

	INTERCERT INC.	Doc No	IC.F.27B.02
	ISMS Surveillance I Audit Report	Rev Dt.	12.03.2023

Client Reg. No.	ICI-IS-2403020 ICI-IS-2403021 ICI-IS-2403022 ICI-IS-2403023 Dated: 07-03-2025		
Date of the Surveillance Audit	25-02-2025		
Name of the Organization	Clarisights GmbH CLARISIGHTS LLP Clarisights Oy GRANULAR INSIGHTS INC.		
Client Location/Site Address	Nostitzstraße 20, 10961 Berlin, Germany No.749, 1st A Cross, Krishna Temple Road, CPB Complex, Indiranagar Double Road, Bengaluru, Karnataka 560038, India Käenkuja 3 A, 6th floor 00500 HELSINKI, Finland 16192, Coastal Highway, Lewes, Delaware 19958, United States		
Number of audit man days	3 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	Gaurav Chaturvedi	Designation: Site Reliability Engineering Manager	
Auditor Name	Anupam Saha	Role: Lead Auditor	
Technical Expert Name	Abhijith Rajesh	Role: Audit Team Member	
Scope of Certification	“Design, Development, Maintenance, Technical Support, Sales, and Marketing of Clarisights Products.” SOA Detail: CLS/CISO/SOA/001 Dated: 10-05-2023		
Applicable Legal, statutory & regulatory requirements and other requirements.	IT Act, no other requirements are applicable related to their services.		
Any changes in scope, address, company name	Yes		

	INTERCERT INC.	Doc No	IC.F.27B.02
	ISMS Surveillance I Audit Report	Rev Dt.	12.03.2023

Previous audit NCR status	Previous Audit findings verified.
Have previous issues been addressed appropriately	Yes
Has there been any significant changes to the company	No

	INTERCERT INC.	Doc No	IC.F.27B.02
	ISMS Surveillance I Audit Report	Rev Dt.	12.03.2023

Surveillance I 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	Entity determines all the parties that have an interest in the organization's needs and expectations has 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 documented and verified on the Sprinto compliance automation tool.
6.1.3 ISMS Risk Treatment and the operational control established over them	Verified - Information Security Risk Assessment process is defined in Risk Management Policy The risk register for the surveillance has been verified on the Sprinto compliance automation tool. Observed 48 identified risks along with required mitigation controls and measures. SOA Detail: CLS/CISO/SOA/001 Dated: 10-05-2023
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.

	INTERCERT INC.	Doc No	IC.F.27B.02
	ISMS Surveillance I Audit Report	Rev Dt.	12.03.2023

6.3 Planning of Changes to ISMS	Organization has a Change Management Policy evidenced 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 Management Policy 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 15-01-2025.
9.3 Management Review Meeting	Verified MRM was done on 15-01-2025 and its frequency is every twelve months. MRM Output is documented.
10.1 Continual Improvement	Organization utilizes Sprinto as a continual compliance automation tool. Some of the major observations are:
10.2 Non-Conformity and Corrective Action	The dashboard is at 99% complete for the entity with no major observations, but with 01 failing check and 11 due checks pending. Checks are in progress and will be delivered by Sprinto as per SLA.

	INTERCERT INC.	Doc No	IC.F.27B.02
	ISMS Surveillance I 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.
A.5.2	Information security roles and responsibilities	Policy is reviewed and communicated regularly. Verified Information Security Roles and Responsibilities in ISMS Information Security Roles and Responsibilities document.
A.5.3	Segregation of duties	Verified Information Security Roles and Responsibilities on the Sprinto compliance automation tool.
A.5.4	Management responsibilities	Information Security Officer verified on the Sprinto compliance automation tool.
A.5.5	Contact with special interest groups	Evidenced within Organization of Information Security Policy.
A.5.6	Contact with special interest groups	Evidenced within Organization of Information Security Policy.
A.5.7	Threat intelligence	Verified Threat Intelligence procedure on Sprinto compliance automation tool.
A.5.8	Information security in project management	Verified the information security awareness training material given to all employees at the time of induction and training records for the same. Inspected training records for Ishan Gupta conducted on 29-04-2024.
A.5.9	Inventory of information and other associated assets	Assets associated with information and information processing facilities identified - Verified.
A.5.10	Acceptable use of information and other associated assets	Verified Organizational Assets Responsibility through Asset Register.
A.5.11	Return of assets	Verified Asset Management Policy.
A.5.12	Classification of information	Verified Data Classification Policy on Sprinto compliance automation tool.
A.5.13	Labelling of information	Network Diagram verified on the Sprinto compliance automation tool.
A.5.14	Information transfer	

	INTERCERT INC.	Doc No	IC.F.27B.02
	ISMS Surveillance I Audit Report	Rev Dt.	12.03.2023

A.5.15	Access control	Access Control Policy verified. Verified access logs for employee Jeffrey Jacson with updated AWS User.
A.5.16	Identity management	
A.5.17	Authentication information	
A.5.18	Access rights	<p>Users of AWS, GCP, Github, Google Workspace, Jenkins, Sentry and Slack have been updated throughout the surveillance period. Verified the same in Sprinto compliance automation tool.</p> <p>21 users of AWS. 36 users of GCP. 35 users of Github. 65 users of Google Workspace. 77 users of Jenkins. 29 users of Sentry. 36 users of Slack.</p>
A.5.19	Information security in supplier relationships	Vendor Management Policy evidenced on the Sprinto compliance automation tool and risk related to suppliers identified and evaluated in Risk Register.
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	Verified Security within supplier agreement by verifying Non-Disclosure Agreement.
A.5.23	Information security for use of cloud services	Organization uses AWS for cloud services. All ISMS relevant controls are in place.
A.5.24	Information security incident management planning and preparation	Verified Incident Management Policy evidenced on the Sprinto compliance automation tool.
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	Verified Incident register.
A.5.28	Collection of evidence	11 Incidents recorded throughout Surveillance 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.5.29	Information security during disruption	Business Continuity Policy and Disaster Recovery Policy verified, documented on the Sprinto compliance automation tool. Business Continuity and Disaster Recovery Policy Framework approved by top management.
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.
A.5.32	Intellectual property rights	
A.5.33	Protection of Records	

	INTERCERT INC.	Doc No	IC.F.27B.02
	ISMS Surveillance I Audit Report	Rev Dt.	12.03.2023

A.5.34	Privacy and protection of personal identifiable information (PII)	<p>Verified the Corporate Legal Documents- Company number: 85115217 Certificate Number: IN-KA50205771425240U Business ID: 3223607-7 File Number: 6721169</p> <p>Organization has implemented appropriate procedures to protect intellectual property rights. Organization has procedures implemented to protect records.</p> <p>Independent review through Certification Body – INTERCERT.</p> <p>Technical review done continuously by Sprinto compliance automation tool.</p>
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	
A.6.1	Screening	<p>Verified the Employee Details and observed that the induction process is followed throughout the surveillance period.</p>
A.6.2	Terms and conditions of employment	
A.6.3	Information security awareness, education, and training	
A.6.4	Disciplinary process	<p>Verified Human Resource processes for employee Aditya Meharia whose Employment Start Date is 14-10-2024. Policy Acknowledgement Date: 17-10-2024. Background Verification Date: 19-10-2024.</p>
A.6.5	Responsibilities after termination or change of employment	
A.6.6	Confidentiality or non-disclosure agreements	
A.6.7	Remote working	<p>Evidenced the Physical Security Policy and Incident Management Policy on the Sprinto compliance automation tool.</p>
A.6.8	Information security event reporting	
A.7.1	Physical security perimeters	<p>Physical Security Policy and Physical and Environmental Security Procedure evidenced.</p> <p>Clear Desk Policy for papers and removable storage media for information processing facilities adopted evidenced within Physical and Environmental Security Procedure.</p> <p>Power and telecommunications cabling carrying data or supporting information services protected from interception, interference, or damage.</p>
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	<p>Organization has procedures implemented for secure disposal of equipment mentioned in Media Disposal Policy.</p>
A.8.1	User end point devices	<p>Access Control Policy verified.</p> <p>Organization has adopted a role-based access control system on need-to-know basis. Access provisioning logs are verified.</p>
A.8.2	Privileged access rights	
A.8.3	Information access restriction	
A.8.4	Access to source code	

	INTERCERT INC.	Doc No	IC.F.27B.02
	ISMS Surveillance I Audit Report	Rev Dt.	12.03.2023

A.8.5	Secure authentication	Verified the access control matrix on user and project level on the Sprinto compliance automation tool.
A.8.6	Capacity management	Capacity Management Procedure evidenced within Operation Security Policy through the Sprinto compliance automation tool.
A.8.7	Protection against malware	
A.8.8	Management of technical vulnerabilities	Separate environment provided and maintained for development and testing.
A.8.9	Configuration management	
A.8.10	Information deletion	Antivirus installed on all machines. Verified Data Backup Policy.
A.8.11	Data masking	
A.8.12	Data leakage prevention	Event Logging is done – verified. Verified the protection of log information.
A.8.13	Information backup	
A.8.14	Redundancy of information processing facilities	Verified Vulnerability Management Policy evidenced . Verified Vulnerability scanner status and Vulnerability logs maintained throughout the surveillance period through Sprinto compliance automation tool.
A.8.15	Logging	
A.8.16	Monitoring activities	Verified Penetration Testing carried out on 23-01-2025.
A.8.17	Clock synchronization	
A.8.18	Use of privileged utility programs	Critical data systems are protected from public internet access.
A.8.19	Installation of software on operational systems	
A.8.20	Networks security	Network Security Policy verified on the Sprinto compliance automation tool. 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	Verified Encryption Policy in Sprinto Compliance automation tool.
A.8.24	Use of cryptography	Software Development Life Cycle practised and evidenced on the Sprinto compliance automation tool.
A.8.25	Secure development life cycle	
A.8.26	Application security requirements	Secure systems engineering practiced and evidenced on the Sprinto compliance automation tool.
A.8.27	Secure system architecture and engineering principles	
A.8.28	Secure coding	Verified Change Management Procedure evidenced within Operation Security Policy and Procedure and change management repositories on Sprinto compliance automation tool.
A.8.29	Security testing in development and acceptance	
A.8.30	Outsourced development	
A.8.31	Separation of development, test and production environments	
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.27B.02
	ISMS Surveillance I Audit Report	Rev Dt.	12.03.2023

Evidence:

Fig 1: Legal Document

Fig 1.1: Clarisights GmbH

Amtsgericht Charlottenburg

Seite 1 von 1

Berlin, den 03.03.2023

Amtsgericht Charlottenburg (zu HRB 211389 B)
Handelsregister: Hardenbergstr. 31, 10623 Berlin
Vereinsregister: Amtsgerichtsplatz 1, 14057 Berlin

Clarisights GmbH
Nostitzstraße 20
10961 Berlin

In oben genannter Registersache erfolgte unter Aktenzeichen HRB 211389 B mit der laufenden Nummer 5 die nachstehende Registereintragung:

1. Nummer der Eintragung
5

2.b) Sitz, Niederlassung, inländische Geschäftsanschrift, empfangsberechtigte Person, Zweigniederlassungen

Geschäftsanschrift:
Nostitzstraße 20, 10961 Berlin

7.a) Tag der Eintragung
03.03.2023

Dieses Schreiben wurde maschinell erstellt und ist ohne Unterschrift gültig.

⚠ Achtung! Hinweis des Registergerichts:

Bekanntmachung der Handelsregistereintragungen erfolgt nur noch online und nicht mehr in Papierform.

Landes- und bundesweit mehren sich die Fälle, dass nach öffentlicher Bekanntmachung von Handelsregistereintragungen private Dritte unter Beifügung amtlich erscheinender Rechnungen zur Zahlung angeblicher Eintragungskosten auffordern. Es wird ausdrücklich darauf hingewiesen, dass Abrechnungen des Registergerichts Charlottenburg (Berlin) für Handelsregistereintragungen ausschließlich über die Kosteneinzugsstelle der Justiz (KEJ) erfolgen. Die Bankverbindung der KEJ lautet wie folgt:

IBAN: DE20 1001 0010 0000 3521 08
BIC: PBNKDEFF

Mittlerweile sind auch Fälle aufgetreten, in denen Originalrechnungen einer Gerichtskasse von privaten Dritten mit einer privaten Bankverbindung versehen wurden. **Leisten Sie daher nur Zahlungen an die KEJ, wenn die oben angegebene Bankverbindung in der Rechnung angegeben ist.**

	INTERCERT INC.		Doc No	IC.F.27B.02
	ISMS Surveillance I Audit Report		Rev Dt.	12.03.2023

Fig 1.2: CLARISIGHTS LLP.



INDIA NON JUDICIAL

Government of Karnataka

Rs. 1,000

e-Stamp

Certificate No.	: IN-KA50205771425240U
Certificate Issued Date	: 25-Feb-2022 08:17 PM
Account Reference	: NONACC (FI)/ kacrsf108/ KORAMANGALA7/ KA-BA
Unique Doc. Reference	: SUBIN-KAKACRSFL0837365260876571U
Purchased by	: CLARISIGHTS LLP
Description of Document	: Article 12 Bond
Description	: SUPPLEMENTARY LIMITED LIABILITY PARTNERSHIP AGREEMENT OF CLARISIGHTS LLP
Consideration Price (Rs.)	: 0 (Zero)
First Party	: CLARISIGHTS LLP
Second Party	: ANKUR GUPTA
Stamp Duty Paid By	: CLARISIGHTS LLP
Stamp Duty Amount(Rs.)	: 1,000 (One Thousand only)







SUPPLEMENTARY LIMITED LIABILITY PARTNERSHIP AGREEMENT OF CLARISIGHTS LLP

Mr. Ankur Gupta (DPIN: 07007916) Authorized Representative and Nominee of Granular Insights Inc.	Arun Srinivasan (DPIN: 05234064)	Aashima Agarwal (DPIN: 08384568)	Sneha Sreedhar (DPIN: 08384569)
			

Statutory Alert:

1. The authenticity of this Stamp certificate should be verified at www.shikshastamp.com or using e-Stamp Mobile App of Shiksha Holding.

2. Any discrepancy in the details on this Certificate and as available on the website / Mobile App renders it invalid.

3. The onus of checking the legitimacy is on the users of the certificate.

4. In case of any discrepancy please inform the Competent Authority.

	INTERCERT INC.	Doc No	IC.F.27B.02
	ISMS Surveillance I Audit Report	Rev Dt.	12.03.2023

Fig 1.3: Clarisights Oy

CLARISIGHTS OY	Luonnos / <i>Draft</i>	1 (1)
Y-tunnus / <i>Business ID</i> : 3223607-7	Pöytäkirja / <i>Minutes</i>	
Hallituksen kokous	1/2022	
<i>Meeting of the Board of Directors</i>		

Aika / [•].2022
Date

Paikka / *per capsulam*
Place

Paikalla / Arun Srinivasan, hallituksen jäsen / *Member of the Board of Directors*
Present

1 §
Kokouksen päätösvaltaisuus / *Quorum of the Meeting*

Todettiin, että kokous, jossa kaikki hallituksen jäsenet olivat saapuvilla, oli päätösvaltainen. /
As all the members of the Board of Directors were present, the Board of Directors was resolved to have a full quorum.

2 §
Toimitusjohtajan valinta / *Election of the Managing Director*

Päätettiin valita toimitusjohtajaksi Arun Srinivasan. /
It was resolved to elect Arun Srinivasan as Managing Director.

3 §
Valtuutus / *Authorization*

Päätettiin valtuuttaa Sonja Heinonen tai määräämänsä Procopé & Hornborg Asianajotoimisto Oy:stä laatimaan, allekirjoittamaan ja huolehtimaan tässä pöytäkirjassa esitettyjen päätösten rekisteröintiin tarvittavat ilmoitukset ja muut asiakirjat kaupparekisteriin ja muihin viranomaisten rekistereihin. /
It was resolved to authorize Sonja Heinonen, or a person appointed by her, from Procopé & Hornborg Attorneys Ltd to draft, sign, and present the notifications and

	INTERCERT INC.	Doc No	IC.F.27B.02
	ISMS Surveillance I Audit Report	Rev Dt.	12.03.2023

Fig 1.4: GRANULAR INSIGHTS INC.

STATE OF DELAWARE
CERTIFICATE OF CHANGE OF REGISTERED AGENT
AND/OR REGISTERED OFFICE
GRANULAR INSIGHTS INC.

The corporation organized and existing under the General Corporation Law of the State of Delaware, hereby certifies as follows:

First: The name of the corporation is GRANULAR INSIGHTS INC..

Second: The name of the Registered Agent therein and in charge thereof upon whom process against this Corporation may be served is Harvard Business Services, Inc. The address of the Registered Agent is 16192 Coastal Highway, Lewes, DE 19958, County of Sussex.

Third: The foregoing change to the registered office/agent was adopted by a resolution of the Board of Directors of the corporation.

By: / S / Arun Srinivasan
CEO

Name: Arun Srinivasan
Please Print

State of Delaware
 Secretary of State
 Division of Corporations
 Delivered 04:55 PM 11/19/2020
 FILED 04:55 PM 11/19/2020
 SR 20200451354 - File Number 6721169

	INTERCERT INC.	Doc No	IC.F.27B.02
	ISMS Surveillance I Audit Report	Rev Dt.	12.03.2023

Fig 2: SOA

Domain 1	ORGANIZATIONAL CONTROLS	A.5.1 A.5.2 A.5.3 A.5.4 A.5.5 A.5.6 A.5.7 A.5.8 A.5.9 A.5.10 A.5.11 A.5.12 A.5.13 A.5.14 A.5.15 A.5.16 A.5.17 A.5.18 A.5.19 A.5.20 A.5.21 A.5.22 A.5.23 A.5.24 A.5.25 A.5.26 A.5.27 A.5.28 A.5.29 A.5.30 A.5.31 A.5.32 A.5.33 A.5.34 A.5.35 A.5.36 A.5.37
Domain 2	PEOPLE CONTROLS	A.6.1 A.6.2 A.6.3 A.6.4 A.6.5 A.6.6 A.6.7 A.6.8
Domain 3	PHYSICAL CONTROLS	A.7.1 A.7.2 A.7.3 A.7.4 A.7.5 A.7.6 A.7.7 A.7.8 A.7.9 A.7.10 A.7.11 A.7.12 A.7.13 A.7.14
Domain 4	TECHNOLOGICAL CONTROLS	A.8.1 A.8.2 A.8.3 A.8.4 A.8.5 A.8.6 A.8.7 A.8.8 A.8.9 A.8.10 A.8.11 A.8.12 A.8.13 A.8.14 A.8.15 A.8.16 A.8.17 A.8.18 A.8.19 A.8.20 A.8.21 A.8.22 A.8.23 A.8.24 A.8.25 A.8.26 A.8.27 A.8.28 A.8.29 A.8.30 A.8.31 A.8.32 A.8.33 A.8.34
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

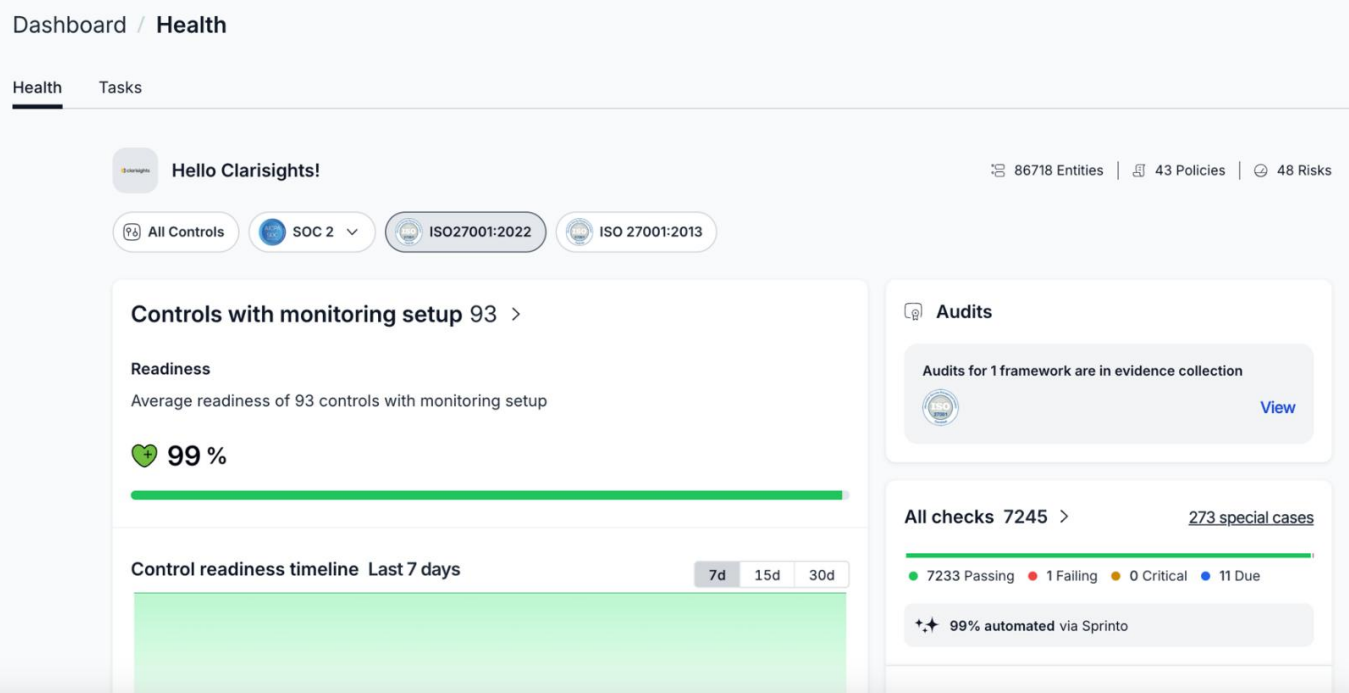


Fig 4: List of Staff Device

User	Device	Hard Disk encrypted?	Reported On
Patrick Bäcker (patrick.boeker@clarisights.com)	patrickb-clarisights (Ubuntu 22.04.5 LTS 22.04.5)	Yes	03-Dec-24
Jasmeet Sethi (jasmeet.sethi@clarisights.com)	Jasmeet-Clarisights.local (macOS 15.0.1)	Yes	06-Jan-25
Nidhi Patil (nidhi.patil@clarisights.com)	Nidhis-MacBook-Pro.local (macOS 15.0.1)	Yes	09-Feb-25
Ashu Pachauri (ashu.pachauri@clarisights.com)	Jupiter (Ubuntu 24.04.1 LTS 24.04.1)	Yes	13-Dec-24
Prateek Tiwari (prateek.tiwari@clarisights.com)	Admins-MBP.lan (macOS 14.0.0)	Yes	19-Dec-24
Chinmay Relkar (chinmay.relkar@clarisights.com)	Chinmays-MacBook-Pro.local (macOS 15.3.0)	Yes	09-Feb-25
Bhanu Prakash Thandu (bhanu.thandu@clarisights.com)	bhanu-clarisights (Ubuntu 24.10 24.10.0)	Yes	09-Feb-25
Lavdeep Raina (lavdeep.raina@clarisights.com)	192.168.1.4 (macOS 14.6.1)	Yes	21-Jan-25
Jeffrey Jacson (jeffrey.jacson@clarisights.com)	K-2SO (Ubuntu 22.04.5 LTS 22.04.5)	Yes	15-Jan-25

	INTERCERT INC.	Doc No	IC.F.27B.02
	ISMS Surveillance I Audit Report	Rev Dt.	12.03.2023

Fig 5: VAPT Report

Scope of the Assessment

The assessment was performed within the predefined scope of this engagement as listed below. No assumptions about the application were made.

Type	Name	Scope	Start Grade	Closure Grade
Web App	Clarisights Web App Target (Website Pentest)	https://app.clarisights.com/	B	B

Resolution Statistics

Severity	Solved	Unsolved	Help Wanted	Under Review	Accepted Risk	Grand Total
Critical	0	0	0	0	0	0
High	0	0	0	0	0	0
Medium	0	0	0	0	0	0
Low	0	2	0	0	0	2
Info	0	0	0	0	0	0
Grand Total	0	2	0	0	0	2

Overall vulnerability statistics

	INTERCERT INC.		Doc No	IC.F.27B.02
	ISMS Surveillance I Audit Report		Rev Dt.	12.03.2023

Fig 6: System Flow

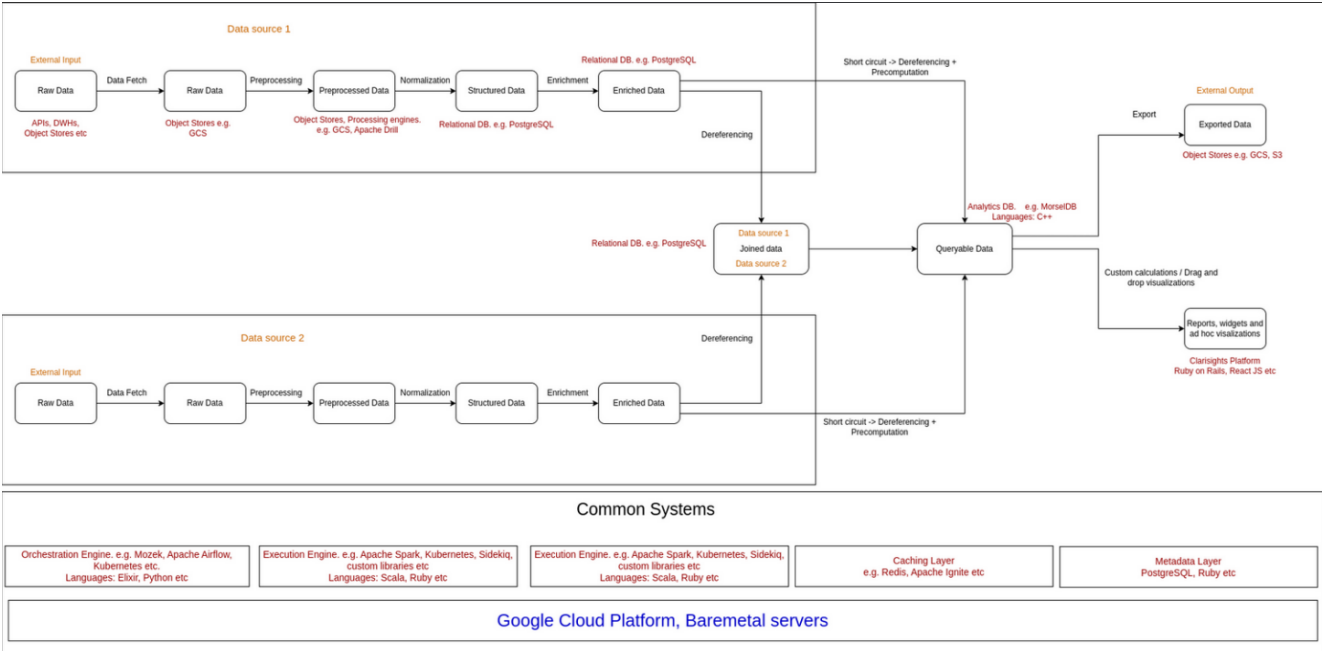


Fig 7: Organization Structure

Reportee	Manager	Assigned Roles
Ankur Gupta (ankur@clarisights.com)	Arun Srinivasan (arun@clarisights.com)	Co founder
Sylvia Kerscher (sylvia.kerscher@clarisights.com)	Arun Srinivasan (arun@clarisights.com)	Enterprise Account Executive
Ashu Pachauri (ashu.pachauri@clarisights.com)	Arun Srinivasan (arun@clarisights.com)	Chief Technology Officer
Monodeep Dutta (monodeep.dutta@clarisights.com)	Arun Srinivasan (arun@clarisights.com)	Solutions Success Manager
Seenivasan Masilamani (seenivasan.masilamani@clarisights.com)	Prashant Vithani (prashant.vithani@clarisights.com)	Software Engineer
Jasmeet Sethi (jasmeet.sethi@clarisights.com)	Ashu Pachauri (ashu.pachauri@clarisights.com)	Head of UX
Clemens Hannen (clemens.hannen@clarisights.com)	João Sousa (joao.sousa@clarisights.com)	Special Projects - GTM
Mihir Khandekar (mihir.khandekar@clarisights.com)	Bhupali Chiplunkar (bhupali.chiplunkar@clarisights.com)	Software Engineer
Arun Srinivasan (arun@clarisights.com)	Arun Srinivasan (arun@clarisights.com)	CEO

Fig 8: Organization Roles and Job Description.

Staff	Assigned Roles
Nidhi Patil (nidhi.patil@clarisights.com)	Site Reliability Engineer
Ankur Gupta (ankur@clarisights.com)	Co founder
Raghvendra Rao (raghvendra.rao@clarisights.com)	Software Engineer
Arun Srinivasan (arun@clarisights.com)	CEO
Clemens Hannen (clemens.hannen@clarisights.com)	Special Projects - GTM
Philip Ziegler (philip.ziegler@clarisights.com)	Customer Success Manager
Jan Rixgens (jan@clarisights.com)	Chief of Staff - CEO
Avishek Rath (avishek.rath@clarisights.com)	Customer Success Manager
Abhishek Khosla (abhishek.khosla@clarisights.com)	Chief Financial Officer

	INTERCERT INC.	Doc No	IC.F.27B.02
	ISMS Surveillance I 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 Surveillance audit but not later than 60 days from the date of Surveillance 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 Surveillance 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 Surveillance 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 (03/2026)		
On behalf of the Certification Body		Name of the organization: Clarisights GmbH CLARISIGHTS LLP Clarisights OY GRANULAR INSIGHTS INC.	
M/s INTERCERT INC.	Name:	Gaurav Chaturvedi	Stamp:
Stamp and Sign Name of the auditor: - Anupam Saha (LEAD AUDITOR)	Designation:	Site Reliability Engineering Manager	
	Date of Audit:	25-02-2025	
Date of Audit: - 25-02-2025	Stage of Audit: -	Surveillance I Audit	Signature: -

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