

Brand Compliance

AUDIT REPORT

CONFIDENTIAL DOCUMENT

GENERAL

Organizational data

Official company name:	Sympower B.V.
Possible trade names:	N/A
Entities under certification	Sympower B.V. Sympower Nederland B.V. Sympower Sweden AB Sympower OY Sympower Greece ΜΟΝΟΠΡΟΣΩΠΗ Ι.Κ.Ε. Sympower Poland sp. z o.o Sympower Spain S.L. Sympower Hungary Kft Sympower Czech Republic s.r.o. Sympower Italy S.R.L. Sympower Israel Ltd. Sympower Denmark ApS Sympower Norway AS
Address (main location):	Prins Hendrikkade 183, 1011 TD AMSTERDAM
Secondary locations:	Karaiskaki 28, 10554 Athens, Greece Lemminkäisenkatu 14-18 A, 20520 Turku, Finland Klarabergsviadukten 63, 111 64 Stockholm, Sweden Akadeemia 3, 51003 Tartu, Estonia

Certification data

Standard:	ISO 27001:2022
Scope:	Information security related to supporting the design, development, deployment and operation of Sympower's software platform and controllers.
Reference standard:	N/A
Possible Dutch translation scope:	N/A
Remote organization:	N/A
Statement of applicability:	Version 1.2 ; dated 27-01-2025
Certificate expiry date:	N/A

Audit data

Contact:	
Type/stage audit:	Initial audit stage 2
Visited location(s):	Prins Hendrikkade 183, 1011 TD AMSTERDAM
Audit date(s):	20/01/2025 – 27/01/2025
Lead Auditor:	Riccardo Dames
Team members:	Anne-Aimée Bun - Auditor Menno Schaatsbergen - Auditor

Subsequent audits

Date next audit in cycle:	26,27,28-01-2026
Date verification nonconformity(ies):	N/a

N.B. The report is automatically given final status if no changes are submitted within 14 days of sending.

CONCEPT

Appendixes to this report

Appendix 1: Checklist opening and closing meeting (included in this document)

Appendix 2: *Only if nonconformities are determined (with the exception of initial audit stage 1):* Registration Form Nonconformities (included as a separate document)

CONCEPT

INTRODUCTION

The audit was carried out in accordance with the audit principles of the ISO 19011:2018 standard. During the opening meeting, the process of the audit was explained to the management of the client, including the detailed planning, the certification criteria and the assessment method of the management system.

Any nonconformities found were discussed and reported during the closing meeting. With the management of the client, the Lead Auditor summarized the findings, classified nonconformities and discussed the procedure for resolving nonconformities. The Lead Auditor also indicated whether the client will be nominated for certification.

Major nonconformities (Category A); non-fulfilment of a requirement that affects the capability of the management system to achieve the intended results.
Nonconformities could be classified as major in the following circumstances:

- if there is a significant doubt that effective process control is in place, or that products or services will meet specified requirements;
- a number of minor nonconformities associated with the same requirement or issue could demonstrate a systemic failure and thus constitute a major nonconformity.

Minor nonconformities (Category B); non-fulfilment of a requirement that does not affect the capability of the management system to achieve the intended results.

The following terms are used to resolve nonconformities, whereby the corrective actions must be demonstrably implemented and effective:

- Major nonconformity = the completed form is to be submitted no later than 6 weeks after the closing meeting, verification on location after a maximum of 5 months in a follow-up audit.
- Minor nonconformity = the completed form is to be submitted no later than 6 weeks after the closing meeting, verification no later than the next regular audit.

Observation; opportunity for improvement which is recorded to indicate inefficiency and area for improvement. This follows indirectly from the certification requirements and must be considered.

CONCEPT

CONCLUSION/SUMMARY

Audit objective

During the audit, it has been tested whether the management system and the controls of the organization meet the requirements of the applicable ISMS standard and whether the system ensures compliance with applicable laws, regulations and contractual obligations. Furthermore, it has been tested whether the management system and the controls make an effective contribution to the realization of the organization's objectives and whether activities are being done in accordance with the agreements of the own management system. Where possible, potential improvements have also been identified.

Conclusion and recommendation regarding granting/continuing certification

The organization can be recommended for certification when the plans for the minor nonconformities have been approved by the lead auditor.

General impression of the management system

The organization has shown to have implemented an functional and effective management system, where policies and procedures are available to support in the (daily) responsibilities.

Sufficient documentation is available as evidence that necessary actions have been executed or are planned. Some documentation is a bit generic, and including more detail can strengthen the management system, however this is something that the organization has already identified and is actively working on.

Via an extensive internal audit, the organization has identified gaps in the management system and has initiated actions to improve. In a management review, management scores their management system and sets necessary actions for coming period.

Positive points

- The use of Vanta for managing the ISMS.
- The extensive internal audit that was performed.
- Strong security presence within business processes.

Observations (opportunities for improvement)

- The organisation could make the policies more concrete to improve their controllability.
- the software installation process on endpoints is not fully controlled.
  The policy states: Avoid installing any unlicenced or pirated software on company devices. The organisation does not verify if installed software on laptops is unlicenced or pirated. The organisation is aware of this and has an improvement plan in place.
- The measurement criteria within monitoring and measurement can be more specific.
- Only the fire-scenario is being tested. Also consider training the other scenarios.
- 2FA is not enabled on Juro. Although this is not required by the organization's policy, the SaaS application contains information that could benefit with 2FA protection.
- HR states they will check and remove personnel files of former employees twice a year. However, there is no automated trigger, such as from Vanta, to prompt this task.
- The organization has an overview of the legal and contractual requirements and their documented approach. However, for SvK (‘Cat. A Provider’), the table only mentions ‘Sympower is fully compliant with the highest IT security requirements of SVK’ without linking to the Notion page that includes the detailed approach.

Follow up of nonconformities from the previous audit (if applicable)

N/a

CONCEPT

Points of attention for the next audit

- Further implementation of SonarCube
- Implementation of Okta
- Adding the new Flexxtools entity within the auditscope
- The ISMS calendar for continual activity setting

Additional

- Has the scope of the certification been found to be suitable: yes
- What percentage of the audit was done using remote audit techniques? 33%
- Have the audit objectives been achieved (including where remote audit activities have been used)? yes
- Has the audit plan been followed during the audit: yes
- Are there significant points that have consequences for the audit programme: no
- Do the factors used for time reduction or time increase correspond to the customer situation: yes
- For the following audit, is additional expertise required to the audit team: no
- Are there any changes that require adjustment of the certification information: no.

Overview controls

Overview excluded controls	
Excluded control	Motivation
8.30 – outsourced development	"We are not using outsourced development"
7.11 – supporting utilities	As Sympower is cloud-only and primarily remote working company, we actively avoid on-premises hardware or confidential data on physical media, no 24/7 monitoring of our offices is in place. For our vendors (for e.g. cloud services) this is applicable, via our Third-Party Management Policy.
7.12 – cabling security	As Sympower is cloud-only and primarily remote working company, we actively avoid on-premises hardware or confidential data on physical media, no 24/7 monitoring of our offices is in place. For our vendors (for e.g. cloud services) this is applicable, via our Third-Party Management Policy.
7.13 – equipment maintenance	As Sympower is cloud-only and primarily remote working company, we actively avoid on-premises hardware or confidential data on physical media, no 24/7 monitoring of our offices is in place. For our vendors (for e.g. cloud services) this is applicable, via our Third-Party Management Policy.
7.4 – physical security monitoring	As Sympower is cloud-only and primarily remote working company, we actively avoid on-premises hardware or confidential data on physical media, no 24/7 monitoring of our offices is in place. For our vendors (for e.g. cloud services) this is applicable, via our Third-Party Management Policy.
7.6 – working in secure areas	As Sympower is cloud-only and primarily remote working company, we actively avoid on-premises hardware or confidential data on physical media, no 24/7 monitoring of our offices is in place. For our vendors (for e.g. cloud services) this is applicable, via our Third-Party Management Policy.
7.8 – equipment siting and protection	As Sympower is cloud-only and primarily remote working company, we actively avoid on-premises hardware or confidential data on physical media, no 24/7 monitoring of our offices is in place. For our vendors (for e.g. cloud services) this is applicable, via our Third-Party Management Policy.
Conclusion: The Lead Auditor agrees with the justification provided for its exclusion.	

CONCEPT

Overview of audit findings

Overview nonconformities				
Total number of nonconformities identified during this audit	Minor[1]	3	Major[2]	0

Notation:
1. NC-B-YEAR-No.
2. NC-A-YEAR-No.

Agreement of the client

By agreeing to this report, the client confirms that it agrees with the contents, that all points from the checklist opening and closing meeting (appendix 1) have been discussed and that the audit plan is part of the report*.
* Through the audit plan, the client has taken note of the audit objectives, audit criteria and use of the calculated audit time.

CONCEPT

FINDINGS PART 1 – MANAGEMENT SYSTEM

Clause 4: Context of the organization

4.1	Understanding the organization and its context
The organization has a documented scope document, in which a context analysis for both internal and external relevant points is included. The organization has determined that the increased fight against climate change will result in more power-grid instability and higher demand for grid balancing services. The organization's growth should result in more resources being available for the ISMS. Increase in security demands and expectations are expected as the amount of gigawatts controlled by the platform increases. The organization focusses on remote working and has employees all across Europe. A total of 5 physical offices are rented, with the location in Amsterdam as headquarters. Other locations are small rented office spaces which are mostly used as meeting space. Work is mostly done from home. No physical data is present/used. The other locations can therefore be marked as reduced risk.	
Verification (including version/date/name documents and registrations)	
01-ISMS Scope of the ISMS Interview with Jouke Waleson	
4.2	**Understanding the needs and expectations of interested parties**
The organization has determined which stakeholders are relevant and what their needs and expectations are. Sample 1: Transmission System Operator (TSO) Type: External Requirements: Relies on our ability to execute on agreed activations/deactivations through resources at our customers/ Needs us to not disrupt the grid with power fluctuations through the resources that we control, some TSO's have specific requirements like CatA for SvK. Addressed by ISMS: Yes The organization's risk analysis includes risks that relate to above mentioned power fluctuations and controls are implemented to make sure the power fluctuations are acceptable. The organization explains that for the Swedish TSO, a additional framework is required. Documented information within Notion is available as evidence that the organization has that the specific requirements are analyzed and relevant changes to implement these are present. Sample 2: Customers Type: External Requirements: Customers expect a reliable service that does not disrupt their energy systems beyond what was agreed, and security of their data. Addressed by ISMS: Yes The organization explains that a risk analysis on the software used is executed and secure data handling principles are implemented. Stakeholder 3: Regulators Type: External Requirements: Compliance with regulations and other applicable privacy laws Addressed in ISMS: Yes The organization has documented which laws and regulations are relevant to the organization and their service, including the NIS2. For the Swedish entity Specific Swedish regulations are included.	

CONCEPT

The organization has the relevant requirements/controls, coming from the relevant regulations and laws, documented within Vanta. Owners are assigned and documented compliance is evidenced.

Sample:

NIS2: 89% implemented
The To Do items are assigned to owners. This is also part of the information security goals. Where noncompliance is present, nonconformities hare been registered.

Minor nonconformity NC-B-2025-01

Specific requirement that is not fulfilled:
The organization shall determine: {…}
b) the relevant requirements of these interested parties; {…}
NOTE The requirements of interested parties can include legal and regulatory requirements and contractual obligations.

Related controls: A.5.34, A.8.10

Description nonconformity:
The organisation has a retention policy that does not meet the requirements by the Dutch Privacy Authority and GDPR.

This is verified in the retention policy, where it states that logging and sales data should be kept indefinitely. Logging data may contain personal data like IP addresses and sales data may contain contact person details. Based on art. 5 GDPR, the organisation should determine when this information is no longer needed to comply with the storage limitation principle.

Verification (including version/date/name documents and registrations)

01-ISMS Scope of the ISMS
SvK Cat A Requirements / Controls
Demo Vanta
Interview with Jouke Waleson
Data management policy > data retention matrix

4.3	Determining the scope of the information security management system

The organization has a clear and documented ISMS scope document available. Boundaries and exceptions are documented, as well as the scope for certification.

Some departments are excluded, such as the recently bought party Flexxtools. Flexxtools will be included in the auditscope in the near future.

Verification (including version/date/name documents and registrations)

01-ISMS Scope of the ISMS
Interview with Jouke Waleson

4.4	Information security management system

The organization has a ISMS build within Vanta. Vanta is the main platform for the storage and maintenance of ISMS documents. The nonconformity register is separately made in Excel.

All employees have read rights for the relevant policies.

Work instructions and other operational documents are available on Teams. Projectplanning consists within Notion.
Verification (including version/date/name documents and registrations)
Demo Vanta Non-conformity Inventory Notion -> ISO 27001 Milestones Interview with Jouke Waleson

Clause 5: Leadership

5.1	Leadership and commitment
Management is committed to Information Security. This is shown by I.E> a written Leadership statement within the ISMS policy, which includes that the organization is committed to establish, maintain and continually improve the ISMS and is demonstrating this by governance. The security policy and goals are in line with the strategic direction. Leadership is shown by approving the relevant ISMS policies and setting sufficient resources. At the implementation phase of the ISMS, the ISMS consultant was closely connected with the management team to make sure the security program is in line with the business. The organization has implemented a (ISMS) Governance-Council, in which the management team is included, together with i.e. the security officer and IT manager.	
Verification (including version/date/name documents and registrations)	
Interview with Jouke Waleson 02 – ISMS Information Security Management System (ISMS) Policy ISO Implementation proposal	
5.2	**Policy**
The organization has a documented information security policy available within Vanta. The policy is approved by the CTO. The policy includes written statement that security is important and that every employee must understand and follow the information security policy., Employees must accept that they have read and agree with the security policy in Vanta. If open items are present, the user will be forced to read the documents after loging in in Vanta. Documented results are present. Currently 230/232. History is present. Agreeing for 2 new employees is due in 6 days. When a policy is updated, the employees have to renew their agreement.	
Verification (including version/date/name documents and registrations)	
Information Security Policy (AUP) v2.2 Interview with Jouke Waleson	
5.3	**Organizational roles, responsibilities and authorities**
The organization has determined which roles are responsibilities are relevant to the ISMS. Documented information is available. The organization has assigned an dedicated ISMS Management leader, who has the authority to drive information security within the Organization and is responsible for the coordination of the ISMS activities. The ISMS governance council is also described in this overview. Responsibilities and authorities are defined for i.e. Risk owners, and other employees, third parties, vendors and consultants.	

CONCEPT

Verification (including version/date/name documents and registrations)
03 – Roles, Responsibilities and authorities Interview with Jouke Waleson

Clause 6: Planning

6.1	Actions to address risks and opportunities
6.1.1	*General*
6.1.2	*Information security risk assessment*
6.1.3	*Information security risk treatment*

The organization has an operational planning available that includes the initial ISMS actions. The organization is currently working on implementing an ISMS calendar, which includes the recurring events.

The organization has a formal risk management policy documented available.

The format is based on ISO27005, NIST 800-30 and NIST 800-37.
Risk scoring criteria for the likelihood and impact are defined, so the scoring of risks can be done objectively.
Acceptance criteria are defined.

Instructions on how the risk analysis should be performed is included in the process.

General risks are reviewed and relevant risks have been selected. In addition, own risks have been added.
Risk owners are assigned. Written owner-approval for treatment is documented in the risk register. Relevant CIA principles are mentioned per risk.

A risk treatment plan should be defined for risk responses other than accept or avoid.

Necessary controls are documented in the risk register, and relevant controls from Annex A are linked.
Inherent risk is separately recorded from the residual risk. Selection for risk treatment is based on the highest risk score.

Risk treatment options are valid for one year. Review and re-approval of treatment is forces yearly, including for accepted risk.

The organization has a documented statement of applicability documented available.
Justification for inclusion is documented, together with the implementation status. If controls are excluded, a reason for justification is given.

Verification (including version/date/name documents and registrations)
Notion -> ISO 27001 Milestones Notion -> ISO 27001 Milestones -> Compliance Calendar Interview with Jouke Waleson and Risk management Policy Vanta Risk Library Vanta Risk Register 11-ISMS Statement of Applicability

6.2	Information security objectives and planning to achieve them

The organization has defined 5 information security goals. The goals are defined together with senior management. Documented results are available.

CONCEPT

Sample 1: Implement, maintain and improve an Information Security Management Systems that Conforms to the requirements of ISO 27001. Effectiveness measure: Obtaining ISO 27001 certification. Owner: Information Security Management Leader Expected Completion Date: Q1 2025 The organization has a project planning within Notion. The planning consists of the necessary actions, which are assigned to an owner. Multiple phases have been defined. The full project is in progress. Sample 2: Improve security on employees computer (disk encryption, screen lock, strong passwords) on >95% of all devices Effectiveness measure: Check statistics in Vanta Owner: IT Manager Expected Completion Date: Q4 2024 The organization has documented statistics in Vanta: Screenlock: 94% (in the management review a statement is included on which the screenlock percentage quota was lowered). Hard drive encrypted: 99% Password manager installed: 98% Sample 3: Comply with NIS2 Effectiveness measure: Policy is in place and accepted by relevant personnel. 70% or more of leadership is certified. Risk analysis is complete and remediation plans for high risks Owner: Information Security Management Leader Expected Completion Date: 17 October 2024 The organization has documented results as evidence that employees have accepted the policy. Leadership training has been given via an external trainer. A risk analysis has been executed.
Verification (including version/date/name documents and registrations)
Interview with Jouke Waleson and Olivier van der Feltz Certificaat van deelname NIS2 boardtraining – Alexandre Jennaoui Statement of Applicability
6.3 Planning of changes
Changes within the ISMS are executed following a change process. A review process is documented and available in Vanta. ISMS documents have to be assigned to a member of the ISMS governance council, who is assigned with the task of approving and publishing the document. Document changes are kept in version history in Google Docs. The version history function is used to fill in the change history part of documents. For minor changes, new agreement from employees is not needed. For major changes in documents, the employees need to give additional agreement to this version. This is automated in Vanta.
Verification (including version/date/name documents and registrations)
Interview with Jouke Waleson and Olivier van der Feltz Demo Vanta policies 05-ISMS Procedure for the control of documented information

Clause 7: Support

7.1	**Resources**

CONCEPT

The organization has determined and assigned sufficient resources to implement and maintain the ISMS.
In the ISO implementation proposal it is mentioned that 3 teams for the implementation and maintenance of the ISMS need to be assigned. Financial costs as internal and external audit have been approved, as well as leadership training for cybersecurity, as this is a NIS2 requirements.

SaaS software (Vanta) has been purchased in order to maintain an governance overview.
The implementation proposal is approved by management via e-mail. The approval is shown during the audit.

External resources are also assigned. A implementation consultant has been hired to lead the ISMS implementation process.

Verification (including version/date/name documents and registrations)

ISO Implementation Proposal
Interview with Jouke Waleson and Olivier van der Feltz
Mail: ISMS proposals dated 16-07-2024 9:22

7.2	Competence

The organization has defined and documented competences for the persons who are working within the ISMS.

For leadership a NIS2 training was required. Documented certificates of completion of the training are available.

In the internal audit procedure are competencies for the internal auditor defined. The auditor should have specific knowledge of conducting an ISO27001 audit. Fulfilling this competence is evidenced by a screenshot of the training page, which shows the training is completed 100%. In addition, a documented record is written which shows the auditors have followed the training.

For the information security officer, competencies are defined in the role description. No documented results are available yet, as there is currently no Information Security Officer. The organization is currently looking for a internal candidate. The current Ad-Interim security Officer is screened for his previous work experience and is verified by previous contacts.

Minor nonconformity NC-B-2025-02

Specific requirement that is not fulfilled:
The organization shall:
a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;
d) retain appropriate documented information as evidence of competence.

Description nonconformity:
The organisation has no competences difined and no documented information as evidence of competence of the Technical Security Officer.

This is verified during the interview with Jouke Waleson

Verification (including version/date/name documents and registrations)

07-ISMS Procedure for internal audits
2024-10-17 Olivier Lead auditor training completed.png
2024-10-14- Training record – Internal Auditors for ISO 27001
ISMS Lead role description
Interview with Jouke Waleson

7.3	Awareness

The information security policy is communicated via Vanta. Employees will receive an forced message that they have to review and agree on the (changed) policy. This is automated in Vanta.

Documented registries are available as evidence that the required employees have reviewed and agreed the policy. Poster/memes have been spread around the office which state that locking your computer when leaving is needed.

When there are mention worthy updates, dedicated time will be spend in the monthly company update presentation. Slides have been shown from the session in January 2025 which shows that security has been discussed. The presentation is recorded and the recording + slides are shared via Slack.

Developers have received a extensive secure development training including on how to find and report incidents. Slides are shown during the audit. The organization notices an positive change in security posture within the development team. More incidents are reported and discussions are going on.

Verification (including version/date/name documents and registrations)

Interview with Jouke Waleson and Olivier van der Feltz
202501 Sym-Monthly January
Demo Vanta
2024-10-22 -Secure Development Training

7.4	Communication

The organization has determined what communication is relevant to the ISMS. A documented Information Security Communication Plan is available.

The types of communication, both internal and external, are described in a matric, together with who the receipients are and what timing is relevant. Communication mechanism and whether approval is required is also included.

Security meetings are held bi-weekly. Documented actions are registered per session and is achieved within the ISO27001 Milestones page on Notion.

11-11 is the final meeting where recorded actions are documented in the previous way. A agenda item has been shown that the most recent meeting was held on 13-01. The version history shows that the general action list has been updated.

A operational security Q&A is held together with an bi-weekly meeting to discuss vulnerabilities. Results are documented within the Slack Channel

Verification (including version/date/name documents and registrations)

Information Security Communication plan v1.0
Slack -> Engineering-cop-security
Interview with Jouke Waleson and Olivier van der Feltz

7.5	Documented information
7.5.1	*General*
7.5.2	*Creating and updating*
7.5.3	*Control of documented information*

Sufficient documentation is available as evidence that necessary actions have been executed or are planned. Some documentation is a bit generic, and including more detail can strengthen the management system, however this is something that the organization has already identified and is actively working on.

The organization has established a policy for the control of documented information. This is outlined in file 05-ISMS Procedure for the Control of Documented Information.

The policy contains details about approval workflows, periodic reviews, version control, protection and security and finally, distribution and access.

ISMS documents have to be assigned to a member of the ISMS governance council, who is assigned with the task of approving and publishing the document. Document changes are kept in version history in Google Docs.

CONCEPT

The version history function is used to fill in the change history part of documents. For minor changes, new agreement from employees is not needed. For major changes in documents, the employees need to give additional agreement to this version. This is automated in Vanta. A naming convention for documents and a document format structure has been defined in the policy. Data retention is included in the data management policy. Other data that is obsolete has to be deleted in a secure manner.
Verification (including version/date/name documents and registrations)
Interview with Jouke Waleson and Olivier van der Feltz Demo Vanta policies 05-ISMS Procedure for the control of documented information Data management policy 1.1

Clause 8: Operation

8.1	Operational planning and control

The operational planning for the implementation and first phase after the certification of the ISMS has been documented within the ISMS 27001

Actions are assigned to an owner and deadline. The status is documented within the ISO27001 milestone project page. For the continual maintenance phase of the ISMA, is a separate planning currently in progress, which includes the recurring ISMS actions.

Sample: Setup owner access in Vanta
Owner is assigned
Status: Done

The organization has shown the assigned roles within the Vanta user permissions settings. Dedicated segregation between admins and editors are made. The action is sufficiently handled

Sample: Setup internal audit program
No owner is assigned, however documentation shows that the action has been done.
Status Done

The organization has shown a documented and approved internal audit program. The action is sufficiently handled.

Minor nonconformity NC-B-2025-03

Specific requirement that is not fulfilled:
"The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6 {…}"

Description nonconformity:
Not all necessary controls have been implemented.

This is evidenced in:

- A.8.12 (DLP): The organisation indicates that classification and awareness are sufficient (compensating controls), and no further measures are required, no specific DLP-control is implemented. However the control is stated as implemented in the Statement of Applicability.

CONCEPT

- A.5.13: The policy states that confidential and public information should be labelled. Samples of listed types of confidential information were taken (e.g. source code) which was not labelled. The interviewees stated not to be aware of any labelled information.

A 6.2: There is no connection between the contractual agreement of employees and the organization's policies (specifically information security). The freelancer contractual agreement, however, includes an Article 13 which states that they must comply to the policies and rules of the organization.

Verification (including version/date/name documents and registrations)

ISO 27001 Milestones
Vanta -> User permissions
ISMS internal audit program 24-26
Interview with Jouke Waleson and Olivier van der Feltz

8.2	Information security risk assessment

The organization performed an risk assessment, following the established procedure and method. Documented results are available.

Verification (including version/date/name documents and registrations)

Vanta -> Risk Register
Interview with Jouke Waleson and Olivier van der Feltz

8.3	Information security risk treatment

Risk are treated in line with the treatment plans.

Sample 1: Risk 31: Risks from mobile device use are not identified or treated
Owner: Justin Charles
Inherent likelihood: 3
Inherent impact: 3
Score: 9
Treatment plan: Mitigate
Acceptance of the treatment plan is included

A treatment plan is available.
Selected controls are: user endpoint devices (A 8.1)

The control has been partly implemented. 6/8 checks have been completed. Open actions consist of forcing automated screenlock. The organization is currently working on the completion. Malware detection and disk encryption is enabled on all systems.

Sample 2: Risk 74: Admin user makes a mistake and deletes e.g. aurora database, pulsar, S3, Timeseries data, leading to outage of platform and inability to get it back up and perform activation
Owner: Siimo Sulev
Inherent likelihood: 3
Inherent impact: 4
Score: 12
Treatment plan: Mitigate

Acceptance of the treatment plan is included
A treatment plan is available.
Selected controls are: Operation planning and control, Incident response training (NIS2), Information security awareness and training, response to information security incidents, access control

The control has been partly implemented. 13/15 checks have been completed. Open actions consist of deprovisioning Miro and Notion accounts when an employee leaves.

CONCEPT

Accounts are managed by SSO, which are deactivated after leave. The existing accounts in Miro and Notion are therefore useless, but cleaning these accounts is preferred. Ongoing action. Sample 3: Risk: 53 Background verification checks are not carried out on all candidates or are not proportional to the business requirements or the classification of the information to be accessed by the role resulting in increased risk of malicious insider threats. Owner: Charmen Inherent likelihood: 2 Inherent impact: 4 Score: 8 Treatment plan: Accept For 3 high risk profiles/functions screening is implemented. Control "Screening" is linked. For the other employees within the organization, screening is not done. This is accepted as risk. Acceptance of the risk owner is included.
Verification (including version/date/name documents and registrations)
Vanta -> Risk Register Risk 53 Risk 74 Risk 31 Interview with Jouke Waleson and Olivier van der Feltz

Clause 9: Performance evaluation

9.1	Monitoring, measurement, analysis and evaluation

The organization has determined what has to be monitored and measured, and has documented results available.

Sample 1: Technical Vulnerability Management
Detail of measurement: Vulnerabilities detected and remediated
Who Gathers metric: Engineering teams
Who receives metric & frequency: Engineering Security CoP – ISMS Governance Council Quarterly
Criteria: Critical and high vulnerabilities are remediated within SLA timelines.

The organization has documented results of vulnerability scans within Vanta.
1 unscanned asset.
0 vulnerability SLA's overdue.

Vulnerability status is set by SLA.
1 critical due in 12 days

Sample 2: User responds to phishing attempts
Detail of measurement: User responses to phishing tests
Who Gathers metric: IT
Who receives metric & frequency: IT Manager – ISMS Governance Council Quarterly
Criteria: Number of users who pass phishing tests, Users who fail tests receive awareness training

The organization is currently using the baseline phishing tests together with the industry benchmark to determine a stronger quota on what percentage is acceptable, for now all clickers have to follow training.

In Knowbe4 it is verified that user B.N, who is in the list of top clickers, has received and followed additional training.

CONCEPT

The organization utilizes KnowBe4 for phishing tests.
Every quarter an phishing campaign is executed.

Recent results: Phish prone 14.4%
Top 50 clickers are identified, additional training will be provided. This is included in the management review.

Sample 3: System patching
Detail of measurement: Number of systems patched / unpatched | Time to patch (TTP)
Who Gathers metric: IT | Engineering department
Who receives metric & frequency: ISMS Lead Quarterly – ISMS Governance Council Quarterly
Criteria: Critical and high vulnerabilities are remediated within SLA timelines.

During the audit is it verified that patching on servers is done automatically and 0 SLA's are overdue.

Verification (including version/date/name documents and registrations)

Interview with Jouke Waleson, Alar Aun and Olivier van der Feltz
10-ISMS Information Security Objectives Plan
Vanta -> Vulnerabilities

9.2	**Internal audit**
9.2.1	***General***
9.2.2	***Internal audit programme***

The organization has a documented audit program available. The Internal audit cycle is running from 2024-2026. For the first cycle after the implementation every year, the whole ISMS (including controls) are subject to the audit.

An internal team is assigned and consists of employees from Organizational support, Finance, Technology and Legal departments. Employees who were involved in the implementation are not included for the sake of objectivity.

The audit method used is described.
Documented results are available. Both Major and Minor nonconformities have been identified. Observations as well have been identified by the internal audit team.

Sample 1: Major NC on 8.15 + 8.16
Missing audit logs on credential creation: we could not see who created and uploaded the non-AWS issued certificated

The organization has registered the NC within the nonconformity registry and is currently following up on the finding.

Sample 2: Minor NC on 8.24 Use of Cryptography
One certificate expires in 2032 but policy states 1 year. Used for internal systems, it will be faded out when external pulsar will be used.

The organization has registered the NC within the nonconformity registry and is and has followed up on the finding. AWS certificate manager is being used now to manage certificates.

Sample 3: Conformity on 6.2

CONCEPT

The internal auditor has checked whether risk treatment plans are defined and communicated with relevant stakeholders. And whether the defined objectives are complying to the requirements set by the standard. This was the case, therefor a conformity statement has been given. During this audit the same conclusion was found.

The organization has bought a standard internal audit checklist to assist with asking the right questions. Considering the extensive findings, it can be concluded that the internal audit has been executed objectively and sufficiently.

Verification (including version/date/name documents and registrations)

Interview with Jouke Waleson, Alar Aun and Olivier van der Feltz
ISMS Internal Audit Program '24-'26
Nov2024 – Internal Audit ISO 27001 – Sympower
Cryptography policy

9.3	**Management review**
9.3.1	**General**
9.3.2	**Management review inputs**
9.3.3	**Management review results**

A documented procedure on how to conduct the management review is present. A management review has been executed and documented results are available.

The ISMS Governance Council was satisfied with the progress booked so far and is looking forward to continue the improvement of the ISMS. A permanent ISMS Lead will be recruited to ensure the ISMS will receive dedicated attention and continuous improvement.

The input for the management review is included in a separate presentation for management to be used on giving their opinions. All topics as required by the standard are included.

Sample 1: Status of objectives
This is reviewed by the management. The management learned about the NIS2 delay quite late, and would have wanted an earlier notification. A action has been made to provide bi-weekly updates on the status objectives.

Sample 2: Risk assessment
This is reviewed by management. Management has approved the risk assessment. The decisions to mitigate, avoid, remediate or transfer are approved. For a few risks a change is requested, as a cyber security insurance is advised by the ISMS Lead for the risk transfer treatment options.
Also a risk for mobile device access had to be added to the risk register.

Sample 3: Internal audit results
This is reviewed by management. Feedback has been given to check again on the status of the minor nonconformities to make sure the right prioritization is addressed.

Actions are registered in a report document and are registered within the ISO27001 Milestones Notion board, where an owner is assigned.

The management has given documented feedback in a scorecard, which related to the review inputs from the presentation, including if all areas were understandable and clear.

Verification (including version/date/name documents and registrations)

Procedure for Management review
ISMS Management Review Report – November 2024
ISMS Management Review Inputs – November 2024
ISMS Management review Inputs – scorecard
Notion -> ISO27001 Milestones
Interview with Jouke Waleson

CONCEPT

Clause 10: Improvement

10.1	Continual improvement
The organization is continual improving the management system. The management has decided to start looking for a dedicated ISMS Lead. Improvement is shown by handling the observations for improvement as identified in the internal audit. Making sure policies are easy understandable and readable is one of the action items identified. Actions are documented in the ISO 27001 Milestones page. Adjusting policy formats is completed. Adjust policy languages is currently on the backlog.	
Verification (including version/date/name documents and registrations)	
Notion -> ISO 27001 Milestones Interview with Jouke Waleson	
10.2	**Nonconformity and corrective action**
The organization has a dedicated register for nonconformities available. Nonconformities are handled according to the requirements. Nonconformities are documented and the findings are detailed described. A root cause is determined, together with immediate actions. A analysis is done to determine if a corrective action is necessary to tackle the root cause. Is yes, than a additional action is defined. Verification methods are included and a target date is set. Sample: Minor NC on 5.13 Labeling of information Finding: There is no mention on how to label public info RCA: “In many places we do have "confidential" e.g. on Sym Monthly presentations, but we don't really use public anywhere. We took the default Vanta policy that suggests to use labeling like this and it made sense. The topic is not as relevant to Sympower yet as we are still a relatively small company and there have not been many issues with sharing restricted or confidential places publicly. Immediate actions: none” Evaluation needed: Yes Corrective actions: A risk analysis should be done to figure out the actual risks and either adapt the policy or make sure that it is implemented properly across the organization. Verification method: See if the policy is in line with the actual practice Target date: September 2025	
Verification (including version/date/name documents and registrations)	
Non-conformity Inventory Interview with Jouke Waleson	

CONCEPT

FINDINGS PART 2 – CONTROLS

Application security

Section	Description
A.5.37	Documented operating procedures
A.8.4	Access to source code
A.8.18	Use of privileged utility programs
A.8.19	Installation of software on operational systems
A.8.25	Secure development lifecycle
A.8.26	Application security requirements
A.8.27	Secure system architecture and engineering principles
A.8.28	Secure coding
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

Explanation:

Based on the interviews and the evidence shown, it can be concluded that the organization has planned, implemented and controls appropriate processes:

- To ensure the correct and secure operation of information processing facilities.
- To prevent the introduction of unauthorized functionality, avoid unintentional or malicious changes and to maintain the confidentiality of valuable intellectual property.
- To ensure the use of utility programs does not harm system and application controls for information security
- To ensure the integrity of operational systems and prevent exploitation of technical vulnerabilities
- To ensure information security is designed and implemented within the secure development life cycle of software and systems.
- To ensure all information security requirements are identified and addressed when developing or acquiring applications.
- To ensure information systems are securely designed, implemented and operated within the development life cycle
- To ensure software is written securely thereby reducing the number of potential information security vulnerabilities in the software.
- To validate if information security requirements are met when applications or code are deployed to the production environment
- To protect the production environment and data from compromise by development and test activities
- To preserve information security when executing changes.

Verification:

Tech 1622
Commit #898 #1460, #692, #352
Dependabot demonstration
GitHub demonstration
Atlassian demonstration
SonarQube demonstration
GitHub: Sympower-actions
Miro demonstration (platform architecture)
GitHub: Security checklist
Secure development policy v1.1
Operations security policy v1.2

CONCEPT

Interview with Alar Aun, Tonis Ojandu

Asset management

Section	Description
A.5.9	Inventory of information and other associated assets
A.5.10	Acceptable use of information and other associated assets
A.5.11	Return of assets
A.5.14	Information transfer
A.5.33	Protection of records
A.5.37	Documented operating procedures
A.6.5	Responsibilities after termination or change of employment
A.6.7	Remote working
A.7.3	Securing offices, rooms and facilities
A.7.8	Equipment siting and protection
A.7.9	Security of assets off premises
A.7.10	Storage media
A.7.13	Equipment maintenance
A.7.14	Secure disposal or reuse of equipment
A.8.1	User endpoint devices
A.8.14	Redundancy of information processing facilities

Explanation:

Based on the interviews and the evidence shown, it can be concluded that the organization has planned, implemented and controls appropriate processes:

- To identify the organization's information and other associated assets in order to preserve their information security and assign appropriate ownership
- To ensure information and other associated assets are appropriately protected, used and handled.
- To protect the organization's assets as part of the process of changing or terminating employment, contract or agreement
- To ensure the correct and secure operation of information processing facilities.
- To protect the organization's interests as part of the process of changing or terminating employment or contracts
- To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets in offices, rooms and facilities.
- To prevent loss, damage, theft or compromise of off-site devices and interruption to the organization's operations.
- To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations caused by lack of maintenance
- To prevent leakage of information from equipment to be disposed or re-used
- To protect information against the risks introduced by using user endpoint devices

Verification:

Asset management policy 1.1
Notion demonstration
Vanta discovery demonstration (scanned SaaS inventory)
Information security policy 2.2
GitHub and AWS are scanned for vulnerabilities with Vanta
Operations security policy 1.2
Second hand laptops tracking.xlsx
Building laptops for new starters. 31 06 2023

CONCEPT

Continuity

Section	Description
A.5.29	Information security during disruption
A.5.30	ICT readiness for business continuity
A.5.37	Documented operating procedures
A.8.6	Capacity management
A.8.13	Information backup
A.8.14	Redundancy of information processing facilities

Explanation:

- The organization has a documented Business Continuity and Disaster Recovery plan available.
- Disaster recovery tests, including backup and restore testing, must be performed at least on an annual basis.
- Communications, escalation paths, roles and responsibilities are defined and documented within the plan.
- Critical business processes are defined and the continuity strategy is documented. The Sympower platform relies on AWS multi-AZ availability.
- Continuity procedures are defined by certain scenarios.
- RTO and RPO are determined and documented per critical asset.
- A recovery procedure is determined. Communication with relevant authorities is included.
- After an disruption is resolved a post-recovery review has to be performed.
- A disaster recovery test has been performed in November 2024. Documented results are available. The recovery test was successful. A detailed technical timeline of the incident and a Root Cause Analysis is documented.
- A documented backup and restore backup and recovery overview is available, which includes all backup strategies and storage locations.
- The Backup plan within AWS has been shown, which shows that continuous backups are created and validated. Documented restore procedures are available.
- Audit logs are stored in Opensearch. Retention times have been defined and set.
- GitHub code repositories are backup via Ansible. The se backups are stored in S3 buckets. The implementation has been shown. Access rights are minimalized to one dedicated account.
- Redundancy is implemented via multi-region setup in AWS. During the audit it is shown that Infrastructure as Code secrets are redundant in Frankfurt as Main location and Ireland and backup site.
- Capacity monitoring is monitored by automated rules and thresholds by Opensearch. In addition, automated scaling is enabled. Auto scaling groups are setup in AWS. Scaling is included in the infrastructure as code.
- Google workspace recovery is continuous tested by regular file recovery requests.
- Availability requirements are documented in SLA's.

Verification:

Business Continuity and Disaster Recovery BC/DR v1.0
Interview with Alar Aun, Stamitas Maritsas and Siimo Sulev
Incident-202411-pulsar-staging
Backup & Recovery Datastore map / playbook
AWS Backup plan
Aurora RDS Conduct backup recovery test
Backup & Recovery w/AWS Backup Service
AWS -> Auto scaling groups
Production-infra-emqx

CONFIDENTIAL

Governance

Section	Description
A.5.1	Policies for information security
A.5.2	Information security roles and responsibilities
A.5.3	Segregation of duties
A.5.4	Management responsibilities
A.5.5	Contact with authorities
A.5.6	Contact with special interest groups
A.5.8	Information security in project management
A.5.24	Information security incident management planning and preparation

Explanation:

- The organization has a documented information security policies in place.
- The ISMS policy is scoped for the specific ISMS implementation and maintenance and has the governance council as main target group. The policy is linked to the ISMS operators and governance group in Vanta, which makes sure that the right employees are forced to read and agree with the policy. The given agreement is valid for 1 year. Vanta is configured in such way that the employees have to give the agreement each year. Results are available.
- The Information security (IS) policy is scoped for the all employees. The policy is linked to the default group in Vanta, which makes sure that the right employees are forced to read and agree with the policy. The given agreement is valid for 1 year. Vanta is configured in such way that the employees have to give the agreement each year. Results are available.
- Roles and responsibilities are defined and documented in a separate document. Roles, responsibilities and authorities are definer per user group. For employees this is included in the Unwanted and Wanted Behaviour policy. All employees have to agree with the policy annually.
- Segregation of duties is implemented on different levels. For example, the security team is responsible for the implementation of policies, but is not mandated to approve policies. This is subject to the security governance council. The CTO has limited access rights to systems. Financial transaction can not be approved by the same employee who creates the task. The organization has an documented overview of who is mandated to sign different types of documents/agreements. In addition, the organization has a whistleblower policy. If an employee suspects conflicting behaviour, they can report this safely. Following up on reports will be done externally.
- The information security policy includes written statement that security is important and that every employee must understand and follow the information security policy.
- The organization is keeping contact with relevant special interest groups and authorities. Currently government contact is only incident-driven, I.E. the Dutch DPA (Autoriteit Persoonsgegevens). The organisation has contact with interest groups with in the energy sector. The organization has shown that they were attending sector related energy conferences.
  From a GDPR/NIS2 point of view, mandatory reporting of incidents is required. The organization has a documented escalation/reporting matrix available.
- Information security within project management is included at the starting of projects. Security impact and risks are determined in the earliest stages. During the audit documentation related to the StreamNative BYOC project is shown. A documented risk assessment is available.
- The organization has a documented incident response plan and strategy in order to prepare for incidents.

Verification:
Interview with Jouke Waleson
02- ISMS Information Security Management Systems (ISMS) Policy
Information Security Policy (AUP)
Vanta -> Policies
03-ISMS Roles, Responsibilities and Authorities
Unwanted and Wanted Behaviour policy

CONCEPT

Our whistleblower policy Incident Response Plan Pulsar management with StreamNative Pulsar StreamNative BYOC risk assessment

Human resource security

Section	Description
A.6.1	Screening
A.6.2	Terms and conditions of employment
A.6.3	Information security awareness, education and training
A.6.4	Disciplinary process
A.6.5	Responsibilities after termination or change of employment
A.6.6	Confidentiality or nondisclosure agreements

Explanation:

Regarding HR and the off/onboarding process, the following has been concluded during interview:

- Different risks, such as retention period, new HR application, things that were not documented; risks on how medical information is handled);
- 2 times per year the Google Drive is checked if personnel files should be wiped;
- Different risks, such as retention periods, undocumented processes, as well as risks related to the handling of medical information, have been identified;
- Different probation periods, such as those in Estonia, present challenges.
- The process for creating job guides is documented;
- A form in Google is used to document the intake process, covering topics such as competencies and criminal background;
- Recruitee is used to register candidates and track all intake steps, as well as to manage consent for retaining candidate information (with respect to GDPR retention guidelines);
- Recruitee is integrated with Hibob to start the onboarding process (via the 'send to Hibob' button).
- Candidates with a job that require access to production environments, as well as management, must provide a Certificate of Conduct (VOG), and this was demonstrated with a recently started employee;
- The onboarding process is documented, and HR uses a checklist;
- Candidates receive an online invitation to register in Hibob and upload sensitive information, such as ID documents;
- Onboarding tasks in Hibob vary by country to comply to local law and were demonstrated ;
- Excel lists are still used to ensure steps are completed, although Hibob already automate many of these tasks;
- A contractual agreement was demonstrated, including provisions for Intellectual Property (Article 110), Non-Disclosure (Article 12), Return of Property (Article 14), and Breach and Penalty (Article 15);
- A training list is maintained to track awareness training completion;
- The offboarding process was demonstrated, showing that all tasks were completed and personnel files were deleted;
- Different folders in Google Drive are used to comply with retention policies per country (2 years, 5 years, and 7 years);
- Twice a year, Google Drive is checked to determine if personnel files should be wiped;
- A disciplinary process is outlined in the Unwanted and Wanted Behaviour Policy;
- Team leads are responsible for tracking training completion;
- New employees receive presentation slides that link to Notion and KnowBe4 training;

There is no connection between the contractual agreement of employees and the organization's policies (specifically information security). The freelancer contractual agreement, however, includes an Article 13 which

CONFI

states that they must comply to the policies and rules of the organization. This is included in NC-B-2025-03 under clause 8.1.

During the interview with a recently onboarded employee, the following points were verified:

- Completion of the onboarding process.
- Assessment of competencies.
- Registration in Hibob and account setup.
- Access to Notion, including various policies.
- Completion of e-learnings and KnowBe4 training.
- Registration in Vanta.
- Awareness of the information security policy.

Based on this, it can be concluded that the onboarding of personnel is conducted according to the organization's rules, ensuring employees are properly informed.

Verification:
Interview with Carmen Kloosterman and Take Abspoel
Notion > New Job Guide for Hiring Managers
TEMPLATE Job Intake
Recruitee > IT Desktop Support Specialist
Notion > Onboarding: Welcome to Sympower!
Hibob > Onboarding – New Employee the Netherlands
Hibob > Onboarding – New Employee Greece
VOG – profile of KE
Employment Agreement Sympower B.V. / Netherland B.V.
Freelancer Service Agreement Sympower B.V.
Hibob > EC (onboarding tasks)
New Hire Sheet
Vanta > Unwanted and Wanted behaviour Policy
Hibob > Remove Personnel Files from
Hibob > AM (offboarding tasks)
Hibob > People's docs (AM)
Vanta > Human Resource Security Policy
Certificaat van deelname – NIS2 boardroom training
2024-10-22 – Training Record – Technology Department – Secure Software Development
9. Working at Sympower
Notion > Inventory > ThinkPad T14s Gen 4

Identity and access management

Section	Description
A.5.3	Segregation of duties
A.5.15	Access control
A.5.16	Identity management
A.5.17	Authentication information
A.5.18	Access rights
A.5.37	Documented operating procedures
A.7.2	Physical entry
A.8.2	Privileged access rights
A.8.3	Information access restriction
A.8.4	Access to source code
A.8.5	Secure authentication
Explanation:	

CONCEPT

Based on the interviews and the evidence shown, it can be concluded that the organization has planned, implemented and controls appropriate processes:

- To reduce the risk of fraud, error and bypassing of information security controls.
- To ensure authorized access and to prevent unauthorized access to information and other associated assets.
- To allow for the unique identification of individuals and systems accessing the organization's information and other associated assets and to enable appropriate assignment of access rights
- To ensure proper entity authentication and prevent failures of authentication processes
- To ensure access to information and other associated assets is defined and authorized according to the business requirements.
- To ensure only authorized users, software components and services are provided with privileged access rights.
- To ensure only authorized access and to prevent unauthorized access to information and other associated assets.
- To prevent the introduction of unauthorized functionality, avoid unintentional or malicious changes and to maintain the confidentiality of valuable intellectual property.
- To ensure a user or an entity is securely authenticated, when access to systems, applications and services is granted.

Verification:
Access control policy v1.1
Asana : Sympower Okta Implementation -> project plan of implementing Okta.
Vanta engineering high risk systems quarterly review (2 dec 2024)
Google workspace demonstration
Access request via email is shown
Sympower IT inbox (email)
Jira Glitch 2522
Sympower offboarding form (responses).xlsx
Sympower onboarding form.xlsx
Google form onboarding.
Notion user groups
Interview with Jouke Waleson, Justin Charles, Alar Aun

Information protection

Section	Description
A.5.10	Acceptable use of information and other associated assets
A.5.12	Classification of information
A.5.13	Labelling of information
A.5.14	Information transfer
A.5.33	Protection of records
A.5.34	Privacy and protection of PII
A.6.6	Confidentiality or nondisclosure agreements
A.6.7	Remote working
A.8.1	User endpoint devices
A.8.7	Protection against malware
A.8.10	Information deletion
A.8.11	Data masking
A.8.12	Data leakage prevention
A.8.33	Test information
A.8.34	Protection of information systems during audit testing
Explanation:	

CONCEPT

Based on the interviews and the evidence shown, it can be concluded that the organization has planned, implemented and controls appropriate processes:

- To ensure information and other associated assets are appropriately protected, used and handled.
- To ensure identification and understanding of protection needs of information in accordance with its importance to the organization.
- To facilitate the communication of classification of information and support automation of information processing and management
- To ensure compliance with legal, statutory, regulatory and contractual requirements, as well as community or societal expectations related to the protection and availability of records.
- To ensure the security of information when personnel are working remotely
- To protect information against the risks introduced by using user endpoint devices
- To ensure information and other associated assets are protected against malware
- To prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory and contractual requirements for information deletion.
- To limit the exposure of sensitive data including PII, and to comply with legal, statutory, regulatory and contractual requirements.
- To detect and prevent the unauthorized disclosure and extraction of information by individuals or systems

The organisation has a retention policy that does not meet the requirements by the Dutch Privacy Authority, GDPR. See minor nonconformity within clause 4.2.

Verification:
Notion Data locations
Vanta vendors list
Vanta monitoring
Vanta discovery
Data management policy v1.1
Vanta customer data deleting records
Data retention matrix (data management policy)
Vanta task: evidence of pseudonymisation procedure implemented; DCH 111 dec 11 2024
Operations security policy
Information security policy v2.2

Information security assurance

Section	Description
A.5.22	Monitoring, review and change management of supplier services
A.5.35	Independent review of information security
A.5.36	Compliance with policies, rules and standards for information security
A.8.29	Security testing in development and acceptance

Explanation:

- Independent reviews are conducted by external annual pentest and Cat-A audits (Sweden) that are being conducted. The organisation also has regular B-Corp audits. The external ISMS audits are also seen a way to receive independent feedback.
- The ISMS Lead is responsible for the compliance with policies and rules. The ISMS Lead
- Vanta gives insights in the formal agreements to the policy documents, as given by the employees. The ISMS Lead has positive signals that the organisation is getting further on a security level, by reporting more incidents and security related discussions are actively going on in Slack.
- The security governance council is tasked with the monitoring of the ISMS. A quarterly presentation is given to the governance council by the ISMS Lead.
- Security testing is included in the standard way of working. Code reviews are mandatory. Dependabot is used to do vulnerability scanning on code.

CONCEPT

Verification: B-Corp Certification ISMS Management Review Inputs – November 2024 Interview with Jouke Waleson

Information security event management

Section	Description
A.5.24	Information security incident management planning and preparation
A.5.25	Assessment and decision on information security events
A.5.26	Response to information security incidents
A.5.27	Learning from information security incidents
A.5.28	Collection of evidence
A.5.37	Documented operating procedures
A.6.8	Information security event reporting
A.8.15	Logging
A.8.16	Monitoring activities
A.8.17	Clock synchronization

Explanation:

- The organization has a documented incident response plan available.
- The incident response plan contains a description of an security event and incident.
- Employees and contractors must report incidents via either mail of service management form.
- The severity will be analysed and/or decided on by the relevant team. (Security, Engineering Operations and/or Glitchbusters). Severity levels and their criteria are defined.
- Escalation and internal reporting, as well as internal communication, is included in the IR plan.
- All reported events, incidents and response activities must be documented in Jira tickets.
- During the audit it is shown that when a incident gets raised, an automated Jira ticket is created and a Slack message is send. The ticket will be assigned to a handler directly.
- Internal communication is being done via Slack. Slack channel Incidents is shown during the audit. If necessary, a incident-specific channel will be created.
- Per severity, steps that need to be taken are documented, as well as the assignments of responsibilities.
- An incident commander is assigned to manage the incident response action.
- The incident plan must be tested at least once per year. Testing was done. Incident report 2281 has been shown as evidence.
- External reporting to authorities, for example Dutch DPA (Autoriteit Persoonsgegevens) is documented with the corresponding timelines .
- Responsibilities of different usergroups are documented
- A Root Cause Analysis is created for Severity 1 and 2 incidents. Documented evidence is shown.
- Incident report related to Jira ticket-2281 is shown. The incident is analysed and a written timeline of activities is included.
- Example shown: Incident: Greece resource selection continuously activating and deactivating resources. The incident has been given the S1 severity. Documentation is present in Slack, which shows the correct steps have been taken. Lessons learned are documented.
- Lessons learned are defined and registered in the ticket details. The incident response policy was deemed to difficult to understand. The organization has raise an action to implement an supporting document for the incident response plan.
- Security incidents are segregated from operational incidents. The Technical Security Officer is responsible for the coordination of the incidents.
- Opensearch is used to retrieve logfiles. Authorities are restricted. Logfiles are read only so no data can be changed. A VPN connection is required to access the dashboard.
- Automated monitoring rules are set within Prometheus, for example certificate expiration and if an Instance is down. The rules are shown during the audit.

COPY

- Example shown: “Alert Logged_errors_are_high fi production…” The alert has raised a message in Slack. Relevant logfiles are present. Analysis is done and the incident has been resolved.
- Login-logs for the VPN are shown. The logs are stored within Opensearch. When a connection fails, a entry is registered. Automated Alertmanager will raise a alert is such event takes place. The Engineering Operations team will analyse these events and raise an incident if needed.
- Clock synchronization is implemented by using the AWS time service. The configuration on vertialanv-ansible has been shown as evidence the AWS provided time server is configured.

Verification:
Interview with Alar Aun and João Dias
Incident Response Plan 2.0
Slack -> Incidents
Sympower Atlassian -> Glitchbusters
Engineering Operations Incidents
Incident report -> Jira ticket-2281
Incident: Greece resource selection continuously activating and deactivating resources
Opensearch dashboard
Prometheus alerts
Slack -> Alerts-fi p> “Alert Logged_errors_are_high fi production…”
Opensearch dashboard
on vertialanv-ansible -> Configuration

Legal and compliance

Section	Description
A.5.31	Legal, statutory, regulatory and contractual requirements
A.5.32	Intellectual property rights
A.5.33	Protection of records
A.5.34	Privacy and protection of PII
A.5.36	Compliance with policies, rules and standards for information security
A.8.10	Information deletion

Explanation:
With regards to legal and compliance, the following has been concluded during interview:

- The organization has documented the legal, statutory, regulatory and contractual requirements with regard to information security;
- External lawyers are hired for advice on local legislation;
- The main legal requirements include NIS2, GDPR, Whistleblower Protection Act, and Trade Secret Directive;
- Regarding GDPR, the organization processes only candidate and employee data, and for customers, only contact information;
- Deletion of information was confirmed during an interview with HR, where it was noted that personnel files are reviewed twice a year for potential deletion;
- A privacy policy for employees is documented, and a privacy policy for website users is available on the website;
- An incident response plan is in place which covers data breach reporting;
- All data breaches occurring in another European countries must be reported locally and to the Dutch authorities;
- Vanta is used to register and comply with the NIS2 directive controls;
- An incident response plan is in place with regards to data breach reporting;
- A Whistleblower policy is documented, and it has been demonstrated how employees can anonymously report a case;
- Investigations are completed within three months of receiving a report;
- Access to the Whistleblower environment is restricted to legal and HR personnel;

CONCEPT

- For compliance with the Trade Secret Directive, the SaaS-application Juro is used to manage NDAs;
- A demonstration was given on how NDAs are generated, and a reminder is sent via email one month before the NDA's expiration;
- Both an NDA and the contractual agreement of a client were demonstrated. The contractual agreement includes confidentiality and intellectual property rights;
- The customer, SvK (cat A. provider), has specific information security requirements, which are documented in Notion.
- It has also been concluded that Juro is used for the protection of contracts (password protection). Access to contracts in Google Drive is restricted to ensure confidentiality and protected with 2FA.

Verification:
Interview with Sonia Moine
12-Relevant Laws, Regulations, and Contractual Requirements
Notion > Our Privacy Policy
Notion > Retention Period for Business Documents
Sympower.net/privacy-notice
Notion > Incident Response Plan
Notion > Our Whistleblowing Policy
Whistleblowersoftware.com > create new report
App.juro.com
E-mail: Reminder on BlueBite GmbH_NDA_Sympower B.V. | Juro (13/11/2024)
20231122 Bluebite_Gmbh_Customer Agreement
Bluebite GmbH_NDA_Sympower B.V.
Customer Flexibility Services Agreement
Notion > SvK Cat A Requirements
Sympower's Vendor Code of Conducut
Demonstration of '2. Legal' Google Drive Folder access

Physical security

Section	Description
A.5.37	Documented operating procedures
A.6.7	Remote working
A.7.1	Physical security perimeter
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 reuse of equipment

Explanation:
- The organization is located in a shared office location in Amsterdam, and is renting 2 floors.
- The organization has a documented and approved physical security policy available on Vanta. The policy is reviewed and adjusted in December 2024.
- Security Perimeters are defined per Office location, additional secure spaces are defined.
- The organization is cloud-based, therefore no physical resources are critical for the business operations.

CONCEPT

- Visitor management is defined. Visitors should always be assigned to a host, who will accompany the guest at all times. When visitor is receiving a key, a registry is made in the visitor log.
- A lost & found box is implemented, found digital keys however should be reported to facilities so they can be blocked.
- Exceptions to the policy have to be requested by facilities.
- The shared office is protected by digital keys, owned by the landlord. A documented registry is available and shown during the audit. Per employee with a key their name, email-address and badge number, together with, if relevant, the date of return.
- Locking computers is also required for remote workers.
- The policy is applicable to all office locations.
- Fire extinguisher and a fire blanket are in place and have had their scheduled maintenance.
- An emergency plan is documented available. Company details and how to act when a emergency erupts is described.
- A physical emergency box is stored in the office, which includes physical copies of emergency plans, flashlights, microphones, walky-talkies, first aid kit. The facilities team is responsible for maintaining the box.
- Responsibilities in case of fire, water. gas leak, power outage and a bomb threat are described.
- Assets are in a locket cabinet, the keys are handed out to only a few employees, plus the facilities manager has a master key. A registration is available.
- When an employee leaves the company, the assets are returned to the facilities department, who hands it over to IT, in order to securely wipe and reuse the hardware.
- A shredder is available for physical documents. Once in a while managers are asked to review the contents of cabinets and check if files can be digitalized and/or destroyed.

Verification
Interview with Catarina de Melo
Physical Security Policy
Sympower Key Log
Visitor Log – Netherlands
Emergency response plan for location Amsterdam
Physical inspection on location

Secure configuration

Section	Description
A.5.37	Documented operating procedures
A.8.4	Access to source code
A.8.9	Configuration management
A.8.18	Use of privileged utility programs
A.8.19	Installation of software on operational systems
A.8.24	Use of cryptography

Explanation:
Based on the interviews and the evidence shown, it can be concluded that the organization has planned, implemented and controls appropriate processes:

- To ensure the correct and secure operation of information processing facilities.
- To prevent the introduction of unauthorized functionality, avoid unintentional or malicious changes and to maintain the confidentiality of valuable intellectual property.
- To ensure hardware, software, services and networks function correctly with required security settings, and configuration is not altered by unauthorized or incorrect changes.
- To ensure the use of utility programs does not harm system and application controls for information security
- To ensure the integrity of operational systems and prevent exploitation of technical vulnerabilities
- To ensure proper and effective use of cryptography to protect the confidentiality, authenticity or integrity of information according to business and information security requirements, and taking into consideration legal, statutory, regulatory and contractual requirements related to cryptography.

CONCEPT

Verification:
Cryptography policy
Infra-ami (git)
Infra-ami.timer.j2
Ami Creation process, 26 nov 2024 (notion)
#22966
Operations security policy
Msa-conn-router/main.yml
Vanta demonstration > findings by asset > platform bx4 production primary
Vulnerabilities mitigation process (notion)
AWS inspector scan
Infra 2401
demqx5/main.yml
Grafana dashboard demonstration
Vanta > compute instances > relational databases
Interview with Stamatis Maritsas, Siimo Sulev, Alar Aun

Supplier relationships security

Section	Description
A.5.19	Information security in supplier relationships
A.5.20	Addressing information security within supplier agreements
A.5.21	Managing information security in the ICT supply chain
A.5.22	Monitoring, review and change management of supplier services
A.5.23	Information security for use of cloud services
A.6.6	Confidentiality or nondisclosure agreements
A.8.30	Outsourced development

Explanation:

- The organization has a documented Third Party management Policy in place.
- Security criteria are documented in review lists in Vanta.
- Suppliers will be receive a risk analysis, based on the types of data used. Results are stored in
- Interfaces and dependencies are documented.
- Vendors are documented in Vanta and are scored based on risk. Critical vendors have been identified.
- Vendor uses automation based on the SSO utility to discover potential new vendors.
- Critical vendors are: Vanta, Amazon Web Services, GitHub and GoDaddy.
- Security owners are assigned per vendor. The owner is responsible for the monitoring.
- Security reviews are being done annually. The review for critical supplier amazon is shown during the audit.
  1 finding has been noted: One user should not be able to delete all information. The activity is registered within Jira and followed up upon.
  Relevant certificates are requested from vendors. The ISO 27001 certificates for vendors Slack and Amazon are shown during the audit.
- Security clauses are present in (general) agreements with the vendors. The Data processing agreement for vendor Slack has been shown.
- Confidentiality is included in the general agreements / Data processing agreements. This is shown in the DPA for Slack.
- Changes within important service details are shared via E-mail and/or slack. The organization analyses the impact and follows up if necessary. An e-mail from the Gemini account manager is shown where changes are initiated. The changes have been discussed in the internal Slack channel
- An exit strategy for cloud services is included part of the policy. This is included in the nonconformity the organization has identified during the internal audit.

CONCEPT

During the internal audit, the organization has identified a nonconformity on controls 5.19-5.23, as the supplier management process is not fully controlled yet. Multiple minor nonconformities have been identified in the ownership and following practices of the supplier management review.

As immediate action the organization is following up on all supplier reviews. As corrective actions ownership over procurement and on/offboarding must be properly defined, Implementing this will start in February with a deadline in June 2025.

Verification:
Third-Party Management Policy 1.0
Vanta – Managed Vendors
Vanta – Security reviews – Amazon Web Services
JIRA -> Engineering Operations -> AWS Root Account Management Process
Data-processing-addendum.pdf
Slack_SOC3_2023_Report
Mail: Gemini AI now included in almost all workspace plans dated 16-01-2025

System and network security

Section	Description
A.5.37	Documented operating procedures
A.6.7	Remote working
A.8.7	Protection against malware
A.8.18	Use of privileged utility programs
A.8.20	Networks security
A.8.21	Security of network services
A.8.22	Segregation of networks
A.8.23	Web filtering
A.8.25	Secure development lifecycle
A.8.26	Application security requirements
A.8.27	Secure system architecture and engineering principles
A.8.28	Secure coding
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.8.34	Protection of information systems during audit testing

Explanation:
Based on the interviews and the evidence shown, it can be concluded that the organization has planned, implemented and controls appropriate processes:

- To ensure the correct and secure operation of information processing facilities.
- To ensure the security of information when personnel are working remotely
- To ensure information and other associated assets are protected against malware
- To ensure the use of utility programs does not harm system and application controls for information security
- To protect information in networks and its supporting information processing facilities from compromise via the network.
- To ensure security in the use of network services.
- To split the network in security boundaries and to control traffic between them based on business needs
- To protect systems from being compromised by malware and to prevent access to unauthorized web resources
- To ensure information security is designed and implemented within the secure development life cycle of software and systems.

- To ensure all information security requirements are identified and addressed when developing or acquiring applications.
- To ensure information systems are securely designed, implemented and operated within the development life cycle
- To validate if information security requirements are met when applications or code are deployed to the production environment
- To protect the production environment and data from compromise by development and test activities
- To preserve information security when executing changes.
- To minimize the impact of audit and other assurance activities on operational systems and business processes.

Verification:
Backup & recovery w/AWS backup service (notion)
AWS health dashboard
Miro Sympower VPC connectivity
Ansible demonstration
Jira engineering operations board
Ticket infra2642 (git 22600)
Spacelift demonstration
AWS security groups
Spacelift production worker pool/main.yaml
AWS opensearch form logs (notion)
Audit logging (notion)
AWS VPC dashboard
AWS peering connections
Network security (vanta control)
Sympower infra gh repos backup (git) Amazon S3
Specelift (notion)
Infra-ami (git)
Infra-ami.timer.j2
Ami Creation process, 26 nov 2024 (notion)
#22966
Operations security policy
Msa-conn-router/main.yml
Vanta demonstration > findings by asset > platform bx4 production primary
Vulnerabilities mitigation process (notion)
AWS inspector scan
Infra 2401
demqx5/main.yml
Grafana dashboard demonstration
Vanta > compute instances > relational databases
Interview with Stamatis Maritsas, Siimo Sulev, Alar Aun

CONCEPT

Threat and vulnerability management

Section	Description
A.5.7	Threat intelligence
A.5.37	Documented operating procedures
A.8.8	Management of technical vulnerabilities

Explanation:

- The organization has a documented Operations security policy available.
- Threat intelligence is collected from multiple sources, mainly online newsletters. Mails from CISA (vulnerability summaries) and KrebsOnSecurity are shown. Amazon security news as well.
- A CERT is not yet connected. This will be done in the near future as this is a NIS2 requitement.
- Vulnerability scans are performed on public-facing systems in production environment.
- A Vulnerability mitigation process is documented, which states how the vulnerability for AWS integrations should be managed.
- Ticket “Upgrade Ansible Core to v2.17.7” is shown during the audit.
- Dependabot is used to perform vulnerability scans on code. Currently no open Dependabot alerts are open.
- Slack is integrated in GitHub, which enables Dependabot to send automated alerts when a vulnerability gets detected in the code. The slack channel with received alerts is shown during the audit.
- Resolve times for vulnerabilities are defined in the policy and are included in the SLA configuration within Vanta.
- Pull requests can only be completed if the testing is completed and if no critical vulnerabilities are open.
- Penetration tests are performed annually. A documented pentest report is available. Pentest findings are registered in JIRA. All pentest findings are closed.
- The security CoP is monitoring the vulnerability resolve times. Vulnerability information is gathered in Vanta, which gives an complete overview of the identified vulnerabilities and the resolve times.
- Infrastructure is managed as Infrastructure as code, which make is easy to manage vulnerabilities and patch network vulnerabilities.

Verification:

Interview with Alar Aun, Aggelos Gamvrinos and Stamatis Maritas
Operations Security Policy 1.2
GitHub -> msa-observability -> Code security
Slack -> Alerts-devboosters
GitHub -> Password exposure in Hs Database
Mail: CISA Vulnerability Summary for the week if January 13, 2025 dated 21 January 2024
Sympower BV. Penetration Testing 2024-14-OCT-2024.pdf
JIRA -> PT2024
JIRA -> Investigate CVE-2021-29921 and consecutively all unised Ansible collections.

CONCEPT

DISCLAIMER

The results of this audit are stated in this report and were provided for validation and discussed with the management of the client during the closing meeting.

The draft report was assessed by the customer before the final report was made available to the client by Brand Compliance B.V..

It is forbidden to modify or split this document in any way.

Brand Compliance B.V. is not liable for any direct, indirect, incidental or consequential damage caused by or with the use of the information or data from this document or the inability to use that information or data.

The audit is based on a sampling process from the available information.

The contents of this document may only be disclosed as a single entity to third parties, provided with the above-mentioned designations regarding copyrights, liability, adaptations and legal validity.

Brand Compliance B.V. accepts no responsibility or liability towards third parties as the report is not intended for any purpose other than described above.

In accordance with section 9.4.8.1 of NEN-EN-ISO 17021-1 version 2015, this report remains the property of Brand Compliance B.V.

Brand Compliance B.V., 's-Hertogenbosch, the Netherlands. All rights reserved.

CONCEPT

APPENDIX 1: CHECKLIST OPENING AND CLOSING MEETING

Discussed points during the opening meeting (in accordance with ISO 17021:2015 section 9.4.2):
1. Introduction of the participants, including an outline of their roles;
2. Confirmation of the scope of certification;
3. Confirmation of the audit plan (including type and scope of audit, objectives and criteria), any changes, and other relevant arrangements with the client, such as the date and time for the closing meeting, interim meetings between the audit team and the client's management;
4. Confirmation of formal communication channels between the audit team and the client;
5. Confirmation that the resources and facilities needed by the audit team are available;
6. Confirmation of matters relating to confidentiality;
7. Confirmation of relevant work safety, emergency and security procedures for the audit team;
8. Confirmation of the availability, roles and identities of any guides and observers;
9. The method of reporting, including any grading of audit findings;
10. Information about the conditions under which the audit may be prematurely terminated;
11. Confirmation that the audit team leader and audit team representing the certification body is responsible for the audit and shall be in control of executing the audit plan including audit activities and audit trails;
12. Confirmation of the status of findings of the previous review or audit, if applicable;
13. Methods and procedures to be used to conduct the audit based on sampling;
14. Confirmation of the language to be used during the audit;
15. Confirmation that, during the audit, the client will be kept informed of audit progress and any concerns;
16. Opportunity for the client to ask questions.
Discussed points during the closing meeting (in accordance with ISO 17021:2015 section 9.4.7):
1. Registration of the attendees;
2. Presentation of the audit conclusions, including the recommendation regarding granting/continuing certification;
3. Presentation of the observed nonconformities;
4. Advising the client that the audit evidence collected was based on a sample of the information; thereby introducing an element of uncertainty;
5. The method and timeframe of reporting, including any grading of audit findings;
6. The certification body's process for handling nonconformities including any consequences relating to the status of the client’s certification;
7. The timeframe for the client to present a plan for correction and corrective action for any nonconformities identified during the audit;
8. The certification body's post audit activities;
9. Information about the complaint handling and appeal processes;
10. Opportunity for the client to ask questions.

CONCEPT