E-WISE B.V.

MANAGEMENT REVIEW TEAM MEETING

Meeting Date and Time:	17 February 2025
Meeting Location:	Janssoniuslaan 38, 3528 AJ Utrecht, Nilufer’s office
Dial in Details:	As per calendar invite

ATTENDEES:

Name	Title / Role / Representing	Accepted? (Y/N)
Nilufer Akpinar	Managing director	Y
Ellen Smit	Improvement Projects	Y
Marjolein van Agtmaal	Finance Manager	Y
Tigran Khatchadrijan	System Administrator	Y
Johan Assen	Projectmanager / ISMS Responsible	Y

Contents

NEW AGENDA ITEMS

- Discuss risk assessments and improvements for 2025 (if there are any)
- Discuss any other security improvements (after internal audit)

EXISTING AGENDA ITEMS

- Audit Results from 2024 have been addressed and solved during the year. See agenda point 5 from management review 2024. There is one remaining point concerning A. 5.15.

AGENDA

Agenda Number	Agenda Item	Notes / Minutes
1	Actions from previous meeting	1. An improvement has been recorded for internal printers in 2023. This is still in progress in 2024. This has been implemented (Task) 2. As of 1 December 2023 we have a centralised password manager “Zoho Vault” implemented. This has been implemented (Task) 3. We are looking into the possibility of max duration of sharing documents outside E-WISE (Google drive) in 2024. Unfortunately this is not possible technically (Task). In the monthly checklist by Tigran there is a check to monitor if there is any user that shares a large amount of documents.

		4. We are looking into the possibility to store raw recordings to a cloud environment 2024. This has been implemented(Task) 5. We have end-point security. We look into the possibility / comparing of adding Crowstrike in 2024. We decided not to pursue this at the moment since we already have endpoint security in ManageEngine and Microsoft Defender. (Task) 6. Simulates a phishing email in 2024. First phishing email has been sent (Task), we are evaluating this (Task) and will plan a followup. (Task) **7.** Security training updates in 2024. The Security training has been updated with a topic on AI(Task). We will send this in Q1 to staff. **8.** Restore tests in 2024. Restore tests have been successfully done (Task)

		9. Communication is key in our organisation. We communicate information security related topics in our 2-monthly “krokettenlunch” We will continue this in 2025
2	Changes in external and internal issues that are relevant to the information security management system	We have centralised the task management and documentation within the Reducate organisation. The co-tennant is moving out of the building on 31-3-2025
3	Nonconformities and corrective actions	See Incident and CAPA log 3 small size incidents with a total of 46 affected records: - Email adresses of small group of students were visible between these students (Task) - Student information of small group were visible to the wrong organisation - Wrong lms organisation connected to lms manager Currently there is a 4th in review with 11 affected records - Groupmanager linked to the wrong department in E-WISE Totaal Plus(In progress)
4	Monitoring and measurement results	See table at the end of the document

5	Audit Results Afwijking beoordeling, norm vaststellen, oorzaak van de afwijking, vaststellen of dat er gelijksoortige afwijkingen zich voor kunnen doen.	**External Audit 2024** **O-2024-02: Some documents have been written in a very general sense and still have traces of the original instructions.** We fixed the specific findings and rewrite chapters of the policy when we update these for another reason. (Task) **O-2024-01 - Stakeholder analysis - co-tennants** We added the co-tennants in the stakeholder analysis. No associated risks (Task). **O-2024-03: Segregation of duties is determined based on Zoho rights and financial system rights. 5.3 Segregation of duties has been tied to a risk of employees not knowing** Risk mapping has been redone **NC-B-2024-01: Operational planning and control** We scheduled regular meetings with the ISWG of other group companies and restructured the ISMS and task system for better overview and integration. **O-2024-04: the organization may need a formal DPO due to the large scale of clients on the platform for which the organization monitors course work and results.** The management of E-WISE and Blueprint Learning investigated this topic and it did not meet the requirements of the GDPR authority. An internal DPO is deemed sufficient. Risk 3.4 is raised for this and accepted. **O-2024-05: Scope documentation should be appropriately updated to**

		accurately include locations and activities in each as well as any dependencies. We have rewritten the Scope documentation to include E-WISE, Blueprint Learning and Thar. (Task) **O-2024-06: Policy documentation at Thar is not shared in the same way and, despite the document being attached to the security training, auditees couldn't find it again during the audit.** Currently this document is shared via the security training and available in the regular locations for staff information (Task) **E-WISE Internal Audit** **9.2: Overweeg het "How to conduct an internal audit (internal)" document te evalueren, zodat het eenduidig stelt dat ieder jaar het gehele ISMS wordt geaudit.** We will redesign our Internal Audit approach (Task) **6.1.3D: Overweeg te kijken naar de reden voor implementatie en wees specifieker in wat de die reden dan inhoud** We will review the descriptions for Vulnerability, Result in the risk register (Task) **A.5.29: Overweeg om het gebruik en scenario's van het continuïteitsplan te testen.** Added to Notion (Task)

		A.5.28: Er is nog geen bewijsmateriaal beschikbaar in de incidentenprocedure. CAPA made and improvement implemented (CAPA / Task)
6	Fulfilment of information security objectives	Recorded in the table at the end of the document.
7	Feedback from interested parties	We have a yearly Finance / IT audit carried out by BDO. These results and improvements are being reported in Notion when the report has been completed.
8	Risk Assessment Results and Status of Risk Treatment Plan	**New Risks** No Single Signon for the central management password vault can lead to a data breach.Risk #1.2.8.11 No technical check for duplicate organization numbers in ZOHO can lead to a data leak. Risk #1.2.8.12 By not having a formal DPO registered at the GDPR authority, E-WISE, Thar and Blueprint Learning risk not complying with GDRP.Risk #3.4 We discussed to add a Risk regarding long term failure of a major cloud provider (Risk 2.8), The ISSC sees this risk as having low probability and thus accepts it. Risk #2.8

9	Opportunities for Continual Improvement	• Policy for laptop updates has been improved (Task) • Blocking deepseek due to privacy concerns (Task) • Improving Spam filters in the Google environment (Task) • We still have a task to implement 2-FA on our E-LEARNING platforms, what to do with this? (Task) The ISSC decided to postpone this topic because both risks and customer demand are limited. In addition: The E-WISE business is hesitant to apply this function because our business demands easy access to e-learning. • Investigate a Reducate wide security training (Task)
10	Any other business	GDPR meetings have been conducted

INFORMATION SECURITY OBJECTIVES MEASURES

It is good practice to record the objectives of the ISMS and to review the measures in the management review team meeting. The objectives here are taken from the Information Security Management System document. If you have changed them there, then change them here. This needs to be your objectives as recorded.

Objective	Planned KPI's	Achieved	Measurement
Risk reduction: by limiting the impact of information security incidents	**MTTD** < 5 minutes **MTTR** < 4 hours	**MTTD** < 5 minutes **MTTR** 3	The process of internal audit, training for employees and continual improvement are operating effectively, monitors and measures are being tracked and within tolerance.
Improving customer satisfaction: by protecting customers' personal information	**Data breach rate** < 0.1%	**Data breach rate** 0.1%	The ISMS continues to improve customer satisfaction. We have added security improvements.
Ensure the confidentiality, integrity and availability of data and services of the company	**System Uptime** > 99.5%	**System Uptime** 99,9%	The current measurements, backups, monitoring and logging are being in place and performing well for all information systems.

	Data incidents resolved < 24 hours	**Data incidents resolved** 48 hours	
Meet legal, regulatory, and contractual obligations for information security	**Compliance Rate** 100%	**Compliance Rate** 100%	The ISMS continues to meet its legal and regulatory obligations. There are no new contractual requirements recorded. Training is on track and well accepted for all employees. There is an onboarding in place for information security.
Improving efficiency: by securing information and reducing downtime	**Percentage of Successful Backups** 95-98% **Restore tests** 100%	**Percentage of Successful Backups** 100% **Restore tests** 100%	The ISMS continues to secure information and reduce downtime. Backups are on track and a restore test has been successfully done

			(A5.29 Restore tests). Requirements will be updated in 2025 for restore tests if applicable.
Implement a culture of information security through training and awareness	**Training Completion** 100%	**Training Completion** 100%	The results of the training plan were noted as on track with all employee's current on planned and taken information security training. Communication was sent to all staff. An updated training is being planned for 2025 Information security goals are being communicated and added to the training. The information security policy is shared with all employees.
Effectively manage third parties to reduce potential information security risk from suppliers	**Vendor Risk Assessment Results** All key suppliers	**Vendor Risk Assessment Results** All key suppliers are	Third party management is operating effectively, and the third-party register is up to date. All reviews are recorded as being on

		audited, in 2025 reports will be added	track any nonconformities are added to Notion to improve.

DOCUMENTS RELEVANT TO MEETING

List documents that are provided as part of the meeting.

Policy

Information Security Policy - [Internal]

External Audit

External Audit report

External Audit report - scope expansion

Internal audit

E-WISE Interne Audit 2024

Risk analyses

Risk register

Other information

GDPR meetings

Business Continuity Plan [Confidential]

Communication plan [Confidential]