



Aibidia

INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT ON THE DESCRIPTION OF CONTROLS, AND THEIR DESIGN AND OPERATING EFFECTIVENESS

ISAE 3402 TYPE II REPORT

July 10th 2026

CONTENTS

SECTION ONE	3
INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT ON THE DESCRIPTION OF CONTROLS, AND THEIR DESIGN AND OPERATING EFFECTIVENESS	4
SECTION TWO	7
STATEMENT BY THE SERVICE ORGANISATION	8
SECTION THREE	10
1 DESCRIPTION OF SERVICES PROVIDED BY AIBIDIA OY	11
1.1 Introduction	11
1.2 Overview of the organisation	11
1.3 Description of services provided	12
1.3.1 System boundaries and services covered in this report	12
1.3.2 Main functions of the system	14
1.3.3 Functional areas of operations	15
1.3.4 Boundaries of the system	16
2 RELEVANT ASPECTS OF THE INTERNAL CONTROL ENVIRONMENT	18
2.1 Internal Control Environment	18
2.2 Governance and responsibility structure	18
2.3 Risk assessment	19
2.4 Control Design and Monitoring	19
2.5 Control activities	20
3 DESCRIPTION OF CONTROLS	22
3.1 OTPM application and OTP process controls	22
3.1.1 OPTM master data management	22
3.1.2 Data Import	23
3.1.3 Allocation and segmentation	24
3.1.4 Transfer price reporting	24
3.2 General IT controls	25
3.2.1 Access to applications and data	25
3.2.2 Software Development and change management	27
3.2.3 System operations	27
4 Complementary User Entity Controls (CUECs)	29
SECTION FOUR	31
DESCRIPTION OF TESTING PERFORMED	32

SECTION ONE



INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT ON THE DESCRIPTION OF CONTROLS, AND THEIR DESIGN AND OPERATING EFFECTIVENESS

To: Management of Aibidia Oy

Scope

We have been engaged to report on the Aibidia Oy's (hereinafter also "Aibidia" or "service organization") description in section 3 of its TMX Platform system throughout the period 1st November 2025 to 30th June 2026 (the description) and on the design and operation of controls related to the control objectives stated in the description.

The description indicates that certain complementary user entity controls must be suitably designed and implemented at user entities for related controls at the service organisation to be considered suitably designed to achieve the related control objectives. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Aibidia uses a subservice organisation Microsoft Azure for cloud computing services as described in the service organisation's description of its system. For its description Aibidia uses the carve-out method. The description of the system therefore excludes the control objectives and related controls of the subservice organisation. Our procedures did not extend to controls of the subservice organisation.

Aibidia's Responsibilities

Aibidia is responsible for preparing the description and the accompanying statement at section 2 including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Our Independence and Quality Control

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 Auditor's Responsibilities

Our responsibility is to express an opinion on Aibidia's description and on the design and operation of controls related to the control objectives stated in that description, based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements 3402, *Assurance Reports on Controls at a Service Organization*, issued by the International Auditing and Assurance Standards Board. That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in



all material respects, the description is fairly presented and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgment, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organization.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our qualified opinion.

Limitations of Controls at a Service Organisation

Aibidia's description is prepared to meet the common needs of a broad range of user entities and their auditors and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Also, because of their nature, controls at a service organization may not prevent or detect all errors or omissions in processing or reporting transactions. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria used in forming our opinion are those described in the Aibidia's statement in section 2. In our opinion, in all material respects:

- (a) The description fairly presents Company's system as designed and implemented throughout the period from 1st November 2025 to 30th June 2026;
- (b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1st November 2025 to 30th June 2026; and
- (c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1st November 2025 to 30th June 2026.

Description of Tests of Controls

The specific controls tested, and the nature, timing and results of those tests are listed in Section 4.

Intended Users and Purpose

This report and the description of tests and controls are intended only for user entities who have used the TMX Platform system provided by Aibidia, and their auditors, who have a sufficient understanding to consider it, along with other information including information about controls operated by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements



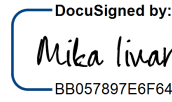
Helsinki, on July 10th 2026

KPMG Oy Ab

DocuSigned by:

2477B01D945A425...

Jussi Paski
Partner
Authorized Public Accountant

DocuSigned by:

BB057897E6F64C0...

Mika Iivari
Partner
Head of Cyber Advisory

SECTION TWO



STATEMENT BY THE SERVICE ORGANISATION

We have prepared the accompanying description at section 3 of Aibidia's TMX Platform system for user entities and their auditors who have a sufficient understanding to consider the description, along with other information including information about controls operated by customers themselves, when assessing the risks of material misstatements of customers' financial statements.

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

- a) The accompanying description fairly presents the Aibidia's TMX Platform system made available to user entities of the system during some or all of the period period 1st November 2025 to 30th June 2026. Aibidia uses Microsoft Azure as a service organization for cloud computing services. The description only includes the controls and related objectives of Aibidia and excludes the control objectives and related controls of Microsoft Azure. The criteria used in making this statement were that the accompanying description:
 - i) presents how the system was designed and implemented, including:
 - the types of services provided, including, as appropriate, classes of transactions processed;
 - the procedures, within both information technology and manual systems, by which those transactions were initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for customers;
 - the information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information and specific accounts involved in initiating, authorizing, recording, processing and reporting transactions; this includes the correction of incorrect information and how information was transferred to the reports and other information prepared for user entities;
 - how the system dealt with significant events and conditions, other than transactions;
 - the process used to prepare reports for customers;
 - relevant control objectives and controls designed to achieve those objectives;
 - controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone;

Aibidia

- other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to processing and reporting customers' transactions;
 - services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them
 - controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved solely by controls implemented by ourselves alone; and
 - other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities and monitoring controls that were relevant to processing and reporting user entities' transactions
- ii) includes relevant details of changes to the service organisation's system during the period 1st November 2025 to 30th June 2026;
- iii) does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment;
- b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1st November 2025 to 30th June 2026. The criteria used in making this statement were that:
- i) the risks that threatened achievement of the control objectives stated in the description were identified; and
 - ii) the identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and
 - iii) the controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 1st November 2025 to 30th June 2026.

Helsinki, on July 10th 2026

Aibidia Oy

Signed by:

 578BC14F67154F0...
 Ryan Collett
 COO

SECTION THREE



1 DESCRIPTION OF SERVICES PROVIDED BY AIBIDIA OY

1.1 Introduction

Aibidia is a private global technology company headquartered in Helsinki, Finland, specializing in the design, development, and operation of software solutions for transfer pricing management.

The company serves multinational enterprises (MNEs), enabling them to meet regulatory and compliance requirements associated with intercompany transactions across multiple jurisdictions. Founded with the objective of introducing a structured, data-driven approach to transfer pricing operations, Aibidia combines expertise in international tax, finance, and information technology to deliver a platform that supports both documentation compliance and real-time execution of transfer pricing models.

1.2 Overview of the organisation

Aibidia operates as a centralized service organization, providing a suite of operational and support functions that underpin the delivery of its core business services. The company's structure and processes are designed to ensure effective governance, risk management, and operational efficiency across all business units, supporting both internal and client-facing activities.

Organizationally, Aibidia operates through four primary functional areas—Operations, Growth, Engineering, and Product—each contributing to the design, execution, and oversight of internal controls essential for SOC 1 compliance.

- **Operations** includes Finance, Legal, Internal IT, Professional Services, People, and Implementation Management. This function ensures enterprise-wide governance, financial integrity, secure internal infrastructure, and a generally compliant workforce management.
- **Growth** comprises Sales, Customer Success, and Marketing. These teams manage the customer lifecycle through controlled and auditable processes, from market engagement and acquisition to service delivery, retention, and support—ensuring consistency with contractual and compliance obligations.
- **Engineering** is responsible for the development, maintenance and security of Aibidia's technology infrastructure. It supports SOC 1 compliance by embedding security, availability, and reliability principles into system design and software development practices.
- **Product** defines and governs the design and evolution of Aibidia's solutions. This function ensures that platform capabilities align with regulatory, contractual, and internal control expectations, enabling consistent service delivery in-line with customer commitments.



Each function operates under structured management oversight and is subject to regular review to ensure alignment with organizational objectives, control requirements, and SOC 1 assurance standards.

Aibidia maintains a formal Information Security Management System (ISMS) that is continuously improved using a maturity model aligned with recognized control frameworks. The ISMS incorporates security controls based on international standards, including ISO/IEC 27001, and these controls are mapped to the relevant criteria under ISAE 3000 and SOC 2.

- Aibidia's ISMS is certified under ISO/IEC 27001, demonstrating adherence to globally recognized information security best practices.
- Security controls are continuously monitored and enhanced to ensure alignment with both regulatory requirements and customer expectations.
- Aibidia undergoes regular independent assessments, including SOC 2 Type II reporting under the ISAE 3000 standard, to validate the design and operating effectiveness of its control environment.

1.3 Description of services provided

Aibidia provides a comprehensive suite of Software-as-a-Service (SaaS) and professional services designed to support the full lifecycle of transfer pricing activities. The service offering is structured around two core areas: Compliance and Operational Transfer Pricing Management.

Compliance

TPDoc solution enables the efficient preparation, management, and maintenance of transfer pricing documentation in accordance with regulatory requirements. The Country-by-Country Reporting (CbCR) solution addresses multinational enterprises' obligations under OECD and local regulations, streamlining the preparation and submission of CbC reports.

Operational Transfer Pricing Management (OTPM)

Operational transfer Pricing Management (OTPM) solution provides a technological solution for execution, monitoring, and alignment of transfer pricing policies with actual financial transactions and business performance, enabling transparency and compliance throughout the fiscal year.

Aibidia's integrated platform allows user organizations to digitize and automate key aspects of their transfer pricing processes, enhancing efficiency, accuracy, and regulatory compliance.

1.3.1 System boundaries and services covered in this report

This report exclusively covers the Operational Transfer Pricing Management (OTPM) Solution provided by Aibidia. It does not include Aibidia TPDoc or CbCR solutions nor does it address any customer enterprise systems (e.g., ERP or financial platforms) or



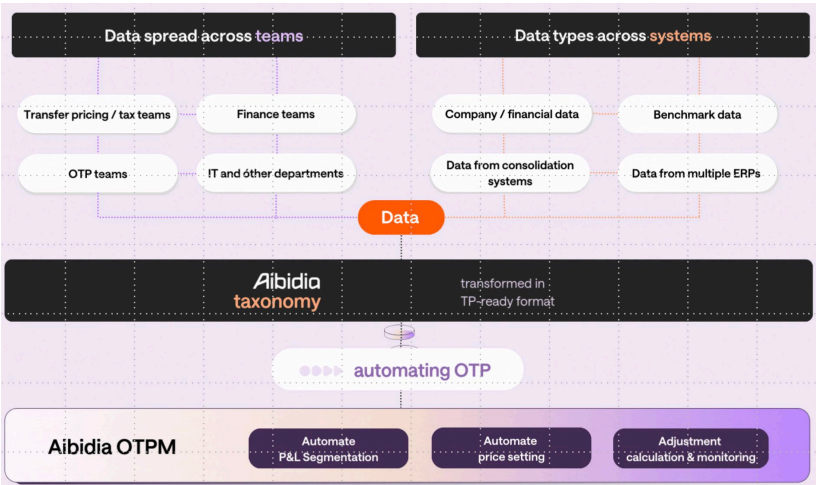
activities performed independently by customer personnel within their own environments.

The OTPM Solution is a core component of Aibidia’s offering, designed to bridge the gap between transfer pricing policy design and its operational execution. It connects transactional and financial data to transfer pricing rules to ensure that intercompany transactions are properly priced, monitored, and adjusted in accordance with internal policies and external regulatory requirements throughout the financial year.

As a cloud-based platform, OTPM enables the digitization and automation of operational transfer pricing processes for multinational enterprises. The system provides users with visibility, proactive controls, and a structured approach to ensuring compliance across complex intercompany transaction networks.

The OTPM solution plays a material role in user entities’ financial reporting processes. It directly supports the recognition, allocation, and adjustment of intercompany revenues and costs—elements that can have a significant impact on consolidated financial statements, tax provisions, and segment reporting. Accurate and timely execution of transfer pricing policies is critical to ensuring alignment with applicable accounting standards, tax regulations, and governance frameworks.

By linking customer-provided data to predefined benchmark models—often based on arm’s-length pricing studies or advance pricing agreements (APAs)—OTPM enables monitoring of actual performance against target profit margins. Deviations are identified according to the customer’s schedule, allowing for timely adjustments to maintain compliance with both internal policies and external requirements.





1.3.2 Main functions of the system

The OTPM Solution comprises a comprehensive set of functionalities that support the end-to-end operationalization of transfer pricing policies. Key capabilities include:

Data Ingestion

Load flat-file extracts into the OTPM solution and map them to the target data schema. Configure multiple extract types when needed to accommodate different data sources with a simple, user-driven method for loading data without requiring IT involvement.

Optionally, automate the delivery of data extracts with API, minimizing manual handling and reducing data latency. It supports configuration of multiple extract types to accommodate different data sources, enabling efficient, scalable, and timely data integration for transfer pricing calculations and monitoring.

Policy management

Centralize creation and maintenance of the transfer pricing policy master data. Define and structure individual transfer pricing policies by specifying the policy type, applied transfer pricing method, and selected profit level indicator (PLI). Through this functionality, users can manage the group-wide policy framework by linking each policy to relevant legal entities and defining their respective roles from TP testing perspective (e.g., tested party or counterparty). This ensures a consistent, transparent, and auditable setup of transfer pricing policies that serve as a foundation for operational execution and periodic compliance testing.

Mapping Management

Configure and maintain mapping rules that enrich source data with transfer pricing attributes across various use cases within the OTPM solution. It supports multiple data sources and allows management of mapping logic for each extract type, ensuring consistent, flexible, and accurate data transformation for downstream transfer pricing calculations and reporting.

P&L segmentation

The P&L Segmentation functionality enables dynamic dissection and analysis of financial performance at a functional level. It allows users to segment profit and loss data according to defined level, ensuring that profitability is monitored consistently with the group's transfer pricing policies. By leveraging multiple Profit Level Indicators (PLIs), users can continuously evaluate actual performance against defined arm's-length targets or ranges. Built-in visual alerts highlight out-of-range results, supporting timely investigation and corrective actions to maintain compliance and operational alignment.

Adjustment calculation



Calculate transfer pricing adjustments based on segmented P&L results, ensuring alignment of transfer prices with market conditions and internal policy targets. Adjustments are calculated to a defined target point or within an arm's-length range specified in the transfer pricing policy. They are available for all periods (monthly) with data, enabling consistent and periodic alignment of intercompany results throughout the year.

Royalty calculation

Automate the determination and allocation of intercompany royalties related to the use of intangible assets. Users can define intangible asset groups, assign applicable royalty rates, and specify participating legal entities. The system supports configuration of the royalty calculation basis (e.g., total or third-party revenue), and applies user-defined mapping logic to identify the relevant revenue streams and intangible assets in scope. This enables automated, transparent, and consistent computation of to-be-paid royalties, ensuring alignment with transfer pricing policies.

Transaction Monitoring

Reconcile transfer pricing deviations at an individual invoice level, providing granular transparency into intercompany transactions. Markups are defined as part of master data for each legal entity and transfer pricing policy combination and are linked to transactions through configurable mapping rules. The functionality enables transaction-level transfer pricing testing, such as Comparable Uncontrolled Price (CUP) analyses, ensuring detailed and compliant monitoring of intercompany pricing accuracy.

Reporting and Audit Support

The system produces standardized reports, dashboards, and audit trails to support internal oversight and external audits. All user actions and system events are logged to maintain traceability and support accountability across the transfer pricing lifecycle.

1.3.3 Functional areas of operations

Executive Management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.

Service Delivery manages, monitors, and supports user entities' information and systems from unauthorized access and use while maintaining integrity and availability. Positions within Service Delivery include, but are not limited to, the following:

- Logical access management (Aibidia's access)
- Secure Application and Software Development process
- Change management
- Backup and recovery
- System operations and monitoring



OTPM is delivered using a Software as a Service (SaaS) model, allowing customers to access the platform through a secure web interface without the need to install or maintain software locally. The platform operates on a multi-tenant cloud architecture, ensuring that each customer's data is logically isolated and securely managed. It features elastic scalability, automatically adjusting its resources based on client demand to maintain stable performance regardless of transaction volumes. Additionally, updates and improvements to functionality, security, and compliance features are deployed continuously and seamlessly, without requiring any customer intervention.

Customer data ingestion is supported via secure APIs and file-based upload mechanisms. Data ingestion processes include validation steps and transformation logic to ensure consistency and integrity prior to processing.

Aibidia's software development lifecycle incorporates secure design, implementation, peer review, automated and manual testing (including vulnerability assessments), and deployment. Change management follows a structured process: Create, Review, Assess Risks, Approve, Implement, and Close. All change requests are categorized as Standard, Normal, or Urgent. Customer-related change management follows the same process, with additional communication and approval steps where required.

Release management is integrated with change management and is organized through weekly release syncs. Release planning and item assignment are managed in Azure DevOps, with testing results attached to release notes for traceability and audit purposes.

Finally, Aibidia's Information Security Incident Response workflow aligns closely with the change management process. Key phases - Review, Assess Risks, Approve, Implement, and Close - are conducted by or under the supervision of the IS management team. All incidents are logged, investigated, and resolved according to documented procedures, with escalation protocols in place for major incidents. Incident logs and root cause analyses are maintained for audit and continuous improvement purposes.

1.3.4 Boundaries of the system

The responsibilities for implementing and operating the OTPM Solution are shared between Aibidia and the customer (user entity).

- Aibidia is responsible for the delivery and maintenance of the OTPM service, including its technical functionality, the integrity of calculation logic and formulas, and the overall system architecture that enables the operational execution of transfer pricing policies.
- The customer (user entity) is responsible for the configuration and setup of transfer pricing policies within the OTPM environment. This includes ensuring that the configurations accurately reflect the intended business logic, organizational policies, and regulatory requirements. In addition, the customer is solely responsible for the accuracy, completeness, and timeliness of all input



data—such as financial, transactional, and benchmarking data—used within the system.

A more detailed allocation of roles and responsibilities between the parties is provided in Chapter 4 – Complementary User Entity Controls of this service description.

Subservice Organizations

OTPM is hosted on Microsoft Azure in the West Europe region (Ireland). The infrastructure leverages Azure's compliance with international security and quality standards, including ISO 27001, ISO 27017, ISO 27701, SOC 1, SOC 2, SOC 3, PCI DSS 3.2, ISO 22301, ISO 9001, and Azure CIS. All client data is encrypted at rest and in transit using industry-standard protocols. Logical data isolation is maintained for each tenant, and access to data is governed by configurable, role-based access controls managed by client administrators.



2 RELEVANT ASPECTS OF THE INTERNAL CONTROL ENVIRONMENT

2.1 Internal Control Environment

Aibidia maintains a structured internal control environment designed to support the reliable and secure delivery of its services, particularly those relevant to user entities' internal control over financial reporting. The control framework is aligned with the principles outlined in the COSO Internal Control, emphasizing effective governance, risk management, and accountability.

Aibidia's leadership fosters a culture of integrity, compliance, and performance throughout the organization. Control responsibilities are clearly defined and delegated across operational, development, and support functions. Employees receive regular training on internal policies, control procedures, and quality standards relevant to their roles.

While information security is a vital supporting layer, Aibidia's control environment also draws upon practices consistent with the ISO/IEC 27001 standard.

2.2 Governance and responsibility structure

Aibidia's governance framework defines clear accountability for the management, oversight, and delivery of services within the scope of this description. The structure ensures that responsibilities for operational performance, compliance, risk management, and client obligations are well-distributed across roles and functions.

Key components of the governance model include:

- **Executive Oversight:** Senior leadership sets strategic objectives, approves control policies, and monitors risk and compliance performance through regular review cycles.
- **Product and Platform Management:** Dedicated teams oversee the development and operation of the OTPM solution, ensuring that platform functionality aligns with customer requirements, regulatory expectations, and internal control standards.
- **Implementation Management, Customer Success and Support:** Customer teams are responsible for onboarding, configuration guidance, and customer support. These teams coordinate closely with product and engineering teams to escalate issues and maintain service quality.



- **Risk and Compliance Oversight:** Aibidia conducts periodic risk assessments to ensure that control responsibilities are clearly assigned. Management evaluates control effectiveness, implements corrective actions where necessary, and tracks remediation efforts.

Responsibility for configuring the transfer pricing models, maintaining master data, and validating the accuracy of uploaded information resides with the customer (user entity), as detailed further in Chapter 4: Complementary User Entity Controls.

2.3 Risk assessment

Risk assessment is a core element of Aibidia's internal control system and is aligned with industry standards for financial reporting assurance and operational risk management. Risk identification, evaluation, and mitigation are integrated into both strategic and day-to-day processes to safeguard service continuity, data integrity, and compliance.

Assessments are conducted regularly as part of Aibidia's annual control and audit cycle. Risks are evaluated across key domains, organizational processes, personnel, infrastructure, applications, and data, are classified by impact and likelihood as High, Medium, or Low. Scenarios relevant to financial reporting, such as unauthorized changes to pricing logic or inaccurate margin calculations, are reviewed with emphasis on confidentiality, integrity, and availability.

Mitigation strategies are documented in formal treatment plans, supported by control design and monitoring responsibilities. Residual risks are reviewed by risk owners and escalated when necessary. All assessments and follow-up actions are recorded in Aibidia's centralized risk management tool and are subject to periodic review.

- ☐ This structured approach ensures that risks with potential financial reporting impact are consistently identified, assessed, and addressed.

2.4 Control Design and Monitoring

Aibidia's internal controls are designed to address identified risks and ensure reliable operation and continuous development of the OTPM solution. The design of control activities follows a top-down approach, beginning with risk analysis and control objective definition, and extending to the implementation of process-level and application-specific safeguards.

Controls are developed collaboratively between relevant stakeholders, engineering teams, and compliance personnel to ensure that both operational and regulatory considerations are addressed. This includes a combination of automated and manual controls designed to validate data quality, ensure processing accuracy, and safeguard system availability.



To ensure the effectiveness and ongoing relevance of these controls, Aibidia has implemented a formal monitoring and review process. This includes:

- **Independent Internal Audits:** Periodic audits performed by qualified internal auditors, focused on areas such as margin calculation validation, change management, data access, and adjustment controls.
- **Statutory Financial Audits:** Aibidia is subject to annual financial audits performed by an independent external audit firm. These audits assess the accuracy and completeness of the company's financial reporting and ensure compliance with applicable accounting standards.
- **Other External Audits:** Engagements with third-party auditors to evaluate the technical and operational robustness of the platform, supplementing internal control assurance.
- **Continuous Monitoring:** Dashboards and metrics are used to monitor the health of core processes, including pricing logic execution, exception handling, and data ingestion routines.

2.5 Control activities

The control objectives and activities that assist in producing Client's Services are described thoroughly in section 4, "Description of Controls". Controls relevant to financial reporting in the ITPM platform are designed in alignment with the COSO internal control framework.

Controls are divided and presented in the following groups:

General IT controls

General IT Controls (GITCs) ensure the reliability of the system environment, including:

- **Logical Access Management:** Controls to ensure that access to systems and data is appropriately authorized, restricted, and reviewed.
- **Secure Software Development Lifecycle:** Integration of secure coding practices, peer reviews, and vulnerability management into the development process.
- **Change Management:** Formalized processes to manage changes to code, configurations, and infrastructure, with appropriate approvals, documentation, and testing.
- **Backup and Recovery:** Procedures to ensure data backup integrity and recovery capabilities, including regular testing of restoration processes.
- **System Operations and Monitoring:** Monitoring of system performance, error logs, and infrastructure health to detect anomalies and maintain platform availability.

In addition to the general IT controls, Aibidia has implemented key application and process controls within the OTPM application that contribute directly to the reliability of financial data processing and reporting. These include:



- Master Data Management: Controls to ensure consistency and accuracy of core reference data such as legal entity hierarchies, transfer pricing policies, and benchmark and comparables.
- Data Import Controls: Automated and manual checks to validate against the accepted schema, including verification of all required fields of data uploaded to the platform.
- Allocation and segmentation: Application logic and configuration controls that ensure transfer pricing rules are applied consistently and as intended, including margin calculations and exception handling.
- Transfer Pricing Reporting: Generation of standardized reports and audit trails that support internal review and external audit requirements, with full traceability of underlying calculations and adjustments.

The control objectives and specific control activities supporting service delivery are described in detail in Section 3.



3 DESCRIPTION OF CONTROLS

3.1 OTPM application and OTP process controls

This section describes the internal controls designed and implemented into the Aibidia OTPM application and associated processes, focusing on transfer pricing configuration, data management, and reporting.

3.1.1 OPTM master data management

Control Objective: Controls provide reasonable assurance that all organization master data elements relevant to transfer pricing are properly created, structured, and maintained in the OTPM application.

Organization legal entities, relevant to transfer pricing, are created and maintained in the OTPM application. Each Entity has a unique Entity ID and OTPM enables legal entity to be divided into one or more reporting units, which will be assigned to a parent legal entity. OTPM application prevents duplicate Entity IDs, ensuring integrity in entity mapping.

The OTPM application enforces the configuration of each transfer pricing (TP) policy with the following mandatory fields:

- Policy Name (TP policy name must be unique)
- Policy Type (Function, Transactional)
- Transfer Pricing Method (e.g. Transactional Net Margin Method, Cost Plus Method, Not Transfer Pricing Method)
- Profit Level Indicator (PLI) (e.g., Operating Margin, Net Cost Plus Margin)

System will prompt a remark if some TP policy is missing mapped benchmark for some TP Policy-Legal Entity combination. Each policy is eventually shown as a segment within an entity in P&L monitoring page.

The OTPM application requires each user organization to establish an Account hierarchy as part of the transfer pricing model configuration. The account hierarchy defines the account groups to which imported financial data will be allocated and segmented. Each account group must be classified with an Account Type (Revenue, COGS, OPEX) and an income or expense definition. These classifications are used to structure segmented P&L and calculate Profit Level Indicator (PLI) value for each relevant Policy segment. Application requires that there is at least one Account Group enabled so that financial data can be allocated.

OTPM allows upload and definition of target margin records for each TP policy segment. Target margins may be based on benchmark studies, internal comparables, or management-defined targets. Each benchmark or target study must have a unique identifier. For Function type TP Policies, every target margin record must be linked to a valid combination of Legal



Entity (Entity ID) and TP Policy. For Transactional type TP Policies, every target margin record must be linked to a valid combination of Legal Entity (Entity ID), Counterparty (Entity ID), and TP Policy. A validity period (e.g., fiscal years) must be specified for each benchmark record to ensure accuracy over time. The system performs validation to ensure all required fields and linkages are present; if any are missing, an error message is generated and the benchmark record is excluded from calculations.

The OTPM application allows the creation of Intangible asset groups, each of which must be linked to an IP Owner, which is a Legal Entity (Entity ID). Royalty calculations related to each Intangible asset group are only performed when a valid Royalty rate (percentage between 0 and 100), Royalty base (Total revenue or Third party revenue), and Legal Entities within the royalty scope have been defined. The system validates the presence and correctness of these required fields before enabling royalty calculations.

3.1.2 Data Import

Control Objective: *Controls provide reasonable assurance that financial data imported into the Aibidia OTPM solution maintains integrity, completeness, and accuracy, and that the data structure aligns with the defined schema throughout the transfer pricing process.*

During the data ingestion process, the mandatory fields required to be mapped from the imported dataset depend on the selected Extract Type. For Multi Level Segmentation, the following fields are mandatory: Company ID, Account ID, and at least one of the following—Local Value or Group Value. For Transaction Monitoring, the following fields are mandatory: Company ID and at least one of the following—FOB Price, TP in sell currency, SAP TP price, TP Base Cost, Other Costs, Total TP Cost, or Markup Amount. The system enforces these requirements by validating the presence and correct mapping of these fields prior to processing the ingested data.

OTPM supports data imports through both manual uploads and secure API connections. Both are using encryption and authentication protocols to ensure secure data transmission.

The OTPM platform automatically performs data validation checks at the time of financial data ingestion (manual and API-based). The application validates whether the data aligns with the Aibidia's data schema/model, including format, structure, and required field population. If any required information is missing (e.g., Company ID not detected) or it is incorrectly mapped, data related to unmapped entities can't be used, and entity mappings need to be first resolved. Only correctly formatted data with valid mappings (e.g., proper linkage to a defined legal entity) may be processed.

Only authorized users with appropriate privileges (administrator role) are permitted to import data into the OTPM application. The system prevents users with insufficient permissions from accessing the data import interface or executing import functions.

Once the data ingestion process (manual or API-based) is completed, application users are not permitted to modify the uploaded transactional data within the OTPM application. Any changes to financial data must occur at the source system level (e.g., ERP) and require a re-import into OTPM for updates to take effect. System ensures that audit trails are maintained, recording the source, timestamp, and user who performed the data import.

Aibidia

All data ingestion activities are logged and traceable for audit purposes. System ensures that audit trails are maintained, recording the source, timestamp, and user who performed the data import. Only admin role has access to log records.

3.1.3 Allocation and segmentation

Control Objective: Controls provide reasonable assurance that all accounts extracted from the ERP system are properly allocated and classified in accordance with the customer-defined account group hierarchy.

For P&L segmentation and Transaction Monitoring, the OTPM application enforces that each data row imported from the source system must be linked to a defined mapping rule prior to inclusion in the calculations. For P&L segmentation each mapping rule is required to be associated with an account group as defined in the customer-specific account hierarchy, an allocation type, and a transfer pricing policy. For Transaction Monitoring each mapping rule is required to be associated with a Transfer Pricing Policy. This control ensures that all data is processed in accordance with established mapping rules, supporting accurate and consistent allocation within the transfer pricing model.

For P&L segmentation OTPM application ensures that non-relevant accounts must be actively selected and marked as "Exclude for segmentation" or "Exclude from P&L" by the user. The system prevents unallocated or unreviewed accounts from being processed, enforcing completeness and accountability in the transfer pricing process.

The OTPM application performs automated validation checks during the creation of mapping rules to identify any conflicts with existing mappings and notifies the user accordingly. The user may choose to proceed with creating an overlapping rule if required. For P&L segmentation, the system enforces that only supported Allocation Types and Policies can be selected, preventing the configuration of invalid combinations. For Transaction Monitoring, the system enforces that user can only select Policy that is associated with the legal entities in the scope of the mapping rule. This control ensures the integrity and consistency of data allocation within the transfer pricing model.

The OTPM application enforces that users must select the Intangible asset dimension and explicitly map each individual asset, based on client-uploaded data, as either included or excluded from royalty calculations. Each included asset must be linked to a defined Intangible asset group. Additionally, users are required to specify, based on the uploaded data, which accounts are to be considered in the revenue base calculation and categorise each included account as either third party revenue or total revenue. This control ensures that all data is processed in accordance with established mapping rules, supporting accurate and consistent allocation in the scope of royalty calculations.

3.1.4 Transfer price reporting

Control Objective: Controls provide reasonable assurance that calculated margins for each legal entity and segment are accurately computed and clearly reported against customer-defined targets, enabling effective monitoring of transfer pricing compliance.



The OTPM application calculates margins (such as gross or operating margin) for each P&L segment within a legal entity based on mapped financial data. The application presents margin compliance status using both numerical values and colour-coded visual indicators: green indicates the target margin has been met, while red indicates the target margin has not been achieved. All calculations and visualisations are updated dynamically to reflect the most recent available data.

The OTPM application allocates and segments the financial data automatically based on the mapping rules identified and managed by the customer. The system compares the customer-defined target margin to the actual financial results and calculates a proposed adjustment amount per segment. Adjustments are calculated using pre-defined formulas based on the selected Profit Level indicators (e.g., Operating Margin, Net Cost Plus Margin). All modifications to OTPM application logic, including allocation rules and adjustment formulas, are managed in line with Aibidia's documented Change Management Process. The calculation methodologies are formally documented by Aibidia.

The OTPM application calculates royalties automatically based on user-defined mapping logic for the selected Intangible asset dimension and revenue base. The system determines and reports the to-be-paid royalty amounts for each Legal Entity, IP Owner, and Intangible asset group, as well as the to-be-received royalties per IP Owner. All calculations are performed using the latest available mapped data, ensuring that royalty obligations and entitlements are accurately monitored and reported in accordance with the established configuration.

The OTPM application performs automated transaction-level transfer pricing monitoring by applying user-defined mapping logic to link each transaction to the relevant transfer pricing policy. The system calculates the actual markup percentage for each transaction and compares it to the customer-defined target markup. Transactions with a deviation exceeding the specified threshold (X%) are automatically flagged as out of range for further review.

The OTPM application provides a built-in export function that enables the generation of structured reports in Excel format. These reports include detailed margin performance by segment, and adjustment calculations, supporting accurate and transparent transfer pricing reporting.

3.2 General IT controls

This section outlines General IT Controls (GITCs) that support the confidentiality, integrity, and availability of the OTPM platform. GITCs are foundational controls applied across an organization's IT environment to ensure that systems operate as intended and data is protected.

3.2.1 Access to applications and data

Control Objective: Controls provide reasonable assurance that logical access to Systems, cloud environments and applications is restricted to authorized personnel. This control objective applies to relevant applications, operating systems, databases and networks.



Aibidia maintains an established and documented Access Control Policy that outlines principles and procedures for user access management. This policy is reviewed periodically by management to ensure alignment with evolving business needs and security standards.

Access to Aibidia's internal network and cloud infrastructure are segregated from public networks. Access to Aibidia internal network is only permitted through a secure Virtual Private Network (VPN). All remote users, including employees and authorized subcontractors, are required to authenticate via the VPN before gaining access to any internal systems or network resources.

A formal access provisioning and de-provisioning process is in place for Aibidia's systems, applications, and cloud environments for all employees and subcontractors. All access requests are documented in an internal Slack channel. Access for terminated or transferred employees is revoked immediately upon role change or departure. All approvals, changes, and revocations are logged.

User access provisioning is governed by a formal process for assigning and revoking access to all systems and services based on user roles and responsibilities. Access requests are processed by the Aibidia Security Operations Control Team. Requests must include a business justification and access evaluation; if this information is missing, the request is escalated to the designated information owner for review and approval.

Privileged access (e.g., admin rights) is restricted to Security Operations Control Team members. The allocation of such permissions is reviewed regularly (on a quarterly basis), and governed by a least-privilege principle.

A formal process is in place for managing and distributing secret authentication information, including initial setup, reset, and revocation of credentials. Users are instructed to keep credentials confidential and follow secure practices.

Access rights for all Aibidia employees and external party users are removed immediately upon termination of their employment, contract, or agreement. If a user's role changes due to an internal transfer or change in responsibilities, their access is adjusted accordingly to reflect their new role. The Aibidia Security Operations Control Team is responsible for executing and verifying the removal or adjustment of access to Aibidia systems.

Aibidia enforces a secure logon process across its systems and infrastructure. All users must authenticate using unique credentials consisting of a username and a strong password that complies with Aibidia's password complexity requirements. In accordance with Aibidia's Information Security Policy, multi-factor authentication (MFA) is highly recommended.

Password management tools require users to create strong, complex passwords and enforce periodic password changes. System-enforced policies ensure password security best practices are met.

Access to program source code shall be restricted. Only authorized development team members can access and modify software source code source code management systems.



3.2.2 Software Development and change management

Control objective: *Controls provide reasonable assurance that applications development process follows the management process and changes to applications are authorized, tested, approved, properly implemented, and documented.*

Documented application development methodology defines Aibidia's formal development, maintenance and change management process that outlines requirements for developing new features and making changes to existing applications.

Changes to systems within the development lifecycle shall be controlled using formal change control procedures. The progress of the developed items from architectural changes to hotfixes follows a product planning process and it is monitored within various recurring meetings. All feature development items are tracked in a ticketing system.

When operating platforms are changed, business critical applications are reviewed and tested to ensure there is no adverse impact on organizational operations or security.

Principles for engineering secure systems has been established, documented, maintained and applied to any information system implementation efforts.

Software Development and change management segregation of environments. The development environment is logically separate from the staging and production environments. All deployments must pass QA and/or peer-review.

A formal testing and sign-off process is established and performed for all new releases. The Quality Assurance team is responsible for quality-assurance testing activities including feature, performance and regression testing as well as code review.

Core review can also have additional peer-review step. Results of performed tests are documented. QA and Product Management ensure that all release activities have been completed before new release can be deployed.

Ability to deploy application changes to customer environment is restricted to assigned and authorized personnel. Access rights to production environments is regularly reviewed.

3.2.3 System operations

Control Objective: *The controls provide reasonable assurance that system operations are appropriately documented, monitored, secured, and maintained to support the integrity, availability, and reliability of systems and data critical to business operations and financial reporting.*

Operating procedures for all critical systems, applications, environments and processes are clearly documented in a formalized format and made available to all users who need them.

System resource utilization, including CPU, memory, disk space, and network bandwidth, is continuously monitored using automated monitoring tools by the Aibidia Security Operations Control Team (SOCT). Predefined threshold limits are set for critical system metrics. When thresholds are exceeded, automated alerts are generated and sent to the SOCT for immediate



investigation and corrective action. Capacity utilization trends are reviewed quarterly, and necessary tuning actions are performed to optimize system performance.

Backup copies of information, software, and system images are performed automatically according to the Aibidia Backup Policy. Backups are scheduled daily for critical systems and weekly for non-critical systems. The Aibidia Infrastructure Team monitors backup completion through automated backup reports. Backup restorations are tested at least annually to validate the integrity and effectiveness of backup processes. Exceptions or backup failures are logged and investigated.

Event logs capturing user activities, security events, exceptions, and system faults are generated automatically across all critical cloud infrastructure environments. Logs are collected and stored centrally in accordance with the Aibidia Logging and Monitoring Policy. Automatic alerts are configured for critical events, which will be investigated by Aibidia Security Operations Control Team (SOCT). All log data generated is protected through encryption, access controls, and monitoring in accordance with the Aibidia Logging and Monitoring Policy. Access to logging facilities is restricted to authorized personnel in the Aibidia Security Operations Control Team (SOCT).

The Aibidia SOC Team monitors technical vulnerabilities utilizing scanning tools and systems. Vulnerability scanning is performed regularly to identify applicable vulnerabilities. All identified vulnerabilities are evaluated based on their severity and impact. Critical vulnerabilities are prioritized in remediation efforts. Remediation actions are tracked through the ticketing system. Any exception cases where vulnerabilities cannot be remediated must be specifically approved.

Vulnerability assessments are performed as needed during normal operations and penetration tests are conducted quarterly by an independent external service provider. The penetration testing scope covers all Aibidia software products, with special focus on new features, particularly where security is a primary concern. Findings are documented in formal test reports. All identified vulnerabilities are evaluated based on severity and impact and prioritized for remediation.

An Information Security Incident Response Procedure is established, documented, and communicated to all relevant employees. The procedure defines roles, responsibilities, escalation paths, and required actions for responding to information security incidents. The Aibidia Information Security Management Team (ISMT) is responsible for executing incident response activities. All information security incidents are handled according to the documented procedure, with incident reports logged, investigated, and resolved in a timely manner. Post-incident reviews are conducted for significant events to identify improvements. Training on the incident response process is provided annually.



4 Complementary User Entity Controls (CUECs)

Aibidia's control framework has been designed with the assumption that the User Entity (the Company) implements certain internal controls to support the achievement of the control objectives outlined in this report. These complementary controls are outside the scope of Aibidia's responsibility and are critical for ensuring that transfer pricing processes operate effectively.

There may also be additional control objectives and related controls specific to the User Entity that are not covered in this report. In some cases, controls implemented by the User Entity may differ from or complement those described herein. Such controls should be considered by the User Entity and its auditors when evaluating the overall effectiveness of its internal control environment in relation to transfer pricing.

The following complementary controls are excluded from the scope of Aibidia's control activities and must be implemented and operated by the User Entity. These controls are provided as considerations and are not intended to be an exhaustive list.

OPTM master data management

Control objective: *Controls provide reasonable assurance that all organization master data elements relevant to transfer pricing are properly created, structured, and maintained in the OTPM application.*

User Entity is responsible for the following:

1. User organization is responsible for defining and maintenance of organization legal entity structure.
2. User organization is responsible for the content and structure of the TP policies.
3. User organization is responsible for ensuring that benchmark data used for transfer pricing is up to date.
4. User organization is responsible for ensuring that Intangible asset group data used for Royalty calculation is up to date.

Data Import

Control Objective: *To provide reasonable assurance that financial data imported into the OTPM application maintains integrity, completeness, and accuracy, and that its structure aligns with the required schema throughout the transfer pricing process.*

User Entity is responsible for the following:

5. The User organization is responsible for ensuring that the source data is complete and structured according to the schema provided by Aibidia.
6. The User organizations must review validation errors and correct data issues before re-attempting the import.
7. The User organizations must also maintain and monitor updates in source systems that could affect data structure (e.g., new fields or formats).

Aibidia

8. The User organization is responsible for assigning and maintaining user roles in line with internal access management policies.

Segmentation and Allocation

Control objective: To provide reasonable assurance that all accounts extracted from the ERP system are accurately allocated and classified in accordance with the defined account group hierarchy.

User Entity is responsible for the following:

9. The User organization must configure and maintain the account group hierarchy in the OTPM solution to reflect their reporting structure, business processes, and transfer pricing policies.
10. The User organization is responsible for defining, maintaining, and regularly reviewing the mapping rules that associate source data with P&L segmentation and transaction monitoring. They must ensure that all relevant data rows are accurately mapped in accordance with their internal allocation logic, and promptly update mappings to reflect any changes in business structure or reporting requirements.
11. The User organization is responsible for performing reconciliation between the source data and the accounts included in or excluded from the transfer pricing calculation.
12. The User organization is responsible for maintaining the mapping of intangible assets and revenue accounts used in royalty calculations. They must also review and update these mappings to reflect changes in their business structure.

Monitoring

Control objective: To provide reasonable assurance that calculated margins for each legal entity and policy segment are accurate and clearly reported against defined targets.

User Entity is responsible for the following:

13. The User organization is responsible for reviewing and validating proposed royalty payments and recording these to ERP or accounting systems.
14. The User organization is responsible for reviewing and validating proposed adjustments and recording adjustments in ERP or accounting systems.

Access to applications and data

Control Objective: To provide reasonable assurance that logical access to Systems, cloud environments and applications is restricted to authorized personnel. This control objective applies to relevant applications, operating systems, databases and networks.

SECTION FOUR



DESCRIPTION OF TESTING PERFORMED

Intended Use of this Section

This report on controls placed in operation and tests of operating effectiveness is intended to provide Aibidia and their end users with information sufficient to obtain an understanding of those aspects of Aibidia's controls that may be relevant to their internal control as it relates to an audit of financial statements.

It is Aibidia's end users' responsibility to evaluate this information in relation to their own internal controls to obtain an understanding of the internal controls and control risk.

Tests of Operating Effectiveness of Controls

Our tests of operating effectiveness of controls included such tests as were considered necessary in the circumstances to determine whether those controls, and the extent of compliance with them, were sufficient to provide reasonable assurance that the specified control objectives were achieved throughout the period 1st November 2025 to 30th June 2026. Our tests of operating effectiveness were designed to cover the period from 1st November 2025 to 30th June 2026 and were applied to those controls relating to control objectives specified by Aibidia. In selecting particular tests of the operating effectiveness of controls, we considered the (a) nature of the items being tested; (b) types and persuasiveness of available evidential matter; (c) nature of the audit objectives to be achieved; (d) assessed level of control risk; and (e) expected efficiency and effectiveness of the tests.

The types of tests of operating effectiveness of controls included the following:

Type of Test	Description
Inquiry	Discussed the controls with control performers and/or management who are 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 documents, reports, and other artefacts indicating the operation of the controls.
Reperformance	Reperformed activities undertaken by the control performer.

Related Parties and their Responsibilities

The control objectives and descriptions of controls presented below are the responsibility of Aibidia. The tests of operating effectiveness and results of those tests are the responsibility of KPMG.



Control #	Control title	Control description	Extent of audit procedures to evaluate the control's operating effectiveness	Testing results
Control Objective 1	Controls provide reasonable assurance that logical access to Systems, cloud environments and applications is restricted to authorized personnel. This control objective applies to relevant applications, operating systems, databases and networks			
APD-01	Access control policy	Aibidia maintains an established and documented Access Control Policy that outlines principles and procedures for user access management. This policy is reviewed periodically by management to ensure alignment with evolving business needs and security standards.	Inspected Aibidia's access control policy and noted that it defines that access to information must be specifically authorized. According to policy, accesses are given with least privilege principle. All users are authenticated using strong authentication methods.	No exceptions noted.
APD-02	Access to networks and network services	Access to Aibidia's internal network and cloud infrastructure are segregated from public networks. Access to Aibidia internal network is only permitted through a secure Virtual Private Network (VPN). All remote users, including employees and authorized subcontractors, are required to authenticate via the VPN before gaining access to any internal systems or network resources.	Inspected Aibidia's information security policy. Inquired if VPN is used everywhere. Auditors were informed that VPN is needed to connect to Aibidia's internal network. Accesses are managed through VPN. Inspected that external users have their own accounts separated from internal users with 'external' prefix in their email.	No exceptions noted.



Control #	Control title	Control description	Extent of audit procedures to evaluate the control's operating effectiveness	Testing results
APD-03	User registration and de-registration	A formal access provisioning and de-provisioning process is in place for Aibidia's systems, applications, and cloud environments for all employees and subcontractors. All access requests are documented in an internal Slack channel. Access for terminated or transferred employees is revoked immediately upon role change or departure. All approvals, changes, and revocations are logged.	Inspected the lists of new joiners and leavers. New users are given training materials containing the basic information of the company. Tickets are created in Asana, where their onboarding is tracked. Leavers are tracked through unique offboarding checklists where access removals are tracked. Inspected a selection of both leaver and joiner tickets.	No exceptions noted.
APD-04	User access provisioning	User access provisioning is governed by a formal process for assigning and revoking access to all systems and services based on user roles and responsibilities. Access requests are processed by the Aibidia Security Operations Control Team. Requests must include a business justification and access evaluation; if this information is missing, the request is escalated to the designated information owner for review and approval.	Observed Aibidia's internal Slack to determine how new accesses are granted to existing users. A new message is sent to a Slack channel where request for access is described. The access is then either approved or disapproved by the Security Operations Control Team. Inspected a selection of access requests to determine that all required steps are taken.	No exceptions noted.
APD-05	Management of privileged access rights	Privileged access (e.g., admin rights) is restricted to Security Operations Control Team members. The allocation of such permissions is reviewed regularly (on a quarterly basis), and governed by a least-privilege principle.	Inspected Aibidia's Security Operation Control team and its members. Inquired if accesses are reviewed time to time. KPMG Inspected Aibidia's Security Operation Control team and its members. Inspected the latest access review. Inquired how often the accesses are reviewed and were informed that the first review has been conducted on 27th of March.	No exceptions noted.



Control #	Control title	Control description	Extent of audit procedures to evaluate the control's operating effectiveness	Testing results
APD-06	Secret authentication information of users	A formal process is in place for managing and distributing secret authentication information, including initial setup, reset, and revocation of credentials. Users are instructed to keep credentials confidential and follow secure practices.	Inspected Aibidia's information security policy to determine how passwords and other secrets are handled. New workers are sent a link where they can create a new password for themselves. Protonpass passwords are used if SSO is not enabled for that service. Password resets are handled through Entra ID.	No exceptions noted.
APD-07	Removal or adjustment of access rights	Access rights for all Aibidia employees and external party users are removed immediately upon termination of their employment, contract, or agreement. If a user's role changes due to an internal transfer or change in responsibilities, their access is adjusted accordingly to reflect their new role. The Aibidia Security Operations Control Team is responsible for executing and verifying the removal or adjustment of access to Aibidia systems.	Inspected Aibidia's leaver checklists to determine that accesses are removed systemically from the leavers. Inquired if external users go through the same process as internal users and were informed that external users go through the same process as internal users.	No exceptions noted.
APD-08	Secure logon procedure	Aibidia enforces a secure logon process across its systems and infrastructure. All users must authenticate using unique credentials consisting of a username and a strong password that complies with Aibidia's password complexity requirements. In accordance with Aibidia's Information Security Policy, multi-factor authentication (MFA) is highly recommended.	Inspected Aibidia's information security policy to determine how secure logon policies are enforced. MFA is in use for all applications that support it. Entra ID is in use for enforcing password policies through company applications	No exceptions noted.



Control #	Control title	Control description	Extent of audit procedures to evaluate the control's operating effectiveness	Testing results
APD-09	Password management system	Password management tools require users to create strong, complex passwords and enforce periodic password changes. System-enforced policies ensure password security best practices are met.	Observed Aibidia's password management tool. Tool clearly shows users what is a strong password, however it allows creation of weaker passwords. The password complexity is always enforced through the system and password manager is only used for storing passwords.	No exceptions noted.
APD-10	Access control to program source code	Access to program source code shall be restricted. Only authorized development team members are able to access and modify software source code source code management systems.	Observed that source code is stored in Azure Devops. Access to repository is maintained through Entra ID groups. Access to code is done through normal access requests.	No exceptions noted.
Control Objective 2	Controls provide reasonable assurance that applications development process follows the management process and changes to applications are authorized, tested, approved, properly implemented, and documented.			
SDLC-01	Secure development policy	Documented application development methodology defines Aibidias formal development, maintenance and change management process that outlines requirements for developing new features and making changes to existing applications.	Inspected Aibidias Secure Development policy. Policy has been updated and followed. Inspected related policies to determine that methodology and engineering steps are described in them.	No exceptions noted.
SDLC-02	System change control procedures	Changes to systems within the development lifecycle shall be controlled using formal change control procedures. The progress of the developed items from architectural changes to hotfixes follows a product planning process and it is monitored within various recurring meetings. All feature development items are tracked in a ticketing system.	Inspected Aibidia's ticketing system to determine that all changes are ticketed. Inspected version control system settings and oted that at least one code review is required before code can be approved. Inspected selection of Aibidia's pull requests to determine that change management process has been followed correctly.	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>



Control #	Control title	Control description	Extent of audit procedures to evaluate the control's operating effectiveness	Testing results
				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 changes are required, Aibidia will require documented justification and retrospective review. The configuration and process reinforcement will be completed by Q3 2026.



Control #	Control title	Control description	Extent of audit procedures to evaluate the control's operating effectiveness	Testing results
SDLC-03	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Inspected Aibidia's Quality assurance processes. All tests are conducted in test environment that is similar to production environment.	No exceptions noted.
SDLC-04	Secure system engineering principles	Principles for engineering secure systems has been established, documented, maintained and applied to any information system implementation efforts.	Inspected Aibidia's ISMS powerpoint to determine how documentation related to engineering processes are reviewed and maintained.	No exceptions noted.
SDLC-05	Segregation of environments	Software Development and change management segregation of environments. The development environment is logically separate from the staging and production environments. All deployments must pass QA and/or peer-review.	Inspected Aibidia's development environment architecture. Development and test environment are in the same network and accessible to developers. UAT and Production environments are in the same network, but only accessible by the customer facing teams.	No exceptions noted.
SDLC-06	Software Development and change management	A formal testing and sign-off process is established and performed for all new releases. The Quality Assurance team is responsible for quality-assurance testing activities including: feature, performance and regression testing as well as code review. Core review can also have additional peer-review step. Results of performed tests are documented.	Inspected Aibidia's Quality Assurance and ISMS processes to determine what tests and activities need to be taken before changes are pushed to production. Different teams have clearly defined roles and what steps these teams need to take during the change management process.	No exceptions noted.
SDLC-07	System acceptance testing	QA and Product Management ensure that all release activities have been completed before new release can be deployed.	Inspected Aibidias Quality Assurance Processes to determine what release activities need to be completed before pushing to production.	No exceptions noted.



Control #	Control title	Control description	Extent of audit procedures to evaluate the control's operating effectiveness	Testing results
			Observed Aibidia's QA board where tests are shown per Epic.	
SDLC-08	Production Deployment	Ability to deploy application changes to customer environment is restricted to assigned and authorized personnel. Access rights to production environments is regularly reviewed.	Inspected Aibidia's deployment plan. After all the tests have been successfully done to release version, any developer can push the version from UAT to production.	No exceptions noted.
Control Objective 3	The controls provide reasonable assurance that system operations are appropriately documented, monitored, secured, and maintained to support the integrity, availability, and reliability of systems and data critical to business operations and financial reporting.			
SO-1	Operating procedures	Operating procedures for all critical systems, applications, environments and processes are clearly documented in a formalized format and made available to all users who need them.	Inspected Aibidia's risk management listing where every Aibidia asset is listed. All assets have asset owner, risk level, classification and if there is any Personally Identifiable Information in the system.	No exceptions noted.
SO-2	System resource utilisation monitoring	System resource utilization, including CPU, memory, disk space, and network bandwidth, is continuously monitored using automated monitoring tools by the Aibidia Security Operations Control Team (SOCT). Predefined threshold limits are set for critical system metrics. When thresholds are exceeded, automated alerts are generated and sent to the SOCT for immediate investigation and corrective action. Capacity utilization trends are reviewed quarterly, and necessary tuning actions are performed to optimize system performance.	Observed Aibidia's resource and utilisation monitoring tool. Alerts are automated to a dedicated Slack channel if any resource is near its limit. Inspected Aibidia's internal documentation related to monitoring and dashboards.	No exceptions noted.



Control #	Control title	Control description	Extent of audit procedures to evaluate the control's operating effectiveness	Testing results
SO-3	Data backup and recovery	Backup copies of information, software, and system images are performed automatically according to the Aibidia Backup Policy. Backups are scheduled daily for critical systems and weekly for non-critical systems. The Aibidia Infrastructure Team monitors backup completion through automated backup reports. Backup restorations are tested at least annually to validate the integrity and effectiveness of backup processes. Exceptions or backup failures are logged and investigated.	Inspected Aibidia's Backup and restore procedure documentation. Documentation shows how often databases are backed up and how restoration is done. Inspected one backup restoration sample.	No exceptions noted.
SO-4	Event monitoring	Event logs capturing user activities, security events, exceptions, and system faults are generated automatically across all critical cloud infrastructure environments. Logs are collected and stored centrally in accordance with the Aibidia Logging and Monitoring Policy. Automatic alerts are configured for critical events, which will be investigated by Aibidia Security Operations Control Team (SOCT).	Inspected Aibidia's logging and monitoring process. Alerts are automated is anything suspicious is found. Observed Aibidia's internal Slack channel where these alerts are posted.	No exceptions noted.
SO-5	Access to log data	All log data generated is protected through encryption, access controls, and monitoring in accordance with the Aibidia Logging and Monitoring Policy. Access to logging facilities is restricted to authorized personnel in the Aibidia Security Operations Control Team (SOCT)	Inspected access to Aibidia's logging tool. Access is handled through Entra ID group. Data is encrypted using Azure's encryption policy.	No exceptions noted.
SO-6	Vulnerability management	The Aibidia SOC Team monitors technical vulnerabilities utilizing scanning tools and systems. Vulnerability scanning is performed regularly to identify applicable vulnerabilities. All identified vulnerabilities are evaluated based on their severity and impact. Critical vulnerabilities are prioritized in remediation	Inspected Aibidia's Vulnerability Management Policy. Automated vulnerability scan is handled through automated software that creates PR's if it finds anything. Auditors inquired if any more steps are taken with these and were informed that these are then manually reviewed.	No exceptions noted.



Control #	Control title	Control description	Extent of audit procedures to evaluate the control's operating effectiveness	Testing results
		efforts. Remediation actions are tracked through the ticketing system. Any exception cases where vulnerabilities cannot be remediated must be specifically approved.	Inspected a selection of vulnerability PR's.	
SO-8	Regular vulnerability and penetration testing	Vulnerability assessments are performed as needed during normal operations and penetration tests are conducted quarterly by an independent external service provider. The penetration testing scope covers all Aibidia software products, with special focus on new features, particularly where security is a primary concern. Findings are documented in formal test reports. All identified vulnerabilities are evaluated based on severity and impact, and prioritized for remediation.	Inspected a sample of Aibidia's quarterly penetration test reports and noted that the tests are done and findings are documented and followed up.	No exceptions noted.
SO-9	Incident management procedures	An Information Security Incident Response Procedure is established, documented, and communicated to all relevant employees. The procedure defines roles, responsibilities, escalation paths, and required actions for responding to information security incidents. The Aibidia Information Security Management Team (ISMT) is responsible for executing incident response activities. All information security incidents are handled according to the documented procedure, with incident reports logged, investigated, and resolved in a timely manner. Post-incident reviews are conducted for significant events to identify improvements. Training on the incident response process is provided annually.	Inspected Aibidia's Incident management process and a sample of incidents and noted that they were properly responded and documented.	No exceptions noted.



Control #	Control title	Control description	Extent of audit procedures to evaluate the control's operating effectiveness	Testing results
Control Objective 4	Controls provide reasonable assurance that all organization master data elements relevant to transfer pricing are properly created, structured, and maintained in the OTPM application.			
1	Legal entity structure	Organization legal entities, relevant to transfer pricing, are created and maintained in the OTPM application. Each Entity has a unique Entity ID and OTPM enables legal entity to be divided into one or more reporting units, which will be assigned to a parent legal entity. OTPM application prevents duplicate Entity IDs, ensuring integrity in entity mapping.	Inspected that the system requires a unique entity ID and entity name when creating a new legal entity and that the system displays an error message if these fields are missing or non-unique. Also inspected that each entity can be divided into one or more reporting units.	No exceptions noted.
2	Transfer Pricing Policy Setup	The OTPM application enforces the configuration of each TP policy with the following mandatory fields: — Policy Name (TP policy name must be unique) — Policy Type (Function, Transactional) — Transfer Pricing Method (e.g. Transactional Net Margin Method, Cost Plus Method, Not Transfer Pricing Method) — Profit Level Indicator (PLI) (e.g., Operating Margin, Net Cost Plus Margin) System will prompt a remark if some TP policy is missing mapped benchmark for some TP Policy-Legal Entity combination. Each policy is eventually shown as a segment within an entity in P&L monitoring page.	Observed in the production environment that the system enforces entry of required fields when creating a TP policy and prevents creation of policies with non-unique names. Also inspected that the system prompts users if a mapped benchmark is missing before completion. Also inspected the P&L monitoring page to confirm that each TP policy appears as a distinct segment within the relevant legal entity.	No exceptions noted.



Control #	Control title	Control description	Extent of audit procedures to evaluate the control's operating effectiveness	Testing results
3	Creation of the Account hierarchy	The OTPM application requires each user organization to establish an Account hierarchy as part of the transfer pricing model configuration. The account hierarchy defines the account groups to which imported financial data will be allocated and segmented. Each account group must be classified with an Account Type (Revenue, COGS, OPEX) and an income or expense definition. These classifications are used to structure segmented P&L and calculate Profit Level Indicator (PLI) value for each relevant Policy segment. Application requires that there is at least one Account Group enabled so that financial data can be allocated.	Inspected that the system requires creation of an account hierarchy before transfer pricing model setup and prevents linking data if no account groups are defined. Also inspected that account groups require classification by account type and income/expense definition. Tested that allocation of financial data cannot proceed until at least one account group is enabled.	No exceptions noted.
4	Targets settings & Benchmark data	OTPM allows upload and definition of target margin records for each TP policy segment. Target margins may be based on benchmark studies, internal comparables, or management-defined targets. Each benchmark or target study must have a unique identifier. For Function type TP Policies, every target margin record must be linked to a valid combination of Legal Entity (Entity ID) and TP Policy. For Transactional type TP Policies, every target margin record must be linked to a valid combination of Legal Entity (Entity ID), Counterparty (Entity ID), and TP Policy. A validity period (e.g., fiscal years) must be specified for each benchmark record to ensure accuracy over time. The system performs validation to ensure all required fields and linkages are present; if any are missing, an error message is generated and the benchmark record is excluded from calculations.	Inspected that each record requires a unique identifier and that the system prevents duplicates. Also inspected that mandatory fields for comparability targets must be completed before saving. Tested that target margin records require appropriate linkages and that unmapped benchmarks prompt user action. Inspected that a validity period is required and validated system restrictions on field entries. Tested that incomplete benchmark records are rejected and excluded from calculations.	No exceptions noted.



Control #	Control title	Control description	Extent of audit procedures to evaluate the control's operating effectiveness	Testing results
5	Intangible asset group setup	The OTPM application allows the creation of Intangible asset groups, each of which must be linked to an IP Owner, which is a Legal Entity (Entity ID). Royalty calculations related to each Intangible asset group are only performed when a valid Royalty rate (percentage between 0 and 100), Royalty base (Total revenue or Third party revenue), and Legal Entities within the royalty scope have been defined. The system validates the presence and correctness of these required fields before enabling royalty calculations.	Inspected that intangible asset groups must be linked to a Legal Entity as IP Owner. Aalso inspected that the system requires valid royalty rate, royalty base, and selection of legal entities before calculations are enabled, and that only valid numeric royalty rates are accepted. Tested that the IP owner cannot be included among royalty payers and that missing or invalid required fields prevent calculation.	No exceptions noted.
Control Objective 5	Controls provide reasonable assurance that financial data imported into the Aibidia OTPM solution maintains integrity, completeness, and accuracy, and that the data structure aligns with the defined schema throughout the transfer pricing process.			
6	Data ingestion process	During the data ingestion process, the mandatory fields required to be mapped from the imported dataset depend on the selected Extract Type. For Multi Level Segmentation, the following fields are mandatory: Company ID, Account ID, and at least one of the following—Local Value or Group Value. For Transaction Monitoring, the following fields are mandatory: Company ID and at least one of the following—FOB Price, TP in sell currency, SAP TP price, TP Base Cost, Other Costs, Total TP Cost, or Markup Amount. The system enforces these requirements by validating the presence and correct mapping of these fields prior to processing the ingested data.	Inspected that the system enforces mandatory field mapping requirements based on the selected Extract Type and prevents saving configurations with missing or incorrectly mapped required fields. Also tested that data ingestion is blocked if required fields are missing or incorrectly typed.	No exceptions noted.



Control #	Control title	Control description	Extent of audit procedures to evaluate the control's operating effectiveness	Testing results
7	Secure data transmission interfaces	OTPM supports data ingestion through both manual uploads and secure API connections. Both are using encryption and authentication protocols to ensure secure data transmission.	Inspected that manual data ingestion is required before enabling automated upload mode and that the system provides a one-time API key notification upon activation. Also inspected technical documentation and system configuration to confirm that both ingestion methods use encryption and authentication protocols.	No exceptions noted.
8	Data validation	The OTPM platform automatically performs data validation checks at the time of financial data ingestion (manual and API-based). The application validates whether the data aligns with the Aibidia's data schema/model, including format, structure, and required field population. If any required information is missing (e.g., Company ID not detected) or it is incorrectly mapped, data related to unmapped entities can't be used, and entity mappings need to be first resolved. Only correctly formatted data with valid mappings (e.g., proper linkage to a defined legal entity) may be processed.	Inspected that the system validates imported data against the required schema and rejects files with missing or incorrectly mapped fields, displaying error messages. Also inspected that only data with valid formatting and correct entity mappings is accepted for processing.	No exceptions noted.
9	Data ingestion permissions	Only authorized users with appropriate privileges (administrator role) are permitted to ingest data into the OTPM application. The system prevents users with insufficient permissions from accessing the data ingestion interface or executing import functions.	Inspected user roles and confirmed that only admin users can access the data ingestion interface and perform data import functions. Tested access with a non-admin account and confirmed that data ingestion functions were not accessible.	No exceptions noted.



Control #	Control title	Control description	Extent of audit procedures to evaluate the control's operating effectiveness	Testing results
10	Data modification is prevented	Once the data ingestion process (manual or API-based) is completed, application users are not permitted to modify the uploaded transactional data within the OTPM application. Any changes to financial data must occur at the source system level (e.g., ERP) and require a re-import into OTPM for updates to take effect. System ensures that audit trails are maintained, recording the source, timestamp, and user who performed the data import.	Inspected that imported transactional data cannot be modified directly in the system and that updates require re-import from the source system. Also inspected the audit trail, confirming that each import records the data source, timestamp, and user, and that audit trail records cannot be altered.	No exceptions noted.
11	Track record of all changes in the application.	All data ingestion activities are logged and traceable for audit purposes. System ensures that audit trails are maintained, recording the source, timestamp, and user who performed the data import. Only admin role has access to log records.	Inspected that all data ingestion activities are automatically logged with source, timestamp, and user details. Tested access to audit logs and confirmed that only admin users can view or access Activity Tracker, while non-admin users are restricted.	No exceptions noted.
Control Objective 6	Controls provide reasonable assurance that all financial data extracted from the source system is properly allocated and classified in accordance with the customer-defined allocation and segmentation logic.			
12	Mapping enforcement	For P&L segmentation and Transaction Monitoring, the OTPM application enforces that each data row imported from the source system must be linked to a defined mapping rule prior to inclusion in the calculations. For P&L segmentation each mapping rule is required to be associated with an account group as defined in the customer-specific account hierarchy, an allocation type, and a transfer pricing policy. For Transaction Monitoring each mapping rule is required to be associated with a Transfer Pricing Policy.	Inspected that each imported data row must be linked to a defined mapping rule before inclusion in calculations. Tested that mapping rules require linkage to an account group, allocation type, and transfer pricing policy, and confirmed that removal of a mapping rule excludes related data from calculations.	No exceptions noted.



Control #	Control title	Control description	Extent of audit procedures to evaluate the control's operating effectiveness	Testing results
		This control ensures that all data is processed in accordance with established mapping rules, supporting accurate and consistent allocation within the transfer pricing model.		
13	Excluded account selection	For P&L segmentation OTPM application ensures that non-relevant accounts must be actively selected and marked as "Exclude for segmentation" or "Exclude from P&L" by the user. The system prevents unallocated or unreviewed accounts from being processed, enforcing completeness and accountability in the transfer pricing process.	Inspected that users must actively mark non-relevant accounts as excluded from segmentation or P&L during the account review process. Tested that the system prompts users to review all accounts and indicates unprocessed accounts, and confirmed that excluded accounts are handled as intended in segmentation and total figures.	No exceptions noted.
14	Data allocation validation and error handling	The OTPM application performs automated validation checks during the creation of mapping rules to identify any conflicts with existing mappings and notifies the user accordingly. The user may choose to proceed with creating an overlapping rule if required. For P&L segmentation, the system enforces that only supported Allocation Types and Policies can be selected, preventing the configuration of invalid combinations. For Transaction Monitoring, the system enforces that user can only select Policy that is associated with the legal entities in the scope of the mapping rule. This control ensures the integrity and consistency of data allocation within the transfer pricing model.	Inspected that the system performs automated validation checks during mapping rule creation and notifies users of conflicts or overlaps. Also inspected that only supported allocation types and transfer pricing policies can be selected, and that TP policies are restricted to those associated with the legal entities in scope.	No exceptions noted.



Control #	Control title	Control description	Extent of audit procedures to evaluate the control's operating effectiveness	Testing results
15	Royalty configuration	The OTPM application enforces that users must select the Intangible asset dimension and explicitly map each individual asset, based on client-uploaded data, as either included or excluded from royalty calculations. Each included asset must be linked to a defined Intangible asset group. Additionally, users are required to specify, based on the uploaded data, which accounts are to be considered in the revenue base calculation and categorise each included account as either third party revenue or total revenue. This control ensures that all data is processed in accordance with established mapping rules, supporting accurate and consistent allocation in the scope of royalty calculations.	Inspected that the system enforces selection of the intangible asset dimension and requires explicit mapping of each asset as included or excluded from royalty calculations. Noted that included assets must be linked to a defined intangible asset group and that accounts in the revenue base must be categorised as either third party revenue or total revenue.	No exceptions noted.
Control Objective 7	Controls provide reasonable assurance that calculated margins for each legal entity and policy segment are accurate and clearly reported against defined targets.			
16	Margin calculation and performance monitoring	The OTPM application calculates margins (such as gross or operating margin) for each P&L segment within a legal entity based on mapped financial data. The application presents margin compliance status using both numerical values and colour-coded visual indicators: green indicates the target margin has been met, while red indicates the target margin has not been achieved. All calculations and visualisations are updated dynamically to reflect the most recent available data.	Inspected that the system calculates margins for each P&L segment based on mapped financial data and confirmed alignment with source data. Tested that operating margin and net cost plus margin calculations are accurate. Also inspected the margin compliance dashboard, confirming that numerical values and colour-coded indicators reflect compliance status and update appropriately when target margins change.	No exceptions noted.
17	P&L monitoring	The OTPM application allocates and segments the financial data automatically based on the mapping rules	Inspected that the system allocates and segments financial data according to mapping	No exceptions noted.



Control #	Control title	Control description	Extent of audit procedures to evaluate the control's operating effectiveness	Testing results
	and adjustments	identified and managed by the customer. The system compares the customer-defined target margin to the actual financial results and calculates a proposed adjustment amount per segment. Adjustments are calculated using pre-defined formulas based on the selected Profit Level indicators (e.g., Operating Margin, Net Cost Plus Margin). All modifications to OTPM application logic, including allocation rules and adjustment formulas, are managed in line with Aibidia's documented Change Management Process. The calculation methodologies are formally documented by Aibidia.	rules and calculates proposed adjustment amounts per segment using pre-defined formulas. Tested the accuracy of proposed adjustments and inspected that calculation methodologies are formally documented.	
18	Royalty monitoring	The OTPM application calculates royalties automatically based on user-defined mapping logic for the selected Intangible asset dimension and revenue base. The system determines and reports the to-be-paid royalty amounts for each Legal Entity, IP Owner, and Intangible asset group, as well as the to-be-received royalties per IP Owner. All calculations are performed using the latest available mapped data, ensuring that royalty obligations and entitlements are accurately monitored and reported in accordance with the established configuration.	Inspected that the system calculates royalties automatically based on user-defined mapping logic for intangible assets and revenue base. Reviewed royalty calculation reports and tested that to-be-paid and to-be-received royalty amounts are determined and calculated correctly for each relevant entity and asset group.	No exceptions noted.
19	Transaction monitoring	The OTPM application performs automated transaction-level transfer pricing monitoring by applying user-defined mapping logic to link each transaction to the relevant transfer pricing policy. The system calculates the actual markup percentage for each transaction and compares it to the customer-defined target markup. Transactions with a deviation exceeding the specified	Inspected that the system applies mapping logic to link transactions to transfer pricing policies and calculates actual markup and markup variance percentages. Tested that transactions exceeding the specified threshold are automatically flagged by the system for further review.	No exceptions noted.



Control #	Control title	Control description	Extent of audit procedures to evaluate the control's operating effectiveness	Testing results
		threshold (X%) are automatically flagged as out of range for further review.		
20	TP Reporting – Data Export	The OTPM application provides a built-in export function that enables the generation of structured reports in Excel format. These reports include detailed margin performance by segment, and adjustment calculations, supporting accurate and transparent transfer pricing reporting.	Inspected that the application provides a built-in export function for generating structured Excel report. Reviewed sample export and confirmed that report include legal entity code, legal entity name, IP owner, legal entity name of the IP owner, intangible asset group name, and royalty amount to be invoices (YTD).	No exceptions noted.