Organization Name	DoControl				**SII NO.**	286086
Address	Walter Moses St. 1 TA				**Tel**	
Date of audit	18/10/2022		Pick a date	Pick a date	**Mail**	
Standards	ISO 27001				**Location**	On site
Type of Audit	Surveillance	Stage 2	Select type	Select type	**Frequency**	Select frequency
Scope:	Development and maintenance of an advanced, agentless solution for protecting Cloud and SaaS applications					

AUDIT SUMMARY REPORT FOR:	**ISO 27001:2013**

Clause	Subject audited	Clause classification	Remarks
4.1	Understanding the organization and its context	Conforms	
4.2	Understanding the needs and expectations of interested parties	Conforms	
4.3	Determining scope of information security management system	Conforms	
5.1	Leadership and commitment	Conforms	
5.2	Policy	Conforms	
5.3	Organizational roles, responsibilities, and authorities	Conforms	
6.1.2	Information security risk assessment	Conforms	
6.1.3	Information security risk treatment	Conforms	
6.2	Information security objectives and planning to achieve them	Conforms	
7.1	Resources	Conforms	
7.2	Competence	Conforms	
7.3	Awareness	Conforms	
7.4	Communication	Conforms	
7.5.1	Documentation - General	Conforms	
7.5.2	Creating and updating of documented information	Conforms	
7.5.3	Control of documented information	Conforms	
8.1	Operational planning and control	Conforms	
8.2	Information security risk assessment.	Conforms	
8.3	Information security risk treatment	Conforms	
9.1	Monitoring, measurement, analysis, and evaluation	Conforms	
9.2	Internal audit	Conforms	
9.3	Management review	Conforms	
10.1	Nonconformity and corrective action	Conforms	
10.2	Continual improvement.	Conforms	
A5	Information security policies	Conforms	
A6	Organization of information security	Conforms	
A7	Human resource security	Conforms	
A8	Asset management	Conforms	
A9	Access control	Conforms	
A10	Cryptography	Conforms	
A11	Physical and environmental security	Conforms	
A12	Operations security	Conforms	
A13	Communications security	Conforms	
A14	System acquisition, development, and maintenance	Conforms	
A15	Supplier relationships	Conforms	
A16	Information security incident management	Conforms	
A17	Information security aspects of business continuity management	Conforms	
A18	Compliance	Conforms	

42 Haim Levanon St. Tel-Aviv 69977 Israel. Tel: 972-3-646-5114 Fax: 972-3-646-5205 www.sii.org.il

Organization Name	DoControl				**SII NO.**	286086
Address	Walter Moses St. 1 TA				**Tel**	
Date of audit	18/10/2022		Pick a date	Pick a date	**Mail**	
Standards	ISO 27001				**Location**	On site
Type of Audit	Surveillance	Stage 2	Select type	Select type	**Frequency**	Select frequency
Scope:	Development and maintenance of an advanced, agentless solution for protecting Cloud and SaaS applications					

Auditors Signatures and Date			
Lead auditor Name	David Kalmanowitz	18/10/2021	
Auditor Name & signature	*David Kalmanowitz*		

Audit Report

1. Opening Meeting:

☒ Introduction of participant	☒ confirmation that the audit team leader is responsible for the audit and shall be in control of executing the audit plan including audit activities and audit trails	☒ Confirmation of the Scope
☒ confirmation of matters relating to confidentiality;	☒ confirmation that the resources and facilities needed by the audit team are available	☒ confirmation of formal communication channels between the audit team and the client
☒confirmation that, during the audit, the client will be kept informed of audit progress and any concerns	☒confirmation of relevant work safety, emergency, and security procedures for the audit team	☒ Confirmation of audit plan (audit type, changes, goals)
☒confirmation of the language to be used during the audit;	☒ information about the conditions under which the audit may be prematurely terminated	☒ The method of reporting, including any grading of audit findings
☒ **Reinforcement of the concept of expected outcomes for an organization with accredited certification**	☒confirmation of the availability, roles and identities of any guides and observers.	☒ confirmation of the status of findings of the previous review or audit, if applicable
		☒ methods and procedures to be used to conduct the audit based on sampling

Organization representative /Accompanying persons	**Role**	**Opening meeting**	**Closing meeting**
Liel Ran	CTO and Co-Founder	Yes	Yes
Kobi Afuta	Head of IT and Security (CISO)	Yes	Yes

Remote Assessment using ICT:	No
What ICT platform(s) was used to conduct the audit?	

42 Haim Levanon St. Tel-Aviv 69977 Israel. Tel: 972-3-646-5114 Fax: 972-3-646-5205 www.sii.org.il

Organization Name	DoControl				**SII NO.**	286086
Address	Walter Moses St. 1 TA				**Tel**	
Date of audit	18/10/2022		Pick a date	Pick a date	**Mail**	
Standards	ISO 27001				**Location**	On site
Type of Audit	Surveillance	Stage 2	Select type	Select type	**Frequency**	Select frequency
Scope:	Development and maintenance of an advanced, agentless solution for protecting Cloud and SaaS applications					

Identify any ICT issues encountered during the audit:	
Did ICT issues impact the scheduled audit time? ☐ Yes ☐ No: Comments	
Did ICT issues impact the team's ability to meet their audit objectives? ☐ Yes ☐ No: Comments	
Did ICT issues impact the audit effectiveness? ☐ Yes ☐ No: Comments	

42 Haim Levanon St. Tel-Aviv 69977 Israel. Tel: 972-3-646-5114 Fax: 972-3-646-5205 www.sii.org.il

Organization Name	DoControl				**SII NO.**	286086
Address	Walter Moses St. 1 TA				**Tel**	
Date of audit	18/10/2022		Pick a date	Pick a date	**Mail**	
Standards	ISO 27001				**Location**	On site
Type of Audit	Surveillance	Stage 2	Select type	Select type	**Frequency**	Select frequency
Scope:	Development and maintenance of an advanced, agentless solution for protecting Cloud and SaaS applications					

Purpose of the assessment and topics presented by the auditor
Surveillance – ISMS

Total number of employees (including Permanent Contractor Workers)	**70**
No. of employees	**70**
Number of IT employees (ISO 27001)	**2**
Number of shifts	

Client significate changes affecting the ISMS since last audit:
Change in the Physical address had positive impact on the physical security. Previous building had limited access restrictions. The new location is more secure, it has an intercom, entry chip issued and managed by Kobi (CISO) with a lot more controls in place. Access to Communication\Network Room is restricted and locked accessible via chip limited to 4 individuals only.
Any significant issues impacting the audit program
/
Departments / sites / processes audited/ Boundaries audited
ISMS+ all applicable controls (According to the SOA)

2. A general assessment of the management system :
Use of certification mark:
☒ Conforms ☐ Doesn't Conforms Please specify:

Certificate Validity	20/10/2023	**Standard**	**ISO 27001**	**Certificate No.**	**110939**

Organization Scope:	
☒ Appropriate ☐ Isn't Appropriate Please specify:	

The management system meets the requirements / expectations	☒ **Yes**	☐ **No**
The conformity & effectiveness of the management system	☒ **Yes**	☐ **No**
Audit Objectives Achieved	☒ **Yes**	☐ **No**

42 Haim Levanon St. Tel-Aviv 69977 Israel. Tel: 972-3-646-5114 Fax: 972-3-646-5205 www.sii.org.il

Organization Name	DoControl				**SII NO.**	286086
Address	Walter Moses St. 1 TA				**Tel**	
Date of audit	18/10/2022		Pick a date	Pick a date	**Mail**	
Standards	ISO 27001				**Location**	On site
Type of Audit	Surveillance	Stage 2	Select type	Select type	**Frequency**	Select frequency
Scope:	Development and maintenance of an advanced, agentless solution for protecting Cloud and SaaS applications					

Audit Criteria Achieved	☒ **Yes**	☐ **No**
Corrective actions (CA) for a previous audit:	**Previous audit date**	Pick a date

☒ No corrective action needed from previous audit

☐ Corrective action & effectiveness reviewed during the audit, see report

☐ Attached to this report is an approved corrective action

☐ No corrective actions were performed as required; improvement required

Reviewer assessment

The company takes very seriously information security and information security management. The company conforms to the audited Standard. Opportunities for improvement were discussed during closing meeting and will be treated accordingly by the company. The Information Security Team and company management expressed their commitment to the continuous improvement of their ISMS.

3. Auditor recommendation to certification/scheme manager (Please sign)

Based on the result of stage 2 audit:

☒ Recommendation for issuing a certificate (based on the closure of CA if required)

☐ No Recommendation for issuing a certificate

Based on the result of surveillance audit :

☒ Recommendation for continued certification (subject to marked in section 5 above)

Based on the result of Reassesment audit:

☐ Recommendation for continued certification (subject to closure of CA if required)

Based on the result of Special audit:

☐ Recommendation for continued certification for exsisting scope (subject to marked in section 5 above)

☐ Recommendation for updating the certification (subject to closure of CA if required)

☐ Recommendation for transfer of certification(subject to closure of CA if required)

Every audit allowes: ☐ Recommendation for suspention / withdraw of certification

42 Haim Levanon St. Tel-Aviv 69977 Israel. Tel: 972-3-646-5114 Fax: 972-3-646-5205 www.sii.org.il

Organization Name	DoControl				**SII NO.**	286086
Address	Walter Moses St. 1 TA				**Tel**	
Date of audit	18/10/2022		Pick a date	Pick a date	**Mail**	
Standards	ISO 27001				**Location**	On site
Type of Audit	Surveillance	Stage 2	Select type	Select type	**Frequency**	Select frequency
Scope:	Development and maintenance of an advanced, agentless solution for protecting Cloud and SaaS applications					

4. Recommendation for providing a general classification of the management system:

☒ .1 Conforms to requirements 2. ☐ Conforms to requirements & awaiting CA

.3 ☐ Improvement required & awaiting CA 4. ☐ Not Conforming

Note: In surveillance audit if one of the options 3,4 above has been marked, it is mandatory to submit the audit report for approval by the certification/scheme manager.

5. Activities required from the organization:

☐ Performance and implementation of corrective action to the remarks of the audit findings shall be checked within the framework of the following audit

Corrective action plan containing responsibilities and schedule according to the remarks detailed shall be submitted until	Pick a date
Next Audit Date	01/10/2023

Closing meeting:

☒ A formal closing meeting (attendance shall be recorded) shall be held with customer's management representatives	☒ The purpose is to present audit conclusions including recommendation regarding certification	☒ advising that the audit evidence obtained was based on sample
☒ The method and time frame of reporting including any grading of audit findings	☒The certification body process for handling nonconformities including any consequences relating to the status of the client's certification	☒information about the complaint & appeal handling processes
☒ Thank you for hospitality and cooperation	☒ Any nonconformities shall be presented and a time frame for responding shall be agreed.	☒ Post activities at SII and recommendation for certification

Distribution

Approval of Audit Report (certification manager/scheme)

Name & Signature		**Date:**	Pick a date

42 Haim Levanon St. Tel-Aviv 69977 Israel. Tel: 972-3-646-5114 Fax: 972-3-646-5205 www.sii.org.il

Organization Name	DoControl				**SII NO.**	286086
Address	Walter Moses St. 1 TA				**Tel**	
Date of audit	18/10/2022		Pick a date	Pick a date	**Mail**	
Standards	ISO 27001				**Location**	On site
Type of Audit	Surveillance	Stage 2	Select type	Select type	**Frequency**	Select frequency
Scope:	Development and maintenance of an advanced, agentless solution for protecting Cloud and SaaS applications					

Findings	**Classification**
Introduction, changes from previous year	
A small Start-up company (70 employees – 2 IT Privileged Users), developing SaaS B2B protecting solution. Approx 40 large paying customers.	
Their infrastructure is based solely on managed services (SaaS solutions).	
ISMS	
Interested parties+ Context+ Scope (ISMS (4.1,4.2,4.3(	
Scope document — The Scope is defined in the document ISMS Policies.	
Information Security Policy Presented – Version 1.2 Dated February 14, 2022, laying out Information Security Commitment.	
Customer focus is privacy based on GDPR. The company is GDPR Compliant, PII information accessed based on the customer's request and requirements. All information is saved by the customer on their respective platforms. DoControl does not save customer data on the DoControl Platform. Customer security is taken very seriously to be discussed in item A14 related to Penetration testing and Vulnerability Scans. Investors – Board receive Security Updates once every Quarter. SOC2 Compliant. Completed GAP Analysis for HIPAA Certification.	
<u>Scope (to be printed on the certification paper)</u> Development and maintenance of an advanced, agentless solution for protecting Cloud and SaaS applications פיתוח ותחזוקה של פתרון מתקדם להגנה על מערכות מידע מבוססות מודל ענן ותוכנה כשירות	
Management leadership & commitment (ISMS 5.1)	
Kobi (CISO) most of his focus is on Security and Privacy. Liel (CTO) oversees Security and Privacy Policies and Procedures.	

42 Haim Levanon St. Tel-Aviv 69977 Israel. Tel: 972-3-646-5114 Fax: 972-3-646-5205 www.sii.org.il

Organization Name	DoControl				**SII NO.**	286086
Address	Walter Moses St. 1 TA				**Tel**	
Date of audit	18/10/2022		Pick a date	Pick a date	**Mail**	
Standards	ISO 27001				**Location**	On site
Type of Audit	Surveillance	Stage 2	Select type	Select type	**Frequency**	Select frequency
Scope:	Development and maintenance of an advanced, agentless solution for protecting Cloud and SaaS applications					

Findings		**Classification**
Risk assessment Matrix presented during Management Review on 6 October 2022. Attended by: Adam Gavish (CEO), Asaf Levy (CFO), Kobi Afuta (CICO), Liele Ran (CTO), Omri Wienberg (CRO) over Zoom due to numerous participants being abroad. Actions Items: Review and Accept RA and RTP. Security and Privacy. Review ISMS Status. Raise business needs. Management Approval. Risk Management Matrix up to date with Status Updates.		
Policies (ISMS 5.2)		
Commitment policy	The Commitment Policy is part of the general Information Security Policy. (I.e., Information Security Policy V1.2 February 2022) presented.	
Roles (ISMS 5.3)		
Board (Founders and Members of investors)– Provides guidance on future of the company per vision. Bi-Weekly - Founder Meeting (Steering Committee) overview the general direction of the organization. Steering Committee (Founder) last held on July 27, 2022 Management Leadership Meeting once a month practical progress updates (e.g., Feature updates) Senior Roles and Responsibilities: CEO VP Finance VP Product CTO Head Of People CRO VP Marketing		
Risks management (ISMS 6.1)		
SoA exists - הצהרת ישימות	Exists and updated	
Risks treatment plan	Presented as part of the risk assessment Matrix.	

42 Haim Levanon St. Tel-Aviv 69977 Israel. Tel: 972-3-646-5114 Fax: 972-3-646-5205 www.sii.org.il

Organization Name	DoControl				**SII NO.**	286086
Address	Walter Moses St. 1 TA				**Tel**	
Date of audit	18/10/2022		Pick a date	Pick a date	**Mail**	
Standards	ISO 27001				**Location**	On site
Type of Audit	Surveillance	Stage 2	Select type	Select type	**Frequency**	Select frequency
Scope:	Development and maintenance of an advanced, agentless solution for protecting Cloud and SaaS applications					

Findings		**Classification**
The Risk Assessment Matrix and treatment report 06.10.2022		
Sampling: - Local Admins - Workstations Hardening - Formal process for updating 3rd party software - OS updates - Off Boarding Process. Offboarding is now automated managed by OKTA to ensure that all relevant permissions have been removed from a departing employee. Employee Lateral moves or promotions are also automated and managed by OKTA. CISO has exclusive access and manages OKTA workflows.		
Goals (ISMS 6.2)		
Plan to achieve goals	Part of the Risk Assessment Matrix, Monday, and Bug Bounty.	
KPI List was presented for Q4, 2022. Managed on Monday. Example Bug Bounty test from 25 to 75.		
Resources, competence, awareness (ISMS 7.1,7.2,7.3)		
competencies of IS staff	Exists.	
Requirements from contractor's employees	All development is done inhouse.	
Awareness Training General Once a year April 2022 via Zoom. Awareness training platform procured Living Security, to be implemented by the beginning of November 2022. Awareness Training for Software Developers – Once a year (Frontal Instruction by Liel and Living Security Platform). There is an exam at the end of each instructional session.		
Communication (In & out ISMS 7.4)		

42 Haim Levanon St. Tel-Aviv 69977 Israel. Tel: 972-3-646-5114 Fax: 972-3-646-5205 www.sii.org.il

Organization Name	DoControl				**SII NO.**	286086
Address	Walter Moses St. 1 TA				**Tel**	
Date of audit	18/10/2022		Pick a date	Pick a date	**Mail**	
Standards	ISO 27001				**Location**	On site
Type of Audit	Surveillance	Stage 2	Select type	Select type	**Frequency**	Select frequency
Scope:	Development and maintenance of an advanced, agentless solution for protecting Cloud and SaaS applications					

Findings	**Classification**
Internal Communication: Slack Cloud Based. Google Workspace. Zoom. WhatsApp – administrative nonofficial, non-sensitive information. **External**: Slack Cloud Based. Google Workspace. Zoom Communication Classifications Guidelines appear in Information Security Management System Edition 1.2 Feb 14, 2022. **Opportunity For Improvement**: Introduce Classification Labels on both Internal and External documentation.	
Document controls (ISMS 7.5)	
Use of G-drive (G-suit Enterprise version) to share document with interested parties' groups managed by Liel and Kobi. Each department manage their own shared drive.	
The access control is based on OKTA to AWS trust definition which defines for each use the connection, creating an SSO to the company cloud resources. OKTA has been added to the off-boarding process to enhance security management and transparency.	
The access is based on a simple RBAC model (Authenticated users, private R&D account, Production account, shared logs accounts) – Least Privilege.	
Operational controls (ISMS 8.1)	
Plan to achieve goals: As part of the Information Security Policy document under Operational Planning and Control, the information Security Plan was presented as evidence.	
Risks (ISMS 8.2 during surveillance audit)	
Refer to 6.1 Risk Management	
Monitoring & measurement of ISMS (ISMS 9.1)	
Logs are kept in the cloud for later technical problems and forensic investigating of any type.	

42 Haim Levanon St. Tel-Aviv 69977 Israel. Tel: 972-3-646-5114 Fax: 972-3-646-5205 www.sii.org.il

Organization Name	DoControl				**SII NO.**	286086
Address	Walter Moses St. 1 TA				**Tel**	
Date of audit	18/10/2022		Pick a date	Pick a date	**Mail**	
Standards	ISO 27001				**Location**	On site
Type of Audit	Surveillance	Stage 2	Select type	Select type	**Frequency**	Select frequency
Scope:	Development and maintenance of an advanced, agentless solution for protecting Cloud and SaaS applications					

Findings		**Classification**
Use of Cloud monitoring " DatadogHQ" for AWS		
No SIEM. OKTA - Alerts received by CISO to email. Logs retained in System. Google - Alerts received by CISO to email. Logs retained in System. Crowdstrike – Alerts received by CISO to email. Logs retained in System. MDM – InfiniPoint - Alerts received by CISO to email. Logs retained in System.		
Internal audits (ISMS 9.2)		
Audit plan including scope	**Opportunity For Improvement:** SOC2 Audit was completed on Feb 2022 and the certification was received in March 2022. An Internal Audit separate and Independent of the SOC2 Audit will be reviewed by next ISO 27001 Audit.	**3**
Management review (**ISMS** 9.3)		
Review MoM	6 October 2022	
Participants: Liel, Adam, Asaf, Omri		
The meeting was via a Zoom Session.		
The Review was documented in Google Notes and presented.		
The goals and objectives presented, dated 28 Sep 2022		
The list of KPIs were presented.		
Corrective actions, Improvement (ISMS 10.1, 10.2)		
The Non-conformities are managed as Corrective Actions to be completed next year as part of the scheduled Internal Audit will be completed by next ISO Audit.		
Controls		
Policies (Controls A5.1, A5.2)		Not in audit plan

42 Haim Levanon St. Tel-Aviv 69977 Israel. Tel: 972-3-646-5114 Fax: 972-3-646-5205 www.sii.org.il

Organization Name	DoControl				**SII NO.**	286086
Address	Walter Moses St. 1 TA				**Tel**	
Date of audit	18/10/2022		Pick a date	Pick a date	**Mail**	
Standards	ISO 27001				**Location**	On site
Type of Audit	Surveillance	Stage 2	Select type	Select type	**Frequency**	Select frequency
Scope:	Development and maintenance of an advanced, agentless solution for protecting Cloud and SaaS applications					

Findings	**Classification**
Roles, segregation of duties, IS in projects, contact with interest groups (Controls A6.1.2, A6.1.3, A6.1.4, A6.1.5 A6.1.1)	Not in audit plan
Mobile working, remote connection (Controls A6.2.1, A6.2.2)	Not in audit plan
Remote access policy	
Use of mobile devices	
Background checks, employee on-board, awareness training, disciplinary actions, termination (Controls A7.1.1, A7.1.2, A7.2.1, A7.2.2, A7.2.3, A7.3.1)	Not in audit plan
Disciplinary actions procedure	
Assets management/classification, labelling (Controls A8.1.1, A8.1.2, A8.1.3, A8.1.4, A8.2.1, A.8.2.2, A8.2.3)	Not in audit plan
Assets classification procedure	
Acceptable use policy	
Assets labelling procedure	
Media in use, Media transfer, media disposal (Controls A8.3.1, A8.3.2, A8.3.3)	Not in audit plan
Media handling procedure	
Disposal of media procedure	
Removable media	

42 Haim Levanon St. Tel-Aviv 69977 Israel. Tel: 972-3-646-5114 Fax: 972-3-646-5205 www.sii.org.il

Organization Name	DoControl				**SII NO.**	286086
Address	Walter Moses St. 1 TA				**Tel**	
Date of audit	18/10/2022		Pick a date	Pick a date	**Mail**	
Standards	ISO 27001				**Location**	On site
Type of Audit	Surveillance	Stage 2	Select type	Select type	**Frequency**	Select frequency
Scope:	Development and maintenance of an advanced, agentless solution for protecting Cloud and SaaS applications					

Findings	**Classification**
Access controls to assets and network services (Controls A9.1.1, A9.1.2)	Not in audit plan
Access control policy	
Users' identification/authentication/Management, privileged users, access rights (Controls A9.2.1, A9.2.2, A9.2.3, A9.2.4, A9.2.5, A9.2.6**,** A9.3.1)	Not in audit plan
Registration and de-registration of users	
Log-in procedures to systems, password management, access to source (Controls A9.4.1, A9.4.2, A9.4.3, A9.4.4, A9.4.5)	Not in audit plan
Log-in procedure	
Data in rest/Encryption, key management (Controls A10.1, A19.2)	Not in audit plan
Encryption policy	
Physical security (premises, offices, environmental) (Controls A11.1, A11.2, A11.3, A11.4, a11.5, A11.6)	Not in audit plan
Working in a secure area	
Maintenance of supporting utilities and equipment, work environment, (Controls A11.2.1, A11.2.2, A11.2.3, A11.2.4, A11.2.5, A11.2.6, A11.2.7, A11.2.8, A11.2.9	Not in audit plan
Clean desk policy	
Operational procedures, change management, capacity, environments separation (Controls A12.1, A12.1.2, A12.1.3, A12.1.4)	Not in audit plan
Operational procedures	

42 Haim Levanon St. Tel-Aviv 69977 Israel. Tel: 972-3-646-5114 Fax: 972-3-646-5205 www.sii.org.il

Organization Name	DoControl				**SII NO.**	286086
Address	Walter Moses St. 1 TA				**Tel**	
Date of audit	18/10/2022		Pick a date	Pick a date	**Mail**	
Standards	ISO 27001				**Location**	On site
Type of Audit	Surveillance	Stage 2	Select type	Select type	**Frequency**	Select frequency
Scope:	Development and maintenance of an advanced, agentless solution for protecting Cloud and SaaS applications					

Findings	**Classification**
Protection from Malware (Controls A12.2.1)	Not in audit plan
Backup (Controls A12.3.1)	
Backup and Disaster Recovery Policy Edition 1.2 dated Feb 14, 2022 was presented. What needs to be backed up: Source Code – GitHub Alerts and Logs via email to CTO and R&D Head (BCP GitHub not critical information). Customer data production – AWS – Databases backed-up once daily. Alerts and Logs via email to CTO and R&D Head. Customer Relationship data – Salesforce (CRM, BCP by Salesforce, non-critical information), Intercom Support (BCP by Intercom). Production Infrastructure Cloud Based (Servers, Workloads) – Daily Database Backup in AWS bucket. Corporate and Financial data (HR HIBOB, Financial Salesforce, ERP in the process of being implemented (BCP per vendor agreement). Restore test completed successfully on October 4, 2022, evidence provided. Data Restoration and Recovery responsibility of the DevOps team. Restoration Test will occur at least once a year of all data to a separate and new AWS bucket.	
Logs and their backup (controls A12.4.1, A12.4.2, A12.4.3, A12.4.4)	Not in audit plan
Operational Software (Controls A.12.5)	Not in audit plan
Installing SW on operational systems	
Endpoint point protection (controls A12.6.1, A12.6.2)	Not in audit plan
Technical inspection of systems (Controls A12.7.1)	Not in audit plan
Networks management (Controls A13.1.1, A13.1.2, A13.1.3)	Not in audit plan

42 Haim Levanon St. Tel-Aviv 69977 Israel. Tel: 972-3-646-5114 Fax: 972-3-646-5205 www.sii.org.il

Organization Name	DoControl				**SII NO.**	286086
Address	Walter Moses St. 1 TA				**Tel**	
Date of audit	18/10/2022		Pick a date	Pick a date	**Mail**	
Standards	ISO 27001				**Location**	On site
Type of Audit	Surveillance	Stage 2	Select type	Select type	**Frequency**	Select frequency
Scope:	Development and maintenance of an advanced, agentless solution for protecting Cloud and SaaS applications					

Findings		**Classification**
Information transfer (Controls A13.2.1, A13.2.2, A13.2.3, A13.2.4)		Not in audit plan
Protection of data in transit		
Security requirements, Web site, safe surfing e-Commerce (**Controls** A14.1.1, A14.1.2, A14.1.3),		Not in audit plan
SDLC, application securing, test data (Controls A14.2.1, A14.2.2, A14.2.3, A14.2.4, A14.2.5, A14.2.6, A (14.2.7, A14.2.8, A14.2.9, A14.3)		
Engineering of secure systems	Secure Development Life Cycle procedure (Process - Agile): • Requirements • Design • Development • 2 weekly meetings R&D Status updates and Demo. • Verification testing includes Security and vulnerability testing. • GitHub dependency testing process. The procedure is managed in GitHub. Development tasks managed on Monday.	
Change management procedures	All automated. Stages and process identical to the Development Cycle above.	
Secure development methodology & procedures	Secure Development Life Cycle Framework Version 1.2 Feb 14, 2022 – Presented.	
According to CI-CD (Continuous development and integration) automated.		
Development Team: CTO Head of R&D Leads of the different sections.		
Training: Both frontal (Liel CTO) and Living Security platform with test.		
Methodology: Agile framework, sprints of 2 weeks, two weekly meeting		
Project Management: Managed on Monday, each item has its own classification. The main epic/sprint was presented as evidence., including tickets and statuses. Security Considerations. Roadmap managed by VP Product.		

42 Haim Levanon St. Tel-Aviv 69977 Israel. Tel: 972-3-646-5114 Fax: 972-3-646-5205 www.sii.org.il

Organization Name	DoControl				**SII NO.**	286086
Address	Walter Moses St. 1 TA				**Tel**	
Date of audit	18/10/2022		Pick a date	Pick a date	**Mail**	
Standards	ISO 27001				**Location**	On site
Type of Audit	Surveillance	Stage 2	Select type	Select type	**Frequency**	Select frequency
Scope:	Development and maintenance of an advanced, agentless solution for protecting Cloud and SaaS applications					

Findings	**Classification**
Code Repository: GitHub Enterprise. All the repositories are private. The repository was presented as evidence. Deployment Steps: Once all manual and automated coded review has been received and approved it is uploaded to production. New and substantial advanced features undergo a complete review by CTO, CISO, R&D Head. Minor updates features are approved by team leads or senior software Developers.	
Technologies: Front End: REACT Back End: NodeJS, python (Data Science – AWS)	
Open Source: Vulnerabilities scanner via Dependabot, License Management Document presented dated Feb 18, 2021**.**	
Secure Code Review: Infrastructure – CDK vulnerability hygiene tool (AWS Solutions HIPAA, NIST) Code – Scan – Study Code Analysis, Code Coverage Code Climate – Automation Tools.	
Test phases – Unit test, Integration Test, Post Deployment Test. Ongoing (Reflect, Datadog).	
Test Environments: Synthetic data.	
Penetration testing: Ongoing Bugcrowd (Current 25 testers goal to reach 75 testers and annual full scale Pen Testing). **Vulnerability Scanning:** Detectify once a week.	
Any major changes to application require CISO Review and Approval.	
VRM (Controls A15.1.1. A15.1.2, A15.1.3, A15.2.1, A15.2.2 ,A15.2.3)	Not in audit plan
Mitigation of **Vendors** risks	
Incidents detection, evaluate, report, response, investigate, evidence collection: (Controls A16.1.1, A16.1.2, A16.1.3, A16.1.4, A16.1.5, A16.1.6, A16.1.7)	
Incident management, response, — No events were registered, 2021 -2022.	
Evidence identification & collection; — As per Security Incident Handling ISMS Edition 1.2, Feb 14, 2022, the policy was presented as evidence.	

Organization Name	DoControl				**SII NO.**	286086
Address	Walter Moses St. 1 TA				**Tel**	
Date of audit	18/10/2022		Pick a date	Pick a date	**Mail**	
Standards	ISO 27001				**Location**	On site
Type of Audit	Surveillance	Stage 2	Select type	Select type	**Frequency**	Select frequency
Scope:	Development and maintenance of an advanced, agentless solution for protecting Cloud and SaaS applications					

Findings	**Classification**
Definitions: Malware – Crowdstrike EDR Unauthorized Access - Two Factor Authentication – Plan is to have OKTA maintain all critical access. Multiple Failed Login Attempts – Currently Managed via Google (Gmail, slack, user access) OKTA future for both production and user access. Significant Latency – Cloud based, DataDog. Unexplained Files – Data Retention per vendor BCP accept Risk Physical break-In to facilities – 24/7 Camera monitoring, Alarm. Phishing or fraud attempts – Built in Google functionality – Additional system will be reviewed. Abnormal behavior. Based on OKTA, Google alerts. **Opportunity for Improvement**: Review independent backup options for CRM, salesforce, Intercom, etc.	
Business continuity, redundancy, availability (Controls A17.1, A17.1.2, A17.1.3, A17.2.1)	
BCM procedures — Critical Functions Business Continuity Plan and Strategy Version 1.2 Feb 14, 2022,	
October 4, 2022, a full-scale drill (exercise) was completed including the Restoration of entire production platform and data restoration.	
Production: RPO - 24 Hours RTO - 12 Hours	
DR Drill \ Playbook (Disaster Recovery Policy) presented detail SOP recovering from a Disaster Step-by-Step including restoring databases and the platform itself.	
Compliance to contract requirements & regulation (Controls A18.1.1, A18.1.2, A18.1.3, A18.1.4, A18.1.5)	Not in audit plan
Identification of Jurisdiction regulations	
SW licensee's management	
Policy and procedures audit, technical inspection (Controls A18.2.1, A18.2.2, A18.2.3)	Not in audit plan

42 Haim Levanon St. Tel-Aviv 69977 Israel. Tel: 972-3-646-5114 Fax: 972-3-646-5205 www.sii.org.il

Organization Name	DoControl				**SII NO.**	286086
Address	Walter Moses St. 1 TA				**Tel**	
Date of audit	18/10/2022		Pick a date	Pick a date	**Mail**	
Standards	ISO 27001				**Location**	On site
Type of Audit	Surveillance	Stage 2	Select type	Select type	**Frequency**	Select frequency
Scope:	Development and maintenance of an advanced, agentless solution for protecting Cloud and SaaS applications					

Findings	**Classification**
Auditor name: David Kalmanowitz	

Classification:1- Major, 2-Minor, 3- Opportunity for improvement

Opportunity for improvement 3			
No.	**Function/Area/Process /Department**	**STD+#Clause/ Documented information of the organization/ applicable regulations/ etc..**	**Evidence**
1	Communication (In & out ISMS 7.4)	Introduce Classification Labels on both Internal and External documentation.	
2	Internal audits (ISMS 9.2)	SOC2 Audit was completed on Feb 2022 and the certification was received in March 2022. An Internal Audit separate and Independent of the SOC2 Audit will be reviewed by next ISO 27001 Audit.	
3	Incidents detection, evaluate, report, response, investigate, evidence collection: (Controls A16.1.1, A16.1.2, A16.1.3, A16.1.4, A16.1.5, A16.1.6, A16.1.7)	Review independent backup options for CRM, salesforce, Intercom, etc.	

42 Haim Levanon St. Tel-Aviv 69977 Israel. Tel: 972-3-646-5114 Fax: 972-3-646-5205 www.sii.org.il

Organization Name	DoControl				**SII NO.**	286086
Address	Walter Moses St. 1 TA				**Tel**	
Date of audit	18/10/2022		Pick a date	Pick a date	**Mail**	
Standards	ISO 27001				**Location**	On site
Type of Audit	Surveillance	Stage 2	Select type	Select type	**Frequency**	Select frequency
Scope:	Development and maintenance of an advanced, agentless solution for protecting Cloud and SaaS applications					

Corrective action required

Part 1 - Details of the Non-Conformity

NC no. according to the report	

Function/ Area/ Process /Department

Non-Conformity Evidence

STD+#Clause/ Documented information of the organization/ applicable regulations/ etc..

בחר פריט.	בחר פריט.	בחר פריט.
בחר פריט.	בחר פריט.	בחר פריט.

Statement of Nonconformity

Classification	בחר פריט.		
Auditor Name	**David Kalmanowitz**	**Date**	לחץ או הקש כאן להזנת תאריך.

Part 2 - Organizational actions to address non-conformity

Root cause analysis

Correction with completion date	לחץ או הקש כאן להזנת תאריך.

Corrective action with completion date לחץ או הקש כאן להזנת תאריך.

Close out Date + Responsible	לחץ או הקש כאן להזנת תאריך.

Evidence

Approval of CA performance by a representative of the organization		**Date**	לחץ או הקש כאן להזנת תאריך.

42 Haim Levanon St. Tel-Aviv 69977 Israel. Tel: 972-3-646-5114 Fax: 972-3-646-5205 www.sii.org.il

Organization Name	DoControl				**SII NO.**	286086
Address	Walter Moses St. 1 TA				**Tel**	
Date of audit	18/10/2022		Pick a date	Pick a date	**Mail**	
Standards	ISO 27001				**Location**	On site
Type of Audit	Surveillance	Stage 2	Select type	Select type	**Frequency**	Select frequency
Scope:	Development and maintenance of an advanced, agentless solution for protecting Cloud and SaaS applications					

Approval of a SII Lead Auditor for acceptance of Corrections / Corrective Actions		**Date**	לחץ או הקש כאן להזנת תאריך.

42 Haim Levanon St. Tel-Aviv 69977 Israel. Tel: 972-3-646-5114 Fax: 972-3-646-5205 www.sii.org.il