

Management System
Audit Report of **Coalesce Automation, Inc.**

ISO/IEC 27001:2022

Initial Certification Audit Report - 2024

TABLE OF CONTENTS

EXECUTIVE SUMMARY .....

COMPANY BACKGROUND .....

AUDIT INFORMATION .....

AUDIT PREPARATION AND METHODOLOGY .....

STAGE 1 CERTIFICATION AUDIT – NON-CONFORMITIES (NC) .....

AUDIT TEST DETAILS .....

AUDIT FINDINGS – INITIAL CERTIFICATION .....

STAGE 2 CERTIFICATION AUDIT – NON-CONFORMITIES (NC) .....

OBSERVATIONS .....

OPPORTUNITIES FOR IMPROVEMENT .....

AUDIT CONCLUSIONS AND AUDIT RECOMMENDATIONS .....

AUDIT CONCLUSIONS .....

AUDIT RECOMMENDATION .....

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

EXECUTIVE SUMMARY

Coalesce Automation, Inc. engaged Prescient Security LLC ("Prescient Security") to review its Information Security Management System (ISMS) against those requirements detailed within the ISO/IEC 27001:2022 standard. The objective of this engagement was to assess the conformance of the client's defined ISMS as an accredited certification body bound by the procedures detailed within ISO/IEC 17021-1:2015, ISO/IEC 27006:2015/Amd 1:2020, and IAF MD 4:2018, where applicable.

This audit report provides Coalesce Automation, Inc. the results of the ISO/IEC 27001:2022 Initial Certification Audit (Stage 1 and Stage 2) conducted from March 12-15, 2024 for the Stage 1 audit and from March 18-26, 2024 for the Stage 2 audit.

The audit team has conducted the audit based on the organization's defined processes in correspondence with the audit plan. The audit conducted by a professional team was a process-based audit with a focus on the significant aspects, risks and objectives.

This report has been developed in accordance with the requirements described in ISO/IEC 17021-1:2015, ISO/IEC 27006:2015, and IAF MD 4:2018. These standards were utilized as a technical reference and guide for determining the audit approach, such as the required number of audit days and minimum competence of the audit team members. This report details activities and conclusions from the Initial Certification Audit (Stage 1 and Stage 2), inclusive of the following items:

- Scope of the Initial Certification Audit
- Results of the Initial Certification Audit
- Recommendations prior to the decision for certification issuance

During the course of the audit process, the management system has proven overall conformity with the requirements of the standard. The audit team has concluded that your organization has established a management system according to the requirements of the standard and proved the ability of the system can consistently achieve the approved requirements for the services within the scope of your organization and on your organization's policy and objectives.

The conformance level with the standard can still be improved even though seven (7) non-conformities have been found during the audit. Five (5) minor non-conformities were raised during the Stage 1 audit and two (2) minor non-conformities were raised during the stage 2 audit. All NCs identified during the course of the audit have been closed. This was a sample-based audit. Non-conformities and other opportunities for improvement can still be found in the audited areas.

Referring to the results of the audit process and the demonstration of the organization's development and maturity, the audit team recommends that your organization's management system should be granted certification for ISO/IEC 27001:2022.

Sanjeev Tiwari

Khushal Lonkar
Lead Auditor

Prepared by: *Deepika Pandey*

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

COMPANY BACKGROUND

Coalesce Automation develops data management platforms that automate data activities. The company's platform combines the speed of an intuitive graphical user interface (GUI), the flexibility of code, and the effectiveness of data transformation automation, allowing businesses to obtain effective data management and analytics capabilities.

Coalesce was incorporated in 2020 and located in San Francisco, California, United States.

SERVICES PROVIDED

Coalesce develops a data management software to automate data operations.

AUDIT INFORMATION

ORGANIZATION INFORMATION

Company name:	Coalesce Automation, Inc.
Company address:	1160 Battery St East, Suite 100, San Francisco, CA 94111
Website:	https://coalesce.io
Phone number:	(347) 324-8663
Client representative name:	Tyler Carbone
Client representative email:	tyler@getagency.com
Total number of employees within the scope:	84

AUDIT INFORMATION

Audit standard(s):	ISO/IEC 27001:2022
Audit #:	ISO - 8680
Audit type:	Initial Certification
Duration:	11 Days
Lead auditor:	Sanjeev Tiwari
Additional team member(s):	Deepika Pandey (Associate Auditor) Marilu Duque (Associate Auditor)
Additional attendees and roles:	N/A
Method of audit:	The audit was performed remotely via Microsoft Teams.
Joint, combined, integrated?	N/A

LOCATIONS VISITED DURING AUDIT

The Initial Certification Audit (Stage 1 and Stage 2) were performed remotely in accordance with IAF MD 4:2018. The organization is remote and fully cloud hosted. There were no physical locations within the scope of the ISMS for this audit.

Date	Location	Auditor
N/A	N/A	N/A

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

CERTIFICATION SCOPE

Scope of Certification	The scope of the ISO/IEC 27001:2022 certification is limited to the Information Security Management System (ISMS) supporting Coalesce Automation, Inc. which provides data transformation solutions for Client Snowflake instances. The scope also includes the people, process, technology, legal, regulatory, and contractual requirements related to the departments such as Information Technology (IT), Software Development (Dev), Human Resources (HR), Information Security (InfoSec), Legal, and Finance. This is in accordance with the Statement of Applicability Version 2.0.
Date	March 15, 2024

AUDIT PREPARATION AND METHODOLOGY

AUDIT OBJECTIVES

The audit objectives included the following:

- Determine the conformance of the ISMS to the ISO/IEC 27001 standard, specifically with regard to achieving the objectives of Coalesce Automation, Inc.'s information security policy and maintenance, monitoring, and improvement activities of the ISMS, specifically applicable to the audit scope.
- Effectiveness of the procedures and processes for evaluation and review of compliance with relevant information security legislation and regulations, specifically applicable to the audit scope.

AUDIT SCOPE

The audit scope covered the documentation requirements of the ISO/IEC 27001 standard, as well as the associated testing, which included evidence of the monitoring, maintenance, and operating effectiveness of the ISMS and test of the applicable control framework, relevant to the audit scope. The audit program included the following, all relevant to the scope of the audit scope:

- The organization's organizational unit
- IT Infrastructure
- Software
- People
- Processes

AUDIT CRITERIA

Audit criteria are:

a) Clauses 4-10 are requirements under ISO/IEC 27001:2022
b) ISO/IEC 27001:2022 Annex – A security controls as per SOA
c) Policy, Process, and Records related to the above requirements

AUDIT METHODOLOGY

The audit team has conducted a process-based audit focusing on the significant aspects, risks, and objectives. The auditors have used audit procedures to collect evidence in order to validate the conformity of the management system of the organization. The use of audit procedures in a systematic way reduces the audit risk and reinforces the objectivity of the audit conclusions.

The audit methods used consisted of remote interviews, using Information and Communication Technology (ICT) for the audit procedures, virtual observations of activities, review of electronic documentation and records, technical tests, and analysis of

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

sampling via the Vanta compliance automation platform. These procedures were deemed to meet the audit objectives completely and effectively.

The analysis procedure allows the audit team to draw conclusions concerning a whole by examining a part. It allows the auditor to estimate characteristics of a population by directly observing a part of the whole population.

Technical tests, including testing of the effectiveness of a process or control have not been performed by the auditor themselves. The operations have always been performed by the personnel of the auditee.

AUDIT PLANNING

Prescient Security has established an initial contact with the auditee to make arrangements for this audit, including scheduling the dates. The Lead Auditor has validated the feasibility of the audit, the audit objectives, the audit scope, the location, and the audit criteria.

Prescient Security facilitated the offsite documentation review of electronic evidence submissions via Vanta compliance automation platform.

The audit plan was sent to the auditee, and it was discussed during the opening meeting between the audit team and the auditee.

The remote audit was started with an opening meeting which has been attended by the individuals responsible for the ISMS. The Prescient Security overview, audit purpose, methodology, reporting system, appeal process and confidentiality were briefly presented to the client during the opening meeting.

There were no deviations or significant issues from the audit plan.

AUDIT ATTENDEES

OPENING MEETING

Name	Position
Client Representative	
Tyler Carbone	Managing Director
Vicky Faintreny	Account Manager
Audit Team	
Sanjeev Tiwari	Lead Auditor
Marilu Duque	Associate Auditor
Deepika Pandey	Associate Auditor

CLOSING MEETING

Name	Position
Client Representative	
Tyler Carbone	Managing Director
Vicky Faintreny	Account Manager
Audit Team	
Sanjeev Tiwari	Lead Auditor
Marilu Duque	Associate Auditor
Deepika Pandey	Associate Auditor

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

STAGE 1 CERTIFICATION AUDIT – NON-CONFORMITIES (NC)

As a result of the Stage 1 Certification Audit, Prescient Security identified five (5) minor non-conformities. The audit team received follow up evidence, as detailed below, so that Prescient Security could conclude its determination of the conformance of the management system with regards to these functional areas.

Ref. No	Reference	Control/Clause Requirement	Corrective Action Plan Verification Status
1	ISO/IEC 27001:2022 Clause 6.1.2	**Information Security Risk Assessment** The organization shall define and apply an information security risk assessment process that a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments; b) ensures that repeated information security risk assessments produce consistent, valid and comparable results; c) identifies the information security risks: 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and 2) identify the risk owners; d) analyses the information security risks: 1) assess the potential consequences that would result if the risks identified in 6.1.2 c were to materialize; 2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and 3) determine the levels of risk; e) evaluates the information security risks: 1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and 2) prioritize the analysed risks for risk treatment. The organization shall retain documented information about the information security risk assessment process.	NC closed on March 25, 2024
2	ISO/IEC 27001:2022 Clause 7.2	**Competence** The organization shall a) determine the necessary competence of person(s) doing work under its control that affects its information security performance; b) ensure that these persons are competent on the basis of appropriate education, training, or experience; c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and d) retain appropriate documented information as evidence of competence.	NC closed on March 25, 2024
3	ISO/IEC 27001:2022 Clause 7.5.2	**Creating and Updating Documented Information** When creating and updating documented information the organization shall ensure appropriate: a) identification and description (e.g. a title, date, author, or reference number); b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and c) review and approval for suitability and adequacy.	NC closed on March 25, 2024

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

4	ISO/IEC 27001:2022 Clause 7.5.3	**Control of Documented Information** Documented information required by the information security management system and by this International Standard shall be controlled to ensure: a) it is available and suitable for use, where and when it is needed; and b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity). For the control of documented information, the organization shall address the following activities, as applicable: c) distribution, access, retrieval and use; d) storage and preservation, including the preservation of legibility; e) control of changes (e.g. version control); and f) retention and disposition. Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.	NC closed on March 25, 2024
5	ISO/IEC 27001:2022 Clause 9.3.3	**Management Review Results** The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system. Documented information shall be available as evidence of the results of management reviews.	NC closed on March 25, 2024

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

AUDIT TEST DETAILS

Notes on usage by the auditor:

Under the column "Status", please use the following key to record your assessment result for each clause:

A = Acceptable, ***N/A*** = Not Applicable (Out of Scope), ***MaNC*** = Major Non-conformity, ***MiNC*** = Minor Non-conformity, ***OBS*** = Observation, ***OFI*** = Opportunity for improvement

CLAUSES

	Clause Requirement	Number of NC	Status	Audit Evidence (Finding and its justification)
			4. Context of the Organization	
4.1	Understanding the Organization and Its context		**A**	01-isms-scope-of-the-isms_Ver. 1.0, Date. 27-Nov-2023. Fully meets the respective clause requirement.
4.2	Understanding the Needs and Expectations of Interested Parties		**A**	01-isms-scope-of-the-isms_Ver. 1.0, Date. 27-Nov-2023. Fully meets the respective clause requirement.
4.3	Determining the scope of the ISMS		**A**	01-isms-scope-of-the-isms_Ver. 1.0, Date. 27-Nov-2023. Fully meets the respective clause requirement.
4.4	Information security management system		**A**	01-isms-scope-of-the-isms_Ver. 1.0, Date. 27-Nov-2023; 02-isms-information-security-management-system-isms-policy_Ver. 1.0, Date. 27-Nov-2023. Fully meets the respective clause requirement.
			5. Leadership	
5.1	Leadership and commitment		**A**	02-isms-information-security-management-system-isms-policy_Ver. 1.0, Date. 27-Nov-2023; 03-isms-roles-responsibilities-and-authorities_Ver. 1.0, Date. 01-10-2024; information-security-policy-bsi_Ver. 1.0, Date. October 1, 2021; 06-isms-information-security-communication-plan_Ver. 1.0, Date. 28-Nov-2023; 10-isms-information-security-objectives-plan_Ver. 1.0, Date. 28-Nov-2023. Fully meets the respective clause requirement.
5.2	Policy		**A**	information-security-policy-bsi_Ver. 1.0, Date. October 1, 2021; 10-isms-information-security-objectives-plan_Ver. 1.0, Date. 28-Nov-2023; access-control-policy-bsi_Ver. 1.0, Date. Oct 1, 2021; asset-management-policy-bsi_Ver. 1.0, Date. Oct 1, 2021; business-continuity-and-disaster-recovery-plan-bsi_Ver. 1.0, Date. Oct 1, 2021; cryptography-policy-bsi_Ver. 1.0, Date. Oct 1, 2021; data-management-policy-bsi_Ver. 1.0, Date. Oct 1, 2021;

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

				human-resource-security-policy-bsi_Ver. 1.1, Date. February 2, 2022; incident-response-plan-bsi_Ver. 1.0, Date. Oct 1, 2021; information-security-roles-and-responsibilities-bsi_Ver. 1.0, Date. November 1, 2021; operations-security-policy-bsi_Ver. May 1, 2021; risk-management-policy-bsi_Ver. 1.0, Date. November 1, 2021; third-party-management-policy-bsi_Ver. 1.0, Date. November 1, 2021; secure-development-policy-bsi_Ver. 2.0, Date. 01-30-2024. Fully meets the respective clause requirement.
5.3	Organizational roles, responsibilities and authorities		**A**	03-isms-roles-responsibilities-and-authorities_Ver. 1.0, Date. 01-10-2024. Fully meets the respective clause requirement.
6. Planning				
6.1	**Actions to address risks and opportunities**			
6.1.1	General		**A**	04-isms-risk-assessment-and-risk-treatment-process; 09-isms-procedure-for-corrective-action-and-continual-improvement; 10-isms-information-security-objectives-plan. Fully meets the respective clause requirement.
6.1.2	Information security risk assessment	1	**MiNC**	Reviewed 04-isms-risk-assessment-and-risk-treatment-process_Ver. 1.0, Date. 27-Nov-2023; risk-management-policy-bsi; Risk Assessment Snapshot 2024-03-13. It was observed that 1. The criteria for risk acceptance and residual risk were not defined in the provided "Risk Management policy". 2. The risk scale outlined in the "Risk Management Policy" is a 3-point scale, whereas the one utilized in Vanta employs a 5-point scale, indicating that the policy and implemented procedure is not in sync. Provided evidences partially do not meet the respective clause/control requirements. Hence, this is considered as Minor-Non Conformity.
6.1.3	Information security risk treatment	1	**OBS**	Reviewed 04-isms-risk-assessment-and-risk-treatment-process; 11-isms-statement-of-applicability; operations-security-policy-bsi. It was observed that Control numbers 7.2, 7.3, 7.4, and 7.10 were not identified as excluded or marked as "NA," even though the physical location falls outside the scope. Provided evidences mostly meets the respective clause/control requirements. However, the potential non-conformity has been observed. Hence, this is considered as Observation.
6.2	Information security objectives and planning to achieve them		**A**	10-isms-information-security-objectives-plan_Ver. 1.0, Date. 28-Nov-2023. Fully meets the respective clause requirement.

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

6.3	Planning of Changes		**A**	information-security-policy-bsi; operations-security-policy-bsi; risk-management-policy-bsi. Fully meets the respective clause requirement.
7. Support				
7.1	Resources		**A**	03-isms-roles-responsibilities-and-authorities_Ver. 1.0, Date. 01-10-2024. Fully meets the respective clause requirement.
7.2	Competence	2	**MiNC**	Reviewed 03-isms-roles-responsibilities-and-authorities; board_of_directors_cvs-links; human-resource-security-policy-bsi; information-security-policy-bsi; isms_and_security_program_leadership_qualifications-links. It was observed that in the "Human Resource Security Policy," it states that HR staff and hiring managers should evaluate the skills and competence of employees and contractors during the hiring process. Job descriptions and requisitions should outline the required skills and competencies. However, there was no evidence available for review regarding the criteria used for competence mapping. Provided evidences partially do not meet the respective clause/control requirements. Hence, this is considered as Minor-Non Conformity.
7.3	Awareness	2	**OBS**	Reviewed 06-isms-information-security-communication-plan; general_security_awareness_training_records_tracked; information-security-policy-bsi. It was observed that the information security training was not completed by one employee (Anandhi Sekaran) Provided evidences mostly meets the respective clause/control requirements. However, the potential non-conformity has been observed. Hence, this is considered as Observation.
7.4	Communication		**A**	06-isms-information-security-communication-plan_Ver. 1.0, Date. 28-Nov-2023. Fully meets the respective clause requirement.
7.5	**Documented Information**			
7.5.1	General		**A**	05-isms-procedure-for-the-control-of-documented-information_Ver. 1.0, Date. 01-09-2024. Fully meets the respective clause requirement.
7.5.2	Creating and Updating	3	**MiNC**	Reviewed 05-isms-procedure-for-the-control-of-documented-information_Ver. 1.0, Date. 01-09-2024. It was observed that information-security-policy-bsi; access-control-policy-bsi; asset-management-policy-bsi; business-continuity-and-disaster-recovery-plan-bsi;

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

				cryptography-policy-bsi; data-management-policy-bsi; human-resource-security-policy-bsi; incident-response-plan-bsi; information-security-roles-and-responsibilities-bsi; operations-security-policy-bsi; risk-management-policy-bsi; third-party-management-policy-bsi; The policies listed above underwent reviews in both years 2021 and 2022. However, according to the "05-isms-procedure-for-the-control-of-documented-information," ISMS documents must undergo annual review by the ISMS Governance Council. Provided evidences partially do not meet the respective clause/control requirements. Hence, this is considered as Minor-Non Conformity.
7.5.3	Control of documented information	4	**MiNC**	Reviewed 05-isms-procedure-for-the-control-of-documented-information_Ver. 1.0, Date. 01-09-2024. It was observed that the "05-isms-procedure-for-the-control-of-documented-information" document did not cover the identification of information sourced from external organizations, nor did it detail the essential security measures and procedures for managing its protection, storage, distribution, retention, disposition, etc. Provided evidences partially do not meet the respective clause/control requirements. Hence, this is considered as Minor-Non Conformity.
8. Operation				
8.1	Operational planning and control		**A**	04-isms-risk-assessment-and-risk-treatment-process_Ver. 1.0, Date. 27-Nov-2023; risk-management-policy-bsi; Risk Assessment Snapshot 2024-03-13. Fully meets the respective clause requirement.
8.2	Information security risk assessment		**A**	04-isms-risk-assessment-and-risk-treatment-process_Ver. 1.0, Date. 27-Nov-2023; risk-management-policy-bsi; Risk Assessment Snapshot 2024-03-13. Fully meets the respective clause requirement.
8.3	Information security risk treatment		**A**	04-isms-risk-assessment-and-risk-treatment-process_Ver. 1.0, Date. 27-Nov-2023; risk-management-policy-bsi; Risk Assessment Snapshot 2024-03-13. Fully meets the respective clause requirement.
9. Performance Evaluation				

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

9.1	Monitoring, measurement, analysis and evaluation		**A**	10-isms-information-security-objectives-plan_Ver. 1.0, Date. 28-Nov-2023; Screenshot 2023-10-04 at 9.55.21 AM. Fully meets the respective clause requirement.
9.2	Internal Auditvd			
9.2.1	General		**A**	07-isms-procedure-for-internal-audits; Coalesce Internal Audit_2024-03-7. Fully meets the respective clause requirement.
9.2.2	Internal Audit Programme	3	**OBS**	Reviewed 07-isms-procedure-for-internal-audits; Coalesce Internal Audit_2024-03-7. It was observed that in the internal audit report, the finding total is mentioned as 1. However, the total number of findings are 3. Provided evidences mostly meets the respective clause/control requirements. However, the potential non-conformity has been observed. Hence, this is considered as Observation.
9.3	**Management Review**			
9.3.1	General		**A**	08-isms-procedure-for-management-review; Coalesce ISMS Management Review; risk-management-policy-bsi. Fully meets the respective clause requirement.
9.3.2	Management Review Inputs		**A**	08-isms-procedure-for-management-review; Coalesce ISMS Management Review; risk-management-policy-bsi. Fully meets the respective clause requirement.
9.3.3	Management Review Results	5	**MiNC**	Reviewed 08-isms-procedure-for-management-review; Coalesce ISMS Management Review; risk-management-policy-bsi. It was observed that the minutes of meeting/ actionable items was not available for review. Provided evidences partially do not meet the respective clause/control requirements. Hence, this is considered as Minor-Non Conformity.
10. Improvement				
10.1	Nonconformity and corrective action		**A**	09-isms-procedure-for-corrective-action-and-continual-improvement. Fully meets the respective clause requirement.
10.2	Continual improvement		**A**	09-isms-procedure-for-corrective-action-and-continual-improvement; Screenshot captured on call (Non conformity tracker). Fully meets the respective clause requirement.

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

ANNEX A CONTROLS

	Control Objective and Control Description	Number of NC	Status	Audit Evidence (Finding and its justification)
	A.5 Organizational Controls			
A.5.1	**Policies for Information Security** **Control:** Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.		**A**	information-security-policy-bsi; access-control-policy-bsi; asset-management-policy-bsi; business-continuity-and-disaster-recovery-plan-bsi; cryptography-policy-bsi; data-management-policy-bsi; human-resource-security-policy-bsi; incident-response-plan-bsi; information-security-roles-and-responsibilities-bsi; operations-security-policy-bsi; risk-management-policy-bsi; third-party-management-policy-bsi; (Ver. 1.1, Date. March 21, 2024). Fully meets the respective control requirement.
A.5.2	**Information Security Roles and Responsibilities** **Control:** Information security roles and responsibilities shall be defined and allocated according to the organization needs.		**A**	information-security-roles-and-responsibilities-bsi; 03-isms-roles-responsibilities-and-authorities. Fully meets the respective control requirement.
A.5.3	**Segregation of Duties** **Control:** Conflicting duties and conflicting areas of responsibility shall be segregated.		**A**	access-control-policy-bsi; human-resource-security-policy-bsi; Screenshot 2023-10-03 at 4.05.32 PM. Fully meets the respective control requirement.
A.5.4	**Management Responsibilities** **Control:** Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.		**A**	employees_agree_to_information_security_policy_(aup); employees_agree_to_information_security_roles_and_responsibilities; general_security_awareness_training_records_tracked; human-resource-security-policy-bsi; information-security-policy-bsi; information-security-roles-and-responsibilities-bsi. Fully meets the respective control requirement.
A.5.5	**Contact with Authorities** **Control:** The organization shall establish and maintain contact with relevant authorities.	1	**MiNC**	Reviewed incident-response-plan-bsi_Ver. 1.1, Date. March 21, 2024. It was observed that the contact list of external authorities to be contacted in case of an information security incident was not available for review. Provided evidences partially do not meet the respective clause/control requirements. Hence, this is considered as Minor-Non Conformity.

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

A.5.6	**Contact with Special Interest Groups** **Control:** The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.		**A**	human-resource-security-policy-bsi; information-security-roles-and-responsibilities-bsi; membership-certificate-1953173. Fully meets the respective control requirement.
A.5.7	**Threat Intelligence** **Control:** Information relating to information security threats shall be collected and analysed to produce threat intelligence.		**A**	information-security-roles-and-responsibilities-bsi; membership-certificate-1953173; operations-security-policy-bsi; Screenshot1; Screenshot2; Screenshot3; Screenshot4; Screenshot5; Screenshot6; Screenshot7; Summit - Coalesce - 2023_11_03 - AppSec Coalesce - Findings Report. Fully meets the respective control requirement.
A.5.8	**Information Security in Project Management** **Control:** Information security shall be integrated into project management.	2	**MiNC**	Reviewed risk-management-policy-bsi. It was observed that the evidence for information security in project management was not available for review. Provided evidences partially do not meet the respective clause/control requirements. Hence, this is considered as Minor-Non Conformity.
A.5.9	**Inventory of Information and Other Associated Assets** **Control:** An inventory of information and other associated assets, including owners, shall be developed and maintained.		**A**	asset-management-policy-bsi; inventory_items_have_active_owners; inventory_list_tracks_resources_that_contain_user_data; inventory_items_have_descriptions; monitored computers_Vanta. Fully meets the respective control requirement.
A.5.10	**Acceptable use of Information and Other Associated Assets** **Control:** Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.		**A**	asset-management-policy-bsi; data-management-policy-bsi; information-security-policy-bsi. Fully meets the respective control requirement.
A.5.11	**Return of Assets** **Control:** Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.		**A**	asset-management-policy-bsi; human-resource-security-policy-bsi; information-security-policy-bsi; Fwd Laptop return on the way for order 126729 Alex Engelmann; Signed Separation Agreement; Fwd Laptop return on the way for order 126729 Alex Engelmann. Fully meets the respective control requirement.
A.5.12	**Classification of Information**		**A**	data-management-policy-bsi_Ver. 1.1, Date. March 25, 2024. Fully meets the respective control requirement.

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

	Control: Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.			
A.5.13	**Labelling of Information** **Control:** An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.		**A**	data-management-policy-bsi_Ver. 1.1, Date. March 25, 2024. Fully meets the respective control requirement.
A.5.14	**Information Transfer** **Control:** Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.		**A**	third-party-management-policy-bsi; Coalesce MSA - TEMPLATE; cloud_provider_service_agreement-links; https://coalesce.io/terms. Fully meets the respective control requirement.
A.5.15	**Access Control** **Control:** Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.		**A**	access-control-policy-bsi. Fully meets the respective control requirement.
A.5.16	**Identity Management** **Control:** The full life cycle of identities shall be managed.		**A**	access-control-policy-bsi; Onboarding Automation 2; Onboarding Automation 3; Onboarding Automation; onboarding is automated by HRIS Rippling; the vendor handles the entire process and grants access after the employee completes specific tasks. Fully meets the respective control requirement.
A.5.17	**Authentication Information** **Control:** Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.		**A**	access-control-policy-bsi; information-security-policy-bsi; Screenshot 2024-01-16 at 3.13.22 PM; Snowflake Password Policy; GCP Password Policy. Fully meets the respective control requirement.
A.5.18	**Access Rights** **Control:** Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.		**A**	access-control-policy-bsi; Screenshot 2023-10-03 at 4.59.09 PM; Coalesce Access Data; hr_accounts_associated_with_users; Quarterly Access Review. Fully meets the respective control requirement.
A.5.19	**Information Security in Supplier Relationships** **Control:** Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services		**A**	third-party-management-policy-bsi; vendors_assigned_risk_levels. Fully meets the respective control requirement.

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

A.5.20	**Addressing Information Security Within Supplier Agreements** **Control:** Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.		**A**	third-party-management-policy-bsi; MSA agreement; Coalesce Automation_Capacity_Order Form_2023-12-08 (1); https://www.snowflake.com/legal/terms-of-service/. Fully meets the respective control requirement.
A.5.21	**Managing Information Security in the Information and Communication Technology (ICT) Supply Chain** **Control:** Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.		**A**	third-party-management-policy-bsi; vendors_assigned_risk_levels; MSA agreement; Coalesce Automation_Capacity_Order Form_2023-12-08 (1); https://www.snowflake.com/legal/terms-of-service/. Fully meets the respective control requirement.
A.5.22	**Monitoring, Review and Change Management of Supplier Services** **Control:** The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.		**A**	third-party-management-policy-bsi; vendors_assigned_risk_levels. Fully meets the respective control requirement.
A.5.23	**Information Security for Use of Cloud Services** **Control:** Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.		**A**	information-security-policy-bsi; third-party-management-policy-bsi; https://cloud.google.com/terms. Fully meets the respective control requirement.
A.5.24	**Information Security Incident Management Planning and Preparation** **Control:** The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	1	**OBS**	Reviewed incident-response-plan-bsi; Coalesce Incident Response Program Log; information-security-roles-and-responsibilities-bsi. It was observed that the "Coalesce Incident Response Program Log" didn't have a version history table that details the version number, date, author, and approver details. Provided evidences mostly meets the respective clause/control requirements. However, the potential non-conformity has been observed. Hence, this is considered as Observation.
A.5.25	**Assessment and Decision on Information Security Events** **Control:** The organization shall assess information security events and decide if they are to be categorized as information security incidents.		**A**	incident-response-plan-bsi; Coalesce Incident Response Program Log; information-security-roles-and-responsibilities-bsi. Fully meets the respective control requirement.
A.5.26	**Response to Information Security Incidents** **Control:** Information security incidents shall be responded to in accordance with the documented procedures.		**A**	incident-response-plan-bsi; Coalesce Incident Response Program Log; information-security-roles-and-responsibilities-bsi. Fully meets the respective control requirement.

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

A.5.27	**Learning from Information Security Incidents** **Control:** Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.		**A**	incident-response-plan-bsi; Coalesce Incident Response Program Log; information-security-roles-and-responsibilities-bsi. Fully meets the respective control requirement.
A.5.28	**Collection of Evidence** **Control:** The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.		**A**	incident-response-plan-bsi; Coalesce Incident Response Program Log; information-security-roles-and-responsibilities-bsi. Fully meets the respective control requirement.
A.5.29	**Information Security During Disruption** **Control:** The organization shall plan how to maintain information security at an appropriate level during disruption.		**A**	business-continuity-and-disaster-recovery-plan-bsi; Meeting Calendar Invitation; Coalesce1. Fully meets the respective control requirement.
A.5.30	**ICT Readiness for Business Continuity** **Control:** ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	2	**OBS**	Reviewed business-continuity-and-disaster-recovery-plan-bsi; Calendar Invitation; incident-response-plan-bsi; Meeting Calendar Invitation; Meeting Minutes for Incident Response Plan; Minutes of Recovery Exercise Meeting. It was observed that the evidence for table top exercise was not available for review. Provided evidences mostly meets the respective clause/control requirements. However, the potential non-conformity has been observed. Hence, this is considered as Observation.
A.5.31	**Legal, Statutory, Regulatory and Contractual Requirements** **Control:** Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.		**A**	12-isms-relevant-laws-regulations-and-contractual-requirements_Ver. 1.0, Date. 28-Nov-2023. Fully meets the respective control requirement.
A.5.32	**Intellectual Property Rights** **Control:** The organization shall implement appropriate procedures to protect intellectual property rights.		**A**	12-isms-relevant-laws-regulations-and-contractual-requirements_Ver. 1.0, Date. 28-Nov-2023; Employee agreement; Signed confidentiality agreement; MSA template. Fully meets the respective control requirement.
A.5.33	**Protection of Records** **Control:** Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.		**A**	Coalesce MSA - TEMPLATE; cloud_provider_service_agreement-links; https://coalesce.io/terms; Signed agreement;

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

				05-isms-procedure-for-the-control-of-documented-information; access-control-policy-bsi; data-management-policy-bsi. Fully meets the respective control requirement.
A.5.34	**Privacy and Protection of Personal Identifiable Information (PII)** **Control:** The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.		**A**	Coalesce MSA - TEMPLATE; cloud_provider_service_agreement-links; https://coalesce.io/terms; Signed agreement; 05-isms-procedure-for-the-control-of-documented-information; access-control-policy-bsi; data-management-policy-bsi. Fully meets the respective control requirement.
A.5.35	**Independent Review of Information Security** **Control:** The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.		**A**	07-isms-procedure-for-internal-audits; risk-management-policy-bsi; Coalesce Internal Audit-2; Summit - Coalesce - 2023_11_03 - AppSec Coalesce - Findings Report. Fully meets the respective control requirement.
A.5.36	**Compliance with Policies, Rules and Standards for Information Security** **Control:** Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.		**A**	Screenshot; 07-isms-procedure-for-internal-audits; risk-management-policy-bsi; Coalesce Internal Audit-2; Summit - Coalesce - 2023_11_03 - AppSec Coalesce - Findings Report. Fully meets the respective control requirement.
A.5.37	**Documented Operating Procedures** **Control:** Operating procedures for information processing facilities shall be documented and made available to personnel who need them.		**A**	operations-security-policy-bsi; Screenshot1. Fully meets the respective control requirement.
A.6 People Controls				
A.6.1	**Screening** **Control:** Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.		**A**	human-resource-security-policy-bsi; Checker is used for background verification;criminal1710806270pdftmptmpeeunx7z41d68a35cce724125ea6abbf55e18c13c6487fb3d criminal1706734064pdftmptmpriiu2xbp810c7f955e8a176b629467d3b5b813c66aea60b0; criminal1707742245pdftmptmpd6lmxwid2c916a48d71d262a70fa2d171a9aa57b55d15412; criminal1709914217pdftmptmp4yk3elpz69d155cae3fd081874fc737b5d55f962a4deb9ab. Fully meets the respective control requirement.

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

A.6.2	**Terms and Conditions of Employment** **Control:** The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.		**A**	code-of-conduct-bsi; David Irvin Offer Letter; employees_agree_to_code_of_conduct; human-resource-security-policy-bsi; information-security-policy-bsi; information-security-roles-and-responsibilities-bsi; Oleksandr Toropov Offer Letter_signed; Tim Daniels Offer Letter. Fully meets the respective control requirement.
A.6.3	**Information Security Awareness, Education and Training** **Control:** Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	3	**OBS**	Reviewed general_security_awareness_training_records_tracked; human-resource-security-policy-bsi; security_awareness_training_selected. It was observed that the security awareness training was not completed by one of the employee (Guillermo Regalado). Provided evidences mostly meets the respective clause/control requirements. However, the potential non-conformity has been observed. Hence, this is considered as Observation.
A.6.4	**Disciplinary Process** **Control:** A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	4	**OBS**	Reviewed employees_agree_to_human_resource_security_policy; human-resource-security-policy-bsi; information-security-policy-bsi; No such case. It was observed that the disciplinary tracker was not available for review. Provided evidences mostly meets the respective clause/control requirements. However, the potential non-conformity has been observed. Hence, this is considered as Observation.
A.6.5	**Responsibilities after Termination or Change of Employment** **Control:** Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.		**A**	Signed Separation Agreement; Access Control Policy; human-resource-security-policy-bsi; Separation Agreement; Separation Agreement 2; Offboarding Automation. Fully meets the respective control requirement.
A.6.6	**Confidentiality or Non-Disclosure Agreements** **Control:** Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be		**A**	human-resource-security-policy-bsi; NDA Template; Signed Separation Agreement;

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

	identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.			Tim Daniels Offer Letter; external_non-disclosure_agreement_template-links. Fully meets the respective control requirement.
A.6.7	**Remote Working** **Control:** Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.		**A**	access-control-policy-bsi; information-security-policy-bsi; mfa_on_google_workspace; monitored computers_vanta. Fully meets the respective control requirement.
A.6.8	**Information Security Event Reporting** **Control:** The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.		**A**	incident-response-plan-bsi; information-security-policy-bsi; Coalesce Incident Response Program Log. Fully meets the respective control requirement.
A.7 Physical Controls				
A.7.1	**Physical Security Perimeters** **Control:** Security perimeters shall be defined and used to protect areas that contain information and other associated assets.		**N/A**	Statement of Applicability_v2_15March2024 The organization operates in a cloud-based environment and does not own or maintain infrastructure. All infrastructure and physical security thereof are managed by the third-party hosting provider. Hence, this physical security control is marked as not applicable.
A.7.2	**Physical Entry** **Control:** Secure areas shall be protected by appropriate entry controls and access points.		**N/A**	Statement of Applicability_v2_15March2024 The organization operates in a cloud-based environment and does not own or maintain infrastructure. All infrastructure and physical security thereof are managed by the third-party hosting provider. Hence, this physical security control is marked as not applicable.
A.7.3	**Securing Offices, Rooms and Facilities** **Control:** Physical security for offices, rooms and facilities shall be designed and implemented.		**N/A**	Statement of Applicability_v2_15March2024 The organization operates in a cloud-based environment and does not own or maintain infrastructure. All infrastructure and physical security thereof are managed by the third-party hosting provider. Hence, this physical security control is marked as not applicable.
A.7.4	**Physical Security Monitoring** **Control:** Premises shall be continuously monitored for unauthorized physical access.		**N/A**	Statement of Applicability_v2_15March2024 The organization operates in a cloud-based environment and does not own or maintain infrastructure. All infrastructure and physical security thereof are managed by the third-party hosting provider. Hence, this physical security control is marked as not applicable.
A.7.5	**Protecting Against Physical and Environmental Threats** **Control:** Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.		**N/A**	Statement of Applicability_v2_15March2024 The organization operates in a cloud-based environment and does not own or maintain infrastructure. All infrastructure and physical security thereof are

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

				managed by the third-party hosting provider. Hence, this physical security control is marked as not applicable.
A.7.6	**Working in Secure Areas** **Control:** Security measures for working in secure areas shall be designed and implemented.		**N/A**	Statement of Applicability_v2_15March2024 The organization operates in a cloud-based environment and does not own or maintain infrastructure. All infrastructure and physical security thereof are managed by the third-party hosting provider. Hence, this physical security control is marked as not applicable.
A.7.7	**Clear Desk and Clear Screen** **Control:** Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.		**A**	access-control-policy-bsi; information-security-policy-bsi; mfa_on_google_workspace; monitored computers_vanta. Fully meets the respective control requirement.
A.7.8	**Equipment Siting and Protection** **Control:** Equipment shall be sited securely and protected.		**N/A**	Statement of Applicability_v2_15March2024 The organization operates in a cloud-based environment and does not own or maintain infrastructure. All infrastructure and physical security thereof are managed by the third-party hosting provider. Hence, this physical security control is marked as not applicable.
A.7.9	**Security of Assets Off-Premises** **Control:** Off-site assets shall be protected.		**A**	asset-management-policy-bsi; employee_computer_hard_disk_encryption; information-security-policy-bsi. Fully meets the respective control requirement.
A.7.10	**Storage Media** **Control:** Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.		**N/A**	Statement of Applicability_v2_15March2024 The organization operates in a cloud-based environment and does not own or maintain infrastructure. All infrastructure and physical security thereof are managed by the third-party hosting provider. Hence, this physical security control is marked as not applicable.
A.7.11	**Supporting Utilities** **Control:** Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.		**N/A**	Statement of Applicability_v2_15March2024 The organization operates in a cloud-based environment and does not own or maintain infrastructure. All infrastructure and physical security thereof are managed by the third-party hosting provider. Hence, this physical security control is marked as not applicable.
A.7.12	**Cabling Security** **Control:** Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.		**N/A**	Statement of Applicability_v2_15March2024 The organization operates in a cloud-based environment and does not own or maintain infrastructure. All infrastructure and physical security thereof are

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

				managed by the third-party hosting provider. Hence, this physical security control is marked as not applicable.
A.7.13	**Equipment Maintenance** **Control:** Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.		**N/A**	Statement of Applicability_v2_15March2024 The organization operates in a cloud-based environment and does not own or maintain infrastructure. All infrastructure and physical security thereof are managed by the third-party hosting provider. Hence, this physical security control is marked as not applicable.
A.7.14	**Secure Disposal or Re-Use of Equipment** **Control:** tems of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.		**A**	https://cloud.google.com/security/compliance/iso-27001; asset-management-policy-bsi; data-management-policy-bsi; No devices have been disposed up until now. Fully meets the respective control requirement.
A.8 Technological Controls				
A.8.1	**User End Point Devices** **Control:** Information stored on, processed by or accessible via user end point devices shall be protected.		**A**	access-control-policy-bsi; information-security-policy-bsi; mfa_on_google_workspace; monitored computers_vanta. Fully meets the respective control requirement.
A.8.2	**Priviliged Access Rights** **Control:** The allocation and use of privileged access rights shall be restricted and managed.		**A**	access-control-policy-bsi; Coalesce Access Data. Fully meets the respective control requirement.
A.8.3	**Information Access Restriction** **Control:** Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.		**A**	access-control-policy-bsi; Coalesce Access Data; Bitbucket developers. Fully meets the respective control requirement.
A.8.4	**Access to Source Code** **Control:** Read and write access to source code, development tools and software libraries shall be appropriately managed.		**A**	access-control-policy-bsi; github_accounts_associated_with_users; mfa_on_github. Fully meets the respective control requirement.
A.8.5	**Secure Authentication** **Control:** Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.		**A**	access-control-policy-bsi; mfa_on_github; screen_shot_2021-09-29_at_4.30.18_pm; screen_shot_2021-09-29_at_5.22.59_pm. Fully meets the respective control requirement.

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

A.8.6	**Capacity Management** **Control:** The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.		**A**	datadog_integration_reporting_monitors; operations-security-policy-bsi; datadog. Fully meets the respective control requirement.
A.8.7	**Protection Against Malware** **Control:** Protection against malware shall be implemented and supported by appropriate user awareness.		**A**	human-resource-security-policy-bsi; information-security-policy-bsi; crowdstrike_hosts_have_a_non_empty_prevention_policy; operations-security-policy-bsi; monitored computers_Vanta. Fully meets the respective control requirement.
A.8.8	**Management of Technical Vulnerabilities** **Control:** Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.		**A**	operations-security-policy-bsi; risk-management-policy-bsi; vulnerability_scanning_is_enabled_(gcp); Screenshot; Screenshot1; Screenshot2; Screenshot3; Screenshot4; Summit - Coalesce - 2023_11_03 - AppSec Coalesce - Findings Report; vuln_asset_findings_export. Fully meets the respective control requirement.
A.8.9	**Configuration Management** **Control:** Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.		**A**	operations-security-policy-bsi; vpc_flow_logs_enabled_(gcp); SECURE CONFIG BASELINE_ Coalesce. Fully meets the respective control requirement.
A.8.10	**Information Deletion** **Control:** Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.		**A**	data-management-policy-bsi; No customer have requested to delete any data. Fully meets the respective control requirement.
A.8.11	**Data Masking** **Control:** Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.		**N/A**	Statement of Applicability_v2_15March2024 Due to the nature of business of the organization, no data or confidential information is stored within that would require data masking controls. Hence, this control is marked as not applicable.
A.8.12	**Data Leakage Prevention** **Control:** Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.		**A**	data-management-policy-bsi; monitored computer_Vanta; Screenshot 2024-03-26 172153_ssl certificate.

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

				Fully meets the respective control requirement.
A.8.13	**Information Backup** **Control:** Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.		**A**	operations-security-policy-bsi; Meeting Calendar Invitation; Minutes of Recovery Exercise Meeting; Screenshot1; Screenshot2; Info backup screenshots. Fully meets the respective control requirement.
A.8.14	**Redundancy of Information Processing Facilities** **Control:** Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.		**A**	business-continuity-and-disaster-recovery-plan-bsi; operations-security-policy-bsi; image(3); Screenshot1; Coalesce1; Info Backup 1; Info Backup 2; Info Backup 3; Info Backup 4; Info Backup 5; Info Backup 6; Info Backup 7; Info Backup 8. Fully meets the respective control requirement.
A.8.15	**Logging** **Control:** Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.		**A**	operations-security-policy-bsi; crowdstrike_hosts_have_a_non_empty_prevention_policy; screenshot_2024-02-07_at_4.43.55; vpc_flow_logs_enabled_(gcp). Fully meets the respective control requirement.
A.8.16	**Monitoring Activities** **Control:** Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents		**A**	operations-security-policy-bsi; crowdstrike_hosts_have_a_non_empty_prevention_policy; screenshot_2024-02-07_at_4.43.55; vpc_flow_logs_enabled_(gcp); Screenshots Datadog dashboard. Fully meets the respective control requirement.
A.8.17	**Clock Synchronization** **Control:** The clocks of information processing systems used by the organization shall be synchronized to approved time sources.		**A**	operations-security-policy-bsi; Clock Synchronization. Fully meets the respective control requirement.
A.8.18	**Use of Privileged Utility Programs**		**A**	access-control-policy-bsi; operations-security-policy-bsi;

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

	Control: The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.			Screenshot1; CrowdStrike Cloud Admins; CrowdStrike Endpoint admins; Snyk Admins; Snowflake Admin. Fully meets the respective control requirement.
A.8.19	**Installation of Software on Operational Systems** **Control:** Procedures and measures shall be implemented to securely manage software installation on operational systems.		**A**	information-security-policy-bsi; operations-security-policy-bsi; Onboarding Automation 2; Onboarding Automation 3; Onboarding Automation; CrowdStrike Execution Blocking; Firewall System. Fully meets the respective control requirement.
A.8.20	**Network Security** **Control:** Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.		**A**	operations-security-policy-bsi; compute_instance_firewall_rules_do_not_allow_public_port_22_(gcp); ssl_configuration_has_no_known_issues; ssl_tls_certificate_has_not_expired; ssl_tls_enforced_on_company_website; vpc_flow_logs_enabled_(gcp). Fully meets the respective control requirement.
A.8.21	**Security of Network Services** **Control:** Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.		**A**	operations-security-policy-bsi; ssl_configuration_has_no_known_issues; strong_ssl_tls_ciphers_used; third-party-management-policy-bsi; CrowdStrike Execution Blocking; Firewall System. Fully meets the respective control requirement.
A.8.22	**Segregation of Networks** **Control:** Groups of information services, users and information systems shall be segregated in the organization's networks.		**A**	operations-security-policy-bsi; Coalesce1; Production-Segregated; Dev Segregation29-03-2024 Prod Segregation; Test Segregation. Fully meets the respective control requirement.
A.8.23	**Web Filtering** **Control:** Access to external websites shall be managed to reduce exposure to malicious content.		**A**	operations-security-policy-bsi; CrowdStrike Execution Blocking; Firewall System. Fully meets the respective control requirement.

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

A.8.24	**Use of Cryptography** **Control:** Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	5	**OBS**	Reviewed ssl_configuration_has_no_known_issues; ssl_tls_certificate_has_not_expired; ssl_tls_enforced_on_company_website; cryptography-policy-bsi; GCP key manager. It was observed that the evidence for key management was not available for review. Provided evidences mostly meets the respective clause/control requirements. However, the potential non-conformity has been observed. Hence, this is considered as Observation.
A.8.25	**Secure Development Life Cycle** **Control:** Rules for the secure development of software and systems shall be established and applied.		**A**	secure-development-policy-bsi; employees_agree_to_secure_development_policy. Fully meets the respective control requirement.
A.8.26	**Application Security Requirements** **Control:** Information security requirements shall be identified, specified and approved when developing or acquiring applications.		**A**	secure-development-policy-bsi; third-party-management-policy. Fully meets the respective control requirement.
A.8.27	**Secure System Architecture and Engineering Principles** **Control:** Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.		**A**	Secure Development Policy v1.0.0; SECURE CONFIG BASELINE_ Coalesce; Coding Standards. Fully meets the respective control requirement.
A.8.28	**Secure Coding** **Control:** Secure coding principles shall be applied to software development.		**A**	Secure Development Policy v1.0.0; SECURE CONFIG BASELINE_ Coalesce; Coding Standards. Fully meets the respective control requirement.
A.8.29	**Security Testing in Development and Acceptance** **Control:** Security testing processes shall be defined and implemented in the development life cycle.		**A**	image(2); Quality Assurance and Code Review Coalesce.docx; Secure Development Policy v1.0.0. Fully meets the respective control requirement.
A.8.30	**Outsourced Development** **Control:** The organization shall direct, monitor and review the activities related to outsourced system development.		**A**	secure-development-policy-bsi; third-party-management-policy-bsi; Oleksandr Toropov Offer Letter_signed. Fully meets the respective control requirement.
A.8.31	**Separation of Development, Test and Production Environments** **Control:** Development, testing and production environments shall be separated and secured.		**A**	operations-security-policy-bsi; Coalesce1; Production-Segregated; Dev Segregation29-03-2024

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

				Prod Segregation; Test Segregation. Fully meets the respective control requirement.
A.8.32	**Change Management** **Control:** Changes to information processing facilities and information systems shall be subject to change management procedures.		**A**	operations-security-policy-bsi; Quality Assurance and Code Review Coalesce.docx; Screenshot1;secure-development-policy-bsi; Change Management 1; Change Management 2; Change Management 5; Change Management 4; Change Management. Fully meets the respective control requirement.
A.8.33	**Test Information** **Control:** Test information shall be appropriately selected, protected and managed.		**A**	data-management-policy-bsi; operations-security-policy-bsi; Quality Assurance and Code Review Coalesce.docx; Screenshot1; secure-development-policy-bsi. Fully meets the respective control requirement.
A.8.34	**Protection of Information Systems During Audit Testing** **Control:** Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.		**A**	07-isms-procedure-for-internal-audits; operations-security-policy-bsi; risk-management-policy-bsi; Pentest report. Fully meets the respective control requirement.

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

AUDIT FINDINGS – INITIAL CERTIFICATION

Prescient Security attempts to communicate all relevant audit findings at the time of identification with its clients in order to encourage a fluid communication model between all participating team members.

The audit findings were communicated to the client representative of the organization during the closing meeting. The final conclusion of the audit results and recommendation by the audit team was also communicated to the management during the meetings.

As a result of the Stage 2 Certification Audit, the audit team identified two (2) minor non-conformities relevant to the ISO/IEC 27001:2022 standard. All NCs identified during the course of the Stage 2 audit have been closed.

AUDIT FINDING DEFINITIONS

The evaluation of the audit findings is based on the following definitions, in accordance with ISO/IEC 17021-2015:

Major Non-Conformity (MaNC)

A non-conformity that affects the capability of the management system to achieve the intended results.

Minor Non-Conformity (MiNC)

A non-conformity that does not affect the capability of the management system to achieve the intended results.

Observations (OBS)

Any issues which are likely to become a NC, if not treated until the next audit are marked as observations. No response is required.

Opportunity for Improvement (OFI)

An opportunity for improvement is a finding that, should it go unaddressed, could result in more severe findings in subsequent reviews. An OFI can also be used to improve the management system as a whole or named processes. No response is required.

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

STAGE 2 CERTIFICATION AUDIT - NON-CONFORMITIES (NC)

Ref. No	Clause / Control #	Control/Clause Requirement	Details of Non-Conformities	NC Type	Completion Date
1	ISO/IEC 27001:2022 Control 5.5	**Contact with authorities** The organization shall establish and maintain contact with relevant authorities.	Reviewed incident-response-plan-bsi_Ver. 1.1, Date. March 21, 2024. It was observed that the contact list of external authorities to be contacted in case of an information security incident was not available for review. Provided evidences partially do not meet the respective clause/control requirements. Hence, this is considered as Minor-Non Conformity.	Minor	NC closed on April 5, 2024
2	ISO/IEC 27001:2022 Control 5.8	**Information security in project management** Information security shall be integrated into project management.	Reviewed risk-management-policy-bsi. It was observed that the evidence for information security in project management was not available for review. Provided evidences partially do not meet the respective clause/control requirements. Hence, this is considered as Minor-Non Conformity.	Minor	NC closed on April 5, 2024

OBSERVATIONS

Sr. #	Clause	Details
1	ISO/IEC 27001:2022 Control A.5.24	Reviewed incident-response-plan-bsi; Coalesce Incident Response Program Log; information-security-roles-and-responsibilities-bsi. It was observed that the "Coalesce Incident Response Program Log" didn't have a version history table that details the version number, date, author, and approver details. Provided evidences mostly meets the respective clause/control requirements. However, the potential non-conformity has been observed. Hence, this is considered as Observation.
2	ISO/IEC 27001:2022 Control A.5.30	Reviewed business-continuity-and-disaster-recovery-plan-bsi; Calendar Invitation; incident-response-plan-bsi; Meeting Calendar Invitation; Meeting Minutes for Incident Response Plan; Minutes of Recovery Exercise Meeting. It was observed that the evidence for tabletop exercise was not available for review. Provided evidences mostly meets the respective clause/control requirements. However, the potential non-conformity has been observed. Hence, this is considered as Observation.
3	ISO/IEC 27001:2022 Control A.6.3	Reviewed general_security_awareness_training_records_tracked; human-resource-security-policy-bsi; security_awareness_training_selected. It was observed that the security awareness training was not completed by one of the employee (Guillermo Regalado).

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

		Provided evidences mostly meets the respective clause/control requirements. However, the potential non-conformity has been observed. Hence, this is considered as Observation.
4	ISO/IEC 27001:2022 Control A.6.4	Reviewed employees_agree_to_human_resource_security_policy; human-resource-security-policy-bsi; information-security-policy-bsi; No such case. It was observed that the disciplinary tracker was not available for review. Provided evidences mostly meets the respective clause/control requirements. However, the potential non-conformity has been observed. Hence, this is considered as Observation.
5	ISO/IEC 27001:2022 Control A.8.24	Reviewed ssl_configuration_has_no_known_issues; ssl_tls_certificate_has_not_expired; ssl_tls_enforced_on_company_website; cryptography-policy-bsi; GCP key manager . It was observed that the evidence for key management was not available for review. Provided evidences mostly meets the respective clause/control requirements. However, the potential non-conformity has been observed. Hence, this is considered as Observation.

OPPORTUNITIES FOR IMPROVEMENT

Sr. #	Clause	Details
N/A	N/A	N/A

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

AGREED FOLLOW-UP ACTIVITIES

Non-conformities detailed above need to be addressed through the organization's corrective action process, in accordance with the relevant corrective action requirements of the audit standard, including actions to analyze the cause of the non-conformity, prevent recurrence, and complete the maintained records.

Corrective actions to address the identified major non-conformities shall be carried out immediately and Prescient Security must be notified of the actions taken within 30 days.

Corrective actions to address the identified minor non-conformities shall be documented on an action plan and be sent for review by the client to the auditor within 30 days. If the actions are deemed to be satisfactory, they will be followed up during the next scheduled visit.

Non-conformities shall be addressed through the client's corrective action process including:

- Actions taken to determine the extent of and contain the specific non-conformity.
- Root Cause (results of an investigation to determine the most basic cause(s) of the non-conformity)
- Actions taken to correct the non-conformity and, in response to the root cause, to eliminate recurrence of the non-conformity.
- Corrective action response shall be submitted to the Lead Auditor
- Client must maintain corrective action records, including objective evidence, for at least three (3) years.

The following action should be taken by the client:

☒ No action is required.

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.

AUDIT CONCLUSIONS AND AUDIT RECOMMENDATIONS

The Information Security Management System has proven conformity with the requirements of the ISO/IEC 27001:2022 standard. It has also provided the adequate structure to support implementation and maintenance of the information security management system.

Audit Conclusions

Has there been any serious deviation from the audit plan?	No
Are there any significant issues impacting the audit program?	No
Are there any significant changes affecting the management system since last audit took place?	No
Are there any unresolved issues affecting the management system since last audit took place?	No
The management system is designed to achieve the organization's policy objectives?	Yes
The management system meets statutory, regulatory and contractual requirements?	Yes
The internal audit and management review processes are in place and adequate?	Yes
The audit was successful in meeting the stated objectives?	Yes

AUDIT RECOMMENDATION

At the recommendation of the appointed audit team, we have determined that, based on the currently identified audit findings, we can recommend certification issuance to the Prescient Security certification body management team.

Additionally, the audit team found that the certificate scope was appropriate and that all intended audit objectives were sufficiently fulfilled to the extent that there were no unresolved issues that affected the audit team's ability to conclude the assessment.

The audit team recommends Coalesce Automation, Inc. for ISO/IEC 27001:2022 certification.

Signed,

Sanjeev Tiwari

Sanjeev Tiwari
Lead Auditor
Prescient Security LLC

The contents of this audit report are confidential. Findings raised within this report are the result of limited sampling. The audit is based on a sampling process of the available information and the auditors nor Prescient Security can guarantee that all, if any, non-conformities have been discovered.