Global Inc. that was designed and operated effectively throughout the period 13 March 2024 to 13 March 2025.
- b. The controls stated in the description were suitably designed to provide reasonable assurance that the service organizations commitments and system requirements would be achieved if the controls operated effectively based on the applicable trust services criteria and if sub-service organizations and user entities

applied the controls contemplated in the design of NeoFin Global Inc.'s controls throughout the period 13 March 2024 to 13 March 2025.

- c. The controls tested, which were those necessary to provide reasonable assurance that the service organizations commitments and system requirements based on the applicable trust services principles criteria were met, operated effectively throughout the period 13 March 2024 to 13 March 2025.

Restricted Use

This report, including the description of tests of controls and results thereof in the description of tests and results is intended solely throughout information and use of user entities of NeoFin Global Inc.'s Neofin, a cloud-hosted software application throughout the period 13 March 2024 to 13 March 2025, and prospective user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organizations' system interacts with the user entities, subservice organizations, or other parties.
- Internal controls and their limitations.
- Complementary subservice organizations and complementary user entity controls and how those controls interact with the controls at the service organizations to achieve the service organization's service commitments and system requirements.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties.



JAY MARU

Certified Public Accountant

License Number: 41401

07th April 2025

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

Neofin Global Inc.'s Management Assertion for the period 13 March 2024 to 13 March 2025

We have prepared the attached description titled "Description of NeoFin Global Inc.'s Neofin, a cloud-hosted software application" throughout the period 13 March 2024 to 13 March 2025 (the description), based on the criteria in items (a) (i)–(ii) below, which are the criteria for a description of a service organization's system given in DC Section 200 prepared by AICPA's Assurance Services Executive Committee (ASEC), through its Trust Information Integrity Task Force's SOC 2® Guide Working Group to be used in conjunction with the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (the description criteria). The description is intended to provide users with information about Neofin, a cloud-hosted software application provided by NeoFin Global Inc. that may be useful when assessing the risks from interactions with the system throughout the period 13 March 2024 to 13 March 2025 particularly information about the suitability of the design and operating effectiveness of controls to meet NeoFin Global Inc.'s service commitments and system requirements based on the criteria related to Security, Confidentiality, and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy, (AICPA, Trust Services Criteria)*.

NeoFin Global Inc. uses Amazon Web Services Inc. (AWS), a subservice organization, to provide cloud Software-As-A-Service (SaaS), Google Cloud Platform Inc. (GCP), a subservice organization, to provide cloud Software-As-A-Service (SaaS), Microsoft Azure, a cloud computing service operated by Microsoft for application management, GitHub, a cloud computing service operated by GitHub Inc. (GitHub), a subservice organization, to provide and host the GitHub application, and Google Workspace, a collection of cloud computing, productivity and collaboration tools, software, and products such as Gmail, Calendar, Drive, Docs, Sheets, Slides, Meet, and many more. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at NeoFin Global Inc. to achieve NeoFin Global Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents NeoFin Global Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of NeoFin Global Inc.'s controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity organization controls that are suitably designed and operating effectively are necessary, along with controls at NeoFin Global Inc. to achieve NeoFin Global Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents NeoFin Global Inc.'s controls, the applicable trust services criteria and the types of complementary user entity organization controls assumed in the design of NeoFin Global Inc.'s controls. The description does not disclose the actual controls at the user entity organizations.

We confirm, to the best of our knowledge and belief, that.

1. The description fairly presents Neofin, a cloud-hosted software application provided by NeoFin Global Inc. throughout the period 13 March 2024 to 13 March 2025. The criteria for description are identified below under the heading "Description Criteria".
2. The controls stated in the description were suitably designed and operated effectively to meet NeoFin Global Inc.'s service commitments and system requirements based on the applicable trust services criteria throughout the period 13 March 2024 to 13 March 2025, to meet the applicable trust services criteria.

Description Criteria:

- i. The description contains the following information:
 1. The types of services provided.
 2. The principal service commitments and system requirements.
 3. The components of the system used to provide the services, which are the following:
 - Infrastructure - The physical and hardware components of a system (facilities, equipment, and networks).
 - Software - The programs and operating software of a system (systems, applications, and utilities).
 - People - The personnel involved in the operation and use of a system (developers, operators, users, and managers).
 - Procedures - The automated and manual procedures involved in the operation of a system.
 - Data - The information used and supported by a system (transaction streams, files, databases, and tables).
 4. The boundaries or aspects of the system are covered by the description.
 5. The applicable trust services criteria and the related controls are designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.
 6. Other aspects of the service organization's control environment, risk assessment process, communication and information systems and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.
- ii. The description does not omit or distort information relevant to the service organizations' system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore include every aspect of the system that each individual user may consider important to his or her own needs.

For NeoFin Global Inc.



Authorized Signatory

Svitlana Sergiichuk, Co-CEO

SECTION 3

DESCRIPTION OF THE SYSTEM

Overview of Operations

Types of Services Provided

Neofin is a cloud-hosted software application built by NeoFin Global Inc. (hereby referred to as Neofin).

Neofin is an intuitive, no-code, and developer-friendly SaaS platform that allows automating all the loan operations fully.

Our modularized (serverless) platform enables your financial institution to create full-cycle loan apps right from the Neofin Control Panel. Our crucial mission is to provide a better way to create a custom loan management workflow instead of long-term projects.

Principal Service Commitments and System Requirements

Neofin designs its processes and procedures to meet objectives for its software application. Those objectives are based on the service commitments that Neofin makes to customers and the compliance requirements that Neofin has established for their services.

Security commitments to user entities are documented and communicated in Neofin's customer agreements, as well as in the description of the service offering provided online. Neofin's security commitments are standardized and based on some common principles. These principles include but are not limited to, the following.

These principles include but are not limited to, the following:

- The fundamental design of Neofin's software application addresses security concerns such that system users can access the information based on their role in the system and are restricted from accessing information not needed for their role.
- Neofin implements various procedures and processes to control access to the production environment and the supporting infrastructure.
- Monitoring of key infrastructure components is in place to collect and generate alerts based on utilization metrics.

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit.
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties.
- Confidential information must be used only for the purposes explicitly stated in agreements between Neofin and user entities.

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components.
- Responding to customer requests in a reasonably timely manner.
- Business continuity and disaster recovery plans are tested on a periodic basis.
- Operational procedures supporting the achievement of availability commitments to user entities.

Neofin establishes operational requirements that support the achievement of security commitments and other system requirements. Such requirements are communicated in Neofin's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal networks are managed, and how staff is hired.

Components of the System used to provide services

Infrastructure & Network Architecture

The production infrastructure for the Neofin software application is hosted on Amazon Web Services, Google Cloud Platform and Microsoft Azure in their various regions across the United States of America, United Arab Emirates and Europe.

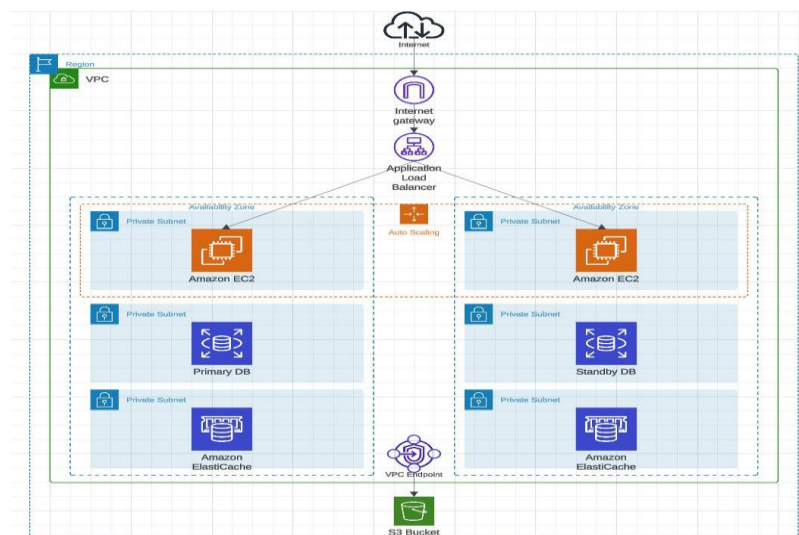
Neofin software application uses a virtual and secure network environment on top of Amazon Web Services, Google Cloud Platform, and Microsoft Azure infrastructure to ensure that the software application is always protected. This is achieved by hosting the application inside a virtual private cloud (VPC) and accompanying firewalls on the infrastructure provider. Neofin software application ensures there are only specific authorized points of entry, and filters traffic to the private networks that support the application.

When a customer's client device connects to the application over the internet, their data is encrypted and secured over HTTPS. It then passes through the Amazon Web Services, Google Cloud Platform and Microsoft Azure Internet Gateway, over to a Virtual Private Cloud that:

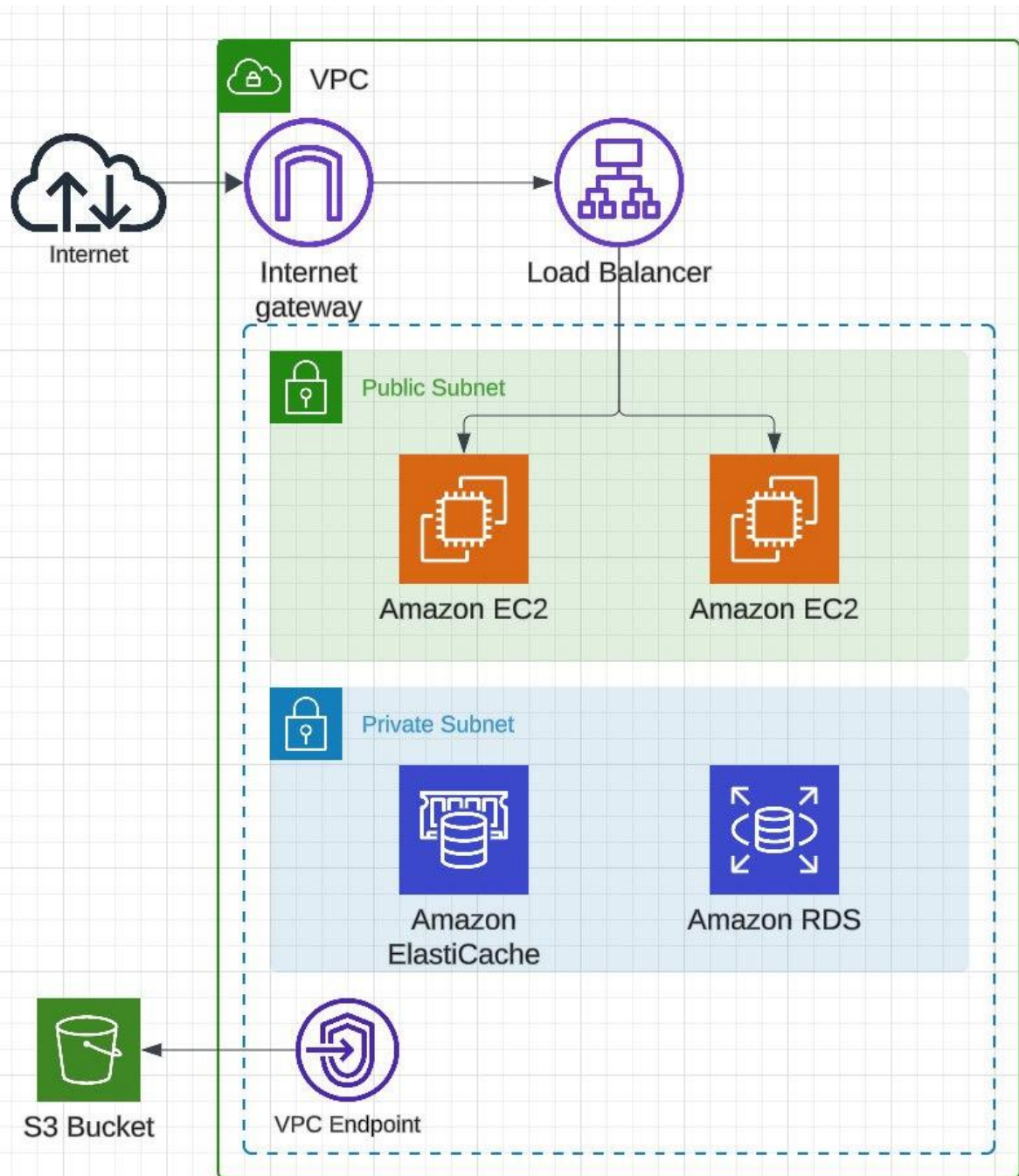
1. Houses the entire application runtime.
2. Protects the application runtime from any external networks.

The internal networks of Amazon Web Services, Google Cloud Platform and Microsoft Azure are protected by deny-by-default security groups and firewalls to ensure that only deliberately allowed traffic can pass through. Further, all VPC network flow logs, DNS logs, and other AWS console events are continuously monitored by AWS Guard duty to spot malicious activity and unauthorized behavior. Specifically, AWS Guard Duty uses machine learning, anomaly detection, and integrated threat intelligence to identify potential threats:

Network Diagram for AWS:

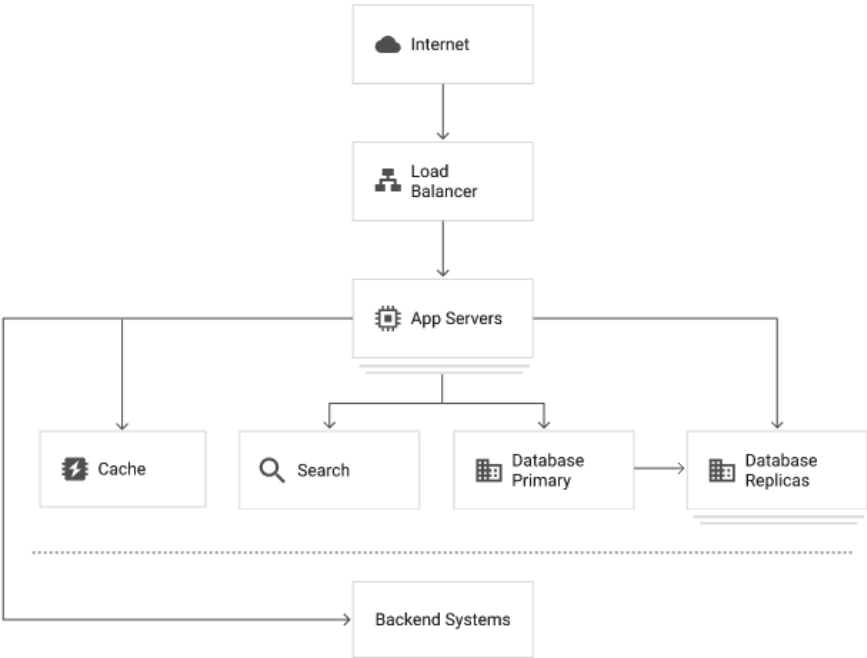


(A) Premium infrastructure version for high-loaded projects

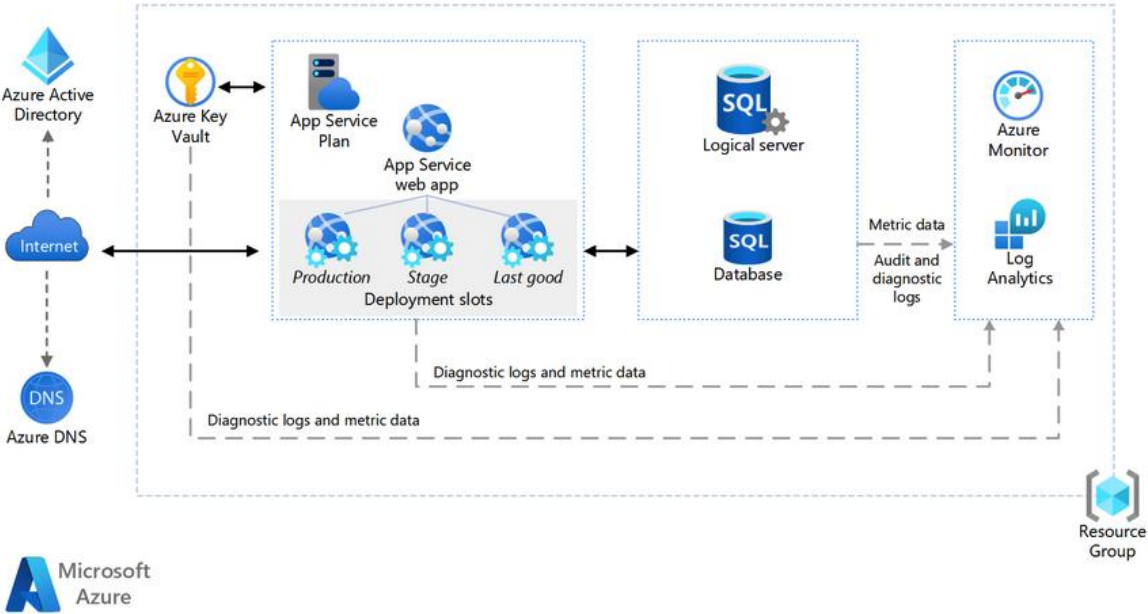


(B) Out-of-the-box configuration for middle-loaded projects

Network Diagram for Google Cloud Platform:



Network Diagram for Microsoft Azure:



Software

Neofin is responsible for managing the development and operation of the Neofin platform including infrastructure components such as servers, databases, and storage systems. The in-scope Neofin infrastructure and software components are shown in the table below:

Primary Infrastructure and Software			
System / Application	Business Function / Description	Underlying Operating System & Storage	Physical Location
Neofin Application	Access to the Neofin SaaS application is through a web/mobile interface and user authentication.	Linux Ubuntu with PostgreSQL	Amazon Web Services, Google Cloud Platform, Microsoft Azure United States of America, United Arab Emirates and Europe
Amazon Web Services, Google Cloud Platform and Microsoft Azure IAM	Identity and access management console for AWS resources.	Amazon Web Services, Google Cloud Platform, Microsoft Azure Proprietary	Amazon Web Services, Google Cloud Platform and Microsoft Azure
Amazon Web Services, Google Cloud Platform and Microsoft Azure Firewalls	Front-end firewalls protect the network perimeter with rule-based ACLs and back-end firewalls segregate the database servers from internal traffic.	Amazon Web Services, Google Cloud Platform, Microsoft Azure Proprietary	Amazon Web Services, Google Cloud Platform and Microsoft Azure
GitHub	Source code repository, version control system, and build software.	GitHub Proprietary	GitHub Cloud
Google Workspace	Identity/Email provider for all Neofin employees.	Google Workspace Proprietary	Google Workspace

Supporting Tools	
System / Application	Business Function / Description
Python and JavaScript	Programming Language used for Neofin application.
Sprinto	Provide continuous compliance monitoring of the company's system.
Google Workspace	Office communication services.

People

Neofin's staff have been organized into various functions like Sales, Support, Engineering, Product Management, etc. The personnel has also been assigned to the following key roles:

Senior Management: Senior management carries the ultimate responsibility for achieving the mission and objectives of the organization. They ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the organization's mission. They also assess and incorporate the results of the risk assessment activity into the decision making process. The senior management understands that their support and involvement is required in order to run an effective risk management program that assesses and mitigates IT related mission risks.

Information Security Officer: The Senior Management assigns the role of Information Security Officer to one of its staff members who is responsible for the performance of the information security program of the organization. Decisions made in these areas are based on an effective risk management program. The Information Security Officer is responsible for identifying risks, threats, and vulnerabilities, and adding controls

to mitigate these risks. Additionally, they also summarize remaining residual risks and report the same to Senior Management in a timely manner.

Compliance Program Manager: The company assigns the role of Compliance Program Manager to a staff member who would be responsible for the smooth functioning of the Information Security Program. The Compliance Program Manager takes care of the effective and timely completion of tasks required for the functioning of all information security controls, across all functions/departments of the organization.

System Users: The organization's staff members are the users of the IT systems. The organization understands that use of the IT systems and data according to an organization's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, staff members that access IT resources are provided with annual security awareness training.

Procedures and Policies

Formal policies and procedures have been established to support the Neofin software application. These policies cover:

- Code of Business Conduct
- Data Retention
- Information Security
- Vendor Management
- Physical Security
- Risk Management
- Media Disposal
- Incident Management
- Change Management
- Data Backup
- Endpoint Security
- Encryption
- Data Classification
- Business Continuity
- Disaster Recovery
- Access Control
- Acceptable Usage
- Vulnerability Management

Via the Sprinto platform, all policies are made available to all staff members to provide direction regarding the staff members' responsibilities related to the functioning of internal control. All staff members are expected to adhere to the policies and procedures that define how services should be delivered. Specifically, staff members are required to acknowledge their understanding of these policies upon hiring (and annually thereafter).

Neofin also provides information to clients and staff members on how to report failures, incidents, concerns, or complaints related to the services or systems provided by the Neofin software application, in the event there are problems, and takes actions within an appropriate timeframe as and when issues are raised.

Data

Data, as defined by Neofin constitutes the following:

- Transaction Data
- Electronic Interface Files
- Output Reports
- Input Reports
- System Files
- Error Logs

All data that is managed, processed and stored as a part of the Neofin software application is classified as per the Data Classification Policy which establishes a framework for categorizing data based on its sensitivity, value, and criticality to achieving the objectives of the organization. All data is to be assigned one of the following sensitivity levels:

Data Sensitivity	Description	Examples
Customer Confidential	Highly valuable and sensitive information where the level of protection is dictated internally through policy and externally by legal and/or contractual requirements. Access to confidential information is limited to authorized employees, contractors, and business partners with a specific need.	<ul style="list-style-type: none">• Customer system and operating data.• Customer PII.• Anything subject to a confidentiality agreement with a customer.
Company Confidential	Information that originated or is owned internally or was entrusted to Neofin by others. Company confidential information may be shared with authorized employees, contractors, and business partners but not released to the general public.	<ul style="list-style-type: none">• Neofin's PII.• Unpublished financial information.• Documents and processes explicitly marked as confidential.• Unpublished goals, forecasts, and initiatives marked as confidential.• Pricing/marketing and other undisclosed strategies.
Public	Information that has been approved for release to the public and is freely shareable both internally and externally.	<ul style="list-style-type: none">• Press releases.• Public website.

Further, all customer data is treated as confidential. The availability of this data is also limited by job function. All customer data storage and transmission follow industry-standard encryption. The data is also regularly backed up as documented in the Data Backup Policy.

Physical Security

The in-scope system and supporting infrastructure are hosted by Amazon Web Services, Google Cloud Platform, Microsoft Azure. As such, Amazon Web Services, Google Cloud Platform, Microsoft Azure is responsible for the physical security controls of the in-scope system. Neofin reviews the SOC 2 report provided by Amazon Web Services, Google Cloud Platform, Microsoft Azure on an annual basis, to ensure their controls are in accordance with standards expected by the customers of the Neofin software application.

Logical Access

The Neofin software application uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. User access, which is role-based, is controlled in the software application and authenticates to the database.

Neofin has identified certain systems that are critical to meet its service commitments. All-access to critical systems is under the principle of least required privilege (wherein a staff member is granted the minimum necessary access to perform their function) and controlled by the role of the staff member as well as a role-based access matrix prior to being issued system credentials and granted the ability to access the system. When a person is relieved of duties from the company, access to critical systems is made inaccessible in a timely manner.

The Information Security Officer is responsible for performing quarterly reviews of everyone who has access to the system and assessing the appropriateness of the access and permission levels and making modifications based on the principle of least privilege, whenever necessary.

Access to critical systems requires multi-factor authentication (MFA) wherever possible. Staff members must use complex passwords, wherever possible, for all of their accounts that have access to Neofin customer data. Staff is encouraged to use passwords that have at least 10 characters, are randomly generated, alphanumeric, and are special-character based. Password configuration settings are configured on each critical system. Additionally, company-owned endpoints are configured to auto-screen-lock after 15 minutes of inactivity.

Change Management

A documented Change Management Policy guides all staff members in documenting and implementing application and infrastructure changes. It outlines how changes to the Neofin system are reviewed, deployed, and managed. The policy covers all changes made to the Neofin software application, regardless of their size, scope, or potential impact.

The Change Management Policy is designed to mitigate the risks of:

- Corrupted or destroyed information.
- Degraded or disrupted software application performance.
- Productivity loss.
- Introduction of software bugs, configuration errors, vulnerabilities, etc.

A change to the Neofin software application can be initiated by a staff member with an appropriate role. Neofin uses a version control system to manage and record activities related to the change management process.

The version control system maintains source code versions and migrates source code through the development and testing process to the production environment. The version control software maintains a history of code changes to support rollback capabilities. It also facilitates the code review process which is mandated for all changes.

To initiate a change, the developer first creates a feature branch with the updated code. Once the code change is ready for review, the developer submits the code for peer review and automated testing, known as a pull request. For all code changes, the reviewer must be different from the author. Once a pull request is approved, the change can be released to production.

The ability to implement changes in the production infrastructure is restricted to only those individuals who require the ability to implement changes as part of their responsibilities.

Incident Management

Neofin has an incident management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers. Customers are directed to contact Neofin via the support email address provided during onboarding to report failures, incidents, concerns, or other complaints in the event there were problems.

Incident response procedures and centralized tracking tools consist of different channels for reporting production system incidents and weaknesses. Production infrastructure is configured to generate audit events for actions of interest related to operations and security. Security alerts are tracked, reviewed, and analyzed for anomalous or suspicious activity.

Where required, security incidents are escalated to privacy, legal, customer, or senior management team(s) and assigned a severity rating. Operational events are automatically resolved by the self-healing system.

- **Low severity incidents** are those that do not require immediate remediation. These typically include a partial service of Neofin being unavailable (for which workarounds exist). These do not require someone to be paged or woken up beyond normal work hours.
- **Medium severity incidents** are similar to low but could include scenarios like suspicious emails or unusual activity on a staff laptop. Again, these do not require immediate remediation or trigger automatic calls outside work hours. Low and medium-severity incidents usually cover the large majority of incidents found.
- **High severity incidents** are problems an active security attack has not yet happened but is likely. This includes situations like backdoors, malware, and malicious access to business data (e.g., passwords, payment information, vulnerability data, etc.). In such cases, the information security team must be informed and immediate remediation steps should begin.
- **Critical severity incidents** are those where a security attack was successful and something important was lost (or irreparable damage caused to production services). Again, in such cases, immediate actions need to be taken to limit the damage.

Post-mortem activities are conducted for incidents with critical severity ratings. Results of post-mortems may include updates to the security program or changes to systems required as a result of incidents.

Cryptography

User requests to Neofin 's systems are encrypted using Transport Layer Security (TLS) using certificates from an established third-party certificate authority. Remote system administration access to Neofin web and application servers is available through cryptographic network protocols (i.e., SSH) or an encrypted virtual private network (VPN) connection. Data at rest is encrypted using Advanced Encryption Standard (AES) 256-bit.

Asset Management (Hardware and Software)

Assets used in the system are inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels, as appropriate, to help ensure assets are classified appropriately, patched, and tracked as part of configuration management. Neofin uses tagging tools to automatically facilitate the company's hardware and software asset inventory. This helps to ensure a complete and accurate inventory of technology assets with the potential to store or process information is maintained.

Vulnerability Management and Penetration Testing

Vulnerability scanning tools are used to automatically scan systems on the network at least monthly to identify potential vulnerabilities. Automated software update tools are used to help ensure operating systems are running the most recent security updates provided by the software vendor. Vulnerabilities identified are risk-ranked to prioritize the remediation of discovered vulnerabilities.

Endpoint Management

Endpoint management solutions are in place that includes policy enforcement on company-issued devices, as well as bring-your-own devices that could connect to or access data within the system boundaries. Policies enforced on endpoints include but are not limited to enabling screen lock, OS updates, and encryption at rest on critical devices/workstations.

Availability

Neofin has a documented Business Continuity Plan (BCP) and testing performed against the Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). At least daily backup schedules are maintained to protect sensitive data from loss in the event of a system failure. Backups are restored at least annually as part of operational activities and are included as part of the BCP test plan.

Boundaries of the System

The scope of this report includes the Neofin software application. It also includes the people, processes, and IT systems that are required to achieve our service commitments toward the customers of this application.

Neofin depends on a number of vendors to achieve its objectives. The scope of this report does not include the processes and controls performed by the vendors. The management understands that risks exist when engaging with vendors and has formulated a process for managing such risks, as detailed in the Risk Assessment section of this document.

Relevant aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

The applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Although the applicable trust services criteria and related controls are included in Section IV, they are an integral part of Neofin's description of the system. This section provides information about the five interrelated components of internal control at Neofin, including:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring Controls

Control Environment

Integrity & Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Neofin's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Neofin's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct.

Neofin and its management team have established the following controls to incorporate ethical values throughout the organization:

- A formally documented "Code of Business Conduct" communicates the organization's values and behavioral standards to staff members.
- Staff members are required to acknowledge (upon hiring and annually thereafter) comprehensive policies and procedures covering the areas of Information Security, Change Management, Incident Management, and Access Control. Staff Members also acknowledge that they understand their responsibility for adhering to the policies and procedures.
- All new employees go through background checks as a part of the hiring process.

Commitment to Competence

Neofin's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. The following controls have been established in order to incorporate the commitment to competence throughout the organization:

- Management outlines the roles and responsibilities of technical staff to ensure that they are clear about their responsibilities in the organization. These roles and responsibilities are reviewed annually by the senior management.
- Annual Security Awareness Training is provided to all staff which focuses on maintaining the security of the proprietary and customer-servicing systems and related data.
- Employees receive periodic reviews by their supervisors inclusive of discussing any deficiencies noted in the execution of their job responsibilities.
- Employees are evaluated for competence in performing their job responsibilities at the time of hiring.

Management Philosophy and Operating Style

Neofin's management philosophy and operating style encompasses a broad range of characteristics. Such characteristics include management's approach to monitoring business risks, and management's attitudes toward personnel and the processing of information.

Neofin's information security function, composed of senior management and the Information Security Officer, meets frequently and includes at least an annual meeting to review policies and procedures and set the information security program roadmap. The security function, under the direction of senior management, oversees the security activities and communication of its policies and procedures.

Specific control activities that the Neofin has implemented in this area are described below:

- Senior management meetings are held to discuss major initiatives and issues that affect the business as a whole.
- Senior management reviews the functioning of internal controls, vendor risk assessment, risk assessment and high severity security incidents annually.

Organizational Structure and Assignment of Authority and Responsibility

Neofin's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

The management is committed to maintaining and improving its framework for how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. This also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties.

In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are accessible to all employees of the company and are updated as required.

Human Resources Policies and Practices

Neofin's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by the management's ability to hire and retain top-quality personnel who ensure the service organization is operating at maximum efficiency.

Specific control activities that Neofin has implemented in this area are described below:

- Background checks are performed on new hires, who are evaluated for competence in performing their job responsibilities at the time of hiring.
- Job positions are supported by job descriptions.
- New employees are required to acknowledge company policy and confidentiality related agreements upon hire and annually thereafter.
- Upon hire and annually thereafter, all employees must complete training courses covering basic information security practices.
- Performance evaluations for each employee are performed on an annual basis.
- If an employee violates the Code of Conduct in the employee handbook or the company's policies, or otherwise acts in a manner deemed contrary to the mission and objectives of the company, the employee is subject to sanctions up to and including termination of employment.
- When a person is relieved of duties from the company, access to critical systems is made inaccessible in a timely manner.

Risk Assessment

Neofin's risk assessment process identifies and manages risks that could potentially affect its ability to provide reliable services to its customers. The management is expected to identify significant risks inherent in products and services as they oversee their areas of responsibility. Neofin identifies the underlying sources of risk, measures the impact on the organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process identifies risks to the services provided by the Neofin software application, and the management has implemented various measures designed to manage these risks.

Neofin believes that effective risk management is based on the following principles:

1. Senior management's commitment to the security of Neofin software application.
2. The involvement, cooperation, and insight of all Neofin staff.
3. Initiating risk assessments with discovery and identification of risks.
4. A thorough analysis of identified risks.
5. Commitment to the strategy and treatment of identified risks.
6. Communicating all identified risks to the senior management.
7. Encouraging all Neofin staff to report risks and threat vectors.

Scope

The Risk Assessment and Management program applies to all systems and data that are a part of the Neofin software application. The Neofin risk assessment exercise evaluates infrastructure such as computer infrastructure, containing networks, instances, databases, systems, storage, and services. The risk assessments also include an analysis of business/IT practices, procedures, and physical spaces as needed.

Risk assessments may be high-level or detailed to a specific organizational or technical change as the stakeholders and technologists see fit.

Overall, the execution, development, and implementation of risk assessment and remediation programs is the joint responsibility of Neofin's Information Security Officer and the department or individuals responsible for the area being assessed. All Neofin staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Staff is further expected to work with the risk assessment project lead in the development of a remediation plan per risk assessment performed.

Vendor Risk Assessment

Neofin uses a number of vendors to meet its business objectives. Neofin understands that risks exist when engaging with vendors and as a result, continuously assesses those risks that could potentially affect the Company's ability to meet its business objectives.

Neofin employs several activities to effectively manage their vendors. Firstly, the Information Security Officer performs an annual exercise of thoroughly examining the nature and extent of risks involved with each vendor relationship. For critical vendors, Neofin assesses vendor compliance commitments through the review of available information security assessment reports and determines whether compliance levels adequately support Neofin's commitments to its customers. If a critical vendor is unable to provide a third-party security report or assessment, Neofin management meets with such vendors periodically to assess their performance, security concerns, and their services. Any vendor risks identified are recorded in the risk assessment matrix, which is reviewed annually by the Senior Management of the company.

Integration with Risk Assessment

As part of the design and operation of the system, Neofin identifies the specific risks that service commitments may not be met, and designs control necessary to address those risks. Neofin's management performs an annual Risk Assessment Exercise to identify and evaluate internal and external risks to the Company, as well as their potential impacts, likelihood, severity, and mitigating action.

Control Activities

Neofin's control activities are defined through its established policies and procedures which address individual risks associated with the achievement of the company's objectives. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions.

Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action.

Monitoring

Neofin management monitors control to ensure that they are operating as intended and that the controls are modified as conditions change. Monitoring activities are undertaken to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Staff activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, independent evaluations, or a combination of the two.

Information and Communication Systems

Neofin maintains a company-wide Information Security Policy, supported by detailed standards and training to ensure that employees understand their individual roles and responsibilities regarding security and significant events.

Further, Neofin also has additional policies and procedures that define access management, change management, and authentication requirements and procedures for critical systems. These policies and procedures are published and made available to internal staff via the company intranet.

Significant Events and Conditions

Neofin has implemented automated and manual procedures to capture and address significant events and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with all relevant information for any impact on the software application.

Trust Services Categories

The following Trust Service Categories are in scope: **Common Criteria (to the Security, Confidentiality, and Availability Categories).**

1. **Security** refers to the protection of:
 - a. Information during its collection or creation, use, processing, transmission, and storage.
 - b. Systems that use electronic information to process, transmit or transfer, and store information

to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or another unauthorized removal of information or system resources, misuse of the software, and improper access to or use of, alteration, destruction, or disclosure of information.

2. **Confidentiality** addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary and intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding the collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.
3. **Availability** refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Any applicable trust services criteria that are not addressed by control activities at Neofin are described within the sections titled "**Complementary Customer Controls**" and "**Complementary Subservice Organization Controls**".

Complementary Customer Controls

Neofin's controls related to Neofin cover a subset of overall internal control for each user of the software application. The control objectives related to Neofin cannot be achieved solely by the controls put in place by Neofin; each customer's internal controls need to be considered along with Neofin's controls. Each customer must evaluate its own internal control to determine whether the identified complementary customer controls have been implemented and are operating effectively.

Complementary Customer Control List	Related Criteria
Customers are responsible for managing their organization's Neofin software application account as well as establishing any customized security solutions or automated processes through the use of setup features.	CC5.1, CC5.2, CC5.3, CC6.1
Customers are responsible for ensuring that authorized users are appointed as administrators for granting access to their Neofin software application account.	CC5.2, CC6.3
Customers are responsible for notifying Neofin of any unauthorized use of any password or account or any other known or suspected breach of security related to the use of Neofin software application.	CC7.2, CC7.3, CC7.4

Complementary Customer Control List	Related Criteria
Customers are responsible for any changes made to user and organization data stored within the Neofin software application.	CC8.1
Customers are responsible for communicating relevant security and availability issues and incidents to Neofin through identified channels.	CC7.2, CC7.3, CC7.4

Complementary Subservice Organization Controls

Neofin uses subservice organizations in support of its system. Neofin's controls related to the system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria over the Neofin to be achieved solely by Neofin. Therefore, user entity controls must be evaluated in conjunction with Neofin's controls described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Neofin periodically reviews the quality of the outsourced operations by various methods including:

- Review of subservice organizations' SOC reports.
- Regular meetings to discuss performance.
- Non-disclosure agreements.

Control Activity Expected to be Implemented by Subservice Organization	Subservice Organization	Applicable Criteria
Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.	Amazon Web Services, Google Cloud Platform and Microsoft Azure	CC6.1, CC6.2, CC6.3, CC6.5, CC7.2
Physical access and security to the data center facility are restricted to authorized personnel.	Amazon Web Services, Google Cloud Platform and Microsoft Azure	CC6.4, CC6.5
Environmental protections, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.	Amazon Web Services, Google Cloud Platform and Microsoft Azure	CC6.4, A1.2
Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically.	Amazon Web Services, Google Cloud Platform and Microsoft Azure	A1.3
Policies and procedures to document repairs and modifications to the physical components of a facility including, but not limited to, hardware, walls, doors, locks, and other physical security components.	Amazon Web Services, Google Cloud Platform and Microsoft Azure	A1.2
A defined Data Classification Policy specifies classification levels and control requirements in order to meet the company's commitments related to confidentiality.	Amazon Web Services, Google Cloud Platform and Microsoft Azure	C1.1

Control Activity Expected to be Implemented by Subservice Organization	Subservice Organization	Applicable Criteria
A defined process is in place to sanitize and destroy hard drives and backup media containing customer data prior to leaving company facilities.	Amazon Web Services, Google Cloud Platform and Microsoft Azure	C1.2
Encryption methods are used to protect data in transit and at rest.	Amazon Web Services, Google Cloud Platform and Microsoft Azure	CC6.1

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report is on the controls relating to Neofin, a cloud-hosted software application provided by NeoFin Global Inc. The scope of the testing was restricted to Neofin, a cloud-hosted software application, and its boundaries as defined in Section 3. NeoFin Global Inc. conducted examination testing throughout the observation period 13 March 2024 to 13 March 2025.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the review period. In selecting the tests of controls, NeoFin Global Inc. considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates.
- The control risk is mitigated by the control.
- The effectiveness of entity-level controls, especially controls that monitor other controls.
- The degree to which the control relies on the effectiveness of other controls; and
- Whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g. resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g. approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, CertPro utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. CertPro, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted” in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

SECURITY PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.0: CONTROL ENVIRONMENT			
CC1.1: COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	Entity has a documented policy to define behavioral standards and acceptable business conduct.	Inspected the company policies & Code of Business Conduct Policy to determine the behavioral standards and acceptable business conduct. Observed that it has been reviewed and acknowledged by staff members.	No exceptions noted.
CC1.1.2	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	Inspected the company policies to determine that the entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding. Observed that the policies have been reviewed and acknowledged by new staff members.	No exceptions noted.
CC1.1.3	Entity outlines and documents cybersecurity responsibilities for all personnel.	Inspected Organization of Information Security Policy to determine that the entity outlines and documents cybersecurity responsibilities for all personnel.	No exceptions noted.
CC1.1.4	Entity has established procedures for staff to acknowledge applicable company policies periodically.	Inspected the company policies to determine that the entity has established procedures for staff to acknowledge applicable company policies periodically. Inspected records that the policies have been reviewed and acknowledged by staff members.	No exceptions noted.
CC1.1.5	Entity requires that new staff members review and acknowledge the Code of Business Conduct upon hire, and that all staff members review and acknowledge it annually.	Inspected the company policies to determine that the entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding. Observed that the policies have been reviewed and acknowledged by onboard staff.	No exceptions noted.
CC1.2: COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	Entity's Senior Management reviews and approves all company policies annually.	Inspected annual records that the company policies have been reviewed and approved by the Senior Management.	No exceptions noted.
CC1.2.2	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	Inspected annual records showing that the Senior Management has reviewed and approved the entity's Organizational Chart.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.2.3	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	Inspected the Management Review Meeting minutes showing review of relevant policies to determine that the Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	No exceptions noted.
CC1.2.4	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inspected annual records showing that the Senior Management has reviewed and approved the "Risk Assessment Report".	No exceptions noted.
CC1.2.5	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Inspected annual records showing that the Senior Management has reviewed and approved the "Vendor Risk Assessment Report".	No exceptions noted.
CC1.3: COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	Entity has established procedures to communicate with staff about their roles and responsibilities.	Inspected job descriptions for various job roles to determine that the entity has established procedures to communicate with staff about their roles and responsibilities.	No exceptions noted.
CC1.3.2	Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.	Inspected the Organizational Chart showing that the role of Information Security Officer has been appropriately assigned to an employee to determine that the Senior Management assigns the role of Information Security Officer who is delegated to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.	No exceptions noted.
CC1.3.3	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Inspected the Management Review Meeting minutes showing review of relevant policies to determine that the Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.3.4	Entity maintains an Organizational Structure to define authorities, facilitate information flow and establish responsibilities.	Inspected the Company Organizational Chart which shows reporting structure by role to determine that the entity maintains an Organizational Structure to define authorities, facilitate information flow and establish responsibilities.	No exceptions noted.
CC1.3.5	Entity appoints a Compliance Program Manager who is delegated the responsibility of planning and implementing the internal control environment.	Observed that a Compliance Program Manager has been appointed who is delegated the responsibility of planning and implementing the internal control environment.	No exceptions noted.
CC1.3.6	Entity has set up mechanism to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.	Observed that an Infrastructure Operations Person has been appointed to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.	No exceptions noted.
CC1.3.7	Entity appoints a People Operations Officer to develop and drive all personnel related security strategies.	Observed that a People Operations Officer has been appointed to develop and drive all personnel related security strategies.	No exceptions noted.
CC1.4: COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Entity has procedures to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	Inspected new hire evaluation with applicant background and competencies for a sample of new hires to determine that the entity has procedures to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	No exceptions noted.
CC1.4.2	Entity has established procedures to perform security risk screening of individuals prior to authorizing access.	Inspected background check details with details of the official documents collected as part of the onboarding process for a sample of new hires to determine that the entity has established procedures to perform security risk screening of individuals prior to authorizing access.	No exceptions noted.
CC1.5: COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.	Inspected the Security Awareness Training material provided to onboarded employees to determine that the entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5.2	Entity has established procedures for staff to acknowledge applicable company policies periodically.	Inspected the company policies to determine that the entity has established procedures for staff to acknowledge applicable company policies periodically. Inspected records that the policies have been reviewed and acknowledged by staff members.	No exceptions noted.
CC1.5.3	Entity requires that all employees in client serving, IT, Engineering and Information Security roles are periodically evaluated regarding their Job responsibilities.	Inspected records of performance evaluations for employees in client serving, IT, Engineering, and Information Security roles to determine that the entity requires that all employees are periodically evaluated regarding their job responsibilities.	No exceptions noted.
CC1.5.4	Entity documents, monitors and retains individual training activities and records.	Inspected the Information Security Training records to determine that the entity documents, monitors and retains individual training activities and records.	No exceptions noted.
CC1.5.5	Entity provides information security and privacy training to staff that is relevant for their job function.	Inspected the Information Security Training document to determine that the entity provides information security and privacy training to staff that is relevant for their job function.	No exceptions noted.
CC1.5.6	Entity requires that new staff members complete Information Security Awareness training upon hire, and that all staff members complete Information Security Awareness training annually.	Inspected records of Security Awareness Training completion for a sample of employees to determine the company requires that new staff members complete Information Security Awareness training annually.	No exceptions noted.
CC1.5.7	Entity requires that all staff members complete Information Security Awareness training annually.	Inspected annual records of Security Awareness Training completion for a sample of employees to determine that the entity requires that all staff members complete Information Security Awareness training.	No exceptions noted.
CC2.0: COMMUNICATION AND INFORMATION			
CC2.1: COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	Entity systems generate information that is reviewed and evaluated to determine impacts to the functioning of internal controls.	Inspected the monitoring alert configurations to determine that the entity systems generate information that is reviewed and evaluated to determine impacts to the functioning of internal controls.	No exceptions noted.
CC2.1.2	Entity makes all policies and procedures available to all staff members for their perusal.	Inspected the list of policies to determine that the entity makes all policies and procedures available to all staff members for their perusal.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.3	Entity displays the most current information about its services on its website, which is accessible to its customers.	Inspected the company's website to determine that the entity displays the most current information about its services on its website, which is accessible to its customers.	No exceptions noted.
CC2.1.4	Entity has a documented policy outlining guidelines for the disposal and retention of information.	Inspected the Data Retention Policy to determine that the entity has a documented policy outlining guidelines for the disposal and retention of information.	No exceptions noted.
CC2.1.5	Entity has documented policy and procedures for physical and/or logical labeling of information via documented policy for data classification.	Inspected the Data Classification Policy to determine that the entity has documented policy and procedures for physical and/or logical labeling of information via documented policy for data classification.	No exceptions noted.
CC2.2: COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.	Inspected the Security Awareness Training material provided to onboarded employees to determine that the entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.	No exceptions noted.
CC2.2.2	Entity has established procedures for staff to acknowledge applicable company policies periodically.	Inspected the company policies to determine that the entity has established procedures for staff to acknowledge applicable company policies periodically. Inspected records that the policies have been reviewed and acknowledged by staff members.	No exceptions noted.
CC2.2.3	Entity makes all policies and procedures available to all staff members for their perusal.	Inspected the list of policies to determine that the entity makes all policies and procedures available to all staff members for their perusal.	No exceptions noted.
CC2.2.4	Entity documents, monitors, and retains individual training activities and records.	Inspected the Information Security Training records to determine that the entity documents, monitors and retains individual training activities and records.	No exceptions noted.
CC2.2.5	Entity has provided information to employees, via the Information Security Policy, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.	Inspected the Information Security Policy and the section that describes how to report incidents to determine that the entity has provided information to employees, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.6	Entity has a documented policy to define behavioral standards and acceptable business conduct.	Inspected the company policies & Code of Business Conduct Policy to determine the behavioral standards and acceptable business conduct. Observed that it has been reviewed and acknowledged by staff members.	No exceptions noted.
CC2.2.7	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	Inspected the company policies to determine that the entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding. Observed that the policies have been reviewed and acknowledged by new staff members.	No exceptions noted.
CC2.2.8	Entity requires that new staff members complete Information Security Awareness training upon hire, and that all staff members complete Information Security Awareness training annually.	Inspected records of Security Awareness Training completion for a sample of employees to determine the company requires that new staff members complete Information Security Awareness training annually.	No exceptions noted.
CC2.2.9	Entity requires that all staff members complete Information Security Awareness training annually.	Inspected annual records of Security Awareness Training completion for a sample of employees to determine that the entity requires that all staff members complete Information Security Awareness training.	No exceptions noted.
CC2.3: COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	Entity displays the most current information about its services on its website, which is accessible to its customers.	Inspected the company's website to determine that the entity displays the most current information about its services on its website, which is accessible to its customers.	No exceptions noted.
CC2.3.2	Entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.	Inspected the customer support page in the company website to determine that the entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.	No exceptions noted.
CC3.0: RISK ASSESSMENT			
CC3.1: COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	Inspected the annual formal risk assessment exercise records to determine that the entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.1.2	Entity has formally documented policies and procedures to govern risk management.	Inspected the Risk Management Policy to determine that the entity has formally documented policies and procedures to govern risk management.	No exceptions noted.
CC3.2: COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	Inspected the annual formal risk assessment exercise records to determine that the entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	No exceptions noted.
CC3.2.2	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	Inspected the risk assessment documentation to determine that each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Observed that Risks are mapped to mitigating factors that address some or all of the risk.	No exceptions noted.
CC3.2.3	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	Inspected the vendor risk assessment documentation to determine that the entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	No exceptions noted.
CC3.2.4	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	Inspected the company policies to determine that the entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding. Observed that the policies have been reviewed and acknowledged by new staff members.	No exceptions noted.
CC3.3: COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	Entity considers the potential for fraud when assessing risks.	Inspected the risk assessment documentation to determine that the entity considers the potential for fraud when assessing risks. Observed an entry in the risk matrix.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.4: COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	Inspected the annual formal risk assessment exercise records to determine that the entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	No exceptions noted.
CC3.4.2	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	Inspected the risk assessment documentation to determine that each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Observed that risks are mapped to mitigating factors that address some or all of the risk.	No exceptions noted.
CC3.4.3	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	Inspected the vendor risk assessment documentation to determine that the entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	No exceptions noted.
CC4.0: MONITORING ACTIVITIES			
CC4.1: COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.	Inspected the Organizational Chart showing that the role of Information Security Officer has been appropriately assigned to an employee to determine that the Senior Management assigns the role of Information Security Officer who is delegated to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.	No exceptions noted.
CC4.1.2	Entity has set up mechanism to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.	Observed that an Infrastructure Operations Person has been appointed to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.	No exceptions noted.
CC4.1.3	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inspected the Internal Audit Report on Sprinto compliance automation tool to determine that the entity continuously monitors, tracks, and reports the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.4	Entity's Senior Management reviews and approves all company policies annually.	Inspected annual records that the company policies have been reviewed and approved by the Senior Management.	No exceptions noted.
CC4.1.5	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Inspected the Management Review Meeting minutes showing review of relevant policies to determine that the Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	No exceptions noted.
CC4.1.6	Entity periodically updates and reviews the inventory of systems as a part of installations, removals and system updates.	Inspected the Asset Management Policy and Procedure and inspected the Internal Audit Report to determine that the entity periodically updates and reviews the inventory of systems as a part of installations, removals and system updates.	No exceptions noted.
CC4.1.7	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	Inspected annual records showing that the Senior Management has reviewed and approved the entity's Organizational Chart.	No exceptions noted.
CC4.1.8	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inspected annual records showing that the Senior Management has reviewed and approved the "Risk Assessment Report".	No exceptions noted.
CC4.1.9	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Inspected annual records showing that the Senior Management has reviewed and approved the "Vendor Risk Assessment Report".	No exceptions noted.
CC4.1.10	Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to entity's customers can be met.	Inspected the vendor risk assessment documentation to determine that the entity reviews and evaluates all subservice organizations periodically, to ensure commitments to entity's customers can be met.	No exceptions noted.
CC4.2: COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	Entity has provided information to employees, via the Information Security Policy, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.	Inspected the Information Security Policy and the section that describes how to report incidents to determine that the entity has provided information to employees, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.2.2	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inspected the Internal Audit Report on Sprinto compliance automation tool to determine that the entity continuously monitors, tracks and reports the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.
CC4.2.3	Entity's Senior Management reviews and approves all company policies annually.	Observed that the company policies have been reviewed and approved by the Senior Management annually.	No exceptions noted.
CC4.2.4	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Inspected the Management Review Meeting minutes showing review of relevant policies to determine that the Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	No exceptions noted.
CC5.0: CONTROL ACTIVITIES			
CC5.1: COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.	Inspected the company Code of Business Conduct and list of policies made available to employees to determine that the entity has developed a set of policies that establish expected behavior with regard to the company's control environment.	No exceptions noted.
CC5.1.2	Entity establishes guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.	Inspected the Acceptable Usage Policy to determine that the entity establishes guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.	No exceptions noted.
CC5.1.3	Entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.	Inspected the Organizational Chart and the roles/responsibilities defined by management to determine that the entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2: COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inspected the Internal Audit Report on Sprinto compliance automation tool to determine that the entity continuously monitors, tracks and reports the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.
CC5.2.2	Entity's Senior Management reviews and approves all company policies annually.	Observed that the company policies have been reviewed and approved by the Senior Management annually.	No exceptions noted.
CC5.2.3	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Inspected the Management Review Meeting minutes showing review of relevant policies to determine that the Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	No exceptions noted.
CC5.2.4	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	Inspected annual records showing that the Senior Management has reviewed and approved the entity's Organizational Chart.	No exceptions noted.
CC5.2.5	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inspected annual records showing that the Senior Management has reviewed and approved the "Risk Assessment Report".	No exceptions noted.
CC5.2.6	Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to entity's customers can be met.	Inspected the vendor risk assessment documentation to determine that the entity reviews and evaluates all subservice organizations periodically, to ensure commitments to entity's customers can be met.	No exceptions noted.
CC5.2.7	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Inspected annual records showing that the Senior Management has reviewed and approved the "Vendor Risk Assessment Report".	No exceptions noted.
CC5.2.8	Entity's Infosec officer reviews and approves the list of people with access to production console annually.	Inspected records where the access to critical systems has been reviewed and approved by the Infosec Officer.	No exceptions noted.
CC5.2.9	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.	Inspected the company Code of Business Conduct and list of policies made available to employees to determine that the entity has developed a set of policies that establish expected behavior with regard to the company's control environment.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.3: COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Entity makes all policies and procedures available to all staff members for their perusal.	Inspected the list of policies to determine that the entity makes all policies and procedures available to all staff members for their perusal.	No exceptions noted.
CC5.3.2	Entity has established procedures for staff to acknowledge applicable company policies periodically.	Inspected the company policies to determine that the entity has established procedures for staff to acknowledge applicable company policies periodically. Inspected records that the policies have been reviewed and acknowledged by staff members.	No exceptions noted.
CC5.3.3	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	Inspected the company policies to determine that the entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding. Observed that the policies have been reviewed and acknowledged by new staff members.	No exceptions noted.
CC5.3.4	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.	Inspected the company Code of Business Conduct and list of policies made available to employees to determine that the entity has developed a set of policies that establish expected behavior with regard to the company's control environment.	No exceptions noted.
CC6.0: LOGICAL AND PHYSICAL ACCESS CONTROLS			
CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	Entity has documented policy and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	Inspected the Access Control Policy and Procedure to determine that the entity manages an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	No exceptions noted.
CC6.1.2	Entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.	Inspected the Password Policy to determine that the entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.	No exceptions noted.
CC6.1.3	Entity uses Sprinto, a continuous monitoring system, to alert the security team to update the access levels of team members whose roles have changed.	Inspected the Sprinto compliance automation tool that continuously monitors and alerts the security team to update the access levels of team members whose roles have changed.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.4	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Inspected that the users of the critical system have been identified and their access has been reviewed by the entity's Senior Management or the Information Security Officer periodically.	No exceptions noted.
CC6.1.5	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Inspected that the users of the critical system have been identified and their administrative access has been reviewed by the entity's Senior Management or the Information Security Officer periodically.	No exceptions noted.
CC6.1.6	Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.	Inspected that access to infrastructure assets has been restricted from the public.	No exceptions noted.
CC6.1.7	Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	Inspected records where Role Based Access to critical systems has been set up and validated to determine that the entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	No exceptions noted.
CC6.1.8	Entity has documented policies and procedures to manage physical and environmental security.	Inspected Physical Security Policy and Physical and Environmental Security Procedure to determine that the entity has documented policies and procedures to manage physical and environmental security.	No exceptions noted.
CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	Entity has documented policy and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	Inspected the Access Control Policy and Procedure to determine that the entity manages an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	No exceptions noted.
CC6.2.2	Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	Inspected records where Role Based Access to critical systems has been set up and validated to determine that the entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2.3	Entity ensures logical access that is no longer required in the event of a termination is made inaccessible in a timely manner.	Inspected records of logical access deactivation for terminated staff as part of the offboarding process to determine that the entity ensures logical access that is no longer required in the event of a termination is made inaccessible in a timely manner.	No exceptions noted.
CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.	Inspected records where the users of the critical system have been identified and their access to production database has been restricted to only those individuals who require such access to perform their job functions.	No exceptions noted.
CC6.3.2	Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	Inspected records where Role Based Access to critical systems has been set up and validated to determine that the entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	No exceptions noted.
CC6.3.3	Entity has documented policy to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	Inspected the Access Control Policy and Procedure to determine that the entity has documented policy to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	No exceptions noted.
CC6.3.4	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Inspected that the users of the critical system have been identified and their administrative access has been reviewed by the entity's Senior Management or the Information Security Officer periodically.	No exceptions noted.
CC6.3.5	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Inspected that the users of the critical system have been identified and their access has been reviewed by the entity's Senior Management or the Information Security Officer periodically.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.6	Entity ensures logical access that is no longer required in the event of a termination is made inaccessible in a timely manner.	Inspected records of logical access deactivation for terminated staff as part of the offboarding process to determine that the entity ensures logical access that is no longer required in the event of a termination is made inaccessible in a timely manner.	No exceptions noted.
CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.5.1	Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	Inspected the Media Disposal Policy to determine that the entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	No exceptions noted.
CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	Entity requires that all staff members with access to any critical system is protected with a secure login mechanism such as Multifactor authentication.	Observed Multifactor Authentication for all critical systems to determine that the entity requires that all staff members with access to any critical system is protected with a secure login mechanism.	No exceptions noted.
CC6.6.2	Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.	Observed the malware-protection software to determine that the entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.	No exceptions noted.
CC6.6.3	Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	Inspected the disk encryption and the endpoint security review results of staff devices to determine that the entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	No exceptions noted.
CC6.6.4	Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.	Observed that access to infrastructure assets has been restricted from the public.	No exceptions noted.
CC6.6.5	Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.	Observed auto-screen lock configuration on staff devices to determine that the entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.	No exceptions noted.
CC6.6.6	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the entity's cloud provider.	Observed the entity's firewall in the system to determine that every Production host is protected by a firewall with a deny-by-default rule.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6.7	Entity has documented policy and procedures for endpoint security and related controls.	Inspected the Endpoint Security Policy and Asset Management Policy and Procedure to determine that the entity has documented policies and procedures for endpoint security and related controls.	No exceptions noted.
CC6.6.8	Entity requires that all critical endpoints are encrypted to protect them from unauthorized access.	Inspected the disk encryption and the endpoint security review results of staff devices to determine that the entity requires that all critical endpoints are encrypted to protect them from unauthorized access.	No exceptions noted.
CC6.6.9	Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	Observed the updated OS versions of staff devices to determine that the entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	No exceptions noted
CC6.6.10	Entity develops, documents, and maintain an inventory of organizational endpoint systems, including all necessary information to achieve accountability.	Observed the staff devices health monitoring checks and Asset Management Policy and Procedure to determine that the entity develops, documents, and maintain an inventory of organizational endpoint systems, including all necessary information to achieve accountability.	No exceptions noted
CC6.6.11	Entity has documented guidelines to manage communications protections and network security of critical systems.	Inspected Communications and Network Security Policy and Network Security Procedure to determine that the entity has documented guidelines to manage communications protections and network security of critical systems.	No exceptions noted
CC6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives			
CC6.7.1	Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	Inspected the disk encryption and the endpoint security review results of staff devices to determine that the entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	No exceptions noted.
CC6.7.2	Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.	Observed that the data at rest has been encrypted to determine that the entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.7.3	Entity has set up processes to utilize standard encryption methods, including HTTPS with the TLS algorithm, to keep transmitted data confidential.	Observed the https (TLS algorithm) and industry standard encryption to determine that the entity has set up processes to utilize standard encryption methods to keep transmitted data confidential.	No exceptions noted.
CC6.7.4	Entity develops, document, and maintain an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.	Observed that the critical infrastructure assets have been identified to determine that the entity develops, document, and maintain an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.	No exceptions noted.
CC6.7.5	Entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment.	Observed that the critical infrastructure assets have been identified to determine that the entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment.	No exceptions noted.
CC6.7.6	Entity has a documented policy to manage encryption and cryptographic protection controls.	Observed the Encryption Policy to determine that the entity has a documented policy to manage encryption and cryptographic protection controls.	No exceptions noted.
CC6.7.7	Entity requires that all critical endpoints are encrypted to protect them from unauthorized access.	Inspected the disk encryption and the endpoint security review results of staff devices to determine that the entity requires that all critical endpoints are encrypted to protect them from unauthorized access.	No exceptions noted.
CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the entity's cloud provider.	Observed the entity's firewall in the system to determine that every Production host is protected by a firewall with a deny-by-default rule.	No exceptions noted.
CC6.8.2	Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	Observed the updated OS versions of staff devices to determine that the entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	No exceptions noted.
CC7.0: SYSTEM OPERATIONS			
CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	Observed that the vulnerabilities have been identified and remediated as per the Vulnerability Management Policy defined to manage vulnerabilities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.2	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	Observed the Production assets and their monitoring alert configurations to determine that the entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	No exceptions noted.
CC7.1.3	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	inspected records of vulnerability scans to determine that the entity identifies vulnerabilities on the Company platform.	No exceptions noted.
CC7.1.4	Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.	Observed that the threat detection system has been enabled to determine that the entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.	No exceptions noted.
CC7.1.5	Entity has a documented policy and procedures to establish guidelines on managing technical vulnerabilities.	Inspected the Vulnerability Management Policy to determine that the entity has a documented policy and procedures to establish guidelines on managing technical vulnerabilities.	No exceptions noted.
CC7.1.6	Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	Observed that the audit logs exist to determine that the entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	No exceptions noted.
CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Inspected the records of vulnerability scans to determine that the entity identifies vulnerabilities on the Company platform.	No exceptions noted.
CC7.2.2	Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	Observed that the vulnerabilities have been identified and remediated as per the Vulnerability Management Policy defined to manage vulnerabilities.	No exceptions noted.
CC7.2.3	Entity has a documented policy and procedures to establish guidelines on managing technical vulnerabilities.	Inspected the Vulnerability Management Policy to determine that the entity has a documented policy and procedures to establish guidelines on managing technical vulnerabilities.	No exceptions noted.
CC7.2.4	Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	Observed that the audit logs exist to determine that the entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2.5	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	Observed the Production assets and their monitoring alert configurations to determine that the entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	No exceptions noted.
CC7.2.6	Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.	Observed that the threat detection system has been enabled to determine that the entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.	No exceptions noted.
CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures			
CC7.3.1	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inspected the Internal Audit Report on Sprinto compliance automation tool to determine that the entity continuously monitors, tracks and reports the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.
CC7.3.2	Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	Observed the updated OS versions of staff devices to determine that the entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	No exceptions noted.
CC7.3.3	Entity maintains a record of information security incidents, its investigation and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.	Inspected the record of information security incidents to determine that the entity maintains a record of information security incidents, its investigation and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.	No exceptions noted.
CC7.3.4	Entity has a documented policy and procedures to establish guidelines on managing technical vulnerabilities.	Inspected the Vulnerability Management Policy to determine that the entity has a documented policy and procedures to establish guidelines on managing technical vulnerabilities.	No exceptions noted.
CC7.3.5	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Inspected records of vulnerability scans to determine that the entity identifies vulnerabilities on the Company platform.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3.6	Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	Observed that the vulnerabilities have been identified and remediated as per the Vulnerability Management Policy defined to manage vulnerabilities.	No exceptions noted.
CC7.3.7	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	Observed the Production assets and their monitoring alert configurations to determine that the entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	No exceptions noted.
CC7.3.8	Entity has documented guidelines on notifying customers and other stakeholders in case of a breach.	Inspected Data Breach Notification Policy to determine that the entity has documented guidelines on notifying customers and other stakeholders in case of a breach.	No exceptions noted.
CC7.3.9	Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.	Observed that the threat detection system has been enabled to determine that the entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.	No exceptions noted.
CC7.3.10	Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	Observed that the audit logs exist to determine that the entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	No exceptions noted.
CC7.3.11	Entity identifies vulnerabilities on the company platform through an annual penetration testing exercise conducted by a qualified third-party service provider.	Inspected records of the annual penetration testing exercise conducted by a qualified third party service provider to determine that the entity identifies vulnerabilities on the company platform annually.	No exceptions noted.
CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inspected the Internal Audit Report on Sprinto compliance automation tool to determine that the entity continuously monitors, tracks and reports the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.
CC7.4.2	Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.	Inspected Incident Management Policy and Procedure to determine that the entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.4.3	Entity maintains a record of information security incidents, its investigation and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.	Inspected the record of information security incidents to determine that the entity maintains a record of information security incidents, its investigation and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.	No exceptions noted.
CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Entity has documented guidelines to manage Disaster Recovery that establishes guidelines and procedures for continuing business operations in case of a disruption or a security incident.	Inspected the Business Continuity Plan, Business Continuity Policy and Disaster Recovery Policy to determine that the entity has documented guidelines to manage Disaster Recovery that establishes guidelines and procedures for continuing business operations in case of a disruption or a security incident.	No exceptions noted.
CC7.5.2	Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	Inspected the Data Backup Policy to determine that the entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	No exceptions noted.
CC7.5.3	Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	Inspected the Business Continuity Plan, Business Continuity Policy and Disaster Recovery Policy to determine that the entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	No exceptions noted.
CC7.5.4	Entity has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	Inspected the Business Continuity Plan, Business Continuity Policy and Disaster Recovery Policy to determine that the entity has documented policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	No exceptions noted.
CC8.0: CHANGE MANAGEMENT			
CC8.1: The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	Entity develops, document, and maintain an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.	Observed that the critical infrastructure assets have been identified to determine that the entity develops, document, and maintain an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.2	Entity has documented policies and procedures to manage changes to its operating environment.	Inspected the Change Management Policy to determine that the entity has documented policies and procedures to manage changes to its operating environment.	No exceptions noted.
CC8.1.3	Entity has procedures to govern changes to its operating environment.	Inspected the Change Management source and repos to determine that the entity has procedures to govern changes to its operating environment.	No exceptions noted.
CC8.1.4	Entity has established procedures for approval when implementing changes to the operating environment.	Observed change request reviews and approval by peers to determine that the entity has established procedures for approval when implementing changes to the operating environment.	No exceptions noted.
CC9.0: RISK MITIGATION			
CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions			
CC9.1.1	Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate entity's service commitments and system requirements.	Inspected the Risk Management Policy to determine that the entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated incorporating the entity's service commitments and system requirements.	No exceptions noted.
CC9.1.2	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	Inspected the annual formal risk assessment exercise records to determine that the entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	No exceptions noted.
CC9.1.3	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	Inspected the risk assessment documentation to determine that each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	No exceptions noted.
CC9.2: The entity assesses and manages risks associated with vendors and business partners			
CC9.2.1	Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate entity's service commitments and system requirements.	Inspected the Risk Management Policy to determine that the entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated incorporating the entity's service commitments and system	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.2.2	Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors.	Inspected the Vendor Management Policy & Procedure to determine that the entity has a documented policy and procedure to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors.	No exceptions noted.
CC9.2.3	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	Inspected the vendor risk assessment documentation to determine that the entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	No exceptions noted.

AVAILABILITY PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.0: ADDITIONAL CRITERIA FOR AVAILABILITY			
A.1.1: The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
A1.1.1	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	Observed the Production assets and their monitoring alert configurations to determine that the entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	No exceptions noted.
A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
A1.2.1	Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	Inspected the Data Backup Policy to determine that the entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	No exceptions noted.
A1.2.2	Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.	Observed that periodical backup has been enabled on the production database to determine that the entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.	No exceptions noted.
A1.2.3	Entity tests backup information periodically to verify media reliability and information integrity.	Observed the database backup restore exercise notes to determine that the entity tests backup information periodically to verify media reliability and information integrity.	No exceptions noted.
A1.2.4	Entity has documented guidelines to manage Disaster Recovery that establishes guidelines and procedures for continuing business operations in case of a disruption or a security incident.	Inspected the Business Continuity Plan, Business Continuity Policy and Disaster Recovery Policy to determine that the entity has documented guidelines to manage Disaster Recovery that establishes guidelines and procedures for continuing business operations in case of a disruption or a security incident.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.5	Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	Inspected the Business Continuity Plan, Business Continuity Policy and Disaster Recovery Policy to determine that the entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	No exceptions noted.
A1.2.6	Entity has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	Inspected the Business Continuity Plan, Business Continuity Policy and Disaster Recovery Policy to determine that the entity has documented policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	No exceptions noted.
A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Entity tests backup information periodically to verify media reliability and information integrity.	Observed the database backup restore exercise notes to determine that the entity tests backup information periodically to verify media reliability and information integrity.	No exceptions noted.
A1.3.2	Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.	Observed the disaster recovery exercise notes to determine that the entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.	No exceptions noted.
A1.3.3	Entity has documented guidelines to manage Disaster Recovery that establishes guidelines and procedures for continuing business operations in case of a disruption or a security incident	Inspected the Business Continuity Plan, Business Continuity Policy and Disaster Recovery Policy to determine that the entity has documented guidelines to manage Disaster Recovery that establishes guidelines and procedures for continuing business operations in case of a disruption or a security incident.	No exceptions noted.
A1.3.4	Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	Inspected the Business Continuity Plan, Business Continuity Policy and Disaster Recovery Policy to determine that the entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.3.5	Entity has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	Inspected the Business Continuity Plan, Business Continuity Policy and Disaster Recovery Policy to determine that the entity has documented policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	No exceptions noted.

CONFIDENTIALITY PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.0: ADDITIONAL CRITERIA FOR CONFIDENTIALITY			
C1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.1	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	Inspected the company policies to determine that the entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding. Observed that the policies have been reviewed and acknowledged by new staff members.	No exceptions noted.
C1.1.2	Entity has established procedures for staff to acknowledge applicable company policies periodically.	Inspected the company policies to determine that the entity has established procedures for staff to acknowledge applicable company policies periodically. Inspected records that the policies have been reviewed and acknowledged by staff members.	No exceptions noted.
C1.1.3	Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.	Observed that the data at rest has been encrypted to determine that the entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.	No exceptions noted.
C1.1.4	Entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification.	Inspected Data Classification Policy to determine that the entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification.	No exceptions noted.
C1.1.5	Entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems.	Inspected Information Security Policy to determine that the entity has a documented policy that govern the confidentiality, integrity, and availability of information systems.	No exceptions noted.
C1.1.6	Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	Inspected the disk encryption and the endpoint security review results of staff devices to determine that the entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.2: The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C1.2.1	Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	Inspected the Media Disposal Policy to determine that the entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	No exceptions noted.
C1.2.2	Entity has a documented policy outlining guidelines for the disposal and retention of information.	Inspected the Data Retention Policy to determine that the entity has a documented policy outlining guidelines for the disposal and retention of information.	No exceptions noted.

GDPR Independent Assessment Report

INTRODUCTION

The General Data Protection Regulation (GDPR) (EU 2016/679) came into force on May 25th, 2018, and since have enabled European citizen to have their data protected by a strong legal framework with significant transparency such as the informed consent, right to erasure and right to modifications.

GDPR requirements

The protection of the rights and freedoms of natural persons with regard to the processing of personal data requires that appropriate technical and organizational measures be taken to ensure that the requirements of this Regulation are met.

In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures that meet in particular the principles of **data protection by design and data protection by default**. Such measures could consist, inter alia, of:

- Minimizing the processing of personal data,
- Pseudonymizing personal data as soon as possible,
- Transparency with regard to the functions and processing of personal data,
- Enabling the data subject to monitor the data processing,
- Enabling the controller to create and improve security features.

When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

GDPR roles and definition

Key definitions:

‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

‘Processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

‘Data processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

‘Data controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

In addition to these definitions, the GDPR brings a new role in the process of managing privacy: the Data Protection Officer (DPO). Given the GDPR, the “role of the data protection officer (DPO) is to ensure that her organization processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules. In the EU institutions and bodies, the applicable Data Protection Regulation (Regulation (EU) 2018/1725) obliges them each to appoint a DPO. Regulation (EU) 2016/679, which obliges some organizations in EU countries to appoint a DPO”, is applicable since 25 May 2018. This role is defined by the following GDPR articles:

- Art. 37 GDPR Designation of the data protection officer
- Art. 38 GDPR Position of the data protection officer
- Art. 39 GDPR Tasks of the data protection officer

The DPO is also the orchestrator of the data privacy impact assessment (DPIA) and shall ensure the following items before signing off the DPIA and record outcomes:

- Whether a DPIA is needed or not?
- How you should the DPIA conducted, especially if it involves third parties regarding data collection and processing?
- Whether to outsource the DPIA or not, via consultancy?
- Assess necessity and proportionality.
- Identify and assess risks.
- Which risk mitigation is necessary (minimization, etc)?
- DPIA is complete with all necessary sections.

GDPR obligations

Main GDPR obligations and data subject's rights:

- Lawfulness of processing, Article 6 GDPR
- Purpose limitation, Article 5 GDPR,
- Data minimisation, Article 5 GDPR,
- Accuracy, Article 5 GDPR
- Storage minimisation, Article 5 GDPR
- Accountability, Article 5 GDPR
- The right to be informed, Articles 13 and 14 GDPR
- Transparency and modalities, Article 12 GDPR
- Consent management, Article 7 GDPR
- The right of access, Article 15 GDPR
- The right to rectification, Article 16 GDPR
- The right to erasure (partial or complete), Article 17 GDPR
- The right to restriction of processing, Article 18 GDPR
- The right to data portability (exporting and importing data), Article 20 GDPR
- Integrity, confidentiality, and security (secure and trusted data protection), Articles 5, 25 and 32 GDPR
- Supervision of processor, Article 28 GDPR
- Records of processing activities, Article 30 GDPR
- Breach notification Articles 33 and 34

SCOPE

Client Reg. No.	EAC-504295 Dated: 11-03-2025
Date of Assessment	25-02-2025
Name of the Organization	Neofin Global Inc.
Client Location / Site Address	919 North Market Street, Suite 950, City of Wilmington, County of New Castle, Zip Code 19801, State of Delaware, US
Assessment Criteria	General Data Protection Regulation (GDPR) standards requirements applicable to the information systems including people, processes, and technology.
Assessment Objective	<ul style="list-style-type: none">• Ensure that the client's management system documentation meets the requirements of the standard/specification.• To confirm that the client organization adheres to its own policies, objectives, and procedures and all the requirements of the GDPR standard and other normative documents.• To verify the implementation of the General Data Protection Regulation (GDPR) as per the Standard Requirement, verification of records for the conformity of said implementation.
Client Contact Person Name	Oleksandr Kshutashvili Designation: Privacy Officer
Assessor Name	Hitesh Kumar Mittal
Scope of Certification	"Design, Development, Maintenance, Technical Support, Sales And Marketing of Neofin Core: Lending Automation SaaS Platform"
Inherent Limitations	A high-level review of operational controls and sample testing of areas may lead to inaccurate sampling bias for this assessment.

ASSESSMENT

Accountability Governance		
Does the organisation maintain a Data Protection Policy that demonstrates compliance with requirements including processing, privacy by design and record keeping?	Yes	Evidenced Data Protection Policy in Sprinto compliance automation tool.
Does the organisation train all employees on GDPR requirements and principles — including processing activities, controls, privacy impact assessments, audits, data subject rights, reporting lines and privacy by design — and the potential impact of noncompliance?	Yes	Evidenced GDPR requirements and principles covered training material in Sprinto compliance automation tool. Instructed to carryout periodic trainings.
Does the organisation regularly test, retrain and maintain records of training for employees who handle personal data on their understanding of GDPR requirements?	Yes	Evidenced training logs for all employees.
Does the organisation require a data protection officer (DPO), does he or she have reporting authority to the highest level of management, necessary resources, independence, and authority to ensure compliance with the GDPR and other data protection laws?	Yes	Privacy Officer has been appointed. Evidenced ISMS Roles and Responsibilities in Sprinto compliance automation tool.
Is the DPO bound by secrecy or confidentiality concerning the performance of his or her tasks?	Yes	
If the DPO has other responsibilities, have they been assessed to avoid conflicts of interest?	Yes	
Does the DPO have the knowledge and ability to fulfil tasks?	Yes	
Has the organisation shared the DPO's contact information internally, publicly and with the relevant supervisory authority?	Yes	Verified that Top management has shared the Privacy Officers's contact information.

Processing Principles		
Does the organisation maintain records management and Data Retention Policies?	Yes	Evidenced within Data Retention Policy in Sprinto compliance automation tool.
Does the organisation have documented principles to justify retention periods?	Yes	
Is personal data processed lawfully, fairly and in a transparent manner?	Yes	Verified that Data Processing Principles are mentioned in Data Protection Policy. Evidenced the same in Sprinto compliance automation tool.
Is personal data collected for specified, explicit and legitimate purposes, and not further processed in a manner incompatible with those purposes?	Yes	
Is personal data relevant, limited and minimized to what is necessary in relation to the purposes for which they are processed?	Yes	
Is personal data accurate and kept up to date — and is every reasonable step taken to ensure inaccurate personal data is erased and rectified without delay?	Yes	
Is personal data kept only for as long as is necessary for the purposes for which it is processed?	Yes	Evidenced within Data Retention Policy in Sprinto compliance automation tool.
Is personal data processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures?	Yes	Evidenced within Privacy by Design Policy in Sprinto compliance automation tool.
Has the organisation clearly identified, detailed, documented and kept up to date the purpose(s) of processing personal data?	Yes	Evidenced Privacy by Design Policy.
Has the organisation implemented appropriate technical or organizational measures to ensure security of personal data, including protection against unauthorized processing, accidental loss, destruction, or damage?	Yes	All relevant technical measures are implemented.
If the organisation processes special categories of sensitive data (revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation), are you in compliance with Article 9(2) conditions?	N/A	
If the organisation processes personal data relating to criminal convictions and offenses or related security measures based on Article 6(1), is this carried out under the control of official authority or authorized by union or member state law?	N/A	

Privacy by Design and Default		
Does the organisation ensure processes are in place to embed Privacy By Design and Default into projects, to include measures that ensure data minimization, pseudonymization, encryption and the processing of only personal data necessary for specified purposes?	Yes	Mentioned and Evidenced Privacy by Design Policy.
Does the organisation restrict access to personal data to only those employees processing the data?	Yes	Evidenced Access Control Policy and Procedure in Sprinto compliance automation tool.
Does the organisation frequently audit and test systems and services to ensure ongoing confidentiality, integrity, availability and resilience?	Yes	Verified that Internal Audit is being conducted on regular intervals.
Does the organisation ensure processes and systems can be restored in the event of physical or technical incidents?	Yes	Evidenced Business Continuity Plan and Business Continuity Policy & Disaster Recovery Policy in Sprinto compliance automation tool.
Does the organisation maintain a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures to ensure the security of the processing?	Yes	ISO 27001 framework in place.
Does the organisation apply storage and processing methods (e.g., redaction) to hard copies of personal data?	N/A	
Does the organisation maintain documented data destruction procedures in place for information that is no longer necessary — and does the organization take steps to ensure employees comply with procedures?	Yes	Mentioned and Evidenced Data Retention Policy in Sprinto compliance automation tool.

Data Protection Impact Assessment		
Does the organisation carry out a Data Protection Impact Assessment (DPIA) whenever the use of new technologies is likely to result in high risk to data subjects, decisions from automated processing have a legal impact, processing involves special categories of data referred to in Article 9(1) or 10, or include large-scale systematic monitoring of publicly accessible areas?	Yes	Information Security risks are addressed in Risk Assessment Worksheet. Evidenced the same in Sprinto compliance automation tool.
Is the DPO always involved when carrying out a DPIA?	Yes	Evidenced in Privacy Officer's roles and responsibilities.
Does the DPIA contain a systematic description of the envisaged processing operations, the purpose of processing, an assessment of the necessity and proportion of processing in relation to the purposes, an assessment of the risks to rights and freedoms of data subjects, and measures envisaged to address the risks, such as safeguards and security measures?	Yes	Information Security risks are addressed in Risk Assessment Worksheet. Evidenced the same in Sprinto compliance automation tool.
Where appropriate, does the organisation seek the views of data subjects or their representatives on intended processing?	N/A	
Does the organisation have a process in place for detecting changes in risks — and do you review DPIAs for changed risks?	Yes	Mentioned in Risk Management Policy, Evidenced the same in Sprinto compliance automation tool.
Are risks arising from each DPIA mitigated?	Yes	Verified that risks are addressed and treated.
When risks cannot be mitigated, does the organisation contact the supervisory authority with a list of controller and processor responsibilities, the purposes and means of intended processing, measures and safeguards provided to protect data subjects, the DPO's contact details, the DPIA and any other requested information?	N/A	

Records of Processing		
If the organisation is a controller employing more than 250 people or processing types of data listed in Article 30(5), does it maintain a record of processing activities containing the name and contact details of the controller and DPO, the purpose of processing, a description of data subject and personal data categories, categories of recipients to whom personal data have been or will be disclosed, international transfers of data, time limits for data erasure, and a description of technical and organizational security measures in place?	N/A	
If the organisation is a processor employing more than 250 people or processing types of data listed in Article 30(5), does it maintain a record of processing activities containing the name and contact details of the processor, controller and DPO; categories of processing carried out on behalf of each controller; international transfers of data; and a description of technical and organizational security measures in place?	N/A	
Does the organisation ensure records of processing activities are maintained in writing and available to the supervisory authority on request?	Yes	Verified that Processing principles are in place in Data Protection Policy.

Data Subject Rights		
Where a data subject exercises their right of access, does the organisation ensure they are provided with all items listed in Article 15(1)?	Yes	Mentioned and Evidenced Data Protection Policy in Sprinto compliance automation tool.
Does the organisation maintain processes for rectifying inaccurate personal data and having incomplete personal data completed?	Yes	Mentioned and Evidenced Data Subject Rights in Data Protection Policy in Sprinto compliance automation tool.
Where a data subject requests the erasure of personal data, does the organisation take every reasonable step to erase all data, links, and copies without undue delay and when Article 17(1) grounds apply?	Yes	Mentioned and Evidenced Data Retention Policy in Sprinto compliance automation tool.
Where the accuracy of personal data is contested, does the organisation restrict processing to enable verification of accuracy?	Yes	Mentioned and Evidenced Data Subject Rights in Data Protection Policy in Sprinto compliance automation tool.
Where processing is no longer necessary or lawful, does the organisation have a process for restricting processing when requested by data subjects?	Yes	
Does the organisation ensure data subjects who have obtained restriction of processing are informed before restrictions are lifted?	Yes	
Does the organisation notify all processors and other personal data recipients of rectifications, erasures and restrictions of processing?	Yes	
Where a data subject exercises their right to data portability, does the organisation transmit data to another controller without hindrance, by automated means, and in a common and machine-readable format?	N/A	
Where data subjects object to having their data processed for direct marketing, does the organisation no longer process their data?	N/A	
Where data subjects object to having their data processed for research or official purposes, do you no longer process their data unless you can present compelling legitimate grounds?	N/A	
Does the organisation ensure data subjects have the right not to be subject to legal or similarly affecting decisions based on automated processing?	N/A	

Consent and Notices		
Is the organisation able to demonstrate that data subjects have consented to the processing of their data?	Yes	Evidenced Data Subject Access Requests Report in Sprinto compliance automation tool.
Are consent requests clearly distinguishable from other matters, in an intelligible and accessible form, and written in clear and plain language?	Yes	
Are data subjects asked to positively opt-in (separate and unticked opt-in boxes per Recital 32)?	Yes	
Do data subjects have the right to withdraw consent at any time — and is withdrawing consent as easy as giving consent?	Yes	Evidenced Data Subject Access Request Rights.
Where processing data of subjects below the age of 16 years, is consent given and authorized by the holder of parental responsibility — and are reasonable efforts made to verify this consent?	N/A	
Are privacy notices and policies clearly provided to data subjects with processor and DPO contact information, purposes of processing, legal bases for processing, recipients of personal data, international transfers, data retention periods and data subject rights?	Yes	Evidenced Privacy by Design Policy and Data Protection Policy in Sprinto compliance automation tool.
Where personal data is not obtained directly from data subjects, does the organisation provide categories of personal data and the originating sources?	N/A	
Are privacy notices and policies provided to data subjects at the time of collection from data subjects or within one month when not obtained from data subjects?	N/A	
Are privacy notices and policies provided to data subjects prior to further processing when they have not previously been communicated?	N/A	
Are all communications with data subjects provided in writing using clear, concise, and transparent language?	Yes	Verified that all communications to data subjects are in transparent language, Popups appear on the website clearly.
If the organisation does not take action on requests of the data subject, does the organisation inform the data subject of reasons for not taking action, without delay and within one month of receipt, and include possibilities for lodging complaints with a supervisory authority or seeking judicial remedy?	Yes	Mentioned and Evidenced Data Subject Rights in Data Protection Policy in Sprinto compliance automation tool.

Breach Management		
Does the organisation maintain breach incident and Notification Policies and Procedures?	Yes	Evidenced Data Breach Notification Policy and PHI Data Breach Notification Procedure in Sprinto compliance automation tool.
Are security measures (e.g., backup, pseudonymization, encryption, testing) implemented and appropriate for data risks?	Yes	Evidenced Encryption Policy in Sprinto compliance automation tool.
Does the organisation have an up-to-date Data Breach Response Plan?	Yes	Evidenced Data Breach Notification Policy in Sprinto compliance automation tool.
Does the organisation investigate and take corrective action for all personal data breaches regardless of size or scope?	Yes	Mentioned and Evidenced Data Breach Notification Policy and PHI Data Breach Notification Procedure in Sprinto compliance automation tool.
For breaches likely to result in a risk to data subjects, does the organization report the breach to the supervisory authority within 72 hours with categories and the number of subjects concerned, the categories and number of data records concerned, the DPO's contact information, the likely consequences of the data breach, and measures proposed or taken to address the breach?	Yes	
If the organisation is a processor, does it notify the controller without undue delay after becoming aware of a data breach?	Yes	
Does the organisation maintain a data breach register including facts related to the breach, effects and remedial actions taken?	Yes	Mentioned and Evidenced Data Breach Notification Policy and PHI Data Breach Notification Procedure in Sprinto compliance automation tool.
Does the organisation communicate breaches to affected data subjects without undue delay and in clear and plain language?	Yes	Mentioned and Evidenced Data Breach Notification Policy and PHI Data Breach Notification Procedure in Sprinto compliance automation tool.

Processors		
Does the organisation maintain policies and procedures for contracting and conducting due diligence on processors and sub processors?	Yes	Covered under Data Protection Policy and Acceptable Usage Policy in Sprinto compliance automation tool.
Does the organisation only use processors that ensure protection of data subject rights using appropriate technical and organizational measures?	Yes	
If the organisation is a processor, does it not engage with other processors without prior specific and general written authorization from the controller?	N/A	
Are all processors governed by a contract that establishes the subject matter of processing, duration of processing, nature and purpose of processing, type of personal data and categories of data subjects, and obligation and rights of the controller?	N/A	
Do contracts and service level agreements with processors outline international data transfers restrictions, ensure confidentiality from persons processing personal data, ensure deletion or return of personal data to controllers at the end of services, allow controllers and auditors to obtain information necessary for inspections and audits, and include all Article 32 security measures?	N/A	
Do processors ensure data protection by design and default in all processing activities?	Yes	Mentioned and Evidenced Privacy by Design Policy.

Data Transfer		
When transferring or disclosing personal information, does the organisation encrypt data and only send necessary data?	Yes	Evidenced Encryption Policy in Sprinto compliance automation tool.
Does the organisation use secure data transfer methods for all communications (e.g., email, file transfers, website forms, payments)?	Yes	Verified that secure data transfer methods are in place.
Has the organisation identified all international data flows and export mechanisms?	Yes	Evidenced the System flow.
Are international data transfers authorized by the Commission (Article 45) or appropriately safeguarded in addition to preserving data subject rights and legal remedies (Article 46)?	N/A	
Does the organization regularly check the Official Journal of the European Union for the commission's withdrawals and changes to data transfer authorizations?	N/A	
Are appropriate data transfer safeguards provided for by contractual clauses or provisions inserted into administrative arrangements?	N/A	
When relying on binding corporate rules for data transfers, does the organisation ensure they are legally binding and apply to and are enforced by every member concerned of the group of undertakings, in addition to expressly conferring enforceable rights on data subjects with regard to the processing of their personal data?	N/A	
Do binding corporate rules specify all items in Article 47(2)?	N/A	

OPINION

Summary of the Assessment

Taking account of the observations made in this report, in our opinion the controls operating within the system, provide only **satisfactory assurance** as part of the process to mitigate risks to an acceptable level.

Limited	Satisfactory	Substantial
There is a risk of objectives not being met due to serious control failings.	A framework of controls is in place, but controls need to be strengthened further.	There is a robust framework of controls which are applied continuously.

Recommendation

Issuance of compliance certification

Reason

The system complies with the requirements of the GDPR standards and other normative documents. Based on the above summary, the Assessor is pleased to put forward a recommendation for the issuance of Compliance Certification.



Hitesh Kumar Mittal
Assessor



European Assessment and Certification

This Certificate of Compliance has been awarded to

Neofin Global Inc.

919 North Market Street, Suite 950,
City of Wilmington, County of New Castle,
Zip Code 19801, State of Delaware, US

In recognition of the organization's Management System that conforms to the
requirements of

GDPR General Data Protection Regulation

The scope of this certificate is applicable to

**Design, Development, Maintenance, Technical Support, Sales
And Marketing of Neofin Core: Lending Automation SaaS
Platform**

Certificate No : EAC-504295

Certificate issue date : 11-03-2025
Certificate expiry date : 10-03-2028

1st Surveillance due before : 10-03-2026
2nd Surveillance due before : 10-03-2027



Authorised Signatory
European Assessment and Certification

