



Aibidia

TXM Platform

ISAE 3000 TYPE 2 REPORT

INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT ON
AIBIDIA OY'S DESCRIPTION OF ITS TXM PLATFORM AND
THE SUITABILITY OF DESIGN AND OPERATING EFFECTIVENESS OF
ITS CONTROLS RELEVANT TO SECURITY THROUGHOUT THE PERIOD
JULY 1ST, 2025 TO JUNE 30TH, 2026

July 10th, 2026



SECTION I	3
<i>Independent Service Auditors' Assurance Report</i>	<i>4</i>
SECTION II	7
<i>Management of Aibidia's Statement</i>	<i>8</i>
SECTION III	9
<i>Management of Aibidia's Description of its TXM Platform</i>	<i>10</i>
3.1 Overview of Operations	10
3.1.1 OVERVIEW OF THE ORGANIZATION.....	10
3.1.2 SYSTEM OVERVIEW	10
3.2 Relevant aspects of the internal control environment	14
3.2.1 CONTROL ENVIRONMENT	14
3.2.2 ROLES AND RESPONSIBILITIES	18
3.2.3 SECURITY MANAGEMENT	18
3.2.4 PHYSICAL SECURITY AND ENVIRONMENTAL CONTROLS	20
3.2.5 CHANGE MANAGEMENT	24
3.2.6 INFORMATION SECURITY INCIDENT RESPONSE	25
3.2.7 DATA BACKUP AND RECOVERY	26
3.2.8 SYSTEM ACCESS MANAGEMENT	27
3.2.9 APPLICATION DEVELOPMENT	29
3.2.10 RISK ASSESSMENT.....	33
3.2.11 INFORMATION AND COMMUNICATION	35
3.2.12 CRYPTOGRAPHY POLICY, KEY AND SECRET MANAGEMENT POLICY, ENCRYPTION: IN TRANSIT AND AT REST	37
3.2.13 MONITORING	38
3.2.14 HUMAN RESOURCES SECURITY	39
3.3 Complementary User Entity Controls.....	40
3.4 Subservice Organizations	41
SECTION IV	43
<i>Description of Control Objectives, Related Controls and Test Results of Independent Auditor</i>	<i>44</i>
Information Provided by the Independent Auditor	44
Testing Procedures.....	44
Applicable Trust Services Principles	45
Testing Results	49

SECTION I



Independent Service Auditors' Assurance Report

To: Management of Aibidia Oy

Scope

We have been engaged to report on Aibidia Oy's (hereinafter "the Service Organization" or "Aibidia") accompanying description of its system titled "Management of Aibidia's Description of its TXM Platform" throughout the period July 1st, 2025 to June 30th, 2026 (the Description), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria* (the Description Criteria), and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period July 1st, 2025 to June 30th, 2026 to provide reasonable assurance that Aibidia's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Aibidia uses Microsoft Azure to host the cloud environment on which Aibidia's TXM Platform is based and Data Group to manage Aibidia devices. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Aibidia, to achieve Aibidia's service commitments and system requirements based on the applicable trust services criteria. The Description presents Aibidia's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Aibidia's controls. The Description does not disclose the actual controls at the subservice organizations. Our engagement did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Aibidia, to achieve Aibidia's service commitments and system requirements based on the applicable trust services criteria. The Description presents Aibidia's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Aibidia's controls. Our engagement did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

Aibidia is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Aibidia's service commitments and system requirements were achieved. Management of Aibidia has provided the accompanying statement titled "Management of Aibidia's Statement" (the Management Statement) about the Description and the suitability of design and operating effectiveness of controls stated therein. Aibidia is also responsible for preparing the Description and Statement, including the completeness, accuracy, and method of presentation of the Description and Statement; providing the services covered by the Description; selecting the applicable trust services criteria and stating the related controls in the Description; and identifying the risks that threaten the achievement of Aibidia's service commitments and system requirements.

Our Independence and Quality Management

We are independent of the company in accordance with the ethical requirements that are applicable in Finland and are relevant to our engagement, and we have fulfilled our other ethical responsibilities in accordance with these requirements.



The firm applies International Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements*, which requires the firm to design, implement and operate a system of quality management including documented policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the Description and on the suitability of the design and operating effectiveness of the controls stated in the Description based on the evidence we have obtained in our engagement.

Our engagement was conducted in accordance with International Standard on Assurance Engagements 3000 (Revised), *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. That standard requires that we plan and perform our engagement to obtain reasonable assurance about whether, in all material respects, the Description is presented in accordance with the Description Criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

A reasonable assurance engagement to report on the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- obtaining an understanding of the system and the service organization's service commitments and system requirements;
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively;
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria;
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based on the applicable trust services criteria if those controls operated effectively;
- testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria;
- evaluating the overall presentation of the description; and
- performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that each individual report user may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.



Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section IV.

Opinion

In our opinion, in all material respects,

- a. the Description presents Aibidia's TXM Platform that was designed and implemented throughout the period July 1st, 2025 to June 30th, 2026 in accordance with the Description Criteria
- b. the controls stated in the Description were suitably designed throughout the period July 1st, 2025 to June 30th, 2026 to provide reasonable assurance that Aibidia's service commitments and system requirements would be achieved based on the applicable trust services criteria if the controls operated effectively throughout that period, and the subservice organizations and user entities applied the complementary controls assumed in the design of Aibidia's controls throughout the period July 1st, 2025 to June 30th, 2026
- c. the controls stated in the Description operated effectively throughout the period July 1st, 2025 to June 30th, 2026 to provide reasonable assurance that Aibidia's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls, assumed in the design of Aibidia's controls, operated effectively throughout the period July 1st, 2025 to June 30th, 2026.

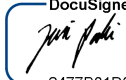
Restricted Use

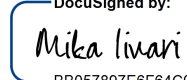
This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Aibidia and user entities of Aibidia's TXM Platform during some or all of the period July 1st, 2025 to June 30th, 2026, who have sufficient knowledge and understanding of the following:

- the nature of the service provided by the service organization;
- how the service organization's system interacts with user entities, business partners, subservice organizations, and other parties;
- internal control and its limitations;
- complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements;
- user entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services;
- the applicable trust services criteria; and
- the risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties.

Helsinki, July 10th 2026
KPMG Oy Ab

DocuSigned by:

2477B01D945A425...
Jussi Paski
Partner
Authorized Public Accountant

DocuSigned by:

BB057897E6F64C0...
Mika Iivari
Partner
Head of Cyber Advisor

SECTION II



Management of Aibidia's Statement

We have prepared the accompanying description in Section III of Aibidia's system titled "Management of Aibidia's Description of its TXM Platform" throughout the period July 1st, 2025 to June 30th, 2026 (the Description), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, (the Description Criteria). The Description is intended to provide report users with information about the TXM Platform system that may be useful when assessing the risks arising from interactions with Aibidia's system, particularly information about system controls that Aibidia has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Aibidia uses carved-out subservice organizations, including Microsoft Azure to host the cloud environment on which Aibidia's TXM Platform is based and Data Group to manage Aibidia devices. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Aibidia, to achieve Aibidia's service commitments and system requirements based on the applicable trust services criteria. The Description presents Aibidia's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Aibidia's controls. The Description does not disclose the actual controls at the subservice organizations.

The Description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Aibidia, to achieve Aibidia's service commitments and system requirements based on the applicable trust services criteria. The Description presents Aibidia's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Aibidia's controls.

We confirm, to the best of our knowledge and belief, that:

- a) The Description presents Aibidia's TXM Platform that was designed and implemented throughout the period July 1st, 2025 to June 30th, 2026, in accordance with the Description Criteria.
- b) The controls stated in the Description were suitably designed throughout the period July 1st, 2025 to June 30th, 2026 to provide reasonable assurance that Aibidia's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and carved-out subservice organization(s) and user entities applied the complementary controls assumed in the design of Aibidia's controls throughout the period July 1st, 2025 to June 30th, 2026.
- c) The controls stated in the Description operated effectively throughout the period July 1st, 2025 to June 30th, 2026 to provide reasonable assurance that Aibidia's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls, assumed in the design of Aibidia's controls, operated effectively throughout the period July 1st, 2025 to June 30th, 2026.

Helsinki, July 10th 2026
Aibidia Oy

Signed by:



578BC44F67454F0...

Ryan Collett
COO

SECTION III



Management of Aibidia's Description of its TXM Platform

3.1 Overview of Operations

3.1.1 OVERVIEW OF THE ORGANIZATION

Aibidia, headquartered in Helsinki, is a global organization specialized in digital transfer pricing management and has a multinational team of tax lawyers, economists, data scientists and software developers. 7 years ago, Aibidia created the methodology to transform international tax law into code. That resulted in the Digital Transfer Pricing Taxonomy 1.0 and the ability to run crossfunctional TP processes on data and intelligence.

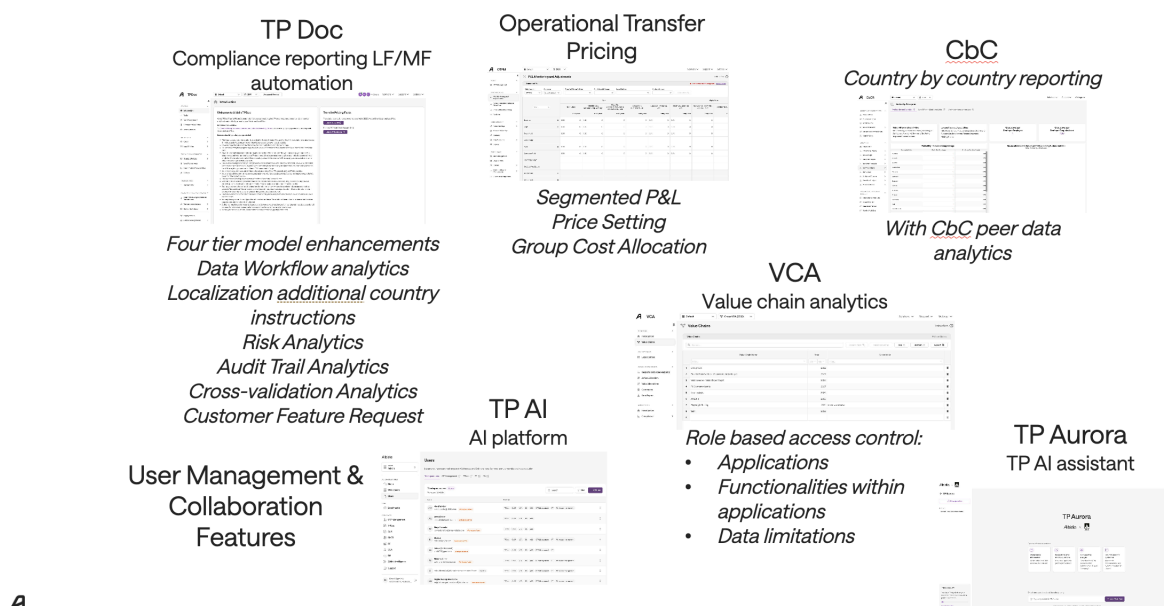
3.1.2 SYSTEM OVERVIEW

Aibidia offers cloud and data era transfer pricing solution for organizations to move towards continuous compliance and intuitive analytics within transfer pricing management.

Aibidia TXM Platform is built on Microsoft Azure, and consists of the following Customer facing applications:

- TPD, Transfer Pricing Documentation
- CBC, Country by Country reporting
- VCA, Value Chain Analytics
- DS, Data Studio
- OTP, Operational Transfer Pricing
- TPAurora, AI assistant
- TP AI, integrated AI platform

Aibidia SaaS Production: H1/2026



A

Aibidia

Description of Services Provided

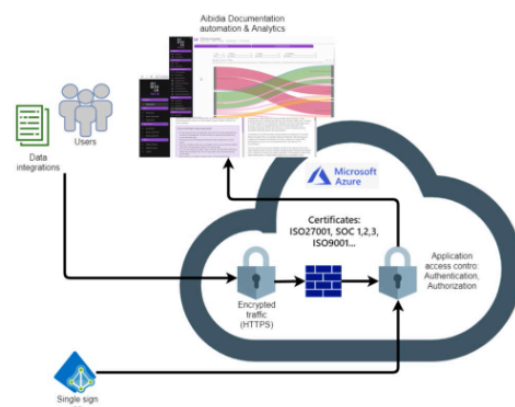
Aibidia offers cloud and data era transfer pricing solution for organizations to move towards continuous compliance and intuitive analytics. The Platform is built according to international standards and high-level architecture corresponds to the EU interoperability framework and OECD best practices.

System Boundaries

The Aibidia TXM platform has been built with an emphasis on security and is based on the highest international standards. The TXM Platform is built in the Microsoft Azure cloud platform, as the platform and its components have been audited and are being security tested continuously.

High-Level Solution Security Architecture

- Aibidia cloud platform is the safest way to handle your transfer pricing analytics and documentation compliance needs. Aibidia platform is based on highest international security standards
- Platform and its components have been audited and penetration tests are running as continuous process

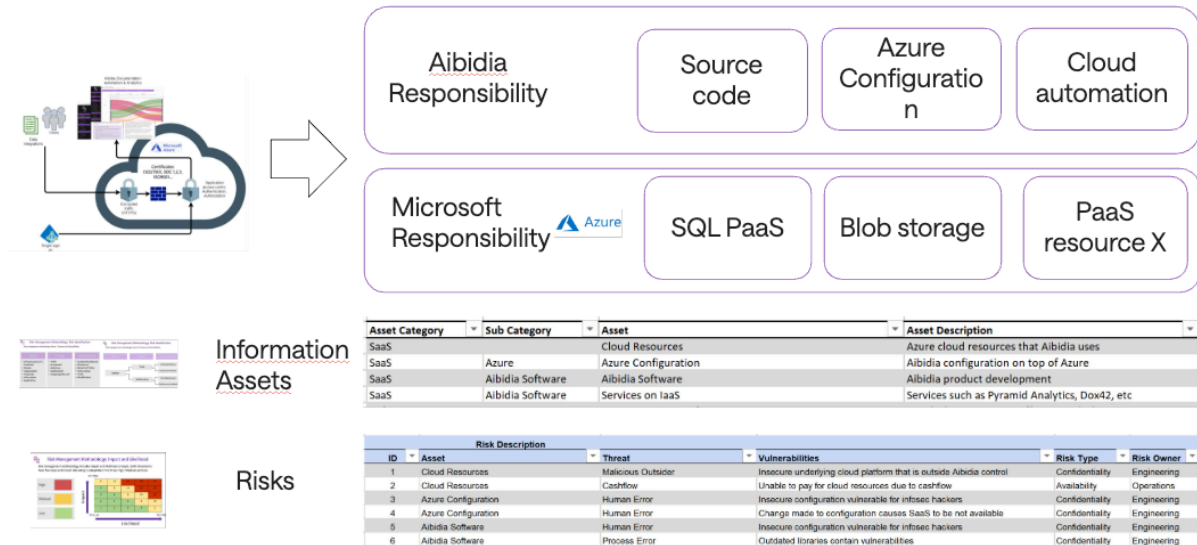


In the TXM Platform, the responsibilities between Aibidia and Microsoft has been clearly defined. While Aibidia controls and maintains source code, Azure configuration and cloud automation, Microsoft controls and maintains all the underlying cloud infrastructure like SQL PaaS, Blob storage and other PaaS resources.

Aibidia has identified the key information assets in their own control within the TXM Platform and actively manages risks related to those assets.



SaaS Responsibilities: Aibidia & Microsoft



Infrastructure and Software

Aibidia operates a modern and scalable cloud-native data management platform hosted in Microsoft Azure.

A modern backend for frontend pattern is used where a dedicated backend service exists for each of the core applications. Frontend uses Vue.js framework and services with APIs are developed in widely adopted and the latest supported versions of Microsoft technologies (mainly the .NET)

Aibidia favours Azure PaaS and managed service offerings to reduce operational overheads. PaaS offerings also provide high levels of scalability and service resilience out of the box.

These services are hosted using Microsoft Azure's managed App Service offering. Where appropriate, asynchronous functions are used for long-running background tasks such as document generation. Asynchronous processing is performed on demand using cost-effective Azure Functions.

Microsoft Azure a.o. holds the following relevant certifications within Security & Compliance:

- ISO27001, ISO27017, ISO27701, SOC 1, SOC 2, SOC 3, PCI DSS 3.2, ISO22301, ISO9001, Azure CIS

People

- Operations
- Sales
- Marketing
- Subject matter experts
- Customer success
- Product

Aibidia

- Engineering

Procedures

The Aibidia information security management process framework includes the following key activities:

- Change Management
- Event Management
- High Availability Activities
- Continuous Security Testing
- Information Security Incident Response
- Access Control
- Risk Management
- Security Patching
- Vulnerability Scanning
- Intrusion Detection Analysis
- Resource Cleanup

Data

Aibidia has defined information classification scheme and identified types of information that are processed within Aibidia business operations.

Aibidia has the following information classification scheme:

Public

- Information that is not confidential and is intended for public use
- Examples: Marketing materials, Materials on public website

Internal

- Information that is required in everyday work tasks and is intended for Aibidia personnel
- Valid work contract and NDA is required to access internal information
- Examples: Slack-messages in non-private channels, Wiki-pages

Company Confidential

- Information collected and processed by Aibidia for conducting business activities, e.g. information on employees and salaries, customer contracts and invoicing as well as company financing.
- Access is restricted to only named personnel. Confidentiality, integrity and availability of company confidential information are important for conducting business activities without interruptions
- Examples: Client contracts and proposals, source code, business plans, passwords for critical IT systems, client contact records, accounts etc.



Customer Confidential

- Customer owned data in Aibidia's possession. Customer confidential information can be accessed only if requested by customer for support purposes. Confidentiality, integrity and availability of customer confidential information are vital for ensuring customer trust and for complying with contract requirements
- Examples: Customer data stored in Aibidia SaaS solution

Aibidia has defined the information types they are processing, and each information type is classified according to the information classification scheme. "Employment related information" information type is classified as Employee confidential; "Client data" and "Client contact records" are classified as Client confidential, "Contracts, business plans and financial data" as well as "Secure code" are classified as Confidential; and "Passwords for critical IT systems" are classified as **Secret**. The information types are applied within, for example, access provisioning processes.

3.2 Relevant aspects of the internal control environment

3.2.1 CONTROL ENVIRONMENT

Internal control environment at Aibidia consists of the Information Security Management System (ISMS) that is a continuous process of planning, prioritizing and guiding the information security work. In addition, Aibidia is audited – by external auditors – several times each year, both on an ISMS level as well as on the technical platform. Further, the Information Security is built into the DevOps practices, by embedding automatic vulnerability scanners, infrastructure hardening guidelines and regular information security training throughout the organization.

Aibidia Information Security Management System (ISMS)

		Information Security Management System • Developed according to ISO27001:2022 • Continuous process • Quarterly security management team meetings • Benchmarks: Microsoft Azure Security Benchmark • Participation from organization branches • Main content • Incident reporting, Document reviews, process updates
	 	Annual External Audits • Conducted by Third party information security experts • Audit methodology is based on OWASP Guide and CSSTMM standard, Severity is analyzed with CVSS methodology • Covers Aibidia technical platform
		SecOps: Information Security Built into DevOps practices • Automatic vulnerability scanners • Infrastructure hardened according to Center for Internet Security (CIS) guidelines • Regular information security trainings in the company

The ISMS is built according to ISO27001:2022 and the processes are evaluated according to ISO 27002.



Process evaluation according to ISO27002

Information Security Management System

- Developed according to ISO27001:2022
- Process evaluation according to ISO27002



0. <u>Introduction</u>	5. <u>Information security policies</u>	8. <u>Asset management</u>	11. <u>Physical and environmental security</u>	14. <u>Systems acquisition, development and maintenance</u>
1. <u>Scope</u>				
2. <u>Normative references</u>	6. <u>Organization of information security</u>	9. <u>Access control</u>	12. <u>Operations security</u>	15. <u>Supplier relationships</u>
3. <u>Terms and conditions</u>				16. <u>Incident Management</u>
4. <u>Structure of this standard</u>	7. <u>Human resource security</u>	10. <u>Cryptography</u>	13. <u>Communications Security</u>	17. <u>Business Continuity</u>
				18. <u>Compliance</u>

The Executive team have not only bought-in to the Information Security work, they get involved and make certain the yearly cycle activities are being performed.

Executive Team

Meets periodically and makes sure yearly cycle activities are being performed



Evgenii Kazmiruk



Ryan Collett



Hannu-Tapani Leppänen



Antonius Rittberg



Brian Tully

VP of Engineering	VP of Finance	CEO	Chief of Staff	CRO
• Overall ISMS responsibility • User Access Management • Risk management process	• Approves policies • User Access Management	• Approves risks • Legislation changes	• Product teams management • Defining priorities	• Sales & business development • Marketing • Customer Success

On behalf of the Executive team an Information Security Management team has been appointed, the Information Security Management team also ensures that yearly cycle activities are being carried out, although on a more granular level.



Information Security Management Team

Meets periodically and makes sure yearly cycle activities are being performed



Evgenii Kazmiruk

VP of Engineering

- User Access Management
- Infosec forums and special interest groups



Ryan Collett

VP of Finance

- Approves policies
- User Access Management



Piia Heliste

Customer Success Manager

- Sales & business development representative



Kim Jämiä

VP of Technologies

- Infrastructure technical security
- User Access Management



Sarah Wasif

Head Of People

- HR processes and policy communication

Security Operations Control Team

Team that grants access to Aibidia SaaS solution and has privileged rights to Aibidia infrastructure.



Evgenii Kazmiruk



Ryan Collett



Eetu Ruponen



Kim Jämiä

SOC team: Scope

- Vulnerability Scan Reports
- Automatic Compliance Report (Azure)
- Azure Defender for Cloud reports
- SaaS performance reports
- Technical Development Roadmap

To provide input for the continuous improvement of the ISMS, an Internal Independent Audit Program has been established. Here, internal audits are being carried out based on the Aibidia risk management methodology and according to the ISMS roadmap and security objectives. The Information Security Management team ensures the auditors selected are independent and competent for the audit scope.

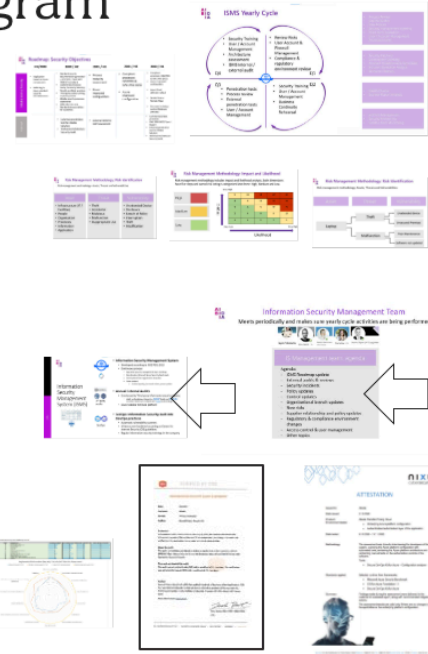


Internal (Independent) Audit Program

- Internal / independent audits are conducted based on risk management methodology and according to ISMS roadmap and security objectives
 - Competence of the auditors is evaluated by ISMS management team
 - Auditors are selected so that they are independent and objective from Aibidia ISMS management team
 - The audit criteria is selected based on the scope, it can contain but is not limited to the relevant standards, legislation, documentation or contractual obligations.
 - The auditing method is selected based on the scope, it can include but is not limited to the review of documentation, review of records, review of information systems or interviews with employees.
- The internal audit must take into consideration the following:
- The audit target defined in the audit plan
 - Importance of the processes concerned
 - Results of the previous audits

The internal auditor(s) should have unrestricted access to information assets that are being audited for proper conduct of the audit. To avoid conflict of interest, auditor(s) are not allowed to audit their own work.

- Results of the independent audits are reported to ISMS management team. The results are used for continuous improvement of the ISMS.



A

On a regular basis Aibidia receives requests – from customer prospects – to audit the information security posture in Aibidia. These requests typically come with a questionnaire addressing on average around 100 security requirements. Aibidia have a process for responding and reviewing these audit requests.

Customer Prospect Security Audits

- Aibidia receives information security and IT review questionnaires from customer prospects on regular basis
- Typically one questionnaire contains about 100 security requirements
- Aibidia process includes answering and reviewing the responses



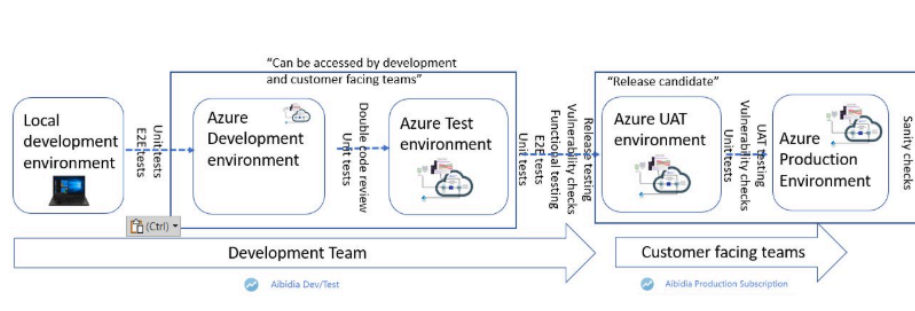
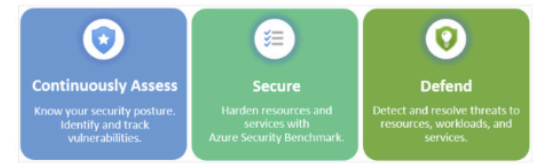
Aibidia's Human Resource Security is covering the recruitment phase with background checks and both document validation and reference validation, ensuring confidentiality is appropriately addressed in employment contracts. Ensuring awareness is effective by communicating updates through Slack and email, having a disciplinary process as well as an effective offboarding process.

Aibidia

Vulnerability Management is effectively handled by automated tools in the TXM Platform. Vulnerabilities are identified and patched automatically, and the result is assured by external penetration tests and automatic scanners.

Vulnerability Management and Patching Policy

- SaaS platform uses automatic tool
 - [Microsoft Defender for Cloud](#)
- External penetration tests
- Automatic scanners



3.2.2 ROLES AND RESPONSIBILITIES

Executive Team

Meets periodically and makes sure yearly cycle activities are being performed.

Information Security Management Team

Meets periodically and makes sure yearly cycle activities are being performed.

Security Operations Control Team

Team that grants access to Aibidia SaaS solution and has privileged rights to Aibidia infrastructure.

3.2.3 SECURITY MANAGEMENT

Security management at Aibidia is executed through the ISMS Yearly Cycle. The critical activities (not an exhaustive list) are as follows:

Q1:

- Review Risks
- User Account & Firewall Management
- Compliance & Regulatory Environment Review

Q2:

- Security Training

Aibidia

- User & Account Management
- Business Continuity Rehearsal

Q3:

- Penetration Tests
- Process Review
- External Penetration Tests
- Policy Review

Q4:

- Security Training
- Architecture Assessment
- ISMS Internal/External Audit
- Supplier Security Review

Furthermore, some activities are carried out in more frequent manner:

Quarterly:

- Process Review
- External Audits
- New Policies
- Security Management Meeting
- Third Party Evaluation
- User / Account Management
- Privileged Rights

Monthly:

- Security Patching
- Vulnerability Scanning
- Prospect Questionnaire Summaries
- Intrusion Detection Analysis
- Resource Cleanup

Weekly:

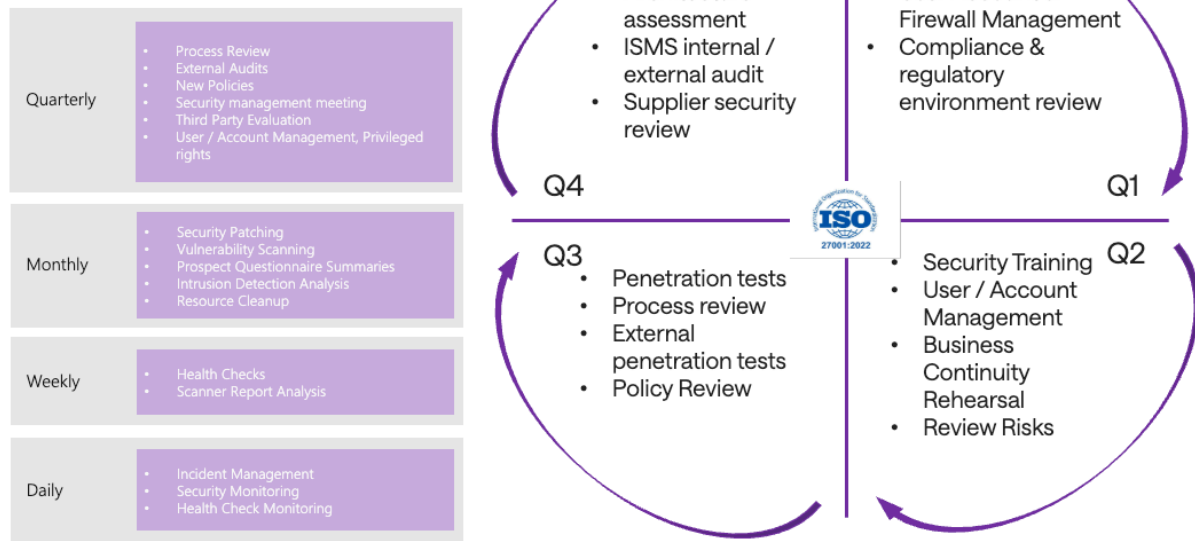
- Health Checks
- Scanner Report Analysis

Daily:

- Incident Management
- Security Monitoring
- Health Check Monitoring



ISMS Yearly Cycle



3.2.4 PHYSICAL SECURITY AND ENVIRONMENTAL CONTROLS

The company has a layout of the head quarter office in Helsinki which describes the physical security perimeter and its boundaries. The physical security and environmental controls are covered by several activities and measures:

- Locked Room for fiber wiring and connections
- CCTV surveillance of entrance and outside perimeter
- Locked wiring closets in each room
- External company inspecting and monitoring physical access 24/7
- Wiring in office areas is not easily accessible for unauthorized parties
- Network equipment is put away in locked cabinets

The windows are placed above the ground level and are not easily accessible.

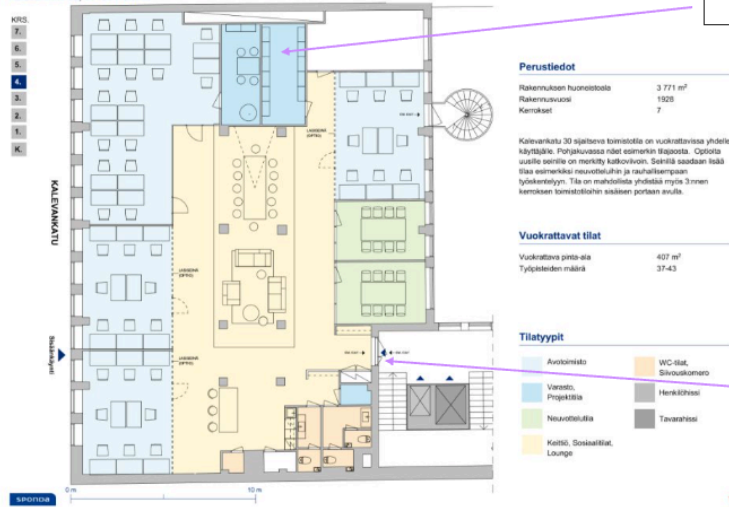
The reception in Helsinki office is inside office space dedicated to Aibidia. There are other companies in same building but not on the same office space described in the illustration below.



Physical Security – Helsinki Office

The reception in Helsinki office is inside office space dedicated to Aibidia. There are other companies in same building but not on the same office space described in the illustration below.

Koy Kalevankatu 30 | Versio 1 | 28.6.2018
Kalevankatu 30, 00100 Helsinki



Facility has video camera recording



Fibre connection room

- Need permission from ISMS management team to access

Visitors can enter this space with Aibidia host except for Fibre connection space

Locked closets in each room

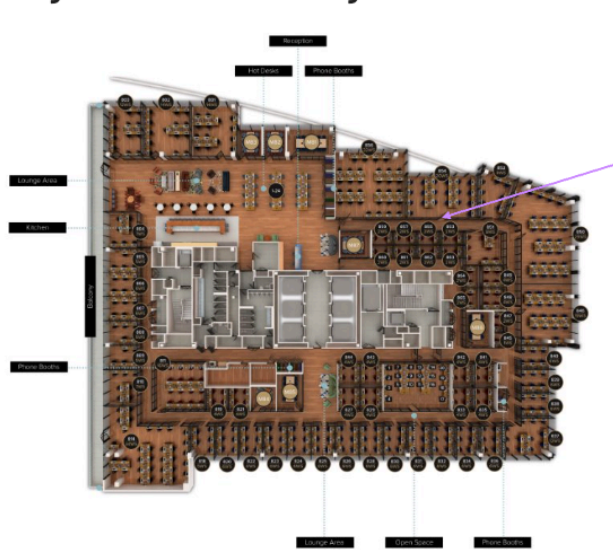
Security control on the entry

- Locked door to be accessed by Aibidia badges only
 - Keys managed by centralized Aibidia team using office building services
- Security service by Securitas



Physical Security: London Office

Address: 9 Appold St, London, EC2A 2AP
Room: 854



Access to the private office room is only possible using a pre-registered keycard.

Access to the premises

- The main entrance of the building has a security guard and front desk staff.
- A keycard is required to go through physical barrier before accessing the lifts.
- Visitors without a keycard must be pre-registered on an app, are given a day badge on a lanyard, and must be collected from reception on the ground floor.
- The day badge doesn't grant access through the physical barrier. The security guard must manually allow guests in and out every time.
- Once on the 8th floor, the keycard is required again to access Aibidia's private office room.
- Guests are issued with a temporary keycard to get in and out of the office room on the day. These are returned to reception after the visit.

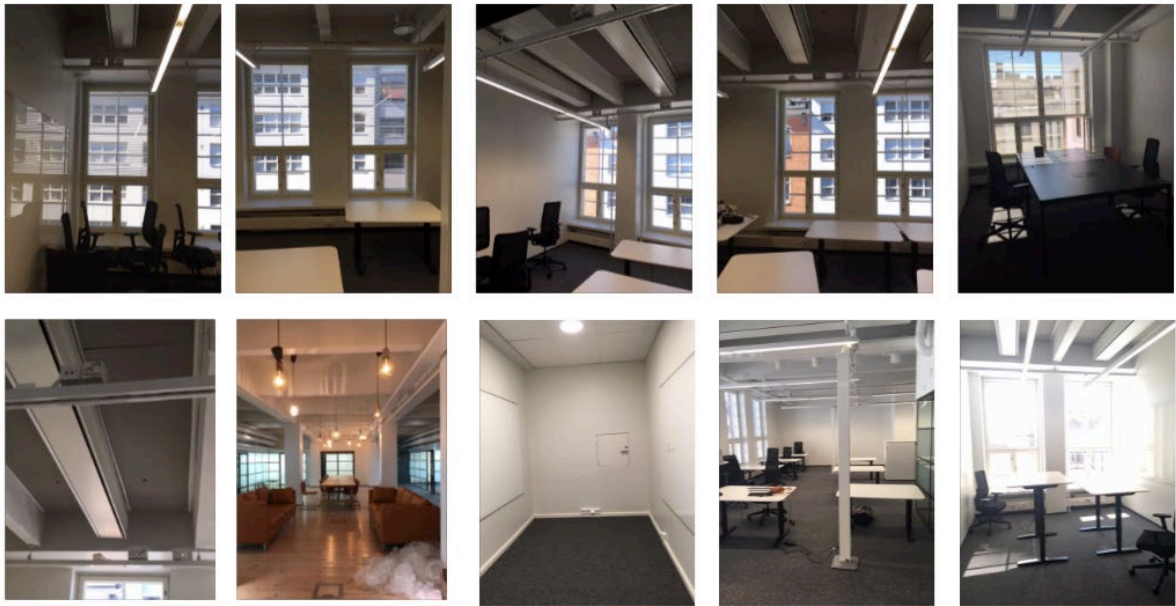


Physical Security Controls

Aibidia has implemented ISO27001 standard section 11 physical security controls in the areas

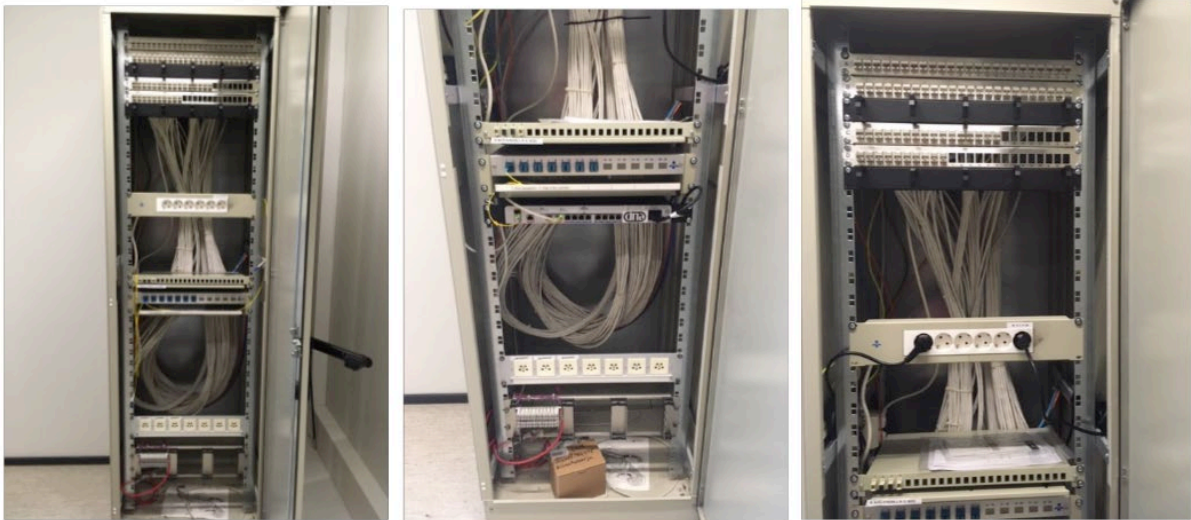
11	1	2	Physical entry controls	entry controls to ensure that only authorized personnel are allowed access.
11	1	3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.
11	1	4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.
11	1	5	Working in secure areas	Procedures for working in secure areas shall be designed and applied.
11	1	6	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
11	2	1	Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
11	2	2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
11	2	3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.
11	2	4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.
11	2	5	Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.
11	2	6	Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.
11	2	7	Secure disposal or re-use of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been

Pictures from the Helsinki office

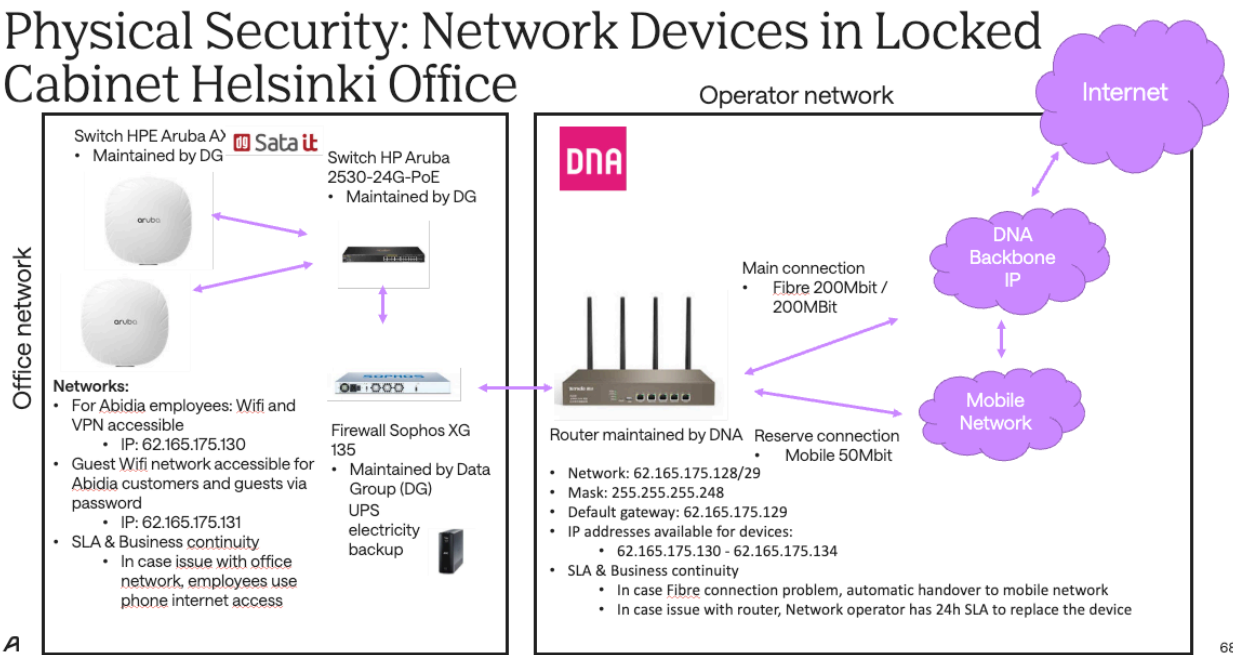




Physical Security: Network Devices in Locked Cabinet in Helsinki office

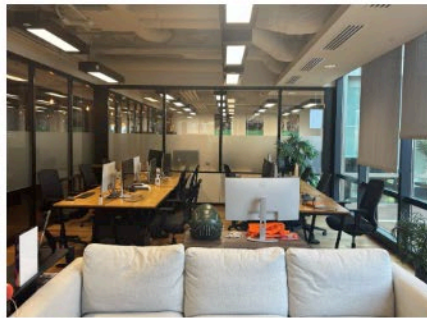
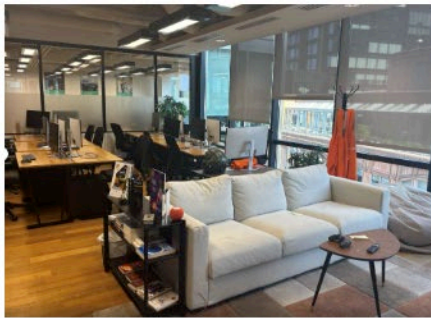


Physical Security: Network Devices in Locked Cabinet Helsinki Office

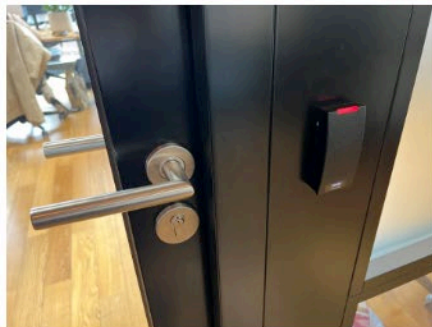




Pictures from the London Office



- The main building requires a keycard to go through the physical barriers. This card can only be acquired by pre-registration of employees.
- The door to the office requires the same keycard.
- Physical copies of confidential information are stored in locked safes.



3.2.5 CHANGE MANAGEMENT

Aibidia's Change Management process is a continuous process based on ITIL framework/principles. For every change created, there is an audit trail. Subject matter experts will review the change request. Risks will be assessed in the case of non-standard changes, and the change must be approved before it is implemented. After implementation, the change can be closed.

Change Management

Aibidia uses ITIL processes for change management workflows. High level change management workflow is described in the following picture

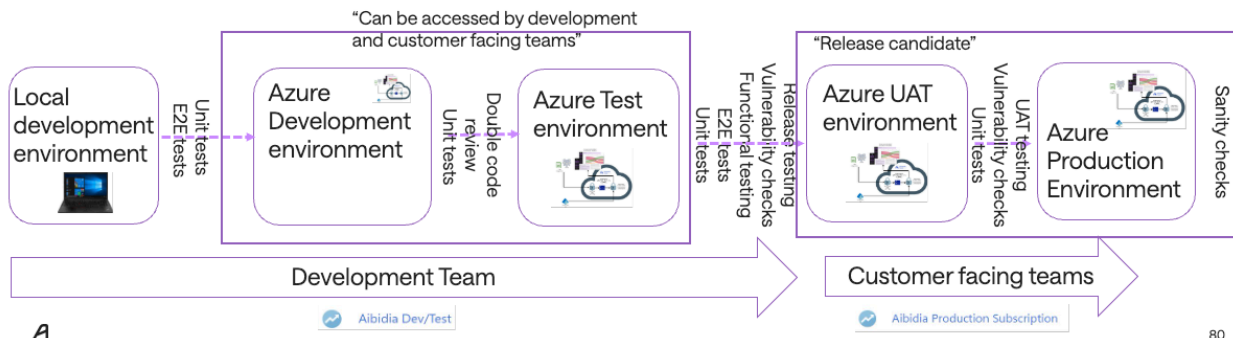




All changes are tested before rollout or production deployment according to quality assurance process described. Rollback and recovery procedures are based on Aibidia business continuity model that includes various levels of backups.

Quality Gates, Environments & QA Process

- ☐ Separate environments for development, testing and production
- ☐ Customer data resides only in production and user acceptance testing (UAT) environment
- ☐ Before any code is accepted, a code review is performed by at least one other developer
- ☐ Continuous integration (CI) and continuous deployment (CD) processes are in-place.
- ☐ The software is tested in our test environment by Quality Engineers and in UAT by substance experts
- ☐ After all the desired new features or fixes have been implemented and tested, a new version is released
- ☐ Developers and substance experts test the new version in production.
- ☐ Audit, performance and error analytics are automatically gathered
- ☐ Security tests including vulnerability checks



80

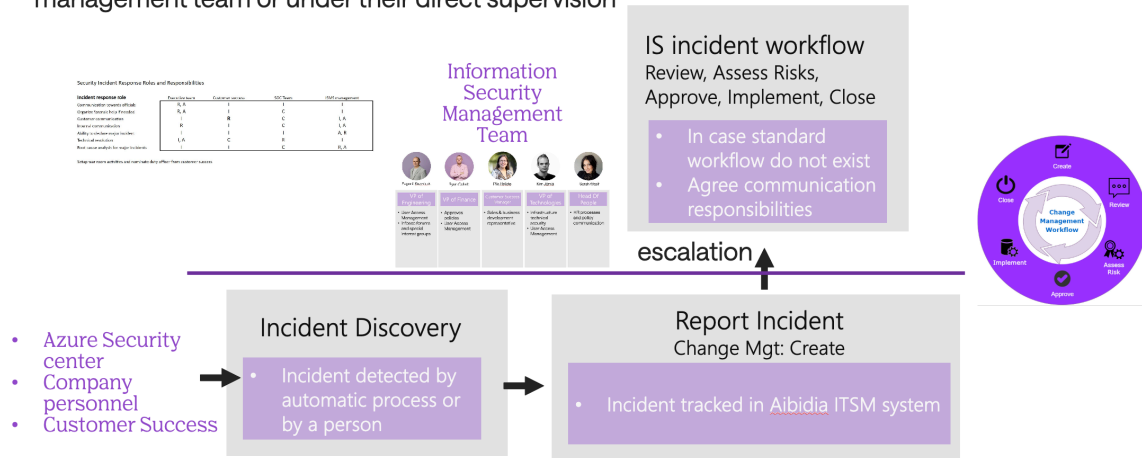
3.2.6 INFORMATION SECURITY INCIDENT RESPONSE

The Aibidia Information Security Incident Response workflow follows – on a high level – the Aibidia Change Management process. The phases: Review, Assess Risks, Approve, Implement, Close are conducted either by the Information Security Management team or under their direct supervision. Incidents are detected by automatic process or by person, the incident will be raised in the Aibidia ITSM system and escalated to the Information Security Incident Management workflow.



Information Security Incident Response

- Aibidia Information Security Incident Response workflow follows on high level Aibidia Change Management process
- Phases 2-6 (Review, Assess Risks, Approve, Implement, Close) are conducted either by IS management team or under their direct supervision



3.2.7 DATA BACKUP AND RECOVERY

Data backup and recovery are sub-processes within Aibidia's Business Continuity process

Aibidia's setup provides secure platform based on following components:

- Aibidia Transfer Pricing cloud is built on top of Microsoft Azure that has business continuity certificate ISO22301
- Aibidia configuration runs on three Availability Zones that tolerate hardware and network failures.

Aibidia Business continuity is based on the following activities:

- Aibidia takes customer data backups
- Incremental individual data changes back one week
- Cold weekly, monthly and yearly backups
- Optional: all documents can be exported as additional backup process to independent cloud service
- Escrow agreement for source code can be provided as extra service

Aibidia sees continuity management – and improvement - as a continuous process. Aibidia Security Operations Control team conducts business continuity rehearsal based on Information Security Management System yearly cycle.



Business Continuity

Secure platform

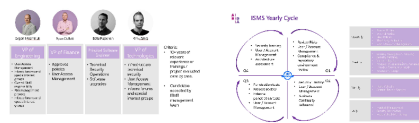
- Aibidia Transfer Pricing cloud is built on top of Microsoft Azure that has [business continuity certificate ISO22301](#)

Aibidia Business continuity

- Aibidia takes customer data backups
 - Incremental data changes back 14 days
 - Cold weekly, monthly and yearly backups
 - Stored 2 months, 6 months and 3 years
 - Optional: all documents can be exported as additional backup process to independent cloud service
 - Escrow agreement for source code can be provided as extra service

Aibidia business continuity as a continuous process

- Aibidia Security Operations Control team conducts business continuity rehearsal based on Information Security Management System yearly cycle



3.2.8 SYSTEM ACCESS MANAGEMENT

System access management is described in Aibidia **SaaS Access Control Policy** and follows Access Control process based on the Segregation of Duties.

SaaS Access Control Policy states that two organizations can grant access to Aibidia SaaS platform. One is the Customer controlling the customerdomain.com, who enables access for Aibidia login. The Customer can use their own access control process. The second organization is Aibidia controlling Aibidia personnel accessing customer environment. Aibidia uses defined access control process granting access to customer environments. Only named persons that have a need to serve the customer may be allowed access. Access requests are recorded and processed according to access control process. The Aibidia SaaS business owner of the SaaS data asset evaluates the requests and contacts the customer if needed. Aibidia SOC team performs actions according to the decision.

Access Control Process states that SOC team processes all Access Control Requests following the change management model. If the Access Control Policy documentation contains a description to evaluate the request, the team implements the request accordingly. If not, the case is escalated to the information owner described in the information asset inventory. Review of user rights is based on the yearly cycle.

In the TXM Platform, **segregation of duties** is implemented by segregating access control duties between the customer and Aibidia's Access Management team. The customer maintains SSO (AD) and provisions the user access. If customer's SSO team removes user rights, the user is not able to access Aibidia SaaS solution.

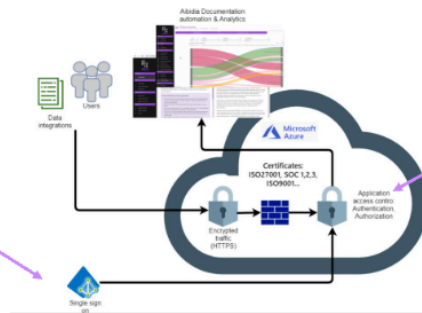
Aibidia Access management team provisions access to customer's SaaS environment. For the user to have access to Aibidia SaaS environment, the Customer Access Management

Aibidia

team and Aibidia Access management team must both grant access for the user.

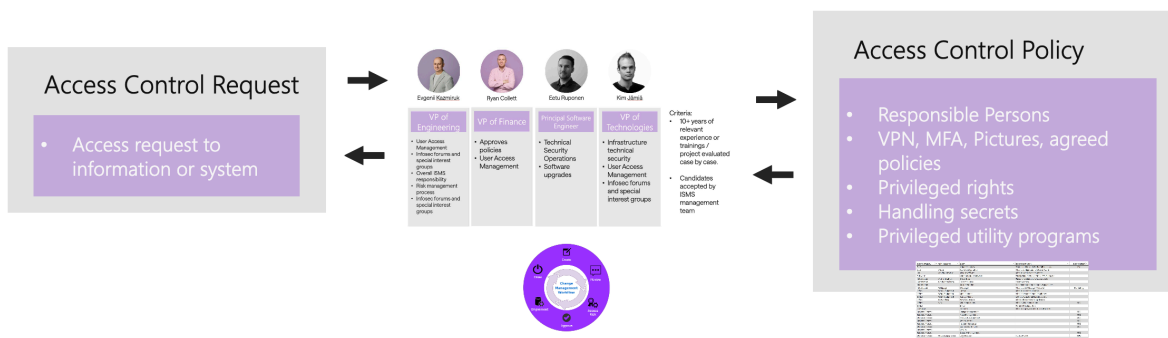
Access Control: Segregation of Duties

- Customer maintains SSO (AD) and provisions users
- If customer SSO team removes user rights the user is not able to access Aibidia SaaS solution



- Aibidia Access management team provisions access to customer SaaS environment
- For user to have access to Aibidia SaaS environment
 - Customer Access Management team has granted access
 - Aibidia Access management has granted access

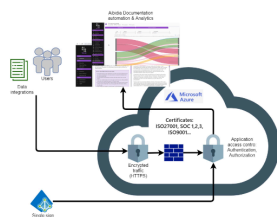
- SOC team processes all Access Control Request following the change management model
 - If Access Control Policy documentation contains description to evaluate request, the team implements the request accordingly
 - If not, the information the case is escalated to the information owner described in information asset inventory
 - Review of user rights based on yearly cycle



Two organizations can grant access to Aibidia SaaS platform:

1. **Customer** controlling customerdomain.com enables access for Aibidia login
 - Customer can use their own access control process
2. **Aibidia** controlling Aibidia personnel accessing customer environment
 - Aibidia uses defined access control process granting access to customer environment

Aibidia SaaS Access Control Policy: only named persons that have a need to serve customer may be allowed access. Access request is recorded and processed according to access control process. Aibidia SaaS data asset business owner evaluates the requests and contacts customer if needed. Aibidia SOC team performs actions according to the decision.



- SOC team processes all Access Control Request following the change management model
 - If Access Control Policy documentation contains description to evaluate request, the team implements the request accordingly
 - If not, the information the case is escalated to the information owner described in information asset inventory
 - Review of user rights based on yearly cycle



3.2.9 APPLICATION DEVELOPMENT

In the **software development**, Aibidia has adopted Microsoft Security Development Lifecycle and implements Practices from Cloud Governance Methodology.

Microsoft's Security Development Lifecycle (SDL) is a security assurance process focused on developing and operating secure software. The SDL provides detailed, measurable security requirements for developers and engineers at Microsoft to reduce the number and severity of vulnerabilities in their products and services.

Microsoft SDL consists of seven components including five core phases and two supporting security activities. The five core phases are requirements, design, implementation,

Aibidia

verification, and release. Each of these phases contains mandatory checks and approvals to ensure all security and privacy requirements and best practices are properly addressed.

- Requirements: Every product, service, and feature Microsoft develops starts with clearly defined security and privacy requirements; they're the foundation of secure applications and inform their design. [Development teams define these requirements based on factors such as the type of data the product will handle, known threats, best practices, regulations and industry requirements, and lessons learned from previous incidents](#)
- Design: Once the security, privacy, and functional requirements have been defined, the design of the software can begin. [As a part of the design process, threat models are created to help identify, categorize, and rate potential threats according to risk](#)
- Implementation: During this phase, developers write code according to the defined design while adhering to secure coding guidelines and best practices. [Tools such as static analysis can be used to automatically check code for common vulnerabilities](#)
- Verification: This phase involves testing the software to ensure that it meets all security and privacy requirements. This includes both manual and automated testing techniques such as fuzz testing, penetration testing, and code review 2
- Release: Before a product is released to customers, it undergoes a final security review to ensure that all security requirements have been met. [After release, the product is monitored for vulnerabilities and incidents are responded to according to an established incident response plan](#)

The two supporting security activities are training and response. Training is conducted before the core phases to ensure that developers are properly informed on security basics and recent trends in secure development. Response is conducted after the core phases to ensure that software remains secure after deployment.

Aibidia **R&D processes** use a modified version of the scaled agile method process where product strategy is defined by Aibidia executive team. Portfolio backlog management is performed by the cross-team Product Committee, the epic owners designing and managing the requirements process are typically substance experts. Features are derived from epics created by Lead Architects and Lead Developers together with Product Management. The development teams use Scrum methodology to develop the specified features. Cross team sprint planning is conducted every three weeks.

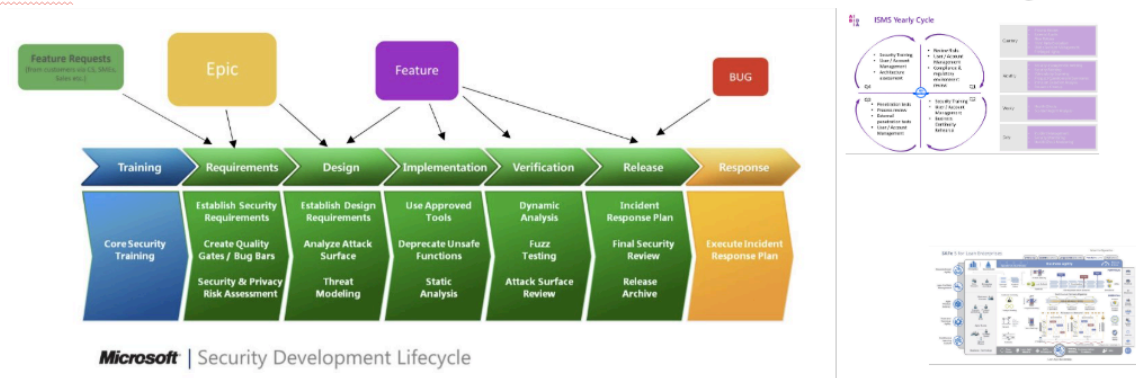
There are separate environments for development, testing and production. Customer data resides only in the production environment and in the user acceptance testing (UAT) environment. Before any code is accepted, a code review is performed by Aibidia senior developers. Continuous integration (CI) and continuous deployment (CD) processes are in-place. The software is tested in the test environment by Quality Engineers and in UAT by substance experts. After the Acceptance testing is finalized, the final version is released to the production environment.



Within the development processes, vulnerability checks, E2E tests, Unit tests and Double code review are applied to ensure quality of the final product.

Aibidia

Aibidia Software Development Process Security



Aibidia has adopted main characteristics from Microsoft Security Development Lifecycle (SDLC) into SaaS platform software development process, which is built in to the Aibidia R&D Process.

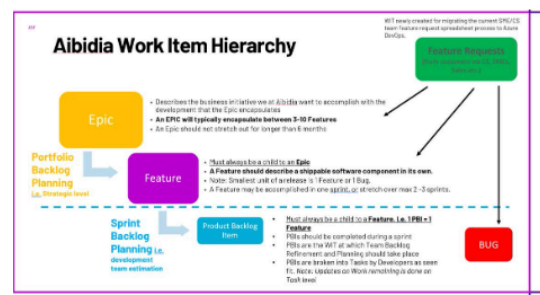
Practices from Cloud Governance Methodology

<https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/methodology>

Aibidia R&D Process

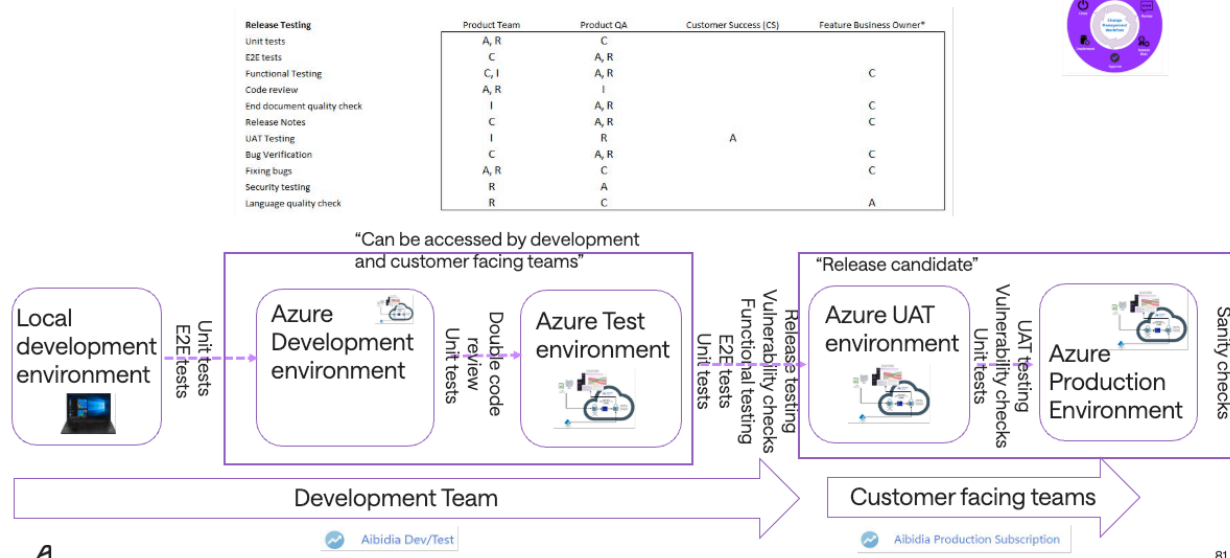
Aibidia uses R&D layout is using Product Teams

- Product strategy defined by Aibidia executive team
- Portfolio backlog management performed by Product Teams
- Epic owners designing and managing requirements process are typically substance experts
- Features derived from Epics by Lead Architects and Lead Developers with Product Management
- The development teams use Kanban methodology to develop the specified features
- Team backlog refinement conducted on weekly basis





Quality Gates, Environments & QA Process



81

3.2.10 RISK ASSESSMENT

Aibidia's general risk management methodology follows industry best practices. Risk assessments are performed according to the yearly cycle.

Risk Identification follows the Asset-Threat-Vulnerability model where the risk itself is a function of threats taking advantage of vulnerabilities to steal or damage assets. At Aibidia, the risks are assessed according to the following assets: Infrastructure (IT / Facilities), People, Organization, Processes, Information and Application. The threat to Aibidia's assets can be Theft, Accidental, Malicious, Malfunction or Inappropriate Use. A Vulnerability can be: Unattended Device, Disclosure, Breach of Policy, Interruption, Theft and Modification.

Risks are evaluated using two-dimensional likelihood and impact grading. Risk management methodology includes impact and likelihood analysis. Both dimensions have five steps and overall risk rating is categorized into three: High, Medium and Low. Impact is evaluated in relation to Confidentiality, Integrity and Availability.

Risks are documented into the Aibidia Risk management tool following modified logic.

There are the following **risk treatment** options: Avoid, Reduce, Transfer or Accept. Risk treatment is based on risk appetite. If risk is evaluated as High, it must be mitigated by default. If risk is Medium, the risk must be evaluated, and mitigation must be decided by relevant stakeholders. Risks evaluated as Low can be accepted by default.

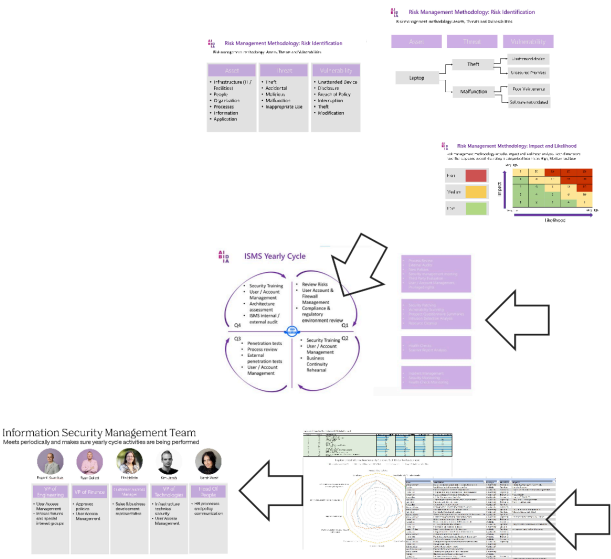
Risks are **reported** to the information security management Team.

The Aibidia yearly cycle includes **periodical review** of all risks and periodical identification of new risks.



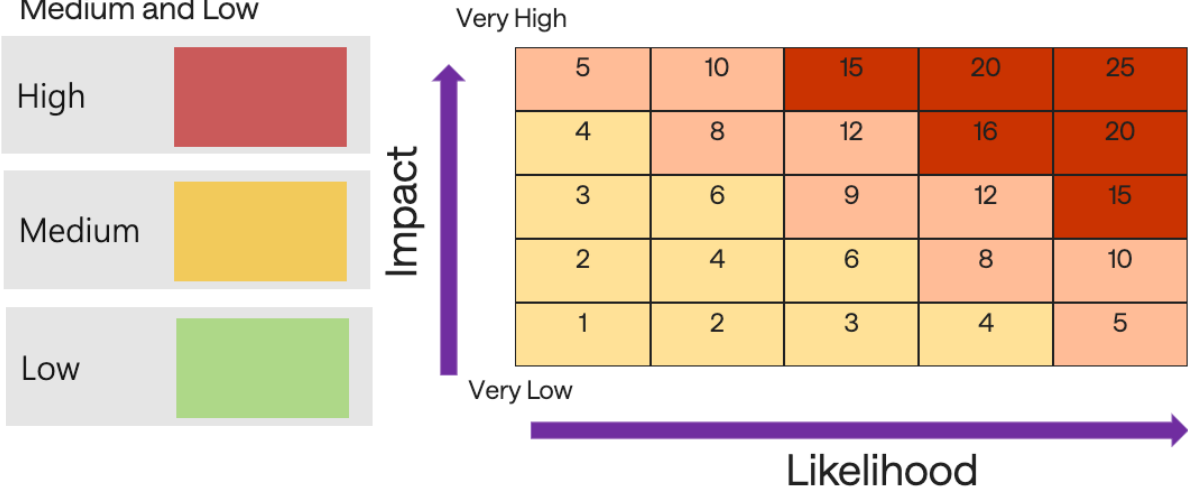
Risk Management Methodology: Summary

- Aibidia general risk management methodology summary:
- Follows industry best practices (Asset-Threat-Vulnerability)
 - Risks are evaluated using two dimensional likelihood and impact grading
- Aibidia yearly clock includes
- Periodical review of all risks
 - Periodical identification of new risks
- Risks are reported to information security management team



Risk Management Methodology: Impact and Likelihood

Risk management methodology includes impact and likelihood analysis. Both dimensions have five steps and overall risk rating is categorized into three: High, Medium and Low





Conducting a Risk Assessment: Documentation outcome

Risks are documented into Aibidia Risk management tool following modified logic

- <https://foundersshield.com/blog/risk-management/>

Treatment

- Avoid
- Reduce
- Transfer
- Accept

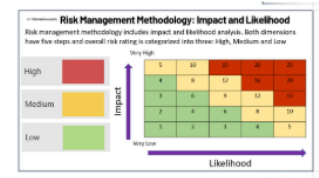
Risk appetite

- High: Mitigated by default
- Medium: Evaluated and decided by relevant stakeholders
- Low: Accepted by default

ID	Asset	Risk Description	Threat	Vulnerabilities	Risk Type	Risk Owner	Risk treatment
1	Cloud Resources	Malicious Outsider	Insider	Insider underlying cloud platform that is outside Aibidia control	Confidentiality	Engineering	Transfer
2	Cloud Resources	Confidence	Unable to pay for cloud resources due to cashflow	Availability	Operations	Reduce	
3	Azure Configuration	Human Error	Insider configuration vulnerable for insider hackers	Confidentiality	Engineering	Reduce	
4	Azure Configuration	Human Error	Change made to configuration causes SaaS to be not available	Confidentiality	Engineering	Reduce	
5	Aibidia Software	Human Error	Insider configuration vulnerable for insider hackers	Confidentiality	Engineering	Reduce	
6	Aibidia Software	Process Error	Outdated libraries contain vulnerabilities	Confidentiality	Engineering	Reduce	
7	Overseas	Cyber Attack	Overseas get accidentally published, stolen, leaked or hacked	Confidentiality	Engineering	Reduce	
8	Customer Data	Cyber Attack	Data leaked while in transit or stored	Confidentiality	Engineering	Reduce	
9	Documentation	Process Error	Documentation is wrong or outdated	Confidentiality	Operations	Reduce	
10	Laptop	Malicious Outsider	Laptop gets stolen. Harddrive data available for outsiders	Confidentiality	Engineering	Reduce	
11	Laptop	Malicious Outsider	Public places outsider might see data from screen	Confidentiality	Operations	Reduce	
12	Laptop	Cyber Attack	Non wanted software installed to Laptop	Confidentiality	Operations	Reduce	
13	Laptop	Malicious Outsider	WiFi	Confidentiality	Operations	Reduce	
14	Communication Software	Malicious Outsider	Outsider tries to get information used in communications	Confidentiality	Engineering	Reduce	
15	Mobile Phone	Human Error	Mobile phone gets lost or stolen and is misused	Confidentiality	Engineering	Reduce	
16	Mobile Phone	Human Error	Mobile phone gets lost or stolen and MFA does not work	Availability	Engineering	Reduce	
17	Storage Media	Human Error	USB stick gets lost and data is misused	Confidentiality	Operations	Reduce	
18	Office	Human Error	Office keys or badges are lost and misused	Confidentiality	Operations	Reduce	
19	Network Devices	Hardware Failure	Network device does not work and unable to work	Availability	Operations	Reduce	
20	Azure Configuration	Human Error	Configuration problem makes Azure resources unavailable	Confidentiality	Engineering	Reduce	
21	Cloud Resources	Malicious Outsider	External denial of service (DDoS) attack	Availability	Engineering	Reduce	

Risk Management Methodology: Impact and Likelihood

The definitions for impact and likelihood in Aibidia risk management model are defined as follows



Impact

1. **Negligible:** This risk will hardly impact your project.
2. **Low:** You can easily handle the consequences of this risk.
3. **Moderate:** It will take some time and effort to mitigate the consequences of this risk.
4. **Significant:** This risk could cause long-term consequences that will be hard to recover from.
5. **Catastrophic:** The impact of this risk might wreck your project.

Likelihood

1. **Very unlikely:** A very slim chance for this risk to occur.
2. **Not likely:** Low chances for this risk to occur
3. **Possible:** Fifty-fifty chances for this risk to occur
4. **Probable:** Good chances for this risk to occur.
5. **Very likely:** You can bet this risk will occur at some point

3.2.11 INFORMATION AND COMMUNICATION

Information and communication aspects are described in **Aibidia Information**

Classification: Definitions. The definitions for the information classification are described in the chapter Data (earlier in the document).

Aibidia provides requirements on the handling of the information based on classification. Information classified as **Public** can be handled without any restrictions. Information classified as **Internal** must be kept on SharePoint only and cannot be shared externally.

Company confidential information must be kept on SharePoint only. Employees must work with screen protection; the information cannot be shared with anybody who is not authorized.



In case of doubt employees are encouraged to ask the company Slack channel #security. In case of loss of information, #security must be informed.

Client confidential information must be kept on SharePoint only. Employees must work with screen protection; the information cannot be shared with anybody who is not authorized. In case of doubt employees are encouraged to ask #security. In case of loss of information, #security must be informed.

Aibidia Information Classification: Definitions

- **Public**
 - Information that is not confidential and is intended for public use
 - Examples: Marketing materials, Materials on public website
- **Internal**
 - Information that is required in everyday work tasks and is intended to Aibidia personnel
 - Valid work contract and NDA is required to access internal information
 - Examples: Slack-messages in non-private channels, Wiki-pages
- **Company Confidential**
 - Information collected and processed by Aibidia for conducting business activities, e.g. information on employees and salaries, customer contracts and invoicing as well as company financing. Access is restricted to only named personnel on need to know basis. Confidentiality, integrity and availability of company confidential personnel. Confidentiality, integrity and availability of company confidential information are important for conducting business activities without interruptions
 - Examples: Client contracts and proposals, source code, business plans, passwords for critical IT systems, client contact records, accounts etc.
- **Customer Confidential**
 - Customer owned data in Aibidia's possession. Customer confidential information can be accessed only if requested by customer for support purposes. Confidentiality, integrity and availability of customer confidential information are vital for ensuring customer trust and for complying with contract requirements
 - Examples: Customer data stored in Aibidia SaaS solution

If you don't know the classification of the information that you process in your work tasks, ask the information owner or your supervisor. Any information without proper classification must be handled as internal until the information owner confirms the classification.

When distributing, communicating or transferring classified information, by means of acceptable handling instructions, the sender is responsible of ensuring that the recipient knows the information classification and the respective handling instructions.

Aibidia Information Classification: Handling

Classification	Example Data / Systems	Instructions
Public	Website www.aibidia.com	No restrictions
Internal	- Knowledge hub - Any kind of internal document	- Keep on SP only - Don't share externally
Company confidential	- Benchmarking files - HubSpot / Salesforce - Future CS system Personio - Breezy recruiting	- Keep on SP only - Work with screen protection - Don't share with anybody not authorized - In case of doubts, ask #security - In case of loss of information, inform #security
Client confidential	- Client project data and files (e.g. Kemira) - Certain proposal documents - Client conversion data	- Keep on SP or in client environment only - Work with screen protection - Don't share with anybody not authorized - In case of doubts, ask #security - In case of loss of information, inform #security

Aibidia

3.2.12 CRYPTOGRAPHY POLICY, KEY AND SECRET MANAGEMENT POLICY, ENCRYPTION: IN TRANSIT AND AT REST

Aibidia has a cryptography policy covering managing and use of keys and algorithms in various contexts.

Generally, keys are managed in Microsoft Azure Key Vault. Data in transfer (in untrusted networks) is always protected by TLS 1.2 with a combination of symmetric and asymmetric keys (key length: 2048). For Microsoft SQL server as a service data is encrypted in transit using TLS, and encrypted at rest, can be encrypted using Azure TDE

For Microsoft Office 365, Email, Office documents are not encrypted by default. Aibidia use standard functionality when sending sensitive information.

On Laptops, Aibidia uses BitLocker with AES-128

Cryptography Policy

- ☐ **Key Management**
 - ☐ Microsoft Azure
- ☐ **Data in transfer: TSL 1.2**
 - ☐ Forced TLS between Aibidia SaaS and customers
 - ☐ Combination of symmetric + asymmetric encryption
 - ☐ Asymmetric key: 2048 bits
- ☐ **Microsoft SQL server as a service**
 - ☐ [Security overview](#): encrypted in transit using TLS and encrypted at rest are encrypted using [Azure TDE](#)
- ☐ Blob Storage
- ☐ **Microsoft Office 365**
 - ☐ Email, Office documents
 - ☐ Not encrypted by default. Use standard functionality when sending sensitive information
- ☐ **Laptops**
 - ☐ Bitlocker
 - ☐ AES-128



Key Management

- Microsoft Azure Key Vault
- <https://docs.microsoft.com/en-us/Azure/keyvault/general/basic-concepts>
- Provides Access Control and Audit Logs
- SOC team creates and deletes keys
- Product SaaS containing client data
- Only selected SOC Team members have access
- In case key is compromised, SOC team follows information security incident process.



Key and Secret Management Policy

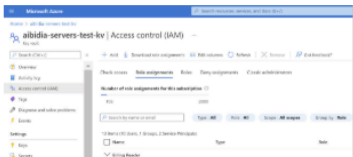
Cryptography and Key Management

- Laptop encryption keys
- Email encryption
- Certificates
- Azure Encryption keys
- Azure Encryption Deletion

	SOC Team	ISMS Management	Office IT provider
	I	A	R
	R	A	
	R	A	
	R	A	
	R	A	

Key Management

- Microsoft Azure Key Vault
 - <https://docs.microsoft.com/en-us/azure/key-vault/general/basic-concepts>
 - Provides Access Control and Audit Logs
- SOC team creates and deletes keys
 - Product SaaS containing client data
 - Only selected SOC Team members have access
 - In case key is compromised, SOC team follows information security incident process



Encryption: in transit and at rest

<https://docs.microsoft.com/en-us/learn/modules/intro-to-security-in-azure/>

Encryption

8 minutes

For most organizations, data is the most valuable and irreplaceable asset. Encryption serves as the last and strongest line of defense in a layered security strategy.

Contoso Shipping knows that encryption is the only protection its data has once it leaves the data center and is stored on mobile devices that could potentially be hacked or stolen.

What is encryption?

Encryption is the process of making data unreadable and unusable to unauthorized viewers. To use or read the encrypted data, it must be decrypted, which requires the use of a secret key. There are two top-level types of encryption: **symmetric** and **asymmetric**.

Symmetric encryption uses the same key to encrypt and decrypt the data. Consider a desktop password manager application. You enter your passwords and they are encrypted with your own personal key (your key is often derived from your master password). When the data needs to be retrieved, the same key is used, and the data is decrypted.

Asymmetric encryption uses a public key and private key pair. Either key can encrypt but a single key can't decrypt its own encrypted data. To decrypt, you need the paired key. Asymmetric encryption is used for things like Transport Layer Security (TLS) (used in HTTPS) and data signing.

Both symmetric and asymmetric encryption play a role in properly securing your data. Encryption is typically approached in two ways:

1. Encryption at rest
2. Encryption in transit

Encryption in transit

Data in transit is the data actively moving from one location to another, such as across the Internet or through a private network. Secure transfer can be handled by several different layers. It could be done by encrypting the data at the application layer prior to sending it over a network. HTTPS is an example of application layer in transit encryption.

You can also set up a secure channel, like a virtual private network (VPN), at a network layer, to transmit data between two systems.

Encrypting data in transit protects the data from outside observers and provides a mechanism to transmit data while limiting risk of exposure.

This diagram shows the process. Here, customer data is encrypted as it's sent over the network. Only the receiver has the secret key that can decrypt the data to a usable form.

3.2.13 MONITORING

Monitoring, measurement, analysis and evaluation at Aibidia is performed according to the ISMS yearly cycle. The management team is responsible for analyzing the results. Monitoring, measurement, analysis and evaluation is described in Aibidia risk management tool. Aibidia has, among others, a target to complete the following activities according to the plan in the yearly cycle:

- Management reviews
- Risk reviews
- Review of security policies
- Reviews of users and accounts



Additionally, there are regular measurements based on Azure security score. Security Monitoring & Health Check Monitoring are performed daily. Third party performance is reported to the information security management team on a quarterly basis as part of the standard process.

Monitoring, measurement, analysis and evaluation

- ISMS management team is responsible for analyzing results
- Monitoring, measurement, analysis and evaluation described in Aibidia risk management tool

Information Security Management Team

Meets periodically and makes sure yearly cycle activities are being performed



IS Management team agenda

• Action time process meeting

• Drafting and delivery

• Final review meeting

• Feedback from experts and customer parties

• Security update and risk assessment

• Risk updates

• Control updates

• QHSE management and results

• Other open internal and external issues

• Organizational process updates

• Risk management process identified risks

• Risk management process updates

• Risk management process updates

• Risk management process updates

• Risk management process updates

• Risk management process updates

• Risk management process updates

Measurement Principle	Measurement target	Frequency of measurement	Source	Format of indicator	Reporting target	Management indicator	KPI value
The ISMS management team is committed to its monitoring responsibility of all responsibility for the information security management system	Management review's compliance according to risk policy cycle	Quarterly	Manual inspection indicating the management review conducted according to this policy cycle	Green/Yellow/Red		Green/Yellow/Red	Green
Information security risks are identified and managed to prevent business continuity	Risk reviews completed according to ISMS policy cycle	Quarterly	Manual inspection indicating the risk management review conducted according to ISMS policy cycle	Green/Yellow/Red			
Service availability	Service availability		Service availability from Aibidia A	High over time			
Security policies and associated compliance expectations are documented and the employees and contractors in security monitoring and employment contracts, and by customer and supplier's framework agreements and contracts	Security policy reviewed according to ISMS policy cycle	Annually	Manual inspection to policy updated according to ISMS policy cycle				
Access to systems and resources is based on the security principle of information confidentiality and the need-to-know	Access control management system compliance according to ISMS policy cycle	Two times a year	Ticket information received from the stakeholders				
Information is classified and handled according to appropriate security levels, and personal data is processed according to the General Data Protection Regulation	None identified						
Security is built into the design, development and acquisition of digital services requested by users	Azure security score	Quarterly	Azure Defender portal				
Networks and devices are segmented, protected, monitored and managed in accordance with network security recommendations	Azure firewall rule engine (Firewall) and Azure configuration	Annually	Azure configuration				
Security incidents are reported and handled in accordance with incident response recommendations	Reported security incidents and incident statistics	Quarterly	Slack channel information				

3.2.14 HUMAN RESOURCES SECURITY

Aibidia Human Resource Security consists of background checks prior to employment where the documents are checked, and references are contacted. The employment contract contains a confidentiality clause. During employment employees are provided with security awareness where updates are communicated via email and slack.

The disciplinary process gives the employee the possibility to improve. There is given a written notice on the lack of improvement. On termination of employment, the account is disabled and the employee no longer has access to Aibidia system.

© 2026 KPMG Oy Ab, a Finnish limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

39



Human Resource Security

Summary of Aibidia Human Resources Security

1. Background checks
 - Check documents, Call references
2. Employment Contract
 - Confidentiality
3. Awareness
 - Updates communicated via slack & email
4. Disciplinary
 - Give possibility to improve, then written notice
5. Termination
 - Accounts are disabled → No access to systems

Human resource security			
7	1	1	Screening
7	1	2	Terms and conditions of employment
7	2	1	Management responsibilities
7	2	2	Information security awareness, education and training
7	2	3	Disciplinary process
7	3	1	Termination or change of employment responsibilities

3.3 Complementary User Entity Controls

Aibidia TXM Platform was designed with the assumption that certain controls would be implemented by its customers (user entities). The application of such controls by user entities is necessary to achieve certain criteria included in this report. This section describes other internal controls that should be in operation at user entities to complement the internal controls at Aibidia. User entities and their auditors should consider whether the following internal controls are present and operating effectively. The user entity control considerations presented here should not be regarded as a comprehensive list of controls that should be employed by user entities.

Aibidia Cloud Environment

Secure cloud application in Microsoft Azure

Aibidia Transfer Pricing Cloud is built on Microsoft Azure. Microsoft Azure Compliance Certificates:

- ISO27001, ISO27017, ISO27701, SOC 1, SOC 2, SOC 3, PCI DSS 3.2, ISO22301, ISO9001, Azure CIS
- See complete listing here: <https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/>
- Azure Security: <https://azure.microsoft.com/en-us/overview/security/>
- Aibidia Privacy Policy <https://aibidia.com/privacy-policy/>
- Aibidia Terms of Service <https://aibidia.com/terms-of-service/>



Aibidia Certified Information Security Management System

- Certified according to ISO27001:2013 Continuous process
- Regular meetings: participation from organization branches ISMS mgt team: Incident reporting, document reviews, process & policy updates

Certification number
FI220630-107

Several Annual External Audits

- Conducted by Third party information security experts
- Cover Aibidia Transfer Pricing Execution management system

SecOps: Information Security Built into DevOps practices

- Microsoft Defender for Cloud Activated
- Software DevOps processes follow industry best practices
- Automatic vulnerability scanners
- Regular information security trainings in the company



A

Logical access controls



Since the TXM Platform offers SSO for authenticating customers' users, the security model of the TXM Platform is dependent on the customers strength of identifying, registering, authorizing and authenticating its employees.

Incident management

Customers are responsible for informing Aibidia timely on any errors or incidents they have detected

3.4 Subservice Organizations

Aibidia's TXM Platform is based on Microsoft Azure cloud environment, hence, there is a strong dependency on the practices and security with which Microsoft design, build and operate their cloud offerings. However, controls of Azure relate to the cloud infrastructure services used by Aibidia are relevant to Aibidia's achievement of its services commitments and certain trust services criteria and have been considered by Aibidia in designing and implementing the control environment as complementary subservice organization controls.

Microsoft Azure is responsible for protecting the infrastructure that runs all of the services offered in the cloud environment. This infrastructure is composed of the hardware, software, networking and facilities that run the cloud services. According to this mode physical and environmental controls are fully operated by Azure while controls related to logical access, system operations etc. are shared between Azure and Aibidia.

While designing and implementing its controls, Aibidia has assumed that Azure has implemented the following controls:

- CC2.2 Internal communication of information, responsibilities and objectives for internal control, such as policies, guidelines and training
- CC6.1 Implements logical access security software, infrastructure and architectures over protected information assets that are Azure's responsibility
- CC6.2 Prior to issuing system credentials and granting access to systems that are Azure's responsibility, registers and authorizes new internal and external users whose access is administered by Azure. For those users whose access is administered by Azure, user system credentials are removed when user access is no longer authorized.
- CC6.3 Azure authorizes, modifies or removes access to protected information assets that are Azure responsibility based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties
- CC6.4 Azure restricts physical access to its facilities and protected information assets
- CC6.5 Azure discontinues logical and physical protections over physical assets only after the ability to read or recover data and software is no longer required
- CC6.6 Azure implements logical access security measures to protect against threats from sources outside its system boundaries

Aibidia

- CC6.7 Azure restricts the transmission, movement and removal of information that it is responsible for to authorize internal and external users and processes, and protects it during transmission, movement or removal
- CC6.8 Azure implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software in the systems that it is responsible for
- CC7.1 Azure uses detection and monitoring procedures to identify changes to the configurations that result in the introduction of new vulnerabilities, and susceptibilities to newly discovered vulnerabilities related to systems that are Azure's responsibility
- CC7.2 Azure monitors system components that are its responsibility and the operation to those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives
- CC7.3 Azure evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives and, if so, takes actions to prevent or address such failures
- CC7.4 Azure responds to identified security incidents by executing a defined incident response program to understand, contain, remediate and communicate security incidents, as appropriate
- CC7.5 Azure identifies, develops and implements activities to recover from identified security incidents
- CC8.1 Azure manages changes to infrastructure, data, software, and procedures that are Azure responsibility

In addition to Azure, Data Group is considered a subservice organization within Aibidia's control environment. Data Group is responsible for leasing and managing Aibidia devices, including provisioning of laptops, associated software licenses, and providing lifecycle support services such as installation, maintenance, and secure wiping of devices. These responsibilities contribute to the achievement of Aibidia's service commitments and relevant Trust Services Criteria, particularly those related to Logical and Physical Access Controls (CC6.1, CC6.2, CC6.7), System Operations (CC7.1), and Change Management (CC8.1). The controls operated by Data Group are considered complementary subservice organization controls and have been evaluated by Aibidia as part of the overall design and implementation of its control environment.

SECTION IV



Description of Control Objectives, Related Controls and Test Results of Independent Auditor

Information Provided by the Independent Auditor

Our examination was conducted in accordance with the International Standard on Assurance Engagements (ISAE) 3000, “Assurance Engagements Other Than Audits or Reviews of Historical Financial Information” issued by the International Auditing and Assurance Standard Board (IAASB).

It is the responsibility of every user entity to evaluate the information on the controls within its organization in order to obtain an understanding of these controls and gauge the internal control risks. The controls of both Aibidia and the user entities must be evaluated together. If user entities do not have suitable controls, the controls of Aibidia do not serve as compensation for such a deficiency in the controls.

Aibidia management has analysed the exceptions presented in Section IV and provided responses to the findings. KPMG has not evaluated these responses and does not present an opinion on them.

Testing Procedures

The control environment represents the collective effect of various elements in establishing, enhancing, or mitigating the effectiveness of specific controls. Tests of the control environment included the following procedures, to the extent we considered necessary: (a) management inquiry and inspection of Aibidia’s organizational structure and policy statements; (b) interviews with management, control operators and other personnel responsible for developing, ensuring adherence to, and applying controls; (c) observation of personnel in the performance of their assigned activities; and (d) inspection of actions taken by the management to improve controls. The control environment was considered in determining the nature, timing, and extent of the testing of controls relevant to achievement of the service commitments and system requirements.

Tests performed in connection with evaluating the design and operating effectiveness of controls detailed in Section IV are described below:

Type of Test	Description
Inquiry	Discussed the controls with control operators and/or management responsible for developing, adhering to, and applying the controls to ascertain their understanding and compliance. As inquiries were performed for substantially all controls, this test was not listed individually for every control listed in the tables below.
Observation	Observed the operation of specific controls.
Inspection	Inspected documentation, reports, and other artefacts indicative of the operation of the controls.



Applicable Trust Services Principles

The following Trust Services Criteria categories are covered by the report:

- Security (S): Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to achieve its objectives.

Tests performed in connection with evaluating the design and operating effectiveness of controls detailed in Section IV correspond to the applicable criteria as follows:

Criterion ID	Criterion	Controls
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	A.5.1 A.5.2 A.5.4
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	A.5.2 A.6.3 CC1.2.1
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	A.5.2 A.5.3
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A.6.1 A.6.2 A.6.3 CC1.4.1
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A.6.2 A.6.4
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	A.5.10 A.5.12 A.5.13 A.5.32
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	CC2.2.1 A.5.6
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	A.6.8 CC2.3.1
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	A.5.5 A.5.36 CC3.1.3
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	A.5.4 CC3.2.1 CC3.2.2



CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	CC3.2.1
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	A.5.22 A.5.31 CC3.4.1
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	CC4.1.1
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	CC4.2.1
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	CC5.1.1
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	CC5.1.1
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	A.5.37
CC6.1	Logical and physical access: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	A.5.9 A.5.16 A.5.17 A.5.34 A.6.5 A.6.6 A.8.3 A.8.11 A.8.20 A.8.21 A.8.22 A.8.27
CC6.2	Logical and physical access: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	A.5.15 A.5.18
CC6.3	Logical and physical access: The entity authorizes, modifies, or removes access to data, software, functions, and other protected	A.8.2 A.8.18



	information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
CC6.4	Logical and physical access: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	A.5.11 A.7.1 A.7.2 A.7.3 A.7.4 A.7.5 A.7.6 A.7.7 A.7.8 A.7.9 A.7.10 A.7.11 A.7.12 A.7.13 A.7.14
CC6.5	Logical and physical access: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	A.8.10
CC6.6	Logical and physical access: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	A.6.7 A.8.5 A.8.23
CC6.7	Logical and physical access: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	A.5.14 A.5.33 A.8.1 A.8.12 A.8.24
CC6.8	Logical and physical access: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	A.8.4 A.8.7 A.8.16 A.8.17 A.8.19
CC7.1	System operations: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	A.8.9 A.8.16
CC7.2	System operations: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's	A.5.7 A.8.8 A.8.15 A.8.16



	ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	
CC7.3	System operations: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	A.5.24 A.5.25
CC7.4	System operations: The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.	A.5.26 A.5.27 A.5.28 A.5.29 A.5.34
CC7.5	System operations: The entity identifies, develops, and implements activities to recover from identified security incidents.	A.5.26 A.5.30 A.8.13
CC8.1	Change management: The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	A.5.8 A.5.34 A.5.35 A.8.4 A.8.6 A.8.26 A.8.28 A.8.29 A.8.33 A.8.34
CC9.1	Risk mitigation: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	A.8.13 A.8.14 CC9.1.1 CC9.1.2
CC9.2	Risk mitigation: The entity assesses and manages risks associated with vendors and business partners.	A.5.19 A.5.20 A.5.21 A.5.22 A.5.23



Testing Results

Control ID	Control Description	Testing Procedures	Testing Results
A.5.1	Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Inspected the Information security policy to determine that it is defined, approved by management and published. Inquired about how the information security policy is communicated to and acknowledged by relevant personnel and were informed that the information security policy is communicated to all employees during all hands meeting.	No exceptions noted.
A.5.2	Information security roles and responsibilities shall be defined and allocated according to Aibidia needs.	Inspected the general information security policy to determine that information security roles and responsibilities are defined and allocated according to Aibidia needs.	No exceptions noted.
A.5.3	Conflicting duties and conflicting areas of responsibility shall be segregated.	Inspected the security policy to determine that roles and responsibilities of different teams have been defined. Inspected the Incident response plan to determine that step-by-step guide to follow when an incident is	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
		suspected and confirmed has been defined. Inspected the risk management policy to determine that risk management R&D processes have been defined.	
A.5.4	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of Aibidia.	Inspected the security policy to determine that roles and responsibilities of different teams have been defined. Inspected the Incident response plan to determine that step-by-step guide to follow when an incident is suspected and confirmed has been defined. Inspected the risk management policy to determine that risk management R&D processes have been defined.	No exceptions noted.
A.5.5	Aibidia shall establish and maintain contact with relevant authorities.	Inquired about the authorities relevant and were informed that the police, Information Security government office, Government	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
		information cybersecurity are the relevant authorities. Inspected the applicable laws and regulation and noted that contact information of relevant authorities have been documented. Inquired if there has been any case that has been reported to the relevant authorities during the audit period and were informed that there have been none.	
A.5.6	Aibidia shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Inspected that Aibidia monitors information available through the relevant interest groups and communication channels to support awareness of the threat landscape and identify possible relevant vulnerabilities.	No exceptions noted.
A.5.7	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	Inspected that responsible personnel at Aibidia receive and analyse information from the security-related communication channels to support awareness of the threat landscape and identify possible relevant vulnerabilities.	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
A.5.8	Information security shall be integrated into project management.	Inspected that Aibidia monitors information available through the relevant interest groups and communication channels to support awareness of the threat landscape and identify possible relevant vulnerabilities.	No exceptions noted.
A.5.9	An inventory of information and other associated assets, including owners, shall be developed and maintained.	Inspected the inventory of information-related assets and applicable policies and noted that those assets are properly maintained.	No exceptions noted.
A.5.10	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	Inspected the Information Security Policy for Employees to determine that the Acceptable Use Policy is defined, documented, and communicated to all employees.	No exceptions noted.
A.5.11	Personnel and other interested parties as appropriate shall return all Aibidia's assets in their possession upon change or termination of their employment, contract or agreement.	Inspected the offboarding checklist for the employees who have left the organization to determine that the return of assets was included and documented as part of the offboarding process.	No exceptions noted.
A.5.12	Information shall be classified according to the information security needs of Aibidia based on confidentiality, integrity, availability	Inspected Aibidia information classification definitions to determine that the relevant classification criteria and instructions for	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
	and relevant interested party requirements.	information handling are defined for each classification type.	
A.5.13	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by Aibidia.	Inspected that the documentation classification is defined and documented in the policy. For a sample of ISMS-related documentation, inspected that the documents were labelled.	No exceptions noted.
A.5.14	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within Aibidia and between Aibidia and other parties.	Inspected that the transfer of information is part of the standard cloud service provider Terms of Service agreement. Inspected that the transfer of information is performed within the secured cloud environment. Communications are established through the dedicated secure channels.	No exceptions noted.
A.5.15	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	Inspected the access control policy and noted that the physical and logical access to assets is managed. Inspected that Aibidia's internal networks are secured with	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
		passwords, and VPN is required for external connections.	
A.5.16	The full life cycle of identities shall be managed.	Inspected the access control policy and a sample of Aibidia's users for their access rights.	No exceptions noted.
A.5.17	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	Inspected the access control policy and information security policy and noted that authentication information is managed.	No exceptions noted.
A.5.18	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	For a sample of new employees inspected their access rights requests tickets and related security groups. Inspected annual access rights review tickets and memos.	No exceptions noted.
A.5.19	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Inspected the Third Party Management Policy and noted that risk assessment is performed as part of the vendor assessment when accepting a new supplier. Inspected a sample of supplier reviews.	During the sample testing it was noted that no supplier review was done due to inactivity from the supplier. <i>Management response:</i> <i>Management acknowledges the finding. The supplier review was</i>



Control ID	Control Description	Testing Procedures	Testing Results
			<i>not completed because the supplier was inactive; however, Aibidia agrees that the status and rationale should have been documented. formally Aibidia will update the supplier review process to require documented review outcomes for all in scope suppliers, including cases where a supplier is inactive, no longer used, or pending termination. Inactive suppliers will either be formally removed from the active supplier register or marked as inactive with documented rationale. This enhancement will be implemented by Q3 2026.</i>
A.5.20	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	Inspected list of new vendors and that Aibidia had created tickets and checked relevant information security documents from the vendors.	During the sample testing it was noted that one ticket for onboarding new supplier has not been completed. <i>Management response:</i> <i>Management acknowledges the finding. The onboarding ticket for the new supplier was not completed as required. Aibidia will</i>



Control ID	Control Description	Testing Procedures	Testing Results
			reinforce the supplier onboarding workflow so that supplier onboarding cannot be considered complete until required security and information contractual checks have been documented and approved. The open ticket will be reviewed and completed, and the supplier onboarding checklist will be updated to clarify mandatory evidence requirements. Completion of this remediation is targeted for Q3 2026. As the supplier onboarding ticket was not completed, the related monitoring and change management evidence was also incomplete. Aibidia will ensure that supplier onboarding, monitoring, and change management activities are linked within the supplier management process so that key supplier information, risk classification, review frequency, and monitoring requirements are documented at onboarding. The existing supplier record will be remediated and the process



Control ID	Control Description	Testing Procedures	Testing Results
			<i>update will be completed by Q3 2026.</i>
A.5.21	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Inspected a sample of the supplier service agreements for key service providers and noted that the security obligations clauses were included in the agreements.	No exceptions noted.
A.5.22	Aibidia shall regularly monitor, inspect, evaluate and manage change in supplier information security practices and service delivery.	Inspected that the supplier review process is in place.	During the sample testing it was noted that one ticket for onboarding new supplier has not been completed. <i>Management response:</i> <i>Management acknowledges the finding. The onboarding ticket for the new supplier was not completed as required. Aibidia will reinforce the supplier onboarding workflow so that supplier onboarding cannot be considered complete until required security and information contractual checks have been documented and approved. The open ticket will be reviewed and completed, and the supplier onboarding checklist will</i>



Control ID	Control Description	Testing Procedures	Testing Results
			be updated to clarify mandatory evidence requirements. Completion of this remediation is targeted for Q3 2026. As the supplier onboarding ticket was not completed, the related monitoring and change management evidence was also incomplete. Aibidia will ensure that supplier onboarding, monitoring, and change management activities are linked within the supplier management process so that key supplier information, risk classification, review frequency, and monitoring requirements are documented at onboarding. The existing supplier record will be remediated and the process update will be completed by Q3 2026.
A.5.23	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with Aibidia's information security requirements.	Inquired and noted that the cloud services follow the standard supplier management process. Inspected the Vendor Management Policy and noted that the full supplier	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
		lifecycle management process is defined and documented.	
A.5.24	Aibidia shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Inspected the Information Security Incident Response procedure to determine that the relevant guidelines are defined and communicated to the employees.	No exceptions noted.
A.5.25	Aibidia shall assess information security events and decide if they are to be categorized as information security incidents.	Inspected the Information Security Incident Response RACI Table to determine that the responsibilities for review and classification of information security incidents are assigned.	No exceptions noted.
A.5.26	Information security incidents shall be responded to in accordance with the documented procedures.	Inspected as sample of incident tickets and related documentation and noted that they were handled in accordance with the documented procedures.	No exceptions noted.
A.5.27	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	Inspected that that knowledge gained from information security incidents is documented and tracked, and action points are defined to support the improvement of information security controls.	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
A.5.28	Aibidia shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Inspected that the guidelines on methods for the identification, collection, acquisition and preservation of evidence related to information security events are defined and documented.	No exceptions noted.
A.5.29	Aibidia shall plan how to maintain information security at an appropriate level during disruption.	Inspected that information security and continuity are considered in the organization's business continuity planning. The cloud platform configurations are continuously evaluated to ensure continuity. Inspected the cloud infrastructure configurations to determine that redundancy and data backups are implemented for the cloud storage to ensure continuity for information security during an adverse situation. Inspected list of incidents and that the incident management guidelines have been followed	No exceptions noted.
A.5.30	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Inspected the documented business plan to and noted that relevant objectives and requirements are documented.	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
		Inspected the backup and restore procedures to determine that steps to follow in order to recover and restore from an identified security incident exists.	
A.5.31	Legal, statutory, regulatory and contractual requirements relevant to information security and Aibidia's approach to meet these requirements shall be identified, documented and kept up to date.	Inquired the management of Aibidia about the operation of the control and inspected applicable laws and regulations documentation to determine that legal, statutory, regulatory and contractual requirements relevant to information security are documented and kept up to date.	No exceptions noted.
A.5.32	Aibidia shall implement appropriate procedures to protect intellectual property rights.	Inspected Aibidia services purchasing agreement template and noted that it includes Intellectual property rights section.	No exceptions noted.
A.5.33	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Inspected the information security policy and noted that practices and means for data protection are documented. Inspected the controls related to access management and data	Noted that while customer data retention is sufficiently defined in the Information Security Policy, requirements for internal data are not adequately documented. Retention periods and references to applicable legal or regulatory requirements are unclear or missing, and retention times are



Control ID	Control Description	Testing Procedures	Testing Results
		retention and noted that those controls are implemented.	not consistently defined across data types. <i>Management response:</i> <i>Management acknowledges the finding. While customer data retention requirements are defined in the Information Security Policy, Aibidia recognizes that internal data retention requirements, including employee data, should be documented more clearly. Aibidia will review and update its internal data retention documentation to define retention periods for relevant internal categories data and reference applicable legal, regulatory, and business requirements. The updated retention guidance will be approved and communicated to relevant process owners by Q4 2026.</i>
A.5.34	Aibidia shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to	Inspected Aibidia terms of service documentation and noted that it includes the requirements regarding	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
	applicable laws and regulations and contractual requirements.	data protection and processing of personal data. Inspected Aibidia's documentation of applicable laws and regulations and noted that it states the relevant regulatory authorities contact information. Inspected Aibidia Information security policy and noted that it states instructions to follow in regards to accessing and processing personal information.	
A.5.35	Aibidia's approach to managing information security and its implementation including people, processes and technologies shall be inspected independently at planned intervals, or when significant changes occur.	Inspected a sample of penetration testing and external audit reports.	No exceptions noted.
A.5.36	Compliance with Aibidia's information security policy, topic-specific policies, rules and standards shall be regularly inspected.	Inquired of management regarding the internal process for identifying non-compliance and noted that instances of non-compliance are identified through internal and external audits.	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
		Inspected a sample of audit reports and noted that compliance is regularly inspected	
A.5.37	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Inspected that the operating procedures are documented and made available to all employees as part of the ISMS documentation. Inspected that the guidelines for secure software development and operation are in place.	No exceptions noted.
A.6.1	Background verification checks on all candidates to become personnel shall be carried out prior to joining Aibidia and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Inquired the management regarding background verification. Inspected a sample of of new employee records and noted that Aibidia performs reference and background checks.	No exceptions noted.
A.6.2	The employment contractual agreements shall state the personnel's and Aibidia's	Inspected a sample of contractual agreements with new employees to determine that the contracts	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
	responsibilities for information security.	included personnels responsibilities regarding information security.	
A.6.3	Personnel of Aibidia and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of Aibidia's information security policy, topic-specific policies and procedures, as relevant for their job function.	Inspected the annual security training records and noted that the trainings are held annually and participation is tracked and followed up.	No exceptions noted.
A.6.4	A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	Inspected the disciplinary policy document. Inquired the management and were informed that there were no cases during the attestation period where the disciplinary process had to be invoked.	No exceptions in design and implementation noted. Auditors did not perform the test of operating effectiveness as there were no occurrences of control operation during the attestation period.
A.6.5	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	Inquired of the Aibidia personnel and noted that distributed responsibility approach for offboarding is adopted. Inspected that the dedicated channel is established to communicate such changes and the offboarding checklist is maintained which was	Noted that for one contractor and one additional employee, email confirmations of the last working day were inspected, however, evidence was not available to confirm that post-termination information security responsibilities had been



Control ID	Control Description	Testing Procedures	Testing Results
		inspected to confirm notifications to relevant personnel. Termination templates were reviewed, confirming that confidentiality, intellectual property, and non-solicitation obligations remain in effect after employment ends.	communicated to the contractor and employee. <i>Management response:</i> <i>Management acknowledges the finding. Aibidia has confidentiality and information security obligations that continue after employment or contractor engagement ends; however, evidence was not available to confirm that these post-termination responsibilities had been separately communicated in the sampled cases. Aibidia will update the checklist to offboarding include a mandatory step confirming communication of continuing information security, confidentiality, protection Evidence and of data responsibilities. this communication will be retained in the offboarding record going forward. The checklist update was completed in Q2 2026.</i>
A.6.6	Confidentiality or non-disclosure agreements reflecting Aibidia's	Inspected that the confidentiality agreement is a standard clause	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
	needs for the protection of information shall be identified, documented, regularly inspected and signed by personnel and other relevant interested parties.	included in the Aibidia's contractual agreements.	
A.6.7	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside Aibidia's premises.	Inspected employee handbook which outlined employee responsibilities for remote working and providing guidance for secure working practices.	No exceptions noted.
A.6.8	Aibidia shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Inspected the information security policy and noted that contains the guidelines and obligations for reporting of security events.	No exceptions noted.
A.7.1	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	Observed the office premises and inspected the plans of the office premises to determine that the security perimeter is defined to protect the working areas.	No exceptions noted.
A.7.2	Secure areas shall be protected by appropriate entry controls and access points.	Observed the office premises and inspected the plans of the office premises to identify main and emergency exits. The key register was inspected to verify tracking of physical access credentials.	Noted during audit interview that one new employee's name and corresponding key were not included in the key register.



Control ID	Control Description	Testing Procedures	Testing Results
			Additionally noted that there is no periodic review performed to validate the completeness and accuracy of the key register. <i>Management response:</i> <i>Management acknowledges the finding. The missing key register entry was a documentation gap identified shortly after the employee had joined. Aibidia will update the key register to include the missing entry and will reinforce the process so that physical key issuance is documented before or at the time of issuance. In addition, Aibidia will introduce a periodic review of the key register, at least annually, to validate its completeness and accuracy against current key holders. These actions will be completed by Q3 2026.</i>
A.7.3	Physical security for offices, rooms and facilities shall be designed and implemented.	Observed the office premises and inspected the plans of the office to determine that security measures for	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
		the office areas are designed and implemented.	
A.7.4	Premises shall be continuously monitored for unauthorized physical access.	Observed the office premises surveillance and alarm equipment and noted that the premises are monitored.	No exceptions noted.
A.7.5	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	Observed the office premises and business continuity plans and note that physical and environmental threats are managed.	No exceptions noted.
A.7.6	Security measures for working in secure areas shall be designed and implemented.	Inspected that the instructions for handling classified information are defined including the secure working practices.	No exceptions noted.
A.7.7	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	Inspected the Employee Information Security Policy to determine that the clear desk policy is in place. Observed the office premises and noted that the policy is followed.	No exceptions noted.
A.7.8	Equipment shall be sited securely and protected.	Observed the office premises and noted that the equipment is protected.	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
A.7.9	Off-site assets shall be protected.	Inquired the management and inspected the information security policy and noted that all the standard information security measures and policies apply in remote settings.	No exceptions noted.
A.7.10	Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with Aibidia's classification scheme and handling requirements.	Inspected the acceptable use policy and noted that storage media usage is managed. Inspected the contractual agreement to determine that the disposal of media is implemented employing an external contractor.	No exceptions noted.
A.7.11	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Observed the UPS power backup equipment in the premises.	No exceptions noted.
A.7.12	Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	Observed the office premises to determine that the cables are adequately protected.	No exceptions noted.
A.7.13	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	Observed the office premises to determine that equipment are protected and maintained. Inspected applicable security related policies	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
		and noted that security guidelines are in place.	
A.7.14	Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Inspected the information security policy and noted that process and methods of secure disposal are in place.	No exceptions noted.
A.8.1	Information stored on, processed by or accessible via user end point devices shall be protected.	Inspected that mobile devices security measures are defined in the Information Security Policy for Employees, including AUP. Inspected that secure configurations are enabled on end point employee devices by the subcontractor maintaining the device. It was tested with a sample of devices that employee devices are encrypted.	Noted that 20 mobile phones were not compliant in Intune. Inquired if these can still access Aibidia's services and were informed that this is possible. <i>Management response:</i> <i>Management acknowledges the finding. Aibidia will review endpoint compliance controls to ensure that access to Aibidia services is restricted appropriately or risk-assessed when devices are not compliant with defined security requirements. Aibidia will assess the technical options for enforcing conditional access based on device compliance status and will document any exceptions with risk</i>



Control ID	Control Description	Testing Procedures	Testing Results
			<i>acceptance where temporary access is required. The remediation plan and required configuration updates will be completed by Q4 2026.</i>
A.8.2	The allocation and use of privileged access rights shall be restricted and managed.	Inspected a list of users with privileged access rights and access rights policy and noted that privileged access rights are restricted to the specified authorized personnel.	No exceptions noted.
A.8.3	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	Inspected the access rights policy and noted that access restrictions are defined. Auditors inspected the cloud infrastructure to determine that the environments are segregated by subscription.	No exceptions noted.
A.8.4	Read and write access to source code, development tools and software libraries shall be appropriately managed.	Inspected Aibidia's version control and development system configurations and noted that read and write accesses are restricted through Entra ID.	No exceptions noted.
A.8.5	Secure authentication technologies and procedures shall be implemented based on	Inspected the access rights policy and Entra ID configurations and noted that secure authentication	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
	information access restrictions and the topic-specific policy on access control.	including credentials, password and MFA is required to access information.	
A.8.6	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	Inquired about capacity monitoring and planning for changes and were informed that Microsoft Azure dashboard is used for capacity monitoring database pool, production resources compute, storage capacity. Inspected Aibidia's monitoring dashboard and alerts.	No exceptions noted.
A.8.7	Protection against malware shall be implemented and supported by appropriate user awareness.	Inspected the AV tool dashboard and relevant guidelines including employee's awareness training.	No exceptions noted.
A.8.8	Information about technical vulnerabilities of information systems in use shall be obtained, Aibidia's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	Inspected a sample of vulnerability scanning reports. Inspected that identified vulnerabilities are reported to the dedicated communications channel for further analysis by the responsible personnel.	No exceptions noted.
A.8.9	Configurations, including security configurations, of hardware, software, services and networks	Inspected that Aibidia maintains guidelines for secure configurations and deploys configuration templates	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
	shall be established, documented, implemented, monitored and inspected.	for secure infrastructure configurations.	
A.8.10	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	Inspected that the policies are defined for information retention and deletion.	No exceptions noted.
A.8.11	Data masking shall be used in accordance with Aibidia's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	Inspected Aibidia's documentation related to data masking. Data masking is used for all production-derived data. Strict requirements need to be met before the data can be masked. Synthetic data or demo-dataset are preferred to be used instead of masked data.	No exceptions noted.
A.8.12	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Inspected Aibidia's documentation related to Data leakage prevention. Documentation describes that DLP is used across the systems and is monitored. Inquired how the monitoring is handled and were informed that all DLP-based alerts are sent to dedicated inbox.	No exceptions noted.
A.8.13	Backup copies of information, software and systems shall be maintained and regularly tested in	Inspected the organization's cloud service infrastructure to determine that the backups are enabled and available for the cloud environments.	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
	accordance with the agreed topic-specific policy on backup.	Inquired if there has been any case where backup had to be restored during the audit period and were informed that backups have been restored once. Inspected the restoration ticket.	
A.8.14	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Inspected that capacity and availability are monitored and managed utilizing cloud service provider capabilities. Inspected that geo-redundancy settings are enabled.	No exceptions noted.
A.8.15	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	Inspected Azure configurations to determine that the cloud environment logs are stored to the dedicated write-only cloud platform database.	No exceptions noted.
A.8.16	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Inquired about the process of monitoring anomalous behaviour of networks, systems and applications and were informed that Azure sentinel monitors the behaviour. There is an automation rule configured, which gets triggered by all incidents. The security team will	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
		then get alerts whenever there is an incident. Inquired about the database logs and were informed that database logs are records of events, changes, and operations that occur within the database system. These logs are not analysed by sentinel.	
A.8.17	The clocks of information processing systems used by Aibidia shall be synchronized to approved time sources.	Inquired if virtual machines sync from the same NTP server and were informed that time is synced from Microsoft's time server. Observed the baseline configurations for virtual machines.	No exceptions noted.
A.8.18	The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	Inquired of Aibidia personnel and noted that privileged utility programs are not in use on the organization's infrastructure. Inspected the information asset list to confirm this.	No exceptions noted.
A.8.19	Procedures and measures shall be implemented to securely manage software installation on operational systems.	Inspected that the Aibidia Employee Security Policy includes instructions on software programs installations and based on the policy installation of software is restricted to the whitelisted applications.	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
A.8.20	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	Inspected various Azure network configurations for network protection and VPN usage.	No exceptions noted.
A.8.21	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	Inspected various Azure network configurations for network protection and VPN usage.	No exceptions noted.
A.8.22	Groups of information services, users and information systems shall be segregated in Aibidia's networks.	Inspected various Azure subscription configurations for network protection and VPN usage.	No exceptions noted.
A.8.23	Access to external websites shall be managed to reduce exposure to malicious content.	Inspected web browsing restriction configurations and acceptable use policy and noted that access to external websites is limited.	No exceptions noted.
A.8.24	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	Inspected Aibidia's policies related to encryption to determine how services and traffic are secured. All traffic is encrypted using minimum TLS 1.2 encryption. Databases are encrypted using cloud providers services.	Noted that 20 mobile phones in active use in Intune were not compliant. <i>Management response:</i> <i>Management acknowledges the finding. Aibidia will review device</i>



Control ID	Control Description	Testing Procedures	Testing Results
		Observed that devices managed in Intune. Encryption is managed through these policies for user devices.	<i>encryption cryptographic and control requirements as part of the endpoint compliance remediation. Devices that do not meet required encryption or compliance standards will be remediated, blocked from access, or subject to formally documented exception handling and risk acceptance. Aibidia will complete the review and implement required improvements by Q4 2026.</i>
A.8.25	Rules for the secure development of software and systems shall be established and applied.	Inspected that the secure process for software development is defined and communicated to the personnel as part of ISMS documentation.	No exceptions noted.
A.8.26	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	Inspected that the secure process for software development is defined and communicated to the personnel as part of ISMS documentation. Inspected internal guidelines for secure application development and configuration.	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
A.8.27	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	Inspected the secure software development process and quality assurance process to determine that secure system engineering principles are established and observed.	No exceptions noted.
A.8.28	Secure coding principles shall be applied to software development.	Inspected the secure software development process and quality assurance process to determine that secure system engineering principles are established and observed.	No exceptions noted.
A.8.29	Security testing processes shall be defined and implemented in the development life cycle.	Inspected a sample of changes within the attestation period that changes are tested in accordance with the change management process. Inspected a sample of changes implemented within the attestation period that the security testing of changes is performed, and regular scanning is enabled. Additionally, inspected that the annual penetration testing was performed.	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
A.8.30	Aibidia shall direct, monitor and inspect the activities related to outsourced system development.	Inspected various development policies and guidelines and noted that outsourced development is monitored properly.	No exceptions noted.
A.8.31	Development, testing and production environments shall be separated and secured.	Inspected the Azure subscription configurations and noted that system environments are properly separated.	No exceptions noted.
A.8.32	Changes to information processing facilities and information systems shall be subject to change management procedures.	Inspected that Aibidia has a defined change management workflow, and all changes undergo review and are subject to approval by the management. For a sample of changes inspected that the changes followed the controlled change management procedure, including the appropriate approvals.	During testing it was noted that one pull request out of 25 had been created, approved and merged by one person. <i>Management response:</i> <i>Management acknowledges the finding. One pull request was created, approved, and merged by the same individual, which was not aligned with the intended segregation of duties in the change management process. Aibidia will reinforce pull request approval rules to ensure that production impacting changes require independent review and approval before merge. Where emergency or exceptional</i>



Control ID	Control Description	Testing Procedures	Testing Results
			<i>changes are required, Aibidia will require documented justification and retrospective review. The configuration and process reinforcement will be completed by Q3 2026.</i>
A.8.33	Test information shall be appropriately selected, protected and managed.	Inspected the policies regarding test data and data masking. Inquired regarding protection of test data and noted that all testing environments, including the user acceptance testing environment, are segregated from the production and development environments. Data used in tests is either synthetic data, generated data-set or anonymized data.	No exceptions noted.
A.8.34	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	Inquired of the Aibidia personnel and noted that the annual penetration testing by an external party is performed. Inspected the penetration testing report for the testing performed to determine that the testing was planned and performed accordingly.	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
		Inspected the internal Slack channel discussion related to penetration testing preparations.	
CC1.2.1	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Inspected composition and competences of the members of the Board of Directors to determine that they demonstrate sufficient independence from the Executive Team and competence adequate to oversee the development and performance of the system of internal control.	No exceptions noted.
CC1.4.1	Aibidia shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.	Inspected that Aibidia has established a dedicated information security management team to enable, maintain and improve the system of internal control for information security.	No exceptions noted.
CC2.2.1	Aibidia internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Inquired of the Aibidia personnel and inspected the ISMS documentation. Noted that internal control objectives, responsibilities, and information security requirements are defined and communicated to employees through policies, onboarding processes, training, and	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
		internal communication channels (e.g., Slack, email). Inspected that the ISMS security objectives roadmap is defined and communicated to the responsible personnel.	
CC2.3.1	Aibidia determines the need for internal and external communications relevant to the information security management system, including what, when, with whom, and who shall communicate and the processes for communication.	Inspected that Aibidia has established a structured approach for managing internal and external communications relevant to information security.	No exceptions noted.
CC3.1.3	Aibidia clearly defines its service commitments and system requirements.	Inspected that Aibidia has established a system of internal control with defined service commitments and system requirements related to information security.	No exceptions noted.
CC3.2.1	Aibidia shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur. Aibidia shall retain documented information of the	Inspected that Aibidia performs annual risk assessment covering the whole organization. Inspected the risk register to determine that the results of the risk	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
	results of the information security risk assessments.	assessment performed within the attestation period are documented. Inspected ISMT meeting minutes. Noted that risk assessment topics were discussed, indicating ongoing monitoring and reassessment.	
CC3.2.2	Aibidia shall implement the information security risk treatment plan. Aibidia shall retain documented information of the results of the information security risk treatment.	Inspected that Aibidia has defined and documented risk treatment plans for identified and ongoing risks.	No exceptions noted.
CC3.4.1	Aibidia complies with applicable accounting standards. Financial reporting objectives are consistent with accounting principles suitable and available for Aibidia. The accounting principles selected are appropriate in the circumstances.	Inspected that Aibidia employs an external contractor to perform financial reporting and accounting functions. Inspected the latest financial audit report to determine that compliance with the accounting standards has been evaluated within the attestation period.	No exceptions noted.
CC4.1.1	Aibidia shall evaluate the information security performance and the effectiveness of the	Inspected that Aibidia evaluates the performance of its system of internal control based on the results of	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
	information security management system.	internal and independent external audit. Additionally, an annual independent security testing is performed to identify potential deficiencies in technological controls.	
CC4.2.1	When a nonconformity occurs, the organization shall react to the nonconformity, and as applicable take action to control and correct it.	Inspected that nonconformities from internal and external audits are analysed, documented, and corrective action plans are developed. Additionally, inspected that Aibidia implemented corrective actions for the nonconformities identified in previous audits.	No exceptions noted.
CC5.1.1	Aibidia shall plan, implement and control the processes needed to meet requirements and address identified risks.	Inspected that Aibidia designed and implemented processes to maintain the system of internal control with consideration for relevant risks identified in the risk assessment process.	No exceptions noted.
CC9.1.1	Aibidia identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Inspected that annual risk review is part of the ISMS Yearly Cycle.	No exceptions noted.



Control ID	Control Description	Testing Procedures	Testing Results
		It was inspected that the latest review was performed within the attestation period and that the risk inventory is in place and up to date.	
CC9.1.2	Aibidia considers the use of insurance to offset the financial impact of business disruptions.	Inspected that Aibidia maintained an active insurance for business disruptions, including security-related events, throughout the attestation period.	No exceptions noted.