



AI
AI & Partners

User Manual for Orthrus

Version 1.0

Last Updated: 03 November 2023

Contents

Introduction	5
About Orthrus	5
Purpose of this Manual	5
Target Audience	5
Getting Started	6
3.1 System Requirements	6
3.2 Accessing the Tool	6
3.3 Logging In	6
3.4 User Roles and Permissions	6
Overview of Orthrus	7
Dashboard	7
Navigation	7
Key Features	7
Terminology and Definitions	8
Inside Orthrus	9
Feature 1 - AI Identification	9
Steps to Use Feature 1:	9
Feature 2 - Risk Classification	9
Steps to Use Feature 2:	9
Feature 3 - Risk Reports	9
Steps to Use Feature 3:	9
Feature 4 - Post-Market Monitoring	10
Steps to Use Feature 4:	10
Specific Processes in Orthrus	11
Adding an AI System to Orthrus	11
Step 1: Logging In	11
Step 2: Navigating to the AIP Sandbox Section	11
Step 3: Opening the 'Governance' Tab and Selecting 'Assets'	12
Step 4: Creating a New Asset	12
Step 5: Inserting Asset Information	13
Risk Classify an AI System in Orthrus	14
Step 1: Logging In	14
Step 2: Navigating to the AIP Sandbox Section	14
Step 3: Opening the 'Governance' Tab and Selecting 'Assets'	15
Step 4: Selecting the Asset to Risk Classify	15



Step 5: Initiating Risk Classification	16
Step 6: Pre-populating Data Fields	17
Step 7: Answering Questions and Providing Documentation.....	17
Step 8: Completing Risk Analysis	18
Adding an User to Orthrus: A Step-by-Step Guide.....	19
Step 1: Logging In	19
Step 2: Navigating to the AIP Sandbox Section.....	19
Step 3: Opening the 'Governance' Tab and Selecting 'People'.....	20
Step 4: Creating a New User	20
Step 5: Entering User Information	21
Step 6: Granting Administrative Authorisation.....	22
Step 7: Setting Authorisation Level	22
Adding a Document to Orthrus: A Step-by-Step Guide	23
Step 1: Logging In	23
Step 2: Navigating to the AIP Sandbox Section.....	23
Step 3: Opening the Compliance Tab and Selecting 'Documents'.....	24
Step 4: Upload a New Document.....	24
Step 5: Upload a New Document.....	25
Step 6: Upload Your File and Select All Salient Information.....	25
Step 7: Setting Authorisation Level	26
Adding a Control to Orthrus: A Step-by-Step Guide	27
Step 1: Logging In	27
Step 2: Navigating to the AIP Sandbox Section.....	27
Step 3: Opening the Risk Tab and Selecting 'Controls'.....	28
Step 4: Insert Salient Information on Control	28
Adding a External Organisation to Orthrus: A Step-by-Step Guide.....	29
Step 1: Logging In	29
Step 2: Navigating to the AIP Sandbox Section.....	29
Step 3: Opening the Governance Tab and Selecting 'External Organisations'.....	30
Step 4: Add a New Organisation	30
Step 5: Add a All Salient Information for the External Organisation	31
Regulatory Compliance	33
EU AI Act Overview	33
Key Regulatory Requirements	33
Compliance Deadlines.....	33
How Orthrus Helps with Compliance	34



AI System Registration	34
Risk Classification	34
Monitoring and Reporting	34
Customization and Flexibility.....	34
Configuring Regulatory Rules.....	35
Rule-Based Configuration	35
Custom Compliance Policies	35
Monitoring and Reporting	36
Automated Monitoring	36
Alerts and Notifications	36
Compliance and Reports	36
Audit Trails.....	36
Data Management and Security	37
Data Input and Import	37
Data Export.....	37
Data Privacy and Security Measures	37
Compliance with Data Regulations.....	37
Troubleshooting	39
Common Issues and Solutions	39
Problem 1: Login Issues.....	39
Problem 2: Slow Performance	39
Problem 3: Data Import Errors.....	39
Reporting Bugs and Issues	39
Technical Support Contacts	40
Updates and Maintenance.....	41
Updating Orthrus.....	41
Step 1: Check for Updates	41
Step 2: Download and Install Updates	41
Step 3: Verify Functionality.....	41
8.2 Backup and Recovery	41
Regular Backups:	41
Data Recovery:	41
8.3 Version History	41
Check Orthrus Documentation:	41
Review Release Notes:.....	41
Ensuring Data Integrity	42



Conclusion	43
Recap and Best Practices	43
Summary of Key Points	43
Best Practices for Efficient Use	43
Checklist for Success	43
Feedback and Improvement	44
We Value Your Feedback	44
How to Provide Feedback	44
Continuous Improvement	44
Appendix A: Glossary of Terms	46
Appendix B: Regulatory Compliance References	48
AI System Identification	48
Recital	48
Article	48
Annex	49
Post-Market Monitoring System	50
Recital	50
Article	50
Risk Management System	52
Recital	52
Article	52
Appendix C: Frequently Asked Questions (FAQs)	54
1. What is Orthrus?	54
2. What are the system requirements for Orthrus?	54
3. How do I configure regulatory rules in Orthrus?	54
4. What should I do if I encounter an issue with Orthrus?	54
5. How often is Orthrus updated?	54
6. What kind of training resources are available for Orthrus users?	54
7. How can I provide feedback or suggestions for improvement?	54
8. How can I access the Glossary of Terms in this manual?	54
9. Where can I find detailed information on the EU AI Act?	54
10. Is there a certification program available for Orthrus users?	54

Introduction

Welcome to the user manual for Orthrus, your trusted RegTech tool designed to streamline compliance with the EU AI Act. This section provides an overview of the manual, giving you essential insights into Orthrus and how to make the most of this guide.

About Orthrus

Orthrus is a powerful Regulatory Technology (“RegTech”) tool that simplifies compliance with the European Union's AI Act. It enables organizations to meet regulatory requirements efficiently, reducing complexity and ensuring adherence to AI governance standards..

Purpose of this Manual

The purpose of this manual (the “Manual”) is to serve as a comprehensive resource for users of Orthrus. It aims to empower you with the knowledge and guidance needed to effectively utilize the software, ensuring you can seamlessly integrate it into your compliance processes. Whether you're a newcomer or an experienced user, the Manual is designed to accommodate users of all levels of expertise.

Target Audience

The Manual is crafted to cater to a diverse audience, including but not limited to:

- **Junior Staff:** Those new to Orthrus or AI compliance will find this manual an invaluable resource to kickstart their journey.
- **Senior Staff:** Experienced professionals can use this manual as a reference guide to ensure they're up-to-date with Orthrus's latest features and capabilities.
- **Compliance Officers:** Those responsible for ensuring their organizations' adherence to AI regulations will discover comprehensive guidance in this manual.
- **Technical Teams:** IT and technical teams will find relevant information to support system requirements, installation, and maintenance.
- **Decision Makers:** Managers and decision-makers can gain insights into how Orthrus enhances AI compliance within their organizations.

By the end of the Manual, you will have a clear understanding of Orthrus's key features, regulatory compliance capabilities, data management, troubleshooting, updates, and the wealth of training and resources available to you. We've designed the Manual to be a user-friendly and informative companion on your journey to AI Act compliance using Orthrus.

If you're ready to dive in, proceed to the "Getting Started" section, where you'll learn about system requirements and the installation and setup of Orthrus. Thank you for choosing Orthrus as your AI compliance solution.

All terms in bold are defined in **Appendix A**.

Getting Started

Welcome to Orthrus, the web-based RegTech tool for EU AI Act compliance. This section will guide you through the process of accessing Orthrus via our online website. Before you begin, ensure that you meet the system requirements outlined in Section 2.

3.1 System Requirements

Before you can access Orthrus, make sure your system meets the following requirements:

- **Internet Connection:** A stable internet connection is essential for seamless access to Orthrus.
- **Web Browser:** We recommend using the latest version of popular web browsers such as Google Chrome, Mozilla Firefox, or Microsoft Edge for the best experience.
- **Device:** You can access Orthrus from various devices, including desktop computers, laptops, and tablets.

3.2 Accessing the Tool

To access Orthrus, follow these simple steps:

- Open your preferred web browser on your device.
- In the address bar, type the Orthrus website URL provided to you.
- Press "Enter" or click the "Go" button.
- You will be directed to the Orthrus login page.

3.3 Logging In

If you already have an Orthrus account, you can log in using your credentials. Here's how:

- Enter your registered email address in the "Email" field.
- Type your password in the "Password" field.
- Click the "Log In" button.
- If your login information is correct, you will be redirected to the Orthrus dashboard.

3.4 User Roles and Permissions

Orthrus offers various user roles with specific permissions to ensure secure and controlled access. The roles may include administrators, analysts, and reviewers, each with their unique access rights. To understand and manage user roles and permissions:

- After logging in, navigate to the "Settings" or "User Management" section.
- Here, you can create and manage user accounts, assign roles, and define permissions.
- Be sure to allocate roles and permissions according to the responsibilities of your team members.

With these steps, you can easily access Orthrus via our online website, ensuring that you are well-prepared to begin your journey towards EU AI Act compliance. If you encounter any issues during the login process, refer to the "Troubleshooting" section (Section 7) for common issues and solutions or contact our technical support for assistance.

Now that you've accessed Orthrus successfully, you're ready to explore the platform's features and capabilities. In the following sections, we will provide an overview of Orthrus, explain its key features, and guide you through the process of using this powerful tool for AI system identification, risk classification, risk reporting, and post-market monitoring.

Overview of Orthrus

Welcome to the section that will give you a comprehensive understanding of Orthrus, your trusted RegTech tool for EU AI Act compliance. In this part, we will delve into the various aspects of Orthrus, ensuring that users of all levels of seniority, including junior staff, can grasp the key features and concepts.

Dashboard

The Orthrus dashboard serves as your command center, providing an at-a-glance overview of the critical information and activities. It's designed to be intuitive and user-friendly. Here's what you can expect from the dashboard:

- **Data at a Glance:** The dashboard displays essential data related to AI systems, risk classifications, risk reports, and post-market monitoring in a visually informative manner.
- **Quick Navigation:** Access key functions directly from the dashboard, such as creating risk reports, setting up monitoring, and viewing recent compliance status.
- **Customization:** Tailor your dashboard to display the information most relevant to your role and responsibilities.
- **Notifications:** Stay informed with real-time notifications about important updates, compliance alerts, and system events.

Navigation

Orthrus offers a straightforward navigation structure to ensure ease of use:

- **Main Menu:** Access various modules and functionalities through the main menu, organized logically based on your tasks and roles.
- **Search:** Use the search bar to locate specific AI systems, risk reports, or other data elements efficiently.

Key Features

Orthrus boasts a range of features to help you effectively manage AI systems and ensure EU AI Act compliance:

- **AI Identification (Feature 1 - AI Identification):** Orthrus enables you to add AI systems to the platform, providing details such as system type, purpose, and manufacturer. You can also import AI system data to streamline the process.
- **Risk Classification (Feature 2 - Risk Classification):** With this feature, you can classify AI systems into risk categories based on predefined criteria or custom rules. The risk classification process is integral to ensuring compliance.
- **Risk Reports (Feature 3 - Risk Reports):** Orthrus allows you to generate comprehensive risk reports for individual AI systems. These reports are based on the risk classification output and provide detailed insights into each system's compliance status.
- **Post-Market Monitoring (Feature 4 - Post-Market Monitoring):** This feature is essential for continuously monitoring AI systems in the post-market phase. It helps identify and address compliance issues that may arise over time.

Terminology and Definitions

Orthrus employs specific terminology and definitions that are essential to understand while using the tool. Some key terms and their meanings include:

- **AI System:** Any software, device, or system that uses artificial intelligence techniques to perform tasks.
- **Risk Classification:** The process of categorizing AI systems into different risk groups based on regulatory criteria.
- **Risk Report:** A detailed document that outlines the risk classification and compliance status of an AI system.
- **Post-Market Monitoring:** The ongoing assessment of AI systems once they are in use to ensure ongoing compliance with the EU AI Act.
- **Compliance Status:** An indication of whether an AI system adheres to the regulatory requirements specified in the EU AI Act.

This overview is designed to provide a foundation of knowledge as you start using Orthrus. For more detailed information on each feature, refer to the subsequent sections in this manual. Whether you're a junior staff member or a seasoned professional, understanding these key concepts will be crucial for effectively using Orthrus to ensure compliance with the EU AI Act.

Inside Orthrus

In this section, we will explore the key features of Orthrus.

Feature 1 - AI Identification

Purpose: Feature 1 enables users to identify AI systems within Orthrus, an essential step in ensuring compliance with the EU AI Act.

Steps to Use Feature 1:

- **Accessing AI Identification:** To access the AI Identification feature, log in to Orthrus and navigate to the main menu. You'll find "AI Identification" listed as a menu item.
- **Adding AI Systems:** Click on "AI Identification" and select "Add AI System." Fill in the required details, such as system type, purpose, and manufacturer.
- **Importing AI System Data:** Orthrus allows you to streamline the process by importing AI system data in bulk. Click on "Import" and follow the prompts.
- **Managing AI System Details:** You can view and edit AI system details by selecting the specific system from the list.

Feature 2 - Risk Classification

Purpose: This feature allows users to categorize AI systems into risk groups, a critical step in ensuring compliance with regulatory requirements.

Steps to Use Feature 2:

- **Accessing Risk Classification:** To access the Risk Classification feature, log in to Orthrus and navigate to the main menu. Click on "Risk Classification."
- **Classifying AI Systems:** Select the AI system you want to classify and choose the appropriate risk category based on predefined criteria or custom rules.
- **Viewing Classification Results:** Once classified, you can view the system's risk category and associated information. Orthrus provides an overview of the classification result.

Feature 3 - Risk Reports

Purpose: Feature 3 empowers users to generate comprehensive risk reports for individual AI systems, providing detailed insights into each system's compliance status.

Steps to Use Feature 3:

- **Accessing Risk Reports:** To create a risk report, log in to Orthrus and navigate to the main menu. Click on "Risk Reports."
- **Selecting AI System:** Choose the AI system for which you want to generate a risk report. Orthrus provides a list of all AI systems and their risk classifications.
- **Generating the Report:** Click "Generate Report" and Orthrus will automatically create a detailed risk report based on the risk classification output. This report outlines the system's compliance status and any associated risks.
- **Review and Distribution:** Review the generated report and distribute it as needed to stakeholders for compliance documentation.

Feature 4 - Post-Market Monitoring

Purpose: Feature 4 is crucial for continuously monitoring AI systems in the post-market phase to ensure ongoing compliance with the EU AI Act.

Steps to Use Feature 4:

- **Accessing Post-Market Monitoring:** To conduct post-market monitoring, log in to Orthrus and navigate to the main menu. Click on "Post-Market Monitoring."
- **Selecting AI Systems:** Choose the AI systems you wish to monitor in the post-market phase. Orthrus provides a list of all AI systems.
- **Setting Monitoring Parameters:** Define the monitoring parameters, including data collection, compliance checks, and reporting frequency.
- **Initiating Monitoring:** Start the post-market monitoring process. Orthrus will continuously assess the AI systems and provide alerts for any compliance issues.

By following these steps, users of all levels of seniority, including junior staff, can effectively use Orthrus to identify AI systems, classify them by risk, generate risk reports, and conduct post-market monitoring in compliance with the EU AI Act. This information is presented clearly and professionally to ensure a smooth and efficient user experience.

Specific Processes in Orthrus

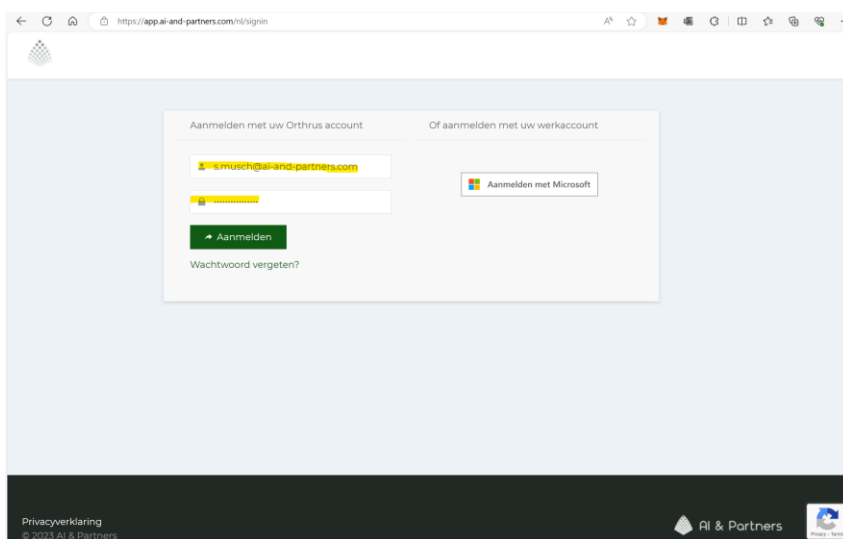
In this section, we will explore how to effectively use Orthrus to undertake specific tasks¹.

Adding an AI System to Orthrus

In Orthrus, you can easily add new assets to your organization. This step-by-step guide will walk you through the process. We've included screenshots to make it even more straightforward.

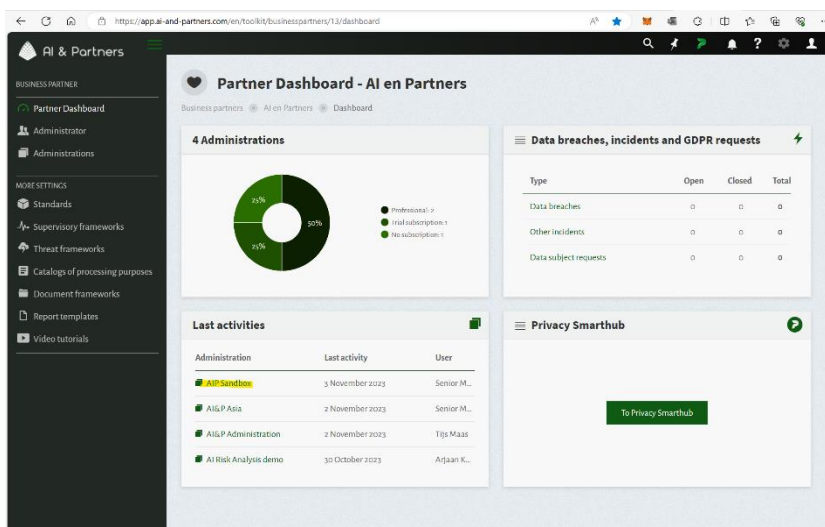
Step 1: Logging In

- Begin by visiting the Orthrus platform.
- Click on the "Sign In" button to log in to your account. Enter your login credentials, including your username and password. Click "Sign In" to access your account.



Step 2: Navigating to the AIP Sandbox Section

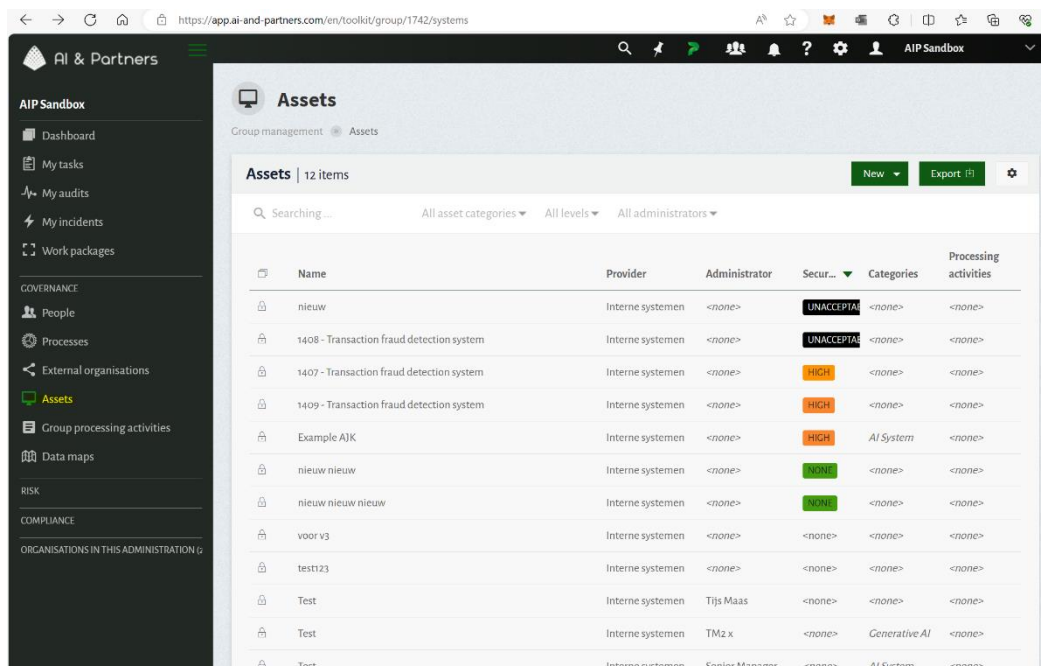
- Once you are logged in, you will arrive at your dashboard.
- Locate the "AIP Sandbox" section in the dashboard menu. Click on "AIP Sandbox" to proceed.



¹ All pictures have sections highlighted to represent the action being referred to in the description.

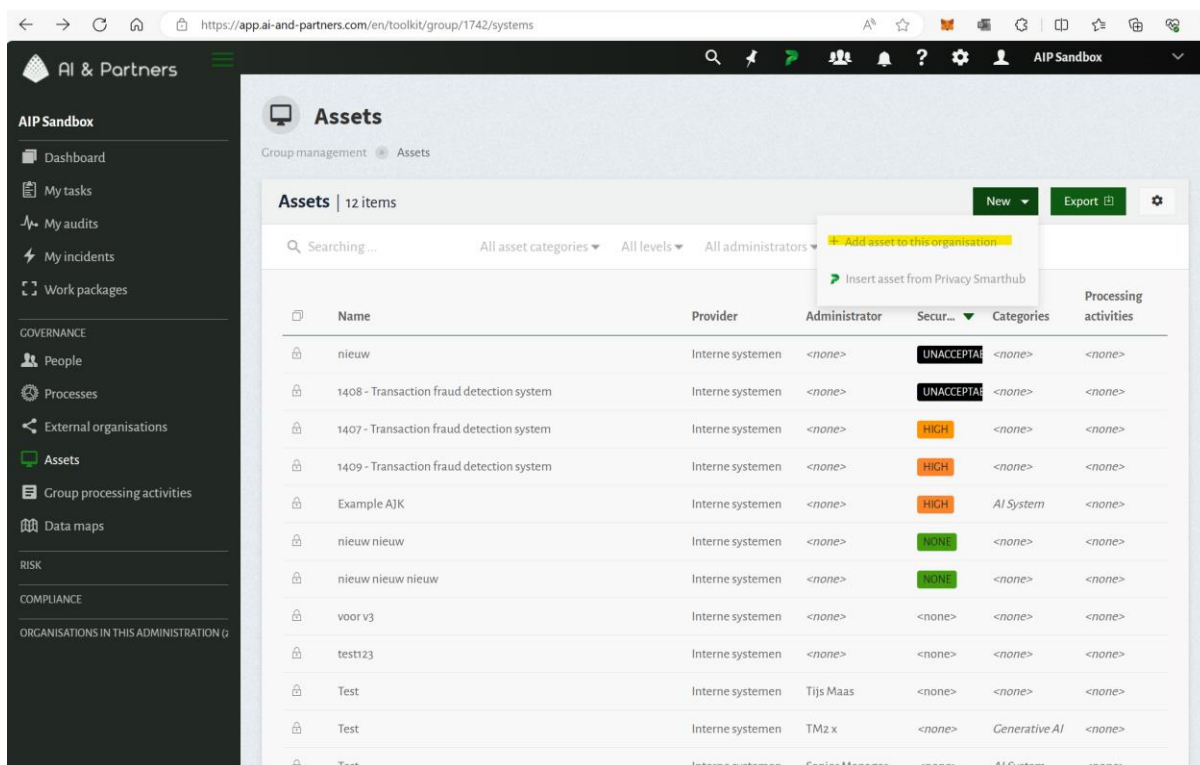
Step 3: Opening the 'Governance' Tab and Selecting 'Assets'

- Inside the AIP Sandbox, you will find the "Governance" tab. Click on it to reveal the available options.
- From the dropdown menu, select "Assets" to access the assets management section.



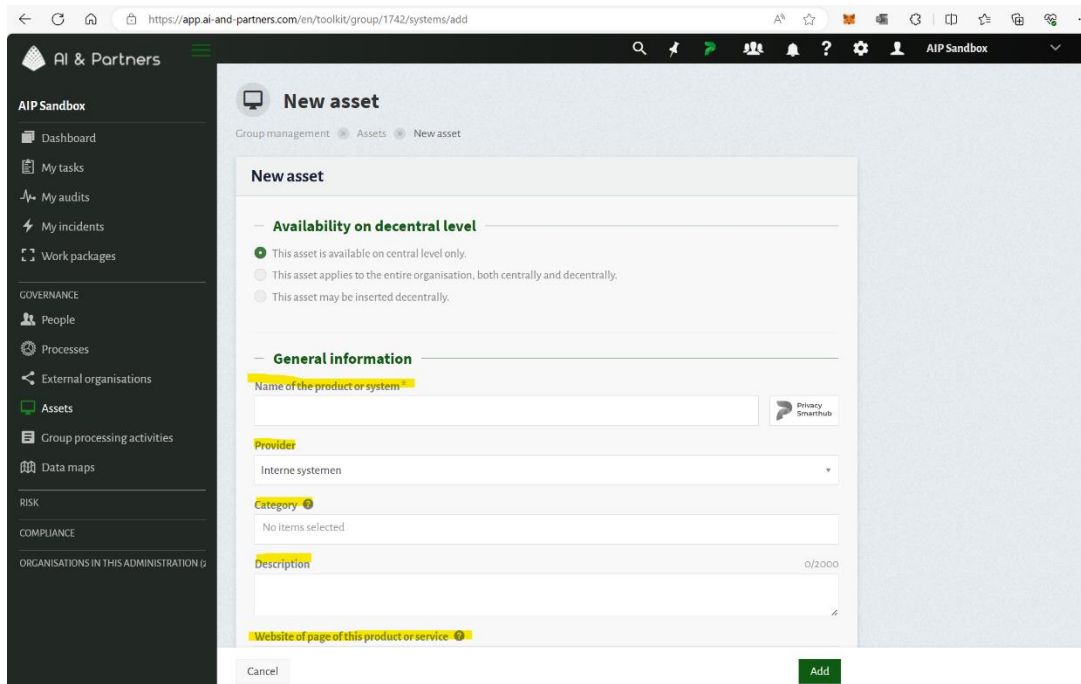
Step 4: Creating a New Asset

- In the "Assets" section, locate the "New" option.
- Hover your cursor over "New" to reveal a submenu.
- Select "Add Asset to this Organization" from the submenu.



Step 5: Inserting Asset Information

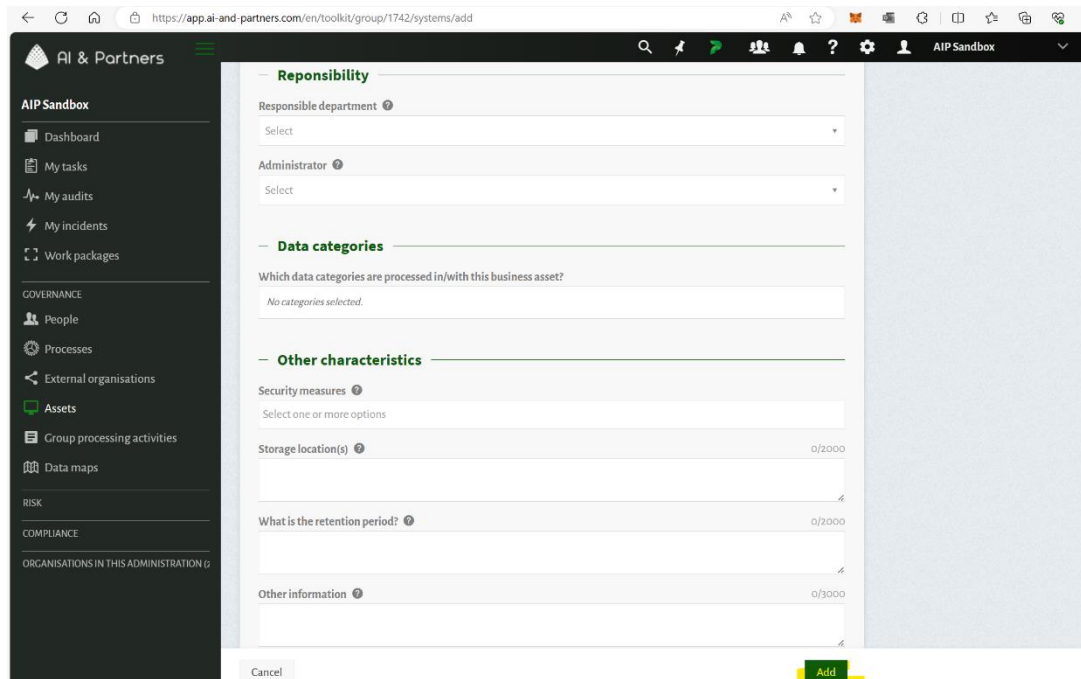
- You will be directed to a new page where you can input all the necessary information for the asset you wish to add.
- Fill in the relevant details, such as the asset name, description, category, and any other required information.
- Double-check the accuracy of the entered data.
- After ensuring all essential information is filled, click the "Add" button to create the new asset.



The screenshot shows the 'New asset' form in the AI & Partners application. The form is titled 'New asset' and is part of the 'Group management' section. It contains several sections for inputting asset information:

- Availability on decentral level:** Three radio buttons are present: 'This asset is available on central level only.' (selected), 'This asset applies to the entire organisation, both centrally and decentrally.', and 'This asset may be inserted decentrally.'
- General information:** Includes a text input for 'Name of the product or system', a dropdown for 'Provider' (currently set to 'Interne systemen'), a dropdown for 'Category' (currently 'No items selected'), a text input for 'Description' (with a 0/2000 character limit), and a text input for 'Website of page of this product or service'.

At the bottom of the form, there are 'Cancel' and 'Add' buttons.



The screenshot shows the 'Responsibility' and 'Data categories' sections of the 'New asset' form. The form is titled 'New asset' and is part of the 'Group management' section. It contains several sections for inputting asset information:

- Responsibility:** Includes a dropdown for 'Responsible department' (currently 'Select') and a dropdown for 'Administrator' (currently 'Select').
- Data categories:** A section titled 'Which data categories are processed in/with this business asset?' with a text input area showing 'No categories selected.'
- Other characteristics:** Includes a dropdown for 'Security measures' (with a note 'Select one or more options'), a text input for 'Storage location(s)' (with a 0/2000 character limit), a text input for 'What is the retention period?' (with a 0/2000 character limit), and a text input for 'Other information' (with a 0/3000 character limit).

At the bottom of the form, there are 'Cancel' and 'Add' buttons.

Congratulations! You've Successfully Added an Asset to Orthrus

Following these steps, you have successfully added a new asset to your Orthrus organization. It's essential to provide accurate and complete information for each asset to ensure effective AI Act compliance and risk management.

If you encounter any issues or need further assistance, please consult the "Troubleshooting" section of the user manual or reach out to our technical support team.

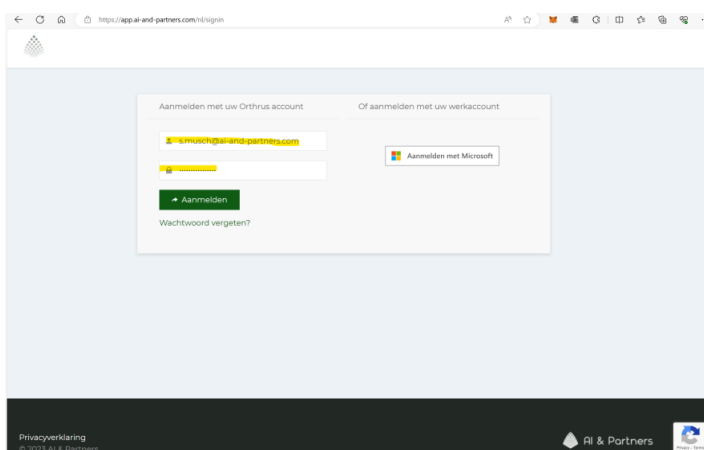
Orthrus is committed to making AI Act compliance a smooth and efficient process for all users, regardless of their level of seniority or experience.

Risk Classify an AI System in Orthrus

In Orthrus, the risk classification of assets is a critical step in ensuring compliance with the EU AI Act. This step-by-step guide will assist you in performing the risk classification process with ease. We have included screenshots to make it user-friendly and clear for users of all levels of seniority, including junior staff.

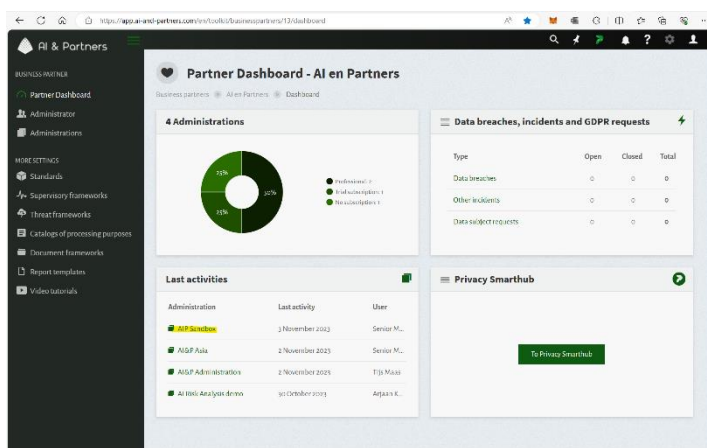
Step 1: Logging In

- Begin by visiting the Orthrus platform.
- Click on the "Sign In" button to log in to your Orthrus account. Enter your login credentials (username and password) and click "Sign In" to access your account.



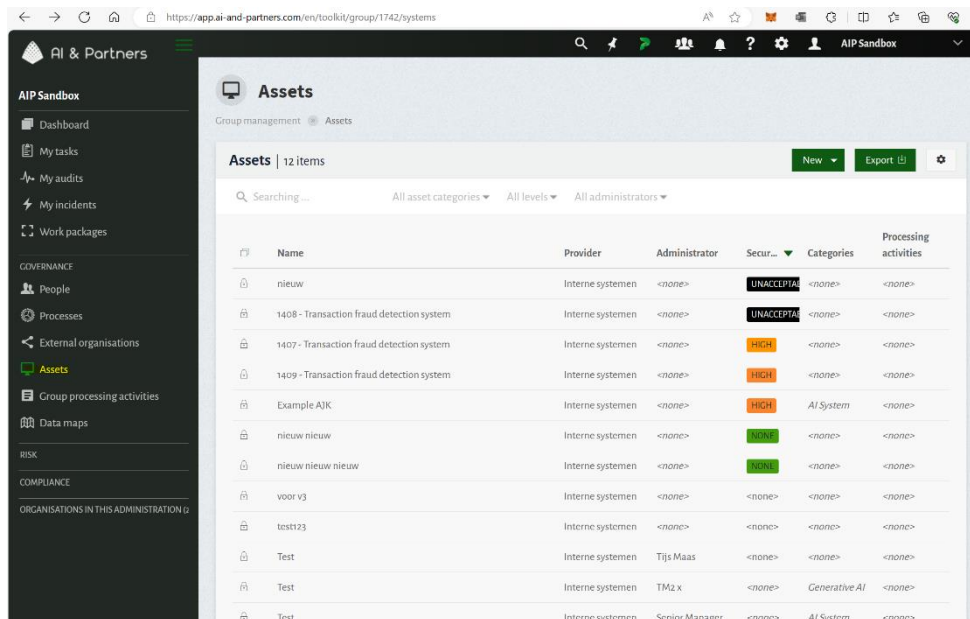
Step 2: Navigating to the AIP Sandbox Section

- After successfully logging in, you will be directed to your Orthrus dashboard.
- Look for the "AIP Sandbox" section in the dashboard menu. Click on "AIP Sandbox" to proceed.



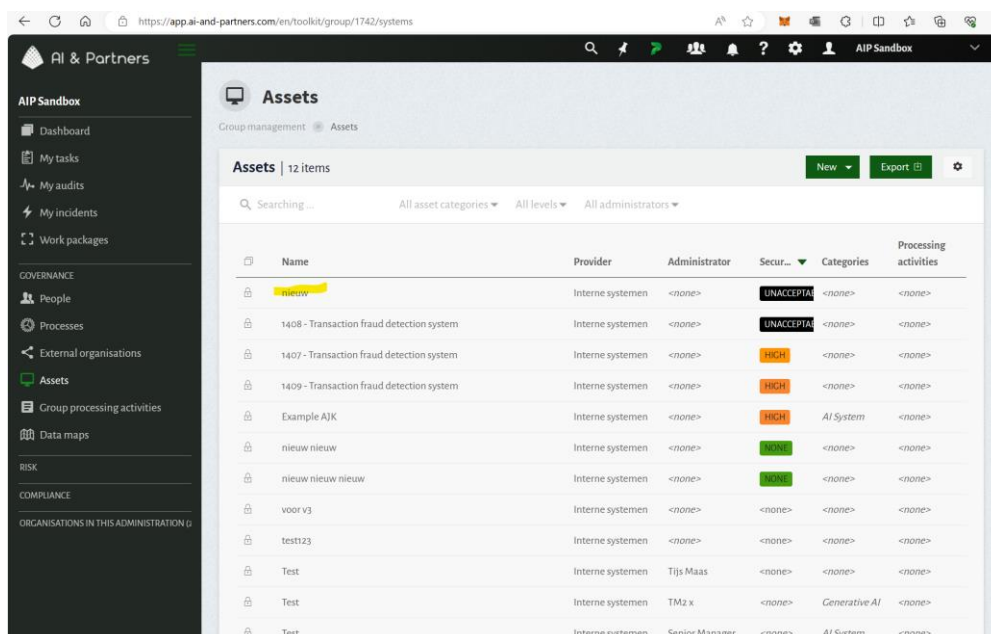
Step 3: Opening the 'Governance' Tab and Selecting 'Assets'

- In the "AIP Sandbox" section, you will find the "Governance" tab. Click on it to unveil the available options.
- From the dropdown menu, select "Assets" to access the assets management section.



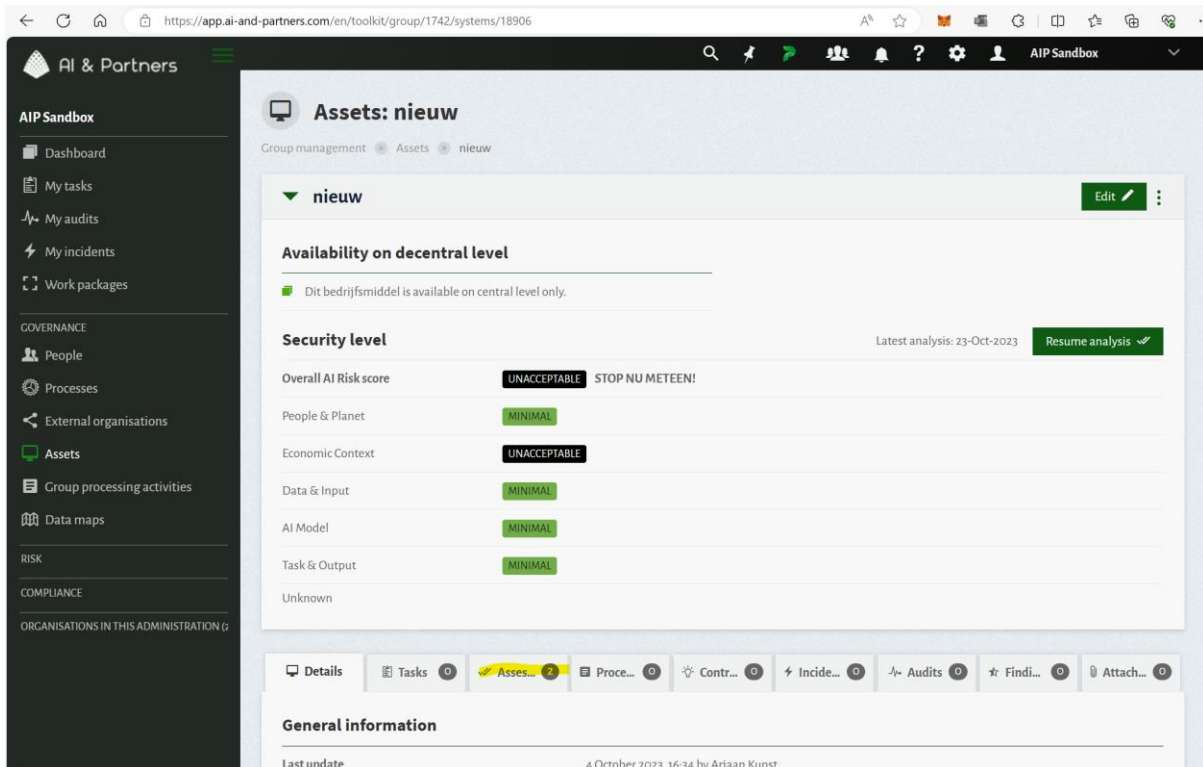
Step 4: Selecting the Asset to Risk Classify

- Inside the "Assets" section, you will see a list of assets associated with your organization.
- Locate and click on the asset that you wish to risk classify.



Step 5: Initiating Risk Classification

- After selecting the asset, navigate to the "Assessment" tab.
- Inside the "Assessment" tab, you will find the option to create a "New Analysis." Click on it.



Assets: nieuw

Group management Assets nieuw

nieuw Edit

Availability on decentral level

Dit bedrijfsmiddel is available on central level only.

Security level Latest analysis: 23-Oct-2023 Resume analysis

Overall AI Risk score **UNACCEPTABLE** STOP NU METEEN!

People & Planet **MINIMAL**

Economic Context **UNACCEPTABLE**

Data & Input **MINIMAL**

AI Model **MINIMAL**

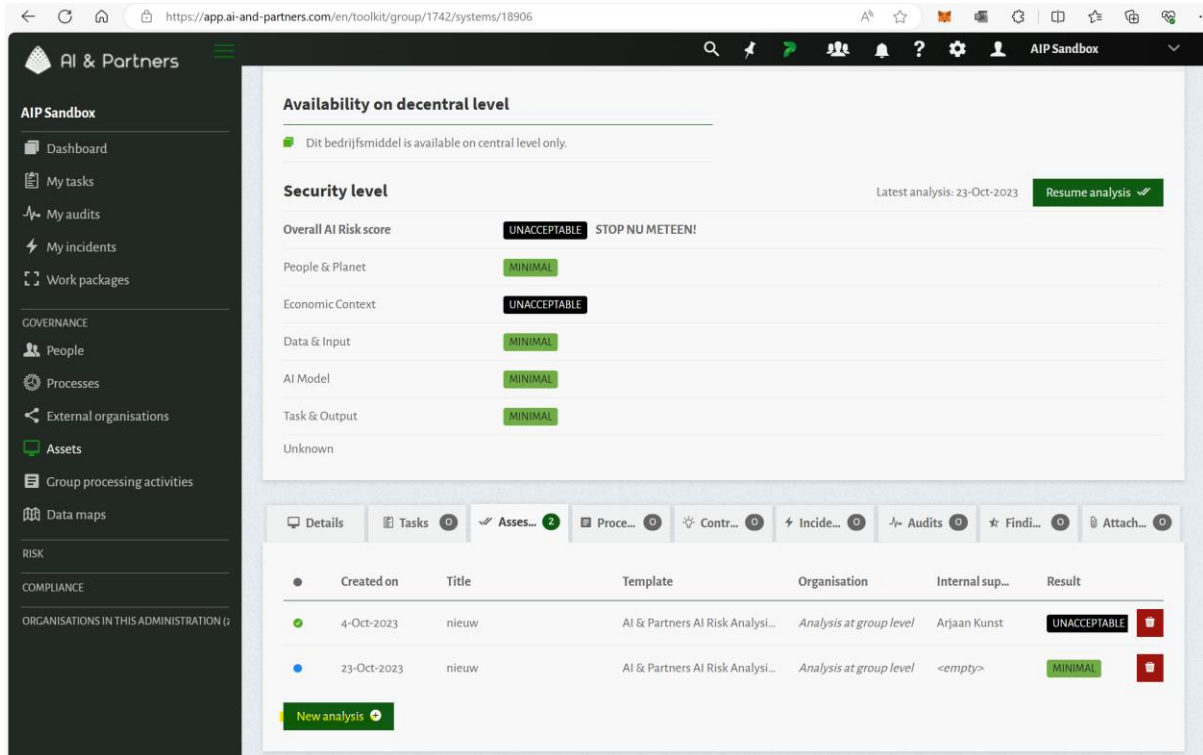
Task & Output **MINIMAL**

Unknown

Details Tasks Asses... 2 Proce... Contr... Incide... Audits Findi... Attach...

General information

Last update 4 October 2023, 16:34 by Arjaan Kunst



Assets: nieuw

Group management Assets nieuw

nieuw Edit

Availability on decentral level

Dit bedrijfsmiddel is available on central level only.

Security level Latest analysis: 23-Oct-2023 Resume analysis

Overall AI Risk score **UNACCEPTABLE** STOP NU METEEN!

People & Planet **MINIMAL**

Economic Context **UNACCEPTABLE**

Data & Input **MINIMAL**

AI Model **MINIMAL**

Task & Output **MINIMAL**

Unknown

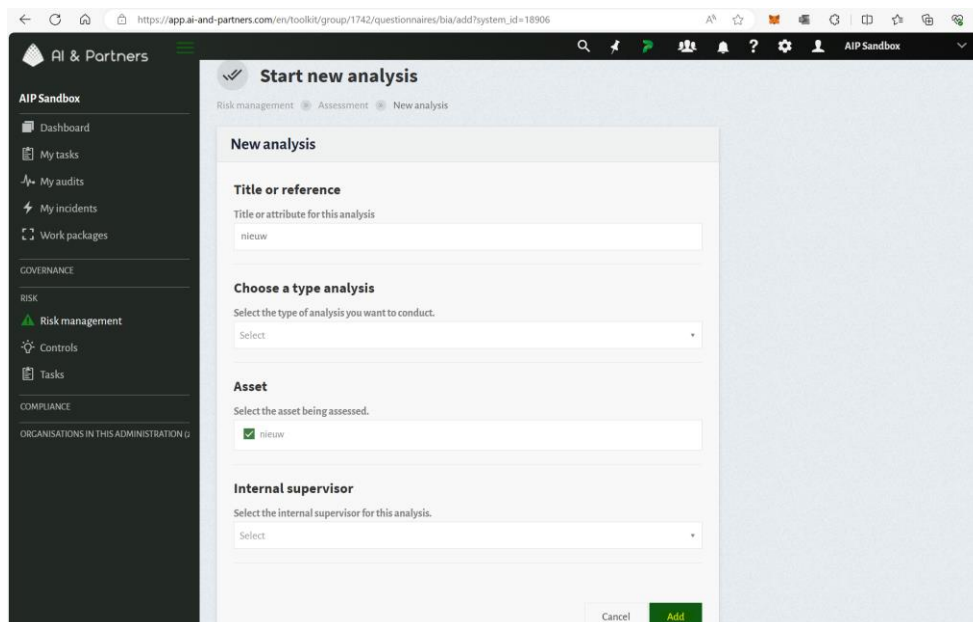
Details Tasks Asses... 2 Proce... Contr... Incide... Audits Findi... Attach...

Created on	Title	Template	Organisation	Internal sup...	Result
4-Oct-2023	nieuw	AI & Partners AI Risk Analy...	Analysis at group level	Arjaan Kunst	UNACCEPTABLE
23-Oct-2023	nieuw	AI & Partners AI Risk Analy...	Analysis at group level	<empty>	MINIMAL

New analysis

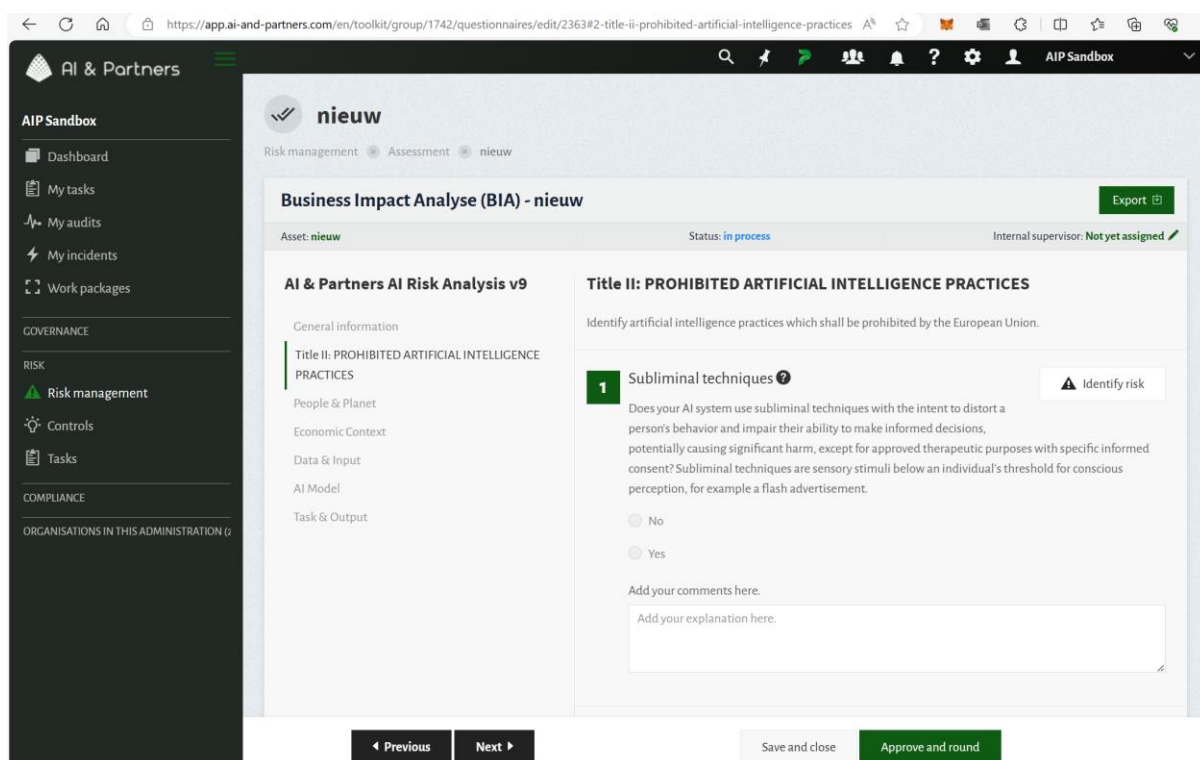
Step 6: Pre-populating Data Fields

- In the "New Analysis" section, you will need to pre-populate various data fields with the necessary information.
- Ensure that you have entered all required information.
- Click "Add" to proceed.



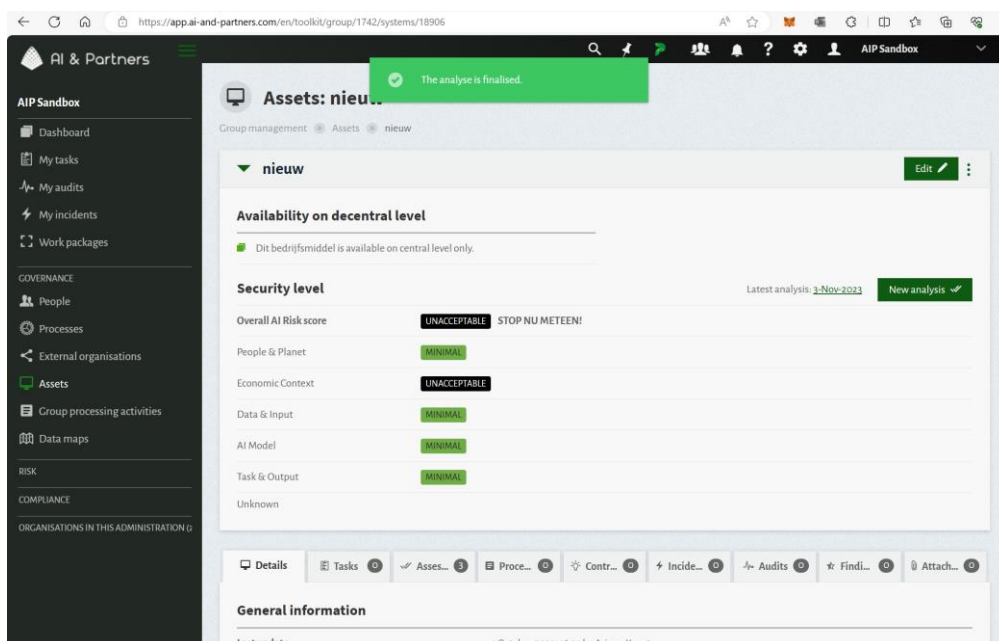
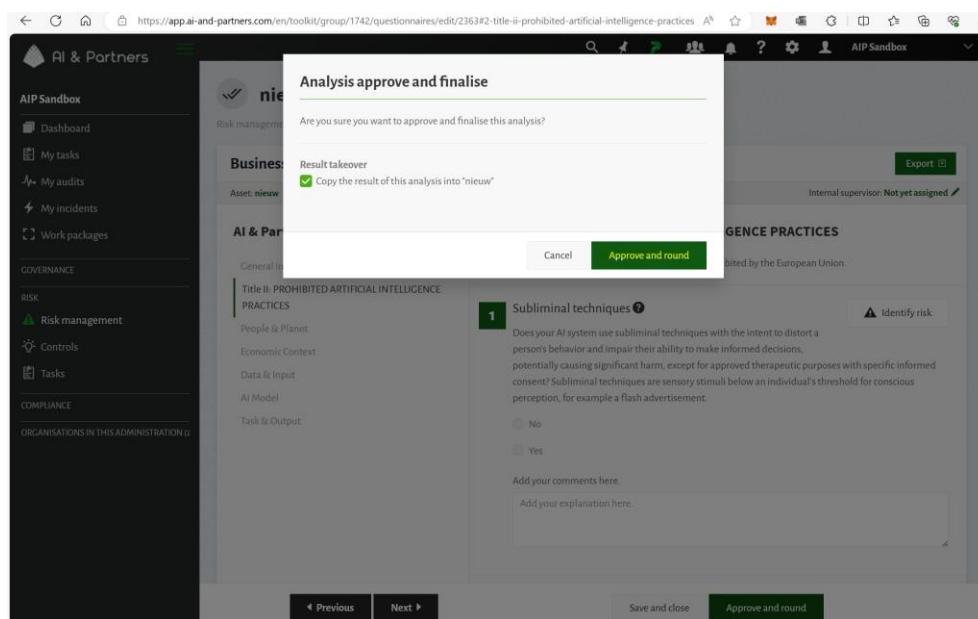
Step 7: Answering Questions and Providing Documentation

- You will be presented with a series of questions related to the risk classification process.
- For each question, select the appropriate answer, upload any required documentation, and provide supporting comments.
- Navigate through each section using the panel on the left-hand side.



Step 8: Completing Risk Analysis

- After going through all the questions and providing the necessary information, you will reach the final step.
- To complete the risk analysis, click "Submit for review."



Congratulations! You've Successfully Risk Classified an Asset in Orthrus

By following these steps, you have effectively risk classified an asset in Orthrus. This is a crucial component of ensuring compliance with the EU AI Act and managing risks associated with AI systems.

If you encounter any issues or require further assistance, please refer to the "Troubleshooting" section of the user manual or contact our technical support team. Orthrus is dedicated to providing a user-friendly experience for users of all levels of seniority.

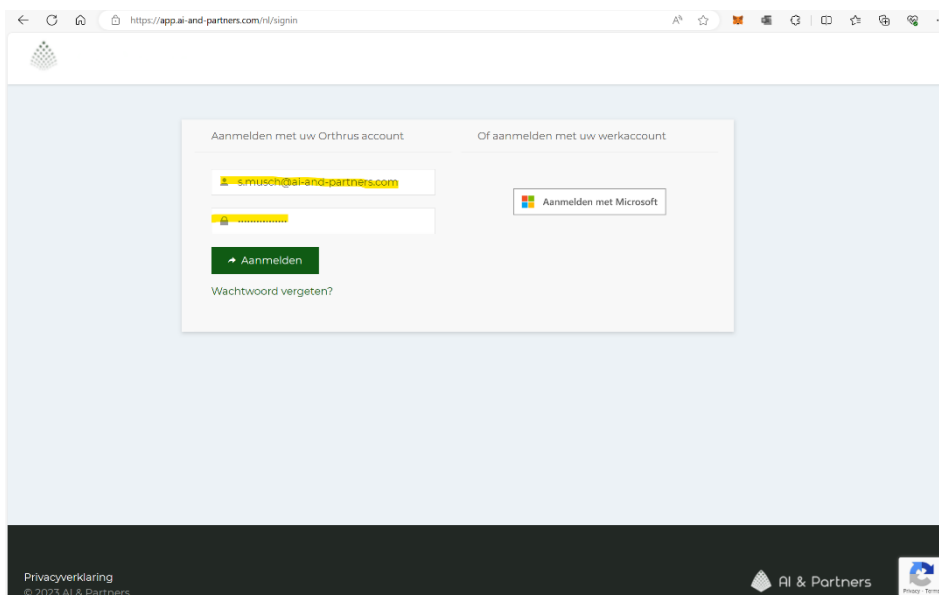
Note: It's essential to ensure that you have all the necessary documentation and information ready for the risk classification process.

Adding an User to Orthrus: A Step-by-Step Guide

In Orthrus, you can easily add new users to your organization. This step-by-step guide will walk you through the process. We've included screenshots to make it even more straightforward.

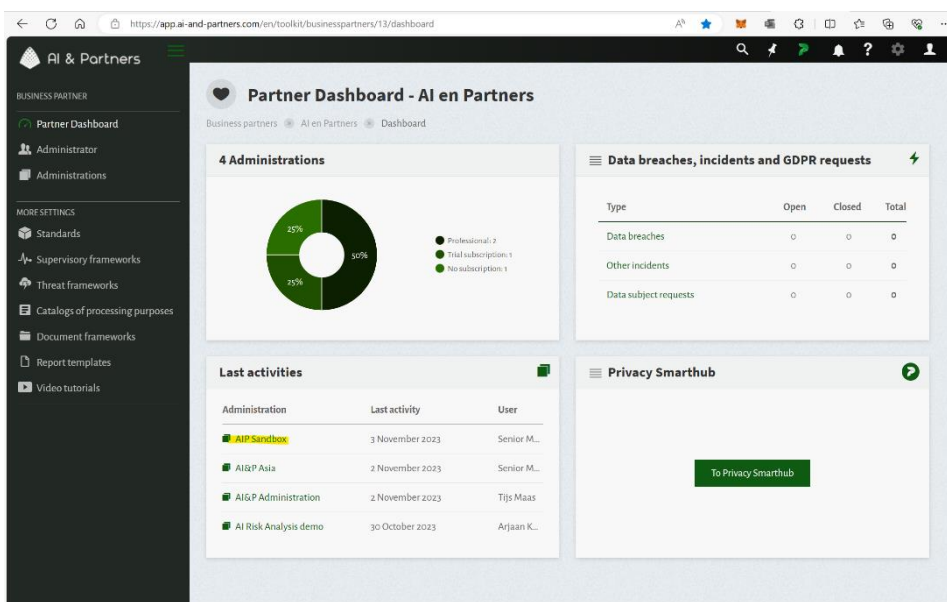
Step 1: Logging In

- Begin by visiting the Orthrus platform.
- Click on the "Sign In" button to log in to your account. Enter your login credentials, including your username and password. Click "Sign In" to access your account.



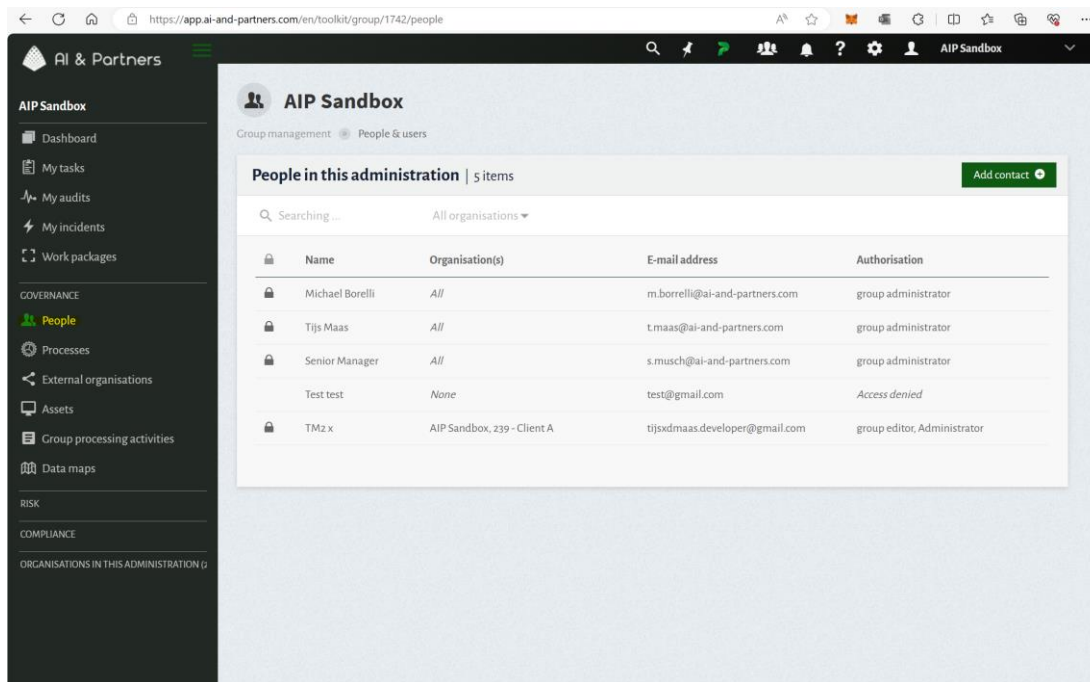
Step 2: Navigating to the AIP Sandbox Section

- Once you are logged in, you will arrive at your dashboard.
- Locate the "AIP Sandbox" section in the dashboard menu. Click on "AIP Sandbox" to proceed.



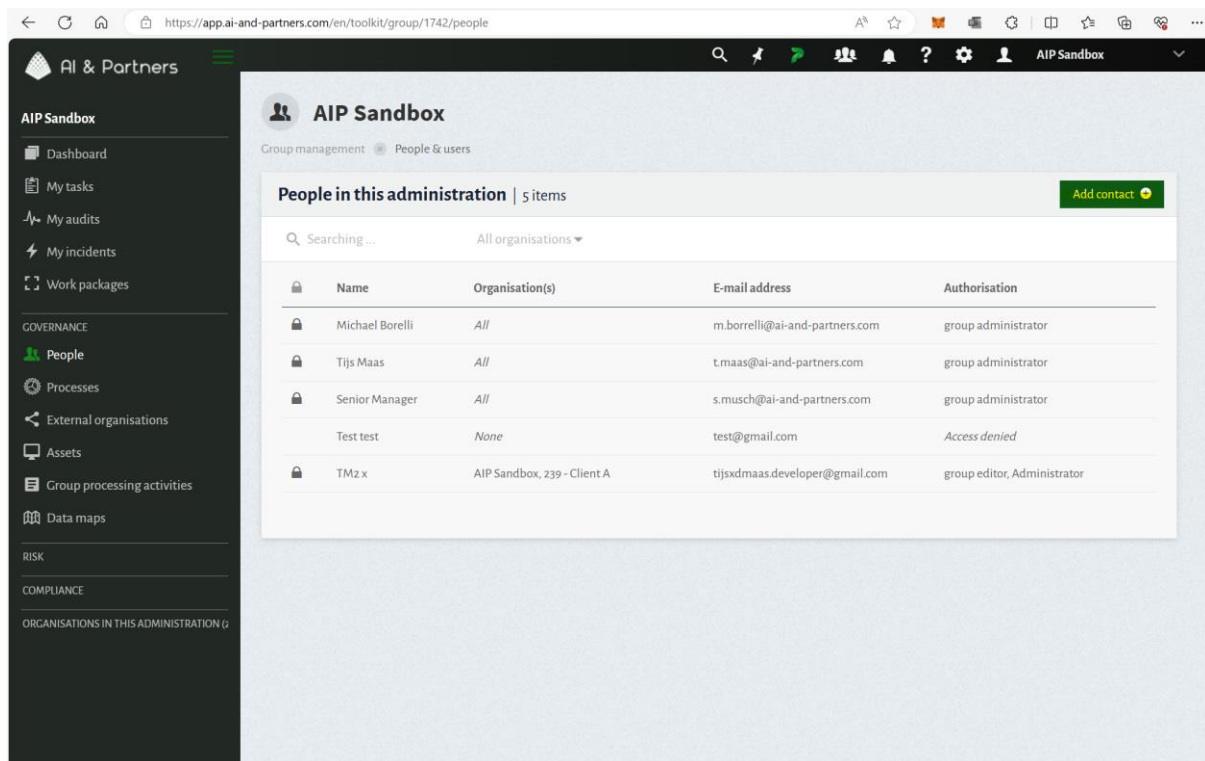
Step 3: Opening the 'Governance' Tab and Selecting 'People'

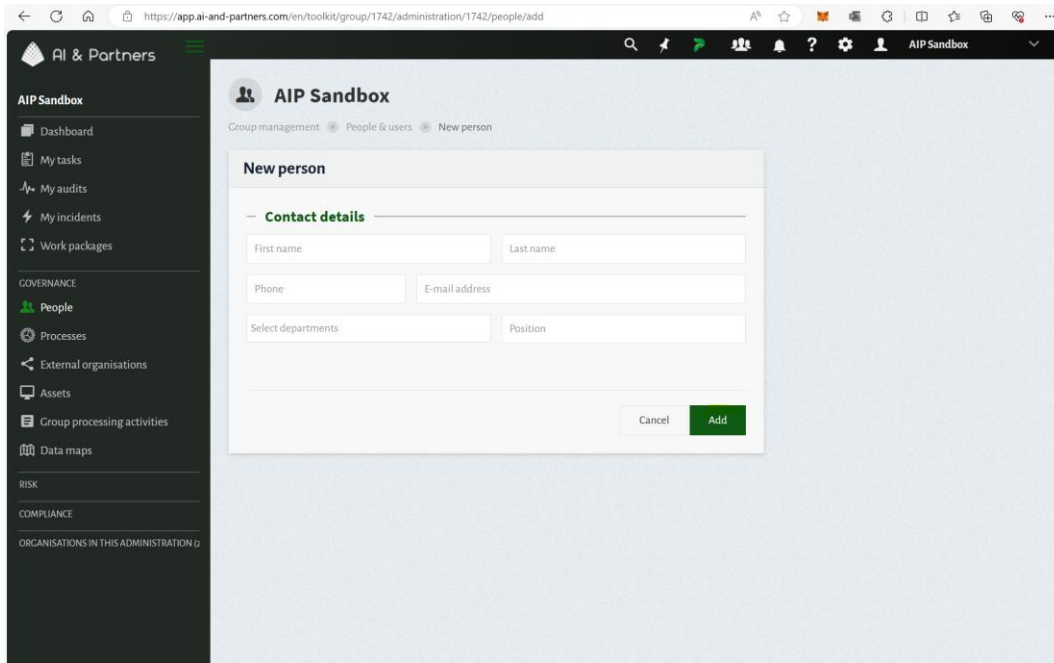
- Inside the AIP Sandbox, you will find the "Governance" tab. Click on it to reveal the available options.
- From the dropdown menu, select "People" to access the assets management section.



Step 4: Creating a New User

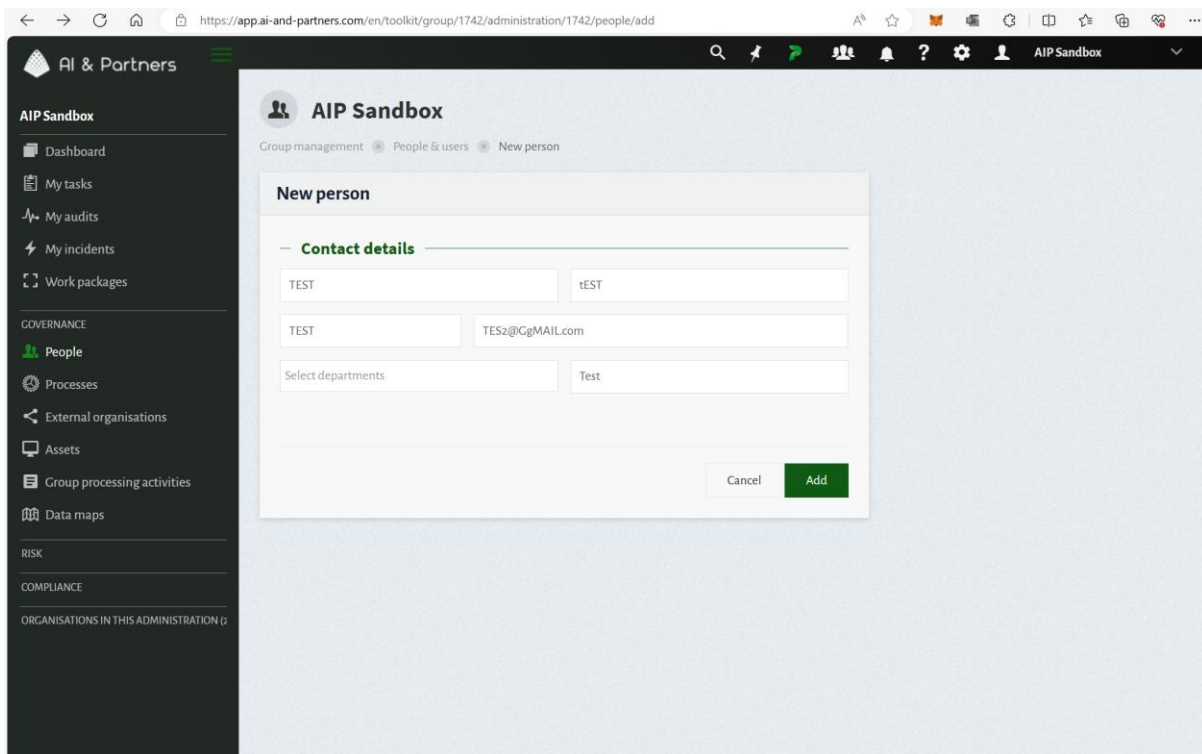
- In the "People" section, locate the "Add contact" option.
- Select "Add contact" to this Organization" from the submenu.
- Select "Add new contact" at the top right hand corner.





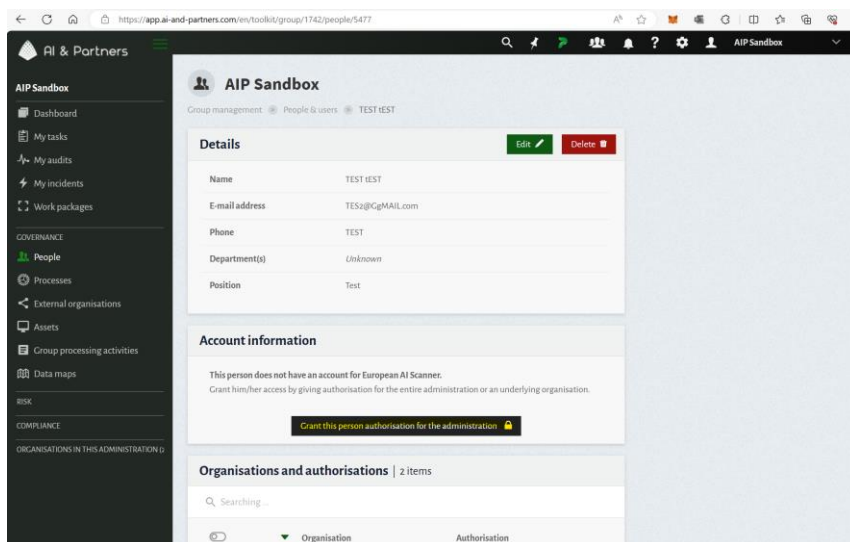
Step 5: Entering User Information

- You will be directed to a user information form.
- Fill in all the necessary details for the new user. This typically includes their full name, email address, and other relevant information.
- Click the “Add” button.



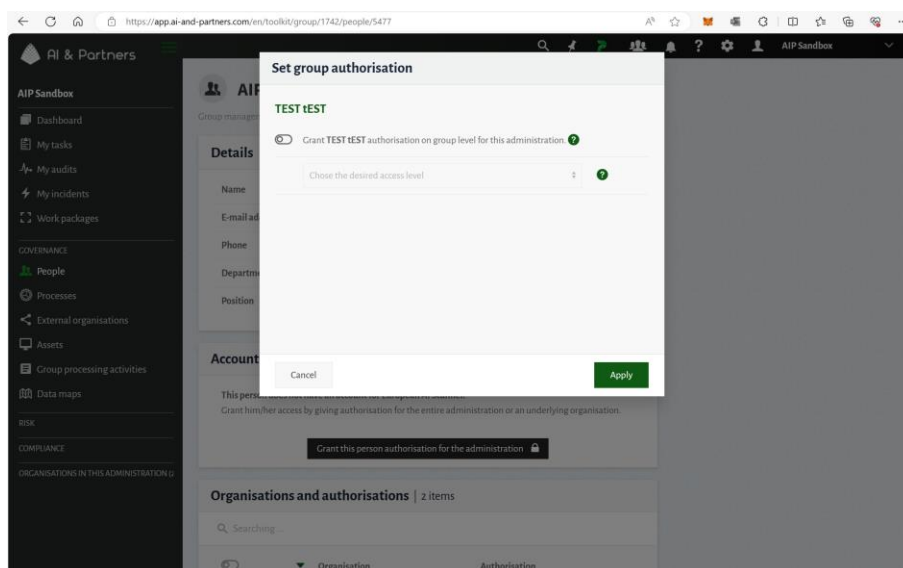
Step 6: Granting Administrative Authorisation

- Scroll down to the authorization section of the form.
- Check the box labelled "Grant This Person Authorization for Administration."



Step 7: Setting Authorisation Level

- Next, choose the appropriate level of authorization for this user. Options often include Administrator, Editor, or Viewer.
- After selecting the desired level, click the "Apply" button to save the authorization settings.



Congratulations! You've Successfully Added a User to Orthrus

Following these steps, you have successfully added a new user to your Orthrus organization. It's essential to provide accurate and complete information for each user to ensure effective AI Act compliance and risk management.

If you encounter any issues or need further assistance, please consult the "Troubleshooting" section of the user manual or reach out to our technical support team.

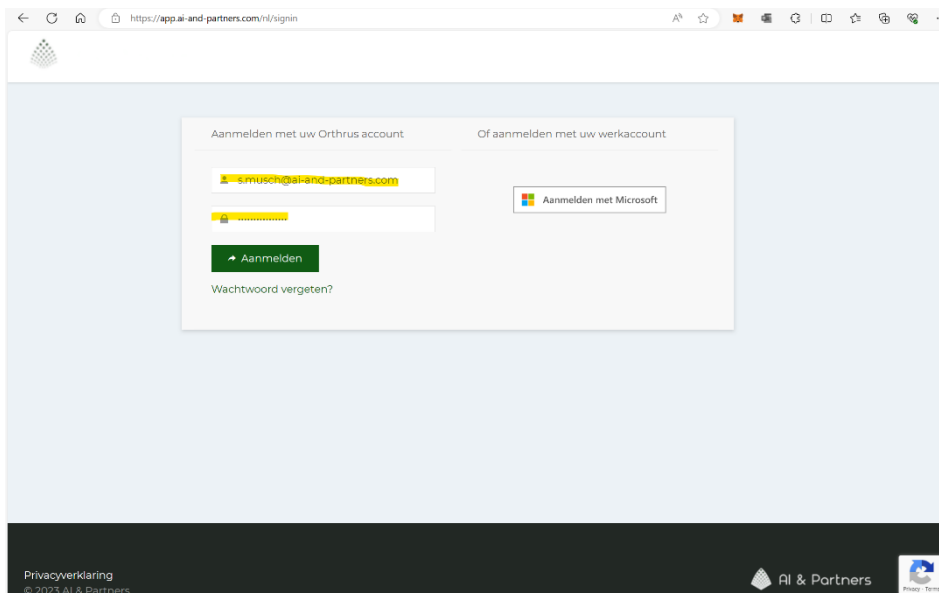
Orthrus is committed to making AI Act compliance a smooth and efficient process for all users, regardless of their level of seniority or experience.

Adding a Document to Orthrus: A Step-by-Step Guide

In Orthrus, you can easily add new documents to your organization. This step-by-step guide will walk you through the process. We've included screenshots to make it even more straightforward.

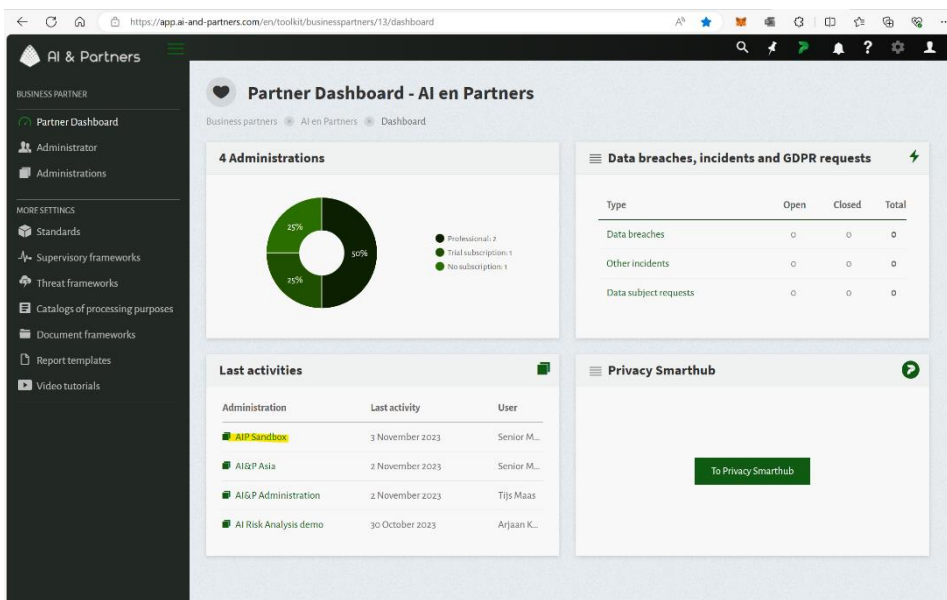
Step 1: Logging In

- Begin by visiting the Orthrus platform.
- Click on the "Sign In" button to log in to your account. Enter your login credentials, including your username and password. Click "Sign In" to access your account.



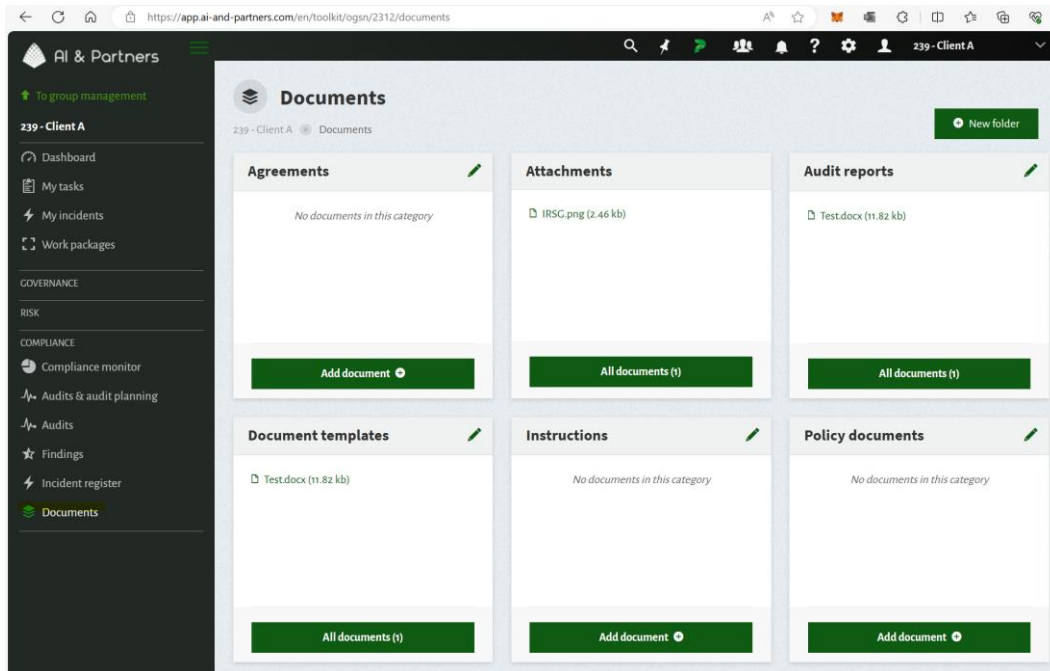
Step 2: Navigating to the AIP Sandbox Section

- Once you are logged in, you will arrive at your dashboard.
- Locate the "AIP Sandbox" section in the dashboard menu. Click on "AIP Sandbox" to proceed.



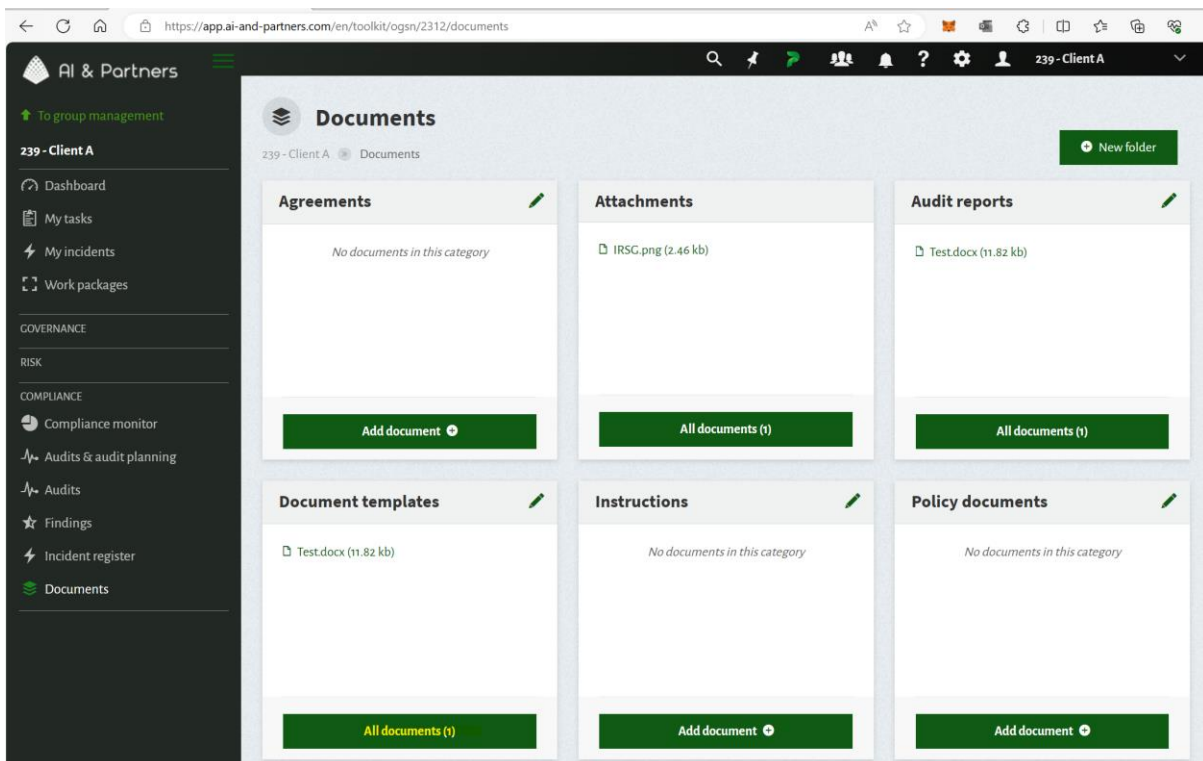
Step 3: Opening the Compliance Tab and Selecting 'Documents'

- Inside the AIP Sandbox, you will find the "Compliance" tab. Click on it to reveal the available options.
- From the dropdown menu, select "Documents" to access the assets management section.



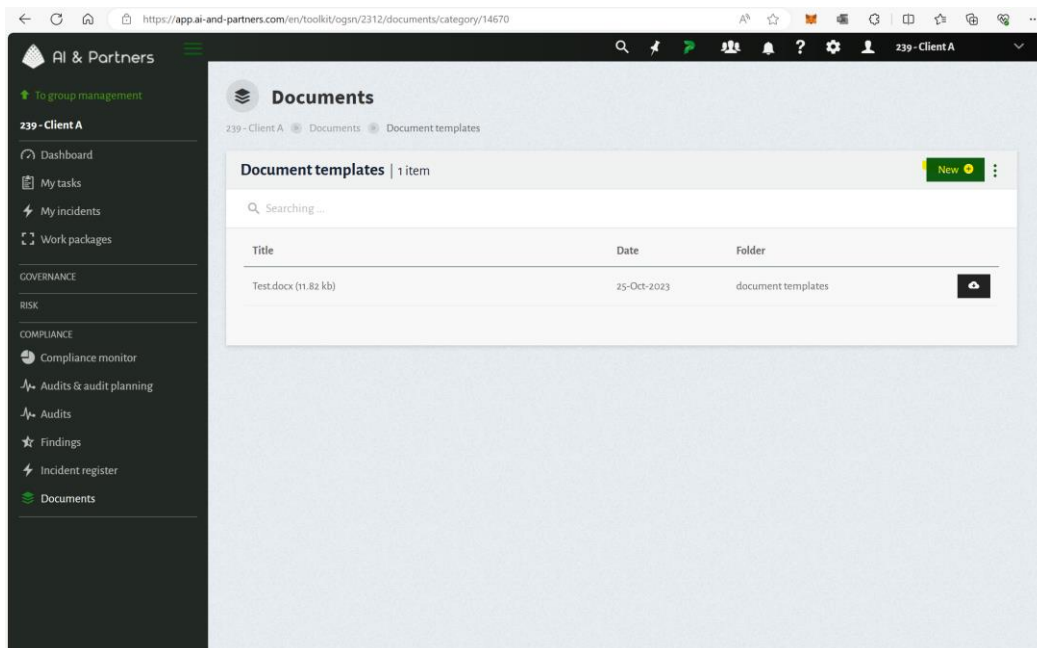
Step 4: Upload a New Document

- In the Documents section, you can either click on "All Documents" or "Add Document" to upload a new document. Choose either of these options based on your preference.



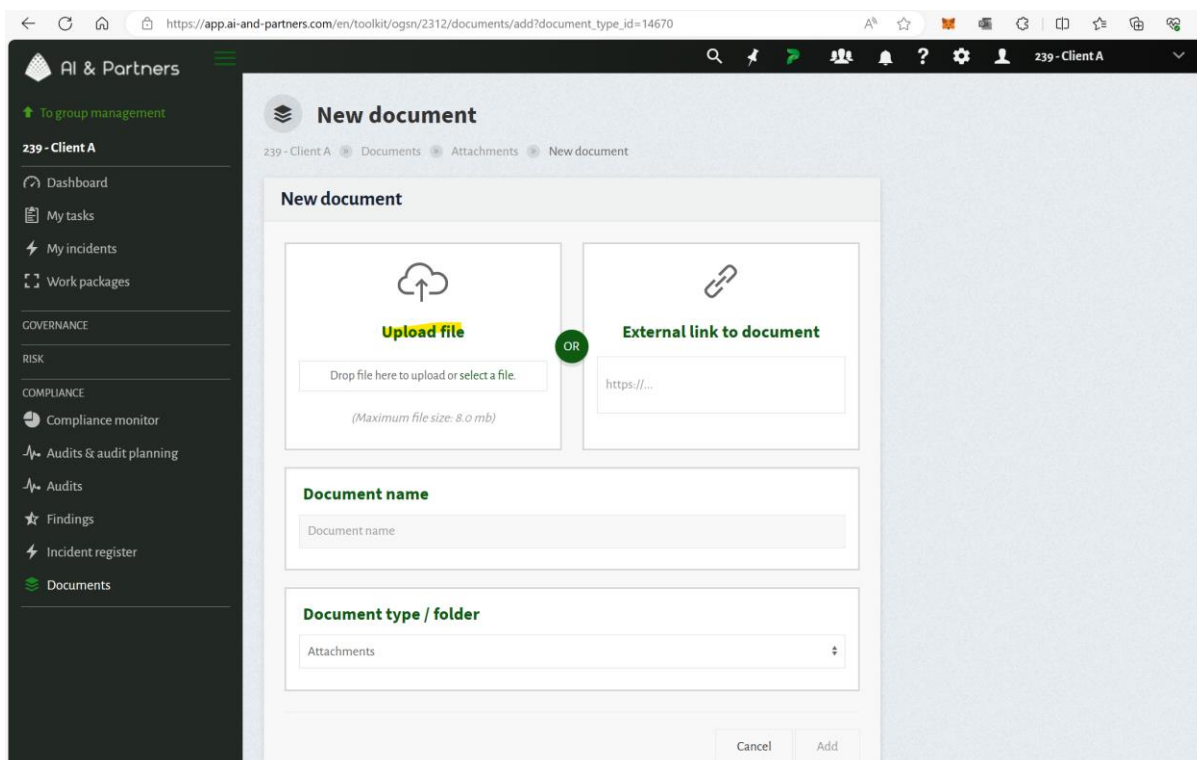
Step 5: Upload a New Document

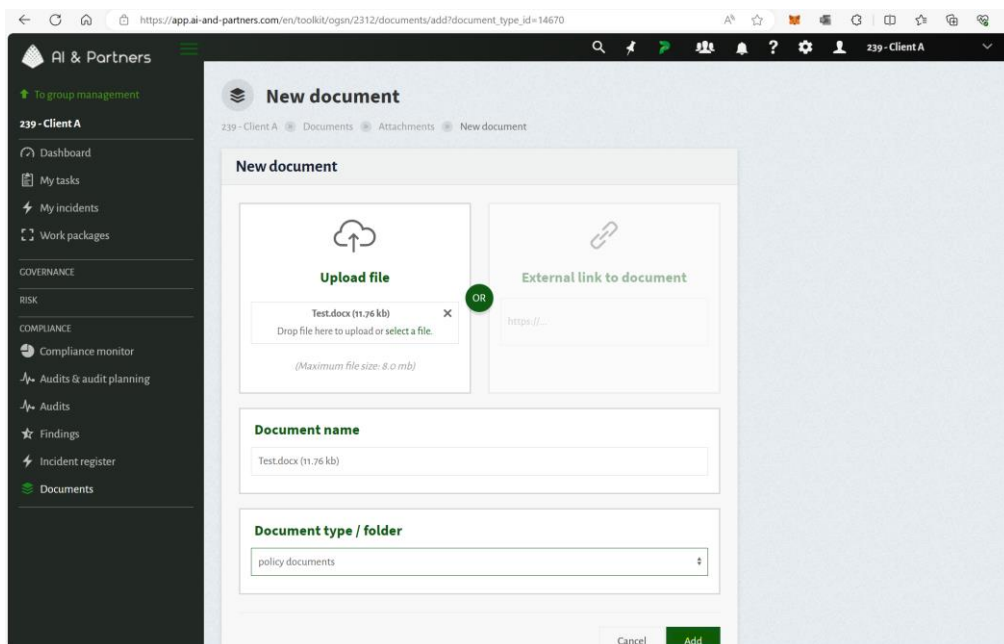
- After clicking on "All Documents" or "Add Document," you'll be presented with a new document creation screen.
- Look for the "New" option and select it to create a new document entry.



Step 6: Upload Your File and Select All Salient Information

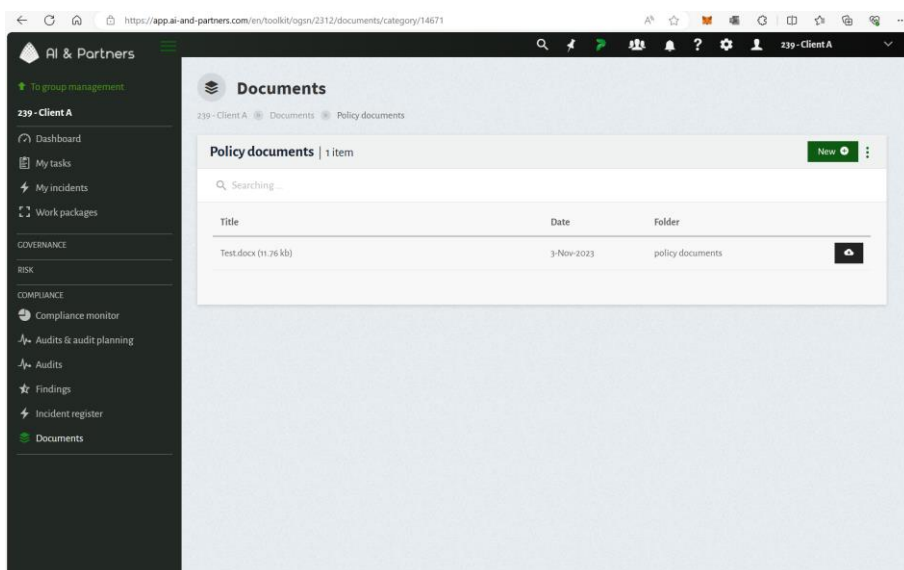
- In the new document entry screen, you will see an option to upload your file.
- Click the "Upload File" button to choose and upload your document.
- Provide relevant information about the document in the fields provided. This may include a document title, description, and any other necessary details.





Step 7: Setting Authorisation Level

- Once you've uploaded the file and filled in the required information, you'll see an option to select the document type from a dropdown menu.
- Choose the appropriate document type.
- Finally, click the "Add" button to save the document in the Orthrus platform.



Congratulations! You've Successfully Added a Document to Orthrus

Following these steps, you have successfully added a new document to your Orthrus organization. It's essential to provide accurate and complete information for each user to ensure effective AI Act compliance and risk management.

If you encounter any issues or need further assistance, please consult the "Troubleshooting" section of the user manual or reach out to our technical support team.

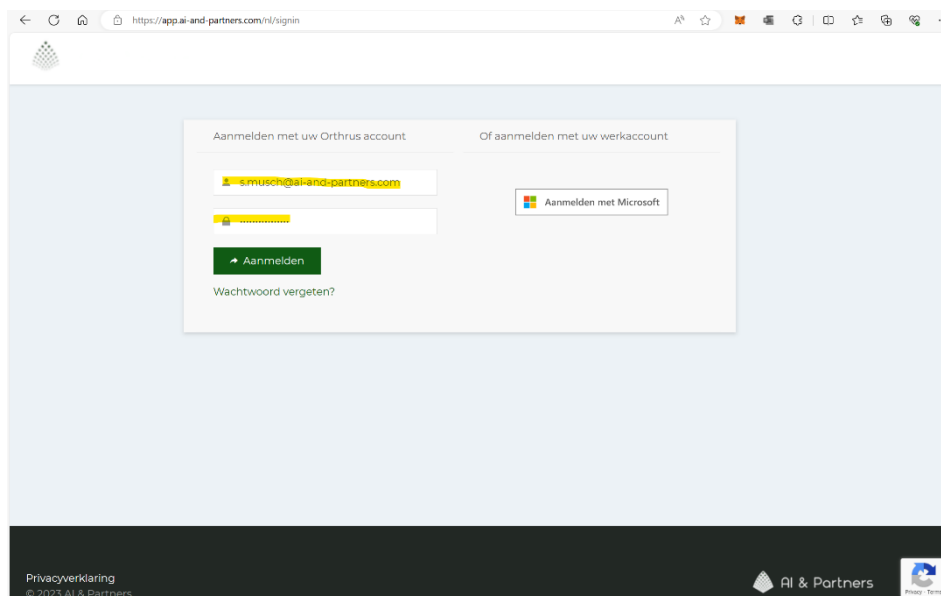
Orthrus is committed to making AI Act compliance a smooth and efficient process for all users, regardless of their level of seniority or experience.

Adding a Control to Orthrus: A Step-by-Step Guide

In Orthrus, you can easily add new controls to your organization. This step-by-step guide will walk you through the process. We've included screenshots to make it even more straightforward.

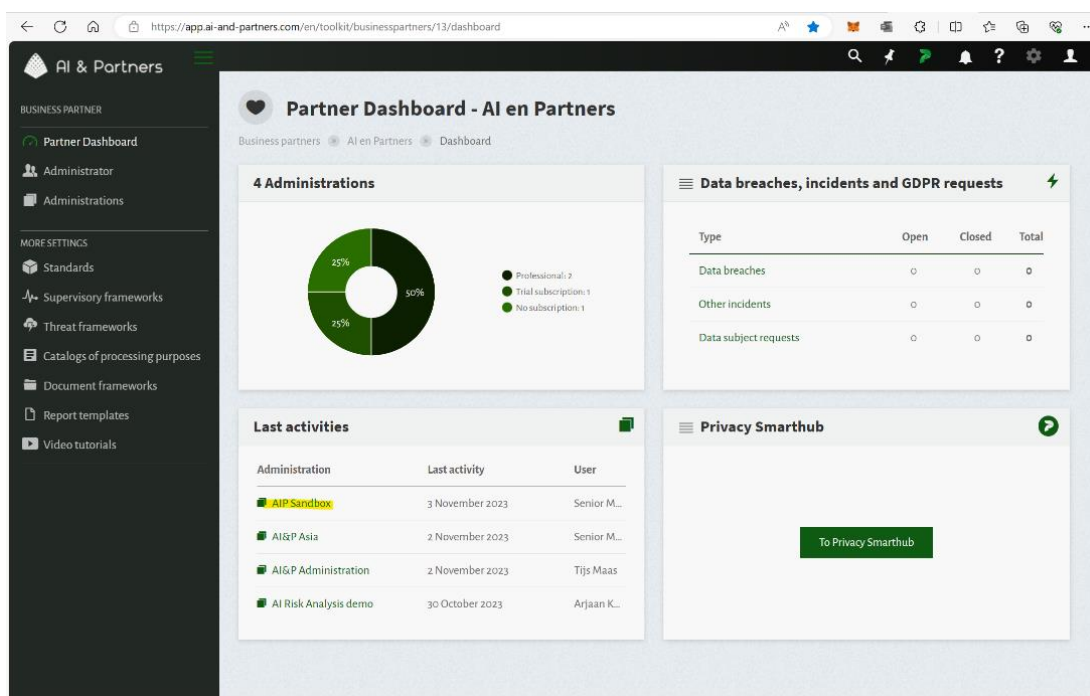
Step 1: Logging In

- Begin by visiting the Orthrus platform.
- Click on the "Sign In" button to log in to your account. Enter your login credentials, including your username and password. Click "Sign In" to access your account.



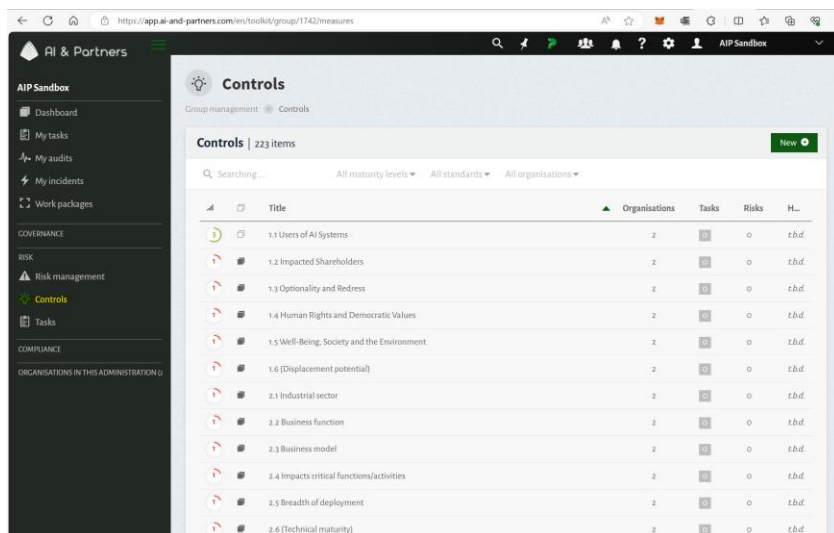
Step 2: Navigating to the AIP Sandbox Section

- Once you are logged in, you will arrive at your dashboard.
- Locate the "AIP Sandbox" section in the dashboard menu. Click on "AIP Sandbox" to proceed.



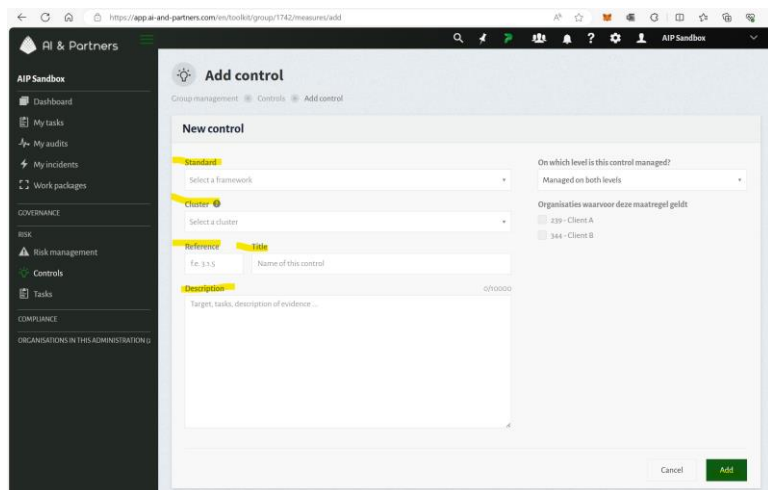
Step 3: Opening the Risk Tab and Selecting 'Controls'

- In the AIP Sandbox section, you will see various tabs. Click on the "Risk" tab.
- Within the Risk tab, choose "Controls."



Step 4: Insert Salient Information on Control

- In the Controls section, you'll see an option to create a new control entry.
- Fill in all the necessary information related to the control, including control name, description, category, and any other required details.
- After entering the information, click the "Add" button to save the control in the Orthrus platform.



Congratulations! You've Successfully Added a Control to Orthrus

Following these steps, you have successfully added a new user to your Orthrus organization. It's essential to provide accurate and complete information for each user to ensure effective AI Act compliance and risk management.

If you encounter any issues or need further assistance, please consult the "Troubleshooting" section of the user manual or reach out to our technical support team.

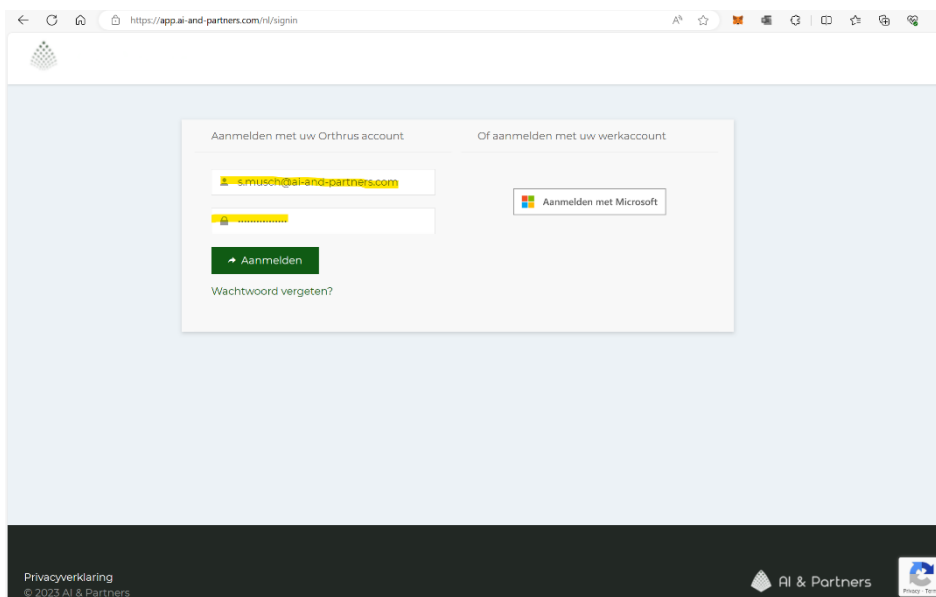
Orthrus is committed to making AI Act compliance a smooth and efficient process for all users, regardless of their level of seniority or experience.

Adding a External Organisation to Orthrus: A Step-by-Step Guide

In Orthrus, you can easily add new external organisation to your organization. This step-by-step guide will walk you through the process. We've included screenshots to make it even more straightforward.

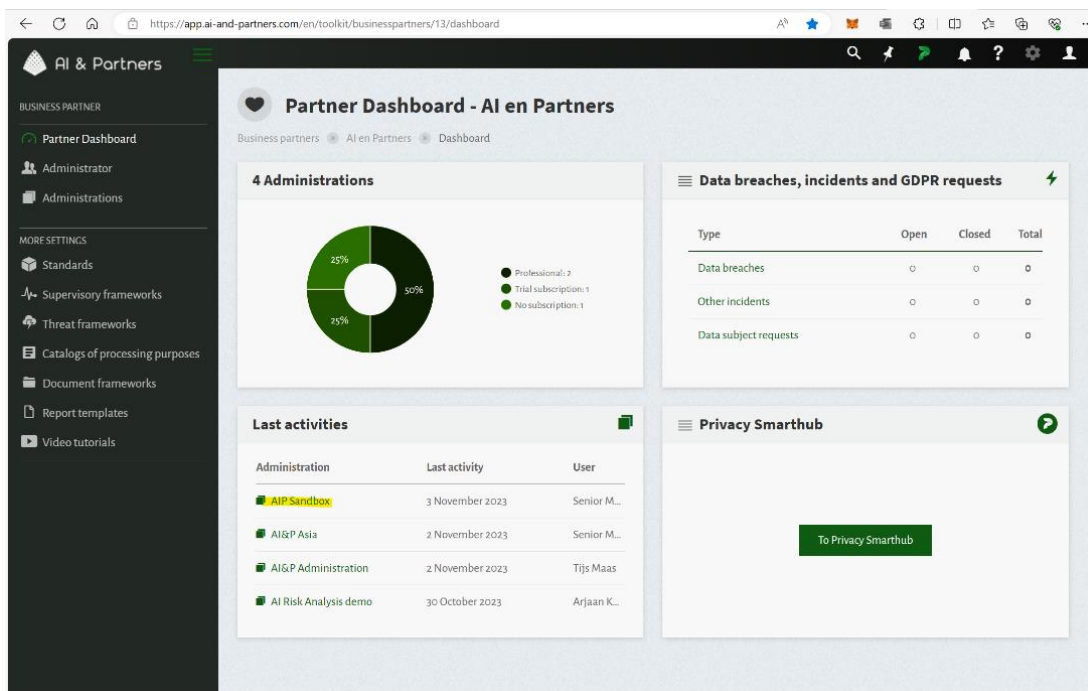
Step 1: Logging In

- Begin by visiting the Orthrus platform.
- Click on the "Sign In" button to log in to your account. Enter your login credentials, including your username and password. Click "Sign In" to access your account.



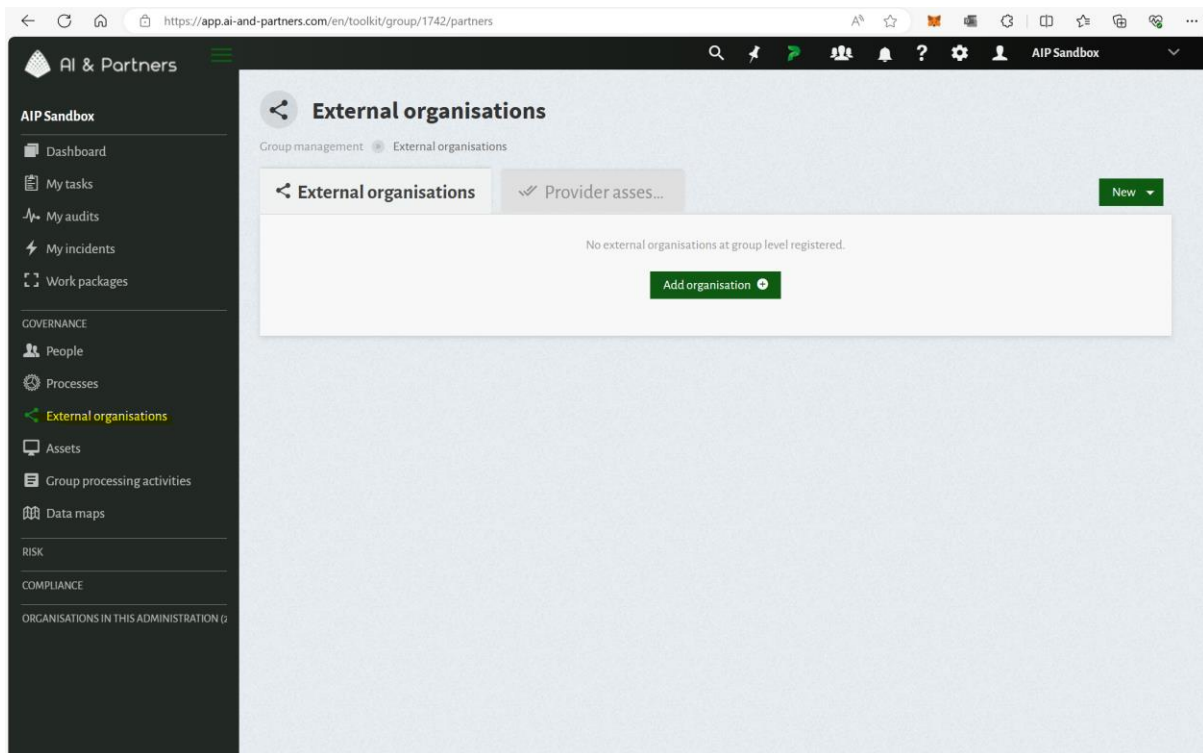
Step 2: Navigating to the AIP Sandbox Section

- Once you are logged in, you will arrive at your dashboard.
- Locate the "AIP Sandbox" section in the dashboard menu. Click on "AIP Sandbox" to proceed.



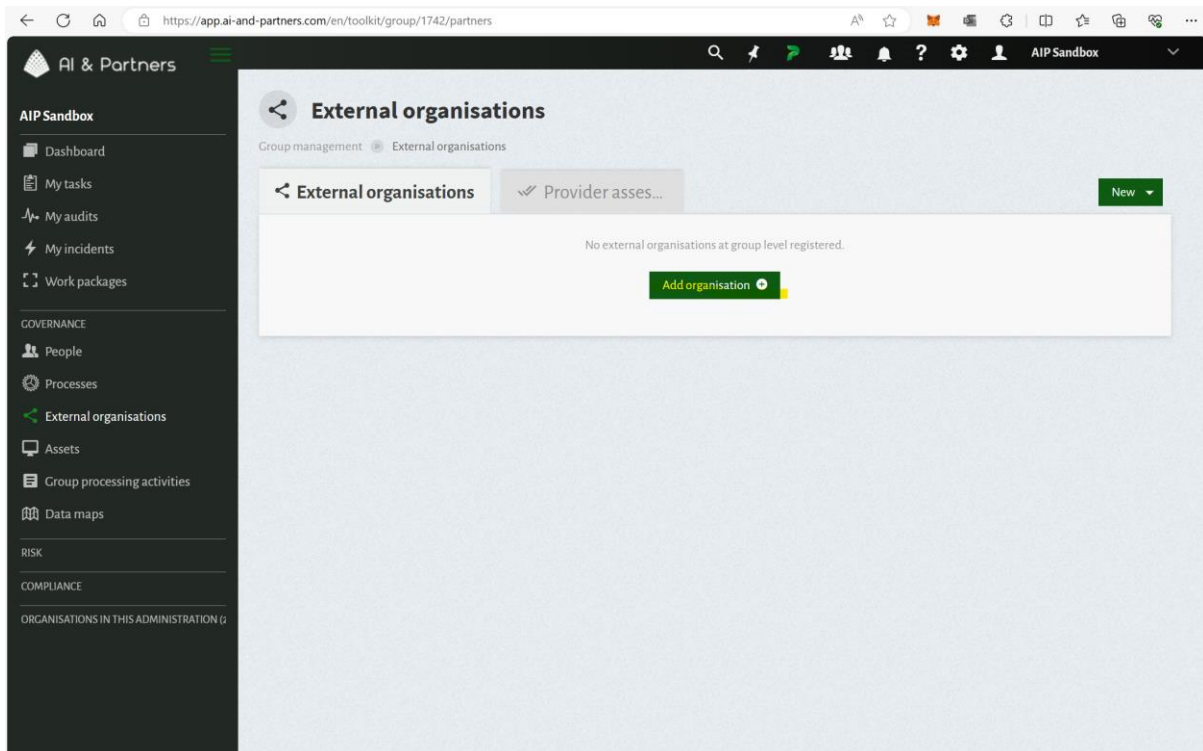
Step 3: Opening the Governance Tab and Selecting 'External Organisations'

- In the AIP Sandbox section, you will see various tabs. Click on the "Governance" tab.
- Within the Governance tab, choose "External Organisations."



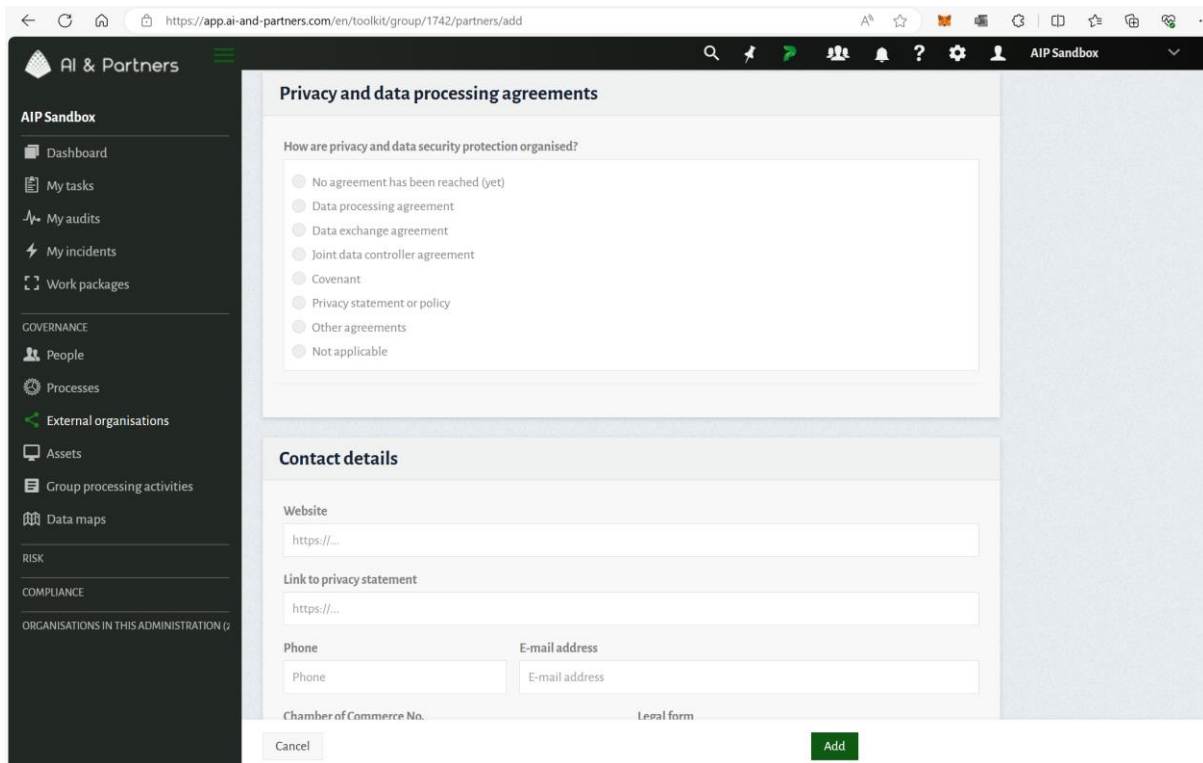
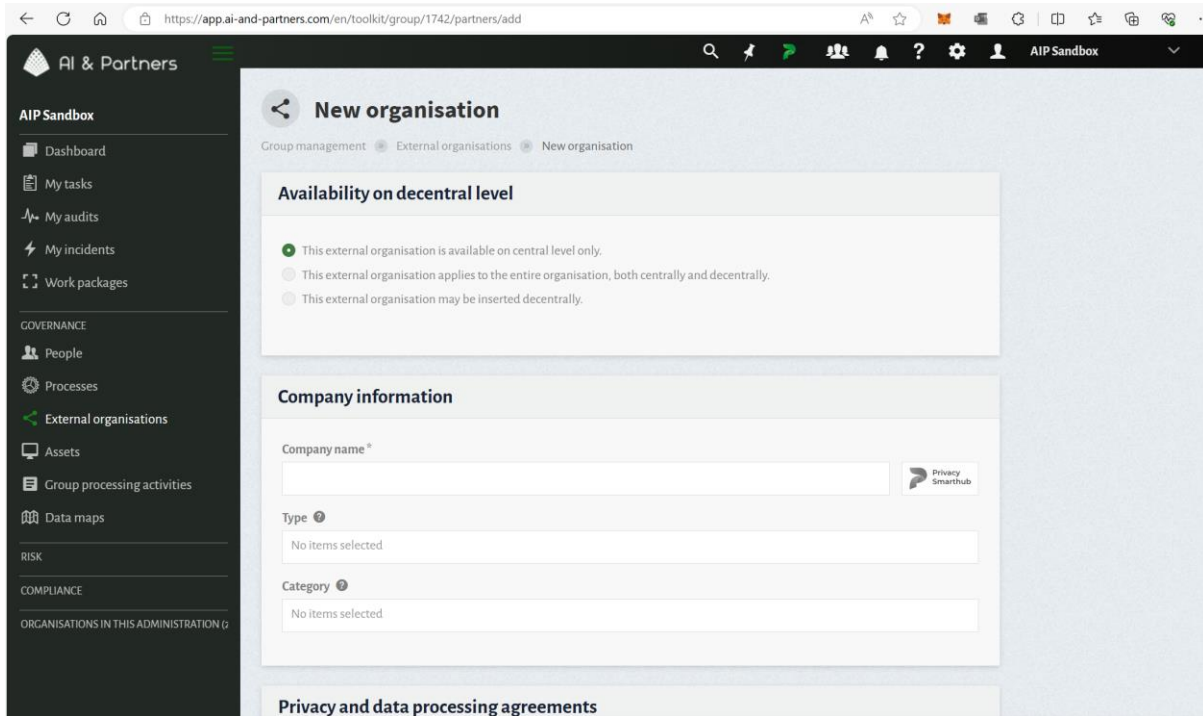
Step 4: Add a New Organisation

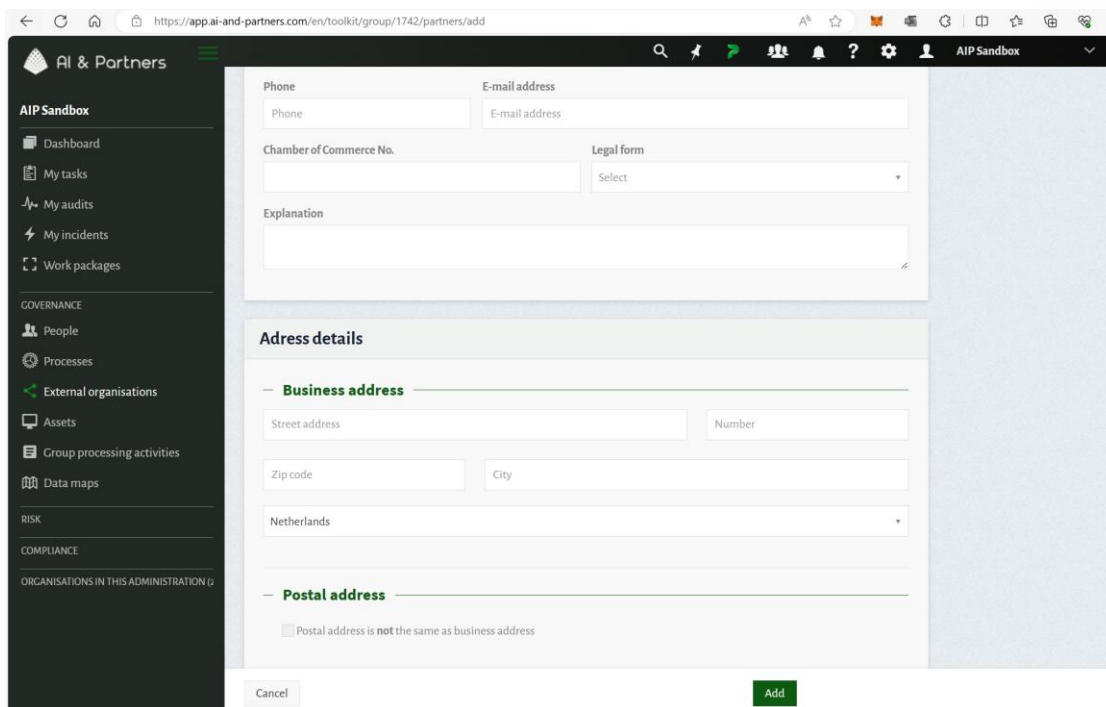
- In the External Organisations section, you will find an option to add a new external organization. Click the "Add Organisation" button.



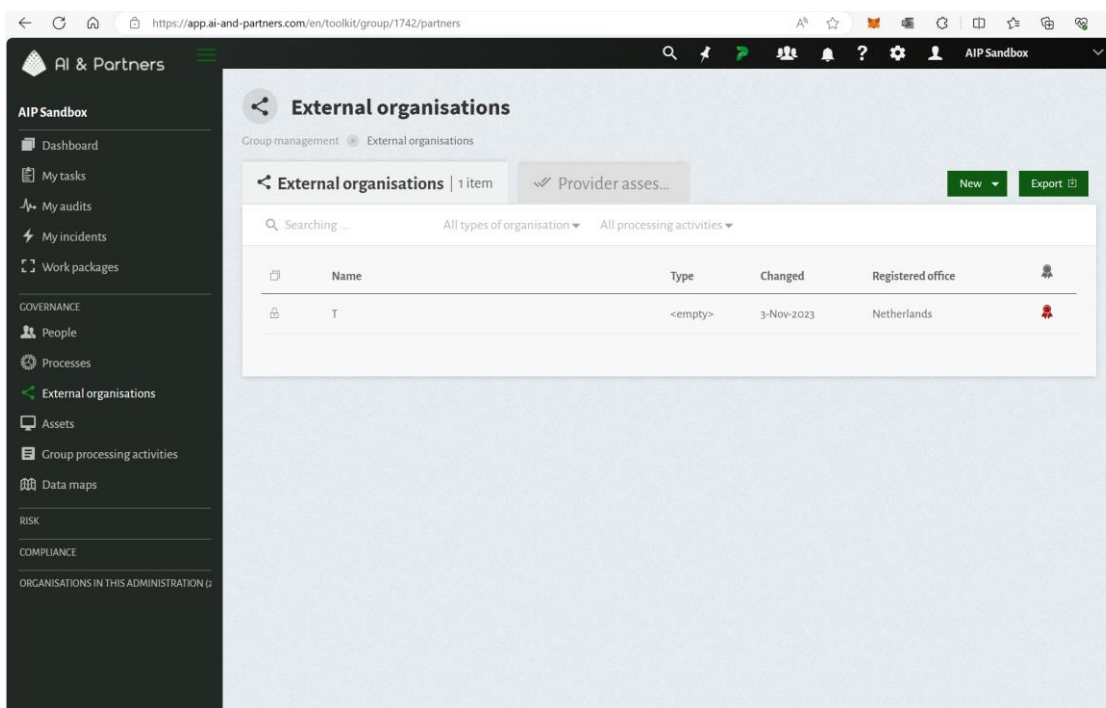
Step 5: Add a All Salient Information for the External Organisation

- You'll be presented with a form to input information about the external organization. Fill in the required information such as organization name, contact details, and any other relevant details.
- After entering the information, click the "Add" button to save the external organization's details in the Orthrus platform.





The screenshot shows a web browser window with the URL <https://app.ai-and-partners.com/en/toolkit/group/1742/partners/add>. The page title is "AIP Sandbox". On the left is a dark sidebar with navigation options: Dashboard, My tasks, My audits, My incidents, Work packages, GOVERNANCE (People, Processes, External organisations, Assets, Group processing activities, Data maps), RISK, COMPLIANCE, and ORGANISATIONS IN THIS ADMINISTRATION G. The main content area is a form with the following fields: Phone (input), E-mail address (input), Chamber of Commerce No. (input), Legal form (dropdown menu), Explanation (text area), Address details section with Business address (Street address, Number, Zip code, City, Country dropdown), and Postal address (checkbox for "Postal address is not the same as business address"). At the bottom are "Cancel" and "Add" buttons.



The screenshot shows the "External organisations" page in Orthrus. The URL is <https://app.ai-and-partners.com/en/toolkit/group/1742/partners>. The page title is "AIP Sandbox". The sidebar is the same as in the previous screenshot. The main content area shows "External organisations" with "1 item" and "Provider asses...". There are "New" and "Export" buttons. Below is a search bar and two dropdown menus: "All types of organisation" and "All processing activities". A table lists the external organisations:

Name	Type	Changed	Registered office	
T	<empty>	3-Nov-2023	Netherlands	

Congratulations! You've Successfully Added a new External Organisation to Orthrus

Following these steps, you have successfully added a new External Organisation to your Orthrus organization. It's essential to provide accurate and complete information for each user to ensure effective AI Act compliance and risk management.

If you encounter any issues or need further assistance, please consult the "Troubleshooting" section of the user manual or reach out to our technical support team.

Orthrus is committed to making AI Act compliance a smooth and efficient process for all users, regardless of their level of seniority or experience.

Regulatory Compliance

In this section, we will delve into how Orthrus assists users in meeting regulatory compliance requirements, with a focus on the EU AI Act. The information provided here is clear, professional, concise, and suitable for users of all levels, including junior staff.

Orthrus is designed to help organizations comply with the EU AI Act by providing tools and features that align with its regulatory requirements. This section will outline the key components of the EU AI Act that are addressed by Orthrus.

EU AI Act Overview

The EU AI Act is a comprehensive legislative framework developed by the European Union to regulate artificial intelligence systems. It aims to strike a balance between promoting AI innovation and ensuring the safety and fundamental rights of individuals and businesses. Here's a concise overview:

- **Scope:** The EU AI Act covers a broad range of AI systems, including those used in critical infrastructure, biometric identification, and high-risk applications.
- **Requirements:** It sets out specific requirements for the development, deployment, and use of AI systems, with a focus on high-risk AI.
- **Conformity Assessment:** The Act outlines procedures for conformity assessment, involving documentation, testing, and certification for high-risk AI systems.
- **Data and Transparency:** It emphasizes transparency and the responsible use of AI, including the provision of information to users and maintaining adequate documentation.

Key Regulatory Requirements

To use Orthrus effectively for EU AI Act compliance, you must be aware of the key regulatory requirements associated with AI systems. These requirements include:

- **Risk Classification:** Under the EU AI Act, high-risk AI systems must undergo a risk classification process to assess their potential impacts on safety, fundamental rights, and public interests.
- **Data Protection:** Compliance with data protection regulations, such as the General Data Protection Regulation (GDPR), is essential when handling personal data within AI systems.
- **Documentation:** Proper documentation, including the AI system's technical documentation and the results of conformity assessments, is mandatory.
- **User Information:** AI system providers must provide users with essential information, including the system's capabilities and limitations.

Compliance Deadlines

The EU AI Act outlines specific deadlines for compliance, and it's crucial to be aware of these to avoid potential penalties. Deadlines may vary depending on the type and risk level of AI systems. Some general guidelines include:

- **Registration:** Certain AI systems may require registration with the competent authority, and the deadline for registration should be strictly adhered to.
- **Conformity Assessment:** High-risk AI systems must undergo conformity assessments by accredited bodies, and the deadline for this assessment should be met.
- **Ongoing Monitoring:** Compliance with the Act involves ongoing monitoring and assessment of AI systems to ensure they meet the required standards.

It's important to stay updated with the latest developments and amendments to the EU AI Act, as regulations may evolve over time. Failure to comply with these regulations can result in legal consequences, making it imperative to prioritize regulatory compliance when using Orthrus for AI system identification, risk classification, risk reporting, and post-market monitoring.

By understanding the EU AI Act, its key requirements, and the associated compliance deadlines, you can effectively navigate the regulatory landscape and use Orthrus in a manner that ensures both regulatory adherence and the responsible use of AI systems within the European Union.

How Orthrus Helps with Compliance

In this section, we elaborate on how Orthrus is a valuable tool for ensuring compliance with the EU AI Act.

AI System Registration

Orthrus assists users in complying with regulatory requirements related to AI system registration by providing the necessary tools and guidance. Here's how:

- **Registration Guidance:** Orthrus offers clear guidance and step-by-step instructions on the process of registering AI systems with the relevant authorities. It outlines the required documentation and information that must be submitted for registration.
- **Documentation Management:** The tool allows users to securely store and manage the documentation required for AI system registration. This includes technical specifications, conformity assessment reports, and any other relevant materials.

Risk Classification

Compliance with risk classification requirements is crucial under regulatory frameworks. Orthrus simplifies this process as follows:

- **Risk Assessment Tools:** Orthrus provides risk assessment tools that allow users to evaluate the potential risks associated with their AI systems. It offers predefined risk criteria and customizable risk factors to help users classify their AI systems accurately.
- **Risk Classification Reports:** Users can generate comprehensive risk classification reports based on the output of the risk assessment. These reports are compliant with regulatory standards and can be easily shared with relevant authorities.

Monitoring and Reporting

To comply with regulatory requirements for ongoing monitoring and reporting, Orthrus offers the following support:

- **Real-time Monitoring:** Orthrus provides real-time monitoring capabilities, allowing users to continuously track the performance and behavior of their AI systems. It alerts users to potential issues or deviations from expected behavior.
- **Automated Reporting:** The tool streamlines the reporting process by automating the collection and generation of reports. Users can easily create compliance reports and share them with regulatory bodies as required.

Customization and Flexibility

Orthrus recognizes that regulatory requirements can vary and that users may have unique needs. It offers customization and flexibility in the following ways:

- **Configurable Compliance Rules:** Users can configure compliance rules within Orthrus to align with specific regulatory requirements. This includes adjusting risk thresholds, reporting intervals, and other parameters.
- **User-Specific Workflows:** Orthrus allows users to define custom workflows for compliance management. This flexibility ensures that the tool can adapt to different organizational processes and regulatory environments.

By providing these features and capabilities, Orthrus empowers users to meet regulatory compliance obligations effectively. Users can confidently navigate the complexities of AI system registration, risk classification, monitoring and reporting, and adapt the tool to their specific compliance needs, thereby ensuring they remain in compliance with the EU AI Act and other relevant regulations.

Configuring Regulatory Rules

This section is dedicated to explaining how users can configure Orthrus to adhere to the specific regulatory rules laid out in the EU AI Act.

Rule-Based Configuration

Orthrus provides users with the ability to configure compliance rules based on specific regulatory requirements. Here's how this feature works:

- **Rule Management:** Orthrus offers a comprehensive rule management system that allows users to define and modify compliance rules. These rules can pertain to various aspects of regulatory requirements, such as data handling, security, reporting intervals, and more.
- **Parameter Customization:** Users can set parameters within the rules, adjusting thresholds, conditions, and other criteria to align with the specific regulations that apply to their organization or industry.
- **Real-Time Monitoring:** The rule-based configuration within Orthrus enables real-time monitoring of AI systems. It continuously checks for compliance with the configured rules and alerts users when deviations or violations occur.

Custom Compliance Policies

Orthrus understands that regulatory compliance can vary between organizations and industries. To accommodate these differences, it allows users to create custom compliance policies. Here's how it facilitates this:

- **Policy Creation:** Users can create custom compliance policies that reflect their unique regulatory obligations. These policies can encompass a wide range of requirements, from data retention to reporting formats.
- **Flexibility and Adaptability:** Custom compliance policies in Orthrus are highly flexible. Users can adapt and modify these policies as regulations change or as their business needs evolve.
- **Automation:** Once custom compliance policies are defined, Orthrus automates the compliance process, ensuring that AI systems adhere to the specified policies without manual intervention.

By offering these rule-based configuration and custom compliance policy features, Orthrus empowers users to tailor their regulatory compliance efforts precisely to their needs. This flexibility allows for a more efficient and adaptable approach to meeting regulatory requirements, ensuring that AI systems adhere to the necessary standards while also accommodating the uniqueness of each user's compliance environment.

Monitoring and Reporting

Automated Monitoring

Orthrus offers robust automated monitoring capabilities to assist users in staying compliant with regulatory requirements. Here's how it works:

- **Continuous Surveillance:** Orthrus continually monitors AI systems, tracking their behavior, performance, and compliance with relevant regulations. This automated process ensures that compliance is maintained without manual intervention.
- **Real-time Data Collection:** The tool collects data in real-time, providing an up-to-the-minute view of AI system operations. This data is essential for assessing and maintaining compliance.

Alerts and Notifications

To keep users informed and proactive, Orthrus provides a system of alerts and notifications designed to address potential compliance issues:

- **Customizable Alerts:** Users can configure alerts based on specific compliance criteria and thresholds. For example, they can set alerts for anomalies in AI system behavior or deviations from regulatory standards.
- **Real-time Notifications:** Orthrus sends real-time notifications through various channels (email, in-app messages, etc.) to ensure that users are promptly informed of compliance issues, allowing for immediate corrective actions.

Compliance and Reports

Orthrus simplifies the process of ensuring compliance with regulatory standards and generating compliance reports:

- **Automated Compliance Checks:** The tool automates compliance checks according to predefined regulatory rules. This ensures that AI systems adhere to established standards consistently.
- **Comprehensive Reporting:** Users can generate detailed compliance reports with a single click. These reports provide an overview of compliance status and can be readily shared with relevant authorities to demonstrate adherence to regulations.

Audit Trails

Maintaining audit trails is crucial for transparency and accountability in regulatory compliance. Orthrus helps users in this aspect by:

- **Logging Activity:** The tool logs all relevant activities, changes, and interactions within the system, creating a comprehensive audit trail.
- **Secure Data Storage:** The audit trail data is securely stored, ensuring its integrity and making it readily available for regulatory inspections or internal auditing.

By incorporating these features of automated monitoring, alerts and notifications, compliance and reports, and audit trails, Orthrus ensures that users can proactively manage regulatory compliance, promptly address issues, and maintain a transparent record of their efforts. This is critical for meeting the requirements of the EU AI Act and other regulatory frameworks, demonstrating a commitment to regulatory adherence and ethical AI practices.

Data Management and Security

This section is dedicated to explaining how Orthrus manages and secures data effectively in compliance with the EU AI Act. The content is designed to be clear, professional, concise, and suitable for users of all levels, including junior staff.

In this section, we will provide comprehensive information on how Orthrus manages data and ensures security. Proper data management and security are crucial components of regulatory compliance and the effective use of Orthrus.

Data Input and Import

Orthrus facilitates the input and import of data for efficient use in the platform. Here's how it's done:

- **Data Input:** Users can manually input data directly into Orthrus. This data may include information about AI systems, risk assessments, and other relevant details.
- **Data Import:** Orthrus supports data import from various sources, allowing users to bulk-import data from spreadsheets, databases, or other compatible formats. This simplifies the process of populating the platform with necessary data.
- **Data Validation:** Before data is incorporated into Orthrus, it undergoes validation processes to ensure accuracy and completeness. This helps in maintaining the integrity of the data.

Data Export

Orthrus also provides options for exporting data when needed:

- **Data Export Formats:** Users can export data in various formats, including CSV, Excel, or PDF, making it accessible and shareable for reporting or record-keeping purposes.
- **Customizable Exports:** Orthrus allows users to customize data exports, selecting specific datasets or information to export, tailoring the output to their specific requirements.

Data Privacy and Security Measures

Ensuring the privacy and security of data is a top priority for Orthrus:

- **Data Encryption:** All data within Orthrus is encrypted both in transit and at rest, ensuring that sensitive information remains confidential and protected.
- **Access Controls:** Orthrus employs role-based access controls, allowing organizations to define who can access, modify, and delete data. This helps in maintaining data integrity and preventing unauthorized access.
- **Compliance with Data Regulations:** Orthrus complies with data privacy regulations such as GDPR, HIPAA, or any other relevant local or industry-specific regulations, providing users with a platform that respects data privacy.

Compliance with Data Regulations

Orthrus takes compliance with data regulations seriously, aligning with international and industry-specific standards:

- **Data Retention Policies:** Orthrus allows users to define and enforce data retention policies in accordance with regulatory requirements. Data is automatically managed based on these policies.

- **Audit Trails:** The platform maintains audit trails to record all data-related activities, ensuring transparency and accountability for compliance purposes.
- **Data Handling Guidelines:** Orthrus offers guidelines and best practices on how to handle data in compliance with regulations, helping users avoid common pitfalls and ensuring they are operating within the boundaries of the law.

By providing robust data management and security measures, Orthrus empowers users to handle data effectively, maintain compliance, and mitigate risks associated with data breaches or non-compliance. These features contribute to the overall success of using Orthrus for EU AI Act compliance and related regulatory obligations.

Troubleshooting

This section is dedicated to helping users identify and resolve common issues they may encounter while using Orthrus. Troubleshooting is essential to ensure a smooth experience with the platform. Here are the key aspects covered in this section:

Common Issues and Solutions

In this part, we address common problems users may face and provide solutions to resolve them. It's essential to equip users with the knowledge to troubleshoot issues independently whenever possible.

Problem 1: Login Issues

Symptoms: Users can't log in or are experiencing login-related errors.

Solution:

- Verify the correctness of the login credentials.
- Reset the password if forgotten.
- Ensure that the internet connection is stable.
- Check if the account is locked due to too many failed login attempts.

Problem 2: Slow Performance

Symptoms: Orthrus is running slowly or experiencing lag.

Solution:

- Ensure that your device meets the system requirements.
- Close unnecessary background applications.
- Clear browser cache and cookies.
- Contact technical support if the issue persists.

Problem 3: Data Import Errors

Symptoms: Errors while importing data.

Solution:

- Verify the data format and integrity.
- Check for any special characters or formatting issues.
- Review the import process and settings.

Reporting Bugs and Issues

Users are encouraged to report any issues, bugs, or unexpected behavior they encounter while using Orthrus. This section provides clear guidance on how to report problems effectively:

- **Contacting Support:** Users can report issues to our dedicated technical support team.
- **Provide Details:** Users are encouraged to provide as much detail as possible, including error messages, steps to reproduce the issue, and any relevant screenshots.
- **Tracking Progress:** Orthrus acknowledges receipt of the report and provides a tracking ID for reference. Users can check the status of their reported issues.

Technical Support Contacts

In this section, we provide contact information for our technical support team. Users can reach out for assistance with any technical issues or questions regarding Orthrus.

Technical Support Email: contact@ai-and-partners.com

Technical Support Phone: +1-XXX-XXX-XXXX

Support Hours: Monday to Friday, 9:00 AM - 5:00 PM (GMT)

We recommend users reach out to our support team for any issues they cannot resolve through the troubleshooting steps provided in the manual. Our technical support staff are here to assist in ensuring a seamless experience with Orthrus.

The Troubleshooting section aims to empower users to overcome common issues and effectively report any problems they encounter. This ensures that users can leverage Orthrus for EU AI Act compliance without being hindered by technical obstacles.

Updates and Maintenance

This section is dedicated to guiding users on how to keep Orthrus up to date and maintain its optimal performance. It covers the processes for updating the tool, ensuring data backup and recovery, and accessing version history. Effective updates and maintenance are essential for the smooth operation of Orthrus.

Updating Orthrus

To ensure that you're using the latest version of Orthrus, follow these steps:

Step 1: Check for Updates

Orthrus will periodically release updates to enhance performance and security. Check for updates to see if a new version is available.

Step 2: Download and Install Updates

If an update is available, download it from the Orthrus website.

Follow the provided instructions for installation.

Step 3: Verify Functionality

After updating, verify that Orthrus functions correctly and that your data is intact.

If you encounter any issues post-update, refer to the Troubleshooting section (Section 7) or contact technical support (Section 7.3).

8.2 Backup and Recovery

Data backup and recovery are crucial to prevent data loss in the event of unforeseen circumstances. Here's how you can back up and recover your data:

Regular Backups:

- Regularly back up your data to an external storage device or a cloud service to ensure data safety.
- Set up automated backup routines for convenience.

Data Recovery:

- In case of data loss or corruption, use your backup to restore the lost data.
- Ensure that you know how to access and use your backup.

8.3 Version History

Understanding the version history of Orthrus is important as it helps users know the changes and improvements made over time. Here's how to access the version history:

Check Orthrus Documentation:

The version history is typically available in the Orthrus documentation. Refer to the user manual's Index or Table of Contents for links to version history details.

Review Release Notes:

Explore release notes for each version to understand what features or changes have been implemented.

This information can help you make the most of Orthrus' capabilities.

Ensuring Data Integrity

During updates and maintenance, it's important to ensure the integrity of your data. Here are some best practices to follow:

- Regularly back up your data to prevent data loss during maintenance or updates.
- Prior to major updates, test the update process in a sandbox environment to identify and mitigate potential issues.
- Document your update and maintenance procedures to ensure consistency and reliability.

By following these guidelines, users can keep Orthrus up to date, ensure data security, and stay informed about the tool's development through version history. This will contribute to a stable and effective experience with Orthrus for EU AI Act compliance.

Conclusion

In this section, we wrap up the user manual for Orthrus by summarizing key points, offering best practices, and inviting feedback and improvement suggestions. The content is designed to be clear, professional, concise, and suitable for users at all levels, including junior staff.

Recap and Best Practices

Summary of Key Points

Let's revisit the critical takeaways from this manual:

- **Understanding Your RegTech Tool:** Orthrus is designed to help you navigate the complexities of EU AI Act compliance. We've explored its various features and functionalities to ensure you make the most of it.
- **Compliance is the Priority:** The EU AI Act introduces substantial regulatory requirements for AI systems. Orthrus streamlines compliance, from system identification to risk classification, reporting, and post-market monitoring.
- **Efficiency Through Configuration:** Learn how to configure regulatory rules and leverage the customizability of Orthrus to meet your specific compliance needs.
- **Data Management and Security:** Ensure the safety of your data through effective data input, export, and adherence to data privacy measures.
- **Troubleshooting and Support:** In case you encounter issues, our troubleshooting section, complete with common solutions and technical support contacts, is here to assist you.
- **Stay Updated and Secure:** Keep Orthrus up to date, create data backups, and review version history to ensure optimal performance and data integrity.
- **Empower Yourself with Training and Resources:** Make the most of our training workshops, online tutorials, and certification programs. Further resources are available for deepening your knowledge.

Best Practices for Efficient Use

To optimize your experience with Orthrus, follow these best practices:

- **Regularly Update Orthrus:** Ensure that you are using the latest version to benefit from enhancements and security updates.
- **Automate Backups:** Regularly back up your data to prevent data loss and streamline the recovery process.
- **Stay Informed:** Keep an eye on the version history and release notes to understand what's new and improved in Orthrus.
- **Practice Secure Data Management:** Follow data privacy and security measures to protect sensitive information.
- **Leverage Training and Resources:** Invest time in training and certifications to maximize your compliance expertise.

Checklist for Success

To achieve success with Orthrus and EU AI Act compliance, use this checklist as a quick reference:

- Familiarized yourself with Orthrus, its features, and its role in EU AI Act compliance.
- Understand the specific regulatory requirements relevant to your AI systems.

- Configured regulatory rules tailored to your compliance needs.
- Know how to monitor and report on AI systems effectively.
- Implement data management and security practices to protect your data.
- Troubleshoot common issues independently using our troubleshooting guide.
- Maintain the tool by keeping it updated and backing up your data.
- Engage in training and resources to enhance your compliance knowledge.
- Follow best practices for efficient use to save time and effort.

By following this checklist, you'll be well on your way to achieving efficient and effective EU AI Act compliance with Orthrus.

Feedback and Improvement

Thank you for choosing Orthrus, your partner in achieving EU AI Act compliance. At Orthrus, we value your feedback and are committed to continuous improvement. This section will guide you on how to provide feedback and share our dedication to enhancing your experience.

We Value Your Feedback

Your feedback is invaluable to us. We strive to make Orthrus the best tool for EU AI Act compliance, and your input helps us achieve that goal. Whether you've encountered challenges, have suggestions for improvements, or want to share your positive experiences, we're here to listen.

How to Provide Feedback

There are several ways to provide feedback:

- **Feedback Form:** You can fill out our online feedback form available on our website. This form is designed to capture your thoughts, suggestions, and concerns in a structured manner.
- **Email:** You can send us an email at feedback@orthruscompliance.com. This allows you to provide detailed feedback or attach relevant documents.
- **Support Portal:** If you've encountered a technical issue or have specific support-related feedback, you can also use our support portal. Our technical support team will be ready to assist and gather your feedback.
- **User Community:** Join our user community, where you can interact with other Orthrus users, share your feedback, and learn from their experiences.

Continuous Improvement

Orthrus is committed to continuous improvement in several ways:

- **Enhanced Features:** Your feedback helps us identify areas for feature enhancements. We regularly release updates to address user needs and improve functionality.
- **Bug Fixes:** If you encounter technical issues, our development team is dedicated to resolving them promptly. We appreciate your reports, as they help us maintain the tool's stability.
- **Compliance Updates:** As regulations evolve, Orthrus adapts to ensure you stay in compliance. We monitor regulatory changes and adjust our tool accordingly.
- **Training and Resources:** We continuously expand our training resources to keep you informed about the latest compliance requirements and how to use Orthrus effectively.

Orthrus: User Manual



Your feedback is the driving force behind Orthrus' evolution. It helps us refine and expand the tool to meet your ever-changing compliance needs. We look forward to hearing from you and appreciate your partnership in creating a safer, more compliant AI landscape. Thank you for choosing Orthrus.

Appendix A: Glossary of Terms

Additional Reading and Resources: A collection of supplementary materials, documents, and external references to further support users in their understanding and usage of Orthrus.

AI System: A comprehensive term for any software or hardware system that uses artificial intelligence techniques to perform tasks that would typically require human intelligence.

Asset: Refers to an AI system, which includes software or hardware that uses artificial intelligence techniques to perform specific tasks or make decisions.

Certification Programs: Formal programs designed to assess and recognize a user's competence and proficiency in using Orthrus.

Common Issues and Solutions: Frequently encountered problems and their respective resolutions, designed to help users address issues independently.

Dashboard: The main interface of Orthrus, providing an overview of critical information and actions available to users.

Data Export: The means by which users can extract data from Orthrus for various purposes, such as reporting or analysis.

Data Input and Import: The methods and processes for entering and bringing data into Orthrus for analysis and compliance management.

Data Privacy and Security Measures: The safeguards and procedures implemented within Orthrus to protect user data and ensure compliance with data privacy regulations.

Governance, Risk and Compliance: Stands for Governance, Risk, and Compliance. It is a framework used by organizations to manage and align their activities with governance, assess and mitigate risks, and ensure compliance with relevant regulations and standards.

Navigation: The system's menus, links, and buttons that enable users to move between different parts of Orthrus.

Online Tutorials: Interactive guides and video demonstrations accessible via Orthrus's online platform for self-paced learning.

Post-Market Monitoring: The ongoing process of tracking and assessing the performance and compliance of AI systems after they have been deployed in the market.

Regulatory Compliance: The adherence to laws, rules, and regulations applicable to AI systems, ensuring they meet legal requirements.

Regulatory Technology (aka 'RegTech'): refers to the use of technology, particularly software and data analytics, to help companies and organizations efficiently and effectively meet their regulatory compliance requirements. Regtech solutions streamline and automate compliance processes, reducing the complexities and costs associated with adhering to various regulations and standards.

Risk Classification: The process of evaluating and categorizing an AI system's potential risks based on predefined criteria and standards.

Risk Reports: Detailed documents that summarize the risk classification and assessment of AI systems, helping stakeholders make informed decisions.

Training Workshops: Formal sessions aimed at educating users about Orthrus's features and functions, often conducted in a classroom or virtual setting.

User Roles: Distinct roles assigned to users within Orthrus, each with specific permissions and responsibilities.

Version History: A record of changes made to Orthrus, including updates and improvements, often organized chronologically.

Appendix B: Regulatory Compliance References

AI System Identification

Determine whether a particular system meets the criteria outlined in the EU AI Act to be classified as an AI system, potentially falling under regulatory requirements.

Recital

(31) The classification of an AI system as high-risk pursuant to this Regulation should not necessarily mean that the product whose safety component is the AI system, or the AI system itself as a product, is considered ‘high-risk’ under the criteria established in the relevant Union harmonisation legislation that applies to the product. This is notably the case for Regulation (EU) 2017/745 of the European Parliament and of the Council and Regulation (EU) 2017/746 of the European Parliament and of the Council, where a third-party conformity assessment is provided for medium-risk and high-risk products.

(32) As regards stand-alone AI systems, meaning high-risk AI systems other than those that are safety components of products, or which are themselves products, it is appropriate to classify them as high-risk if, in the light of their intended purpose, they pose a high risk of harm to the health and safety or the fundamental rights of persons, taking into account both the severity of the possible harm and its probability of occurrence and they are used in a number of specifically pre-defined areas specified in the Regulation. The **identification** of those systems is based on the same methodology and criteria envisaged also for any future amendments of the list of high-risk AI systems.

Article

(2) (1) This Regulation applies to:

(2) (1) (a) providers placing on the market or putting into service **AI systems** in the Union, irrespective of whether those providers are established within the Union or in a third country;

(2) (1) (b) users of **AI systems** located within the Union;

(2) (1) (c) providers and users of **AI systems** that are located in a third country, where the output produced by the system is used in the Union;

(3) For the purpose of this Regulation, the following definitions apply:

(3) (1) ‘**artificial intelligence system**’ (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;

(6) (1) Irrespective of whether an **AI system** is placed on the market or put into service independently from the products referred to in points (a) and (b), that AI system shall be considered high-risk where both of the following conditions are fulfilled:

(6) (1) (a) the **AI system** is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II;

(6) (1) (b) the product whose safety component is the **AI system**, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II.

(6) (2). In addition to the high-risk **AI systems** referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk.

(51) Before placing on the market or putting into service a high-risk **AI system** referred to in Article 6(2), the provider or, where applicable, the authorised representative shall register that system in the EU database referred to in Article 60.

Annex

(I) (a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

(I) (b) Logic- & knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference/deductive engines, (symbolic) reasoning/expert systems;

(I) (c) Statistical approaches, Bayesian estimation, search and optimization methods.

(VIII) The following information shall be provided and thereafter kept up to date with regard to high-risk AI systems to be registered in accordance with Article 51.

(VIII) (1) Name, address and contact details of the provider;

(VIII) (2) Where submission of information is carried out by another person on behalf of the provider, the name, address and contact details of that person;

(VIII) (3) Name, address and contact details of the authorised representative, where applicable;

(VIII) (4) AI system trade name and any additional unambiguous reference allowing identification and traceability of the AI system;

(VIII) (5) Description of the intended purpose of the AI system;

(VIII) (6) Status of the AI system (on the market, or in service; no longer placed on the market/in service, recalled);

(VIII) (7) Type, number and expiry date of the certificate issued by the notified body and the name or identification number of that notified body, when applicable;

(VIII) (8) A scanned copy of the certificate referred to in point 7, when applicable;

(VIII) (9) Member States in which the AI system is or has been placed on the market, put into service or made available in the Union;

(VIII) (10) A copy of the EU declaration of conformity referred to in Article 48;

(VIII) (11) Electronic instructions for use; this information shall not be provided for high-risk AI systems in the areas of law enforcement and migration, asylum and border control management referred to in Annex III, points 1, 6 and 7.

(VIII) (12) URL for additional information (optional).

Post-Market Monitoring System

Implement procedures and mechanisms to monitor the performance, safety, and compliance of an AI system after it has been introduced to the market, as mandated by the EU AI Act.

Recital

(54) The provider should establish a sound quality management system, ensure the accomplishment of the required conformity assessment procedure, draw up the relevant documentation and establish a robust **post-market monitoring system**. Public authorities which put into service high-risk AI systems for their own use may adopt and implement the rules for the quality management system as part of the quality management system adopted at a national or regional level, as appropriate, taking into account the specificities of the sector and the competences and organisation of the public authority in question.

(78) In order to ensure that providers of high-risk AI systems can take into account the experience on the use of high-risk AI systems for improving their systems and the design and development process or can take any possible corrective action in a timely manner, all providers should have a **post-market monitoring system** in place. This system is also key to ensure that the possible risks emerging from AI systems which continue to ‘learn’ after being placed on the market or put into service can be more efficiently and timely addressed. In this context, providers should also be required to have a system in place to report to the relevant authorities any serious incidents or any breaches to national and Union law protecting fundamental rights resulting from the use of their AI systems.

Article

(3) For the purpose of this Regulation, the following definitions apply:

(3) (9) ‘**placing on the market**’ means the first **making available** of an AI system on the Union market;

(3) (10) ‘**making available on the market**’ means any supply of an AI system for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge;

(3) (11) ‘**putting into service**’ means the supply of an AI system for first use directly to the user or for own use on the Union market for its intended purpose;

(3) (25) ‘**post-market monitoring**’ means all activities carried out by providers of AI systems to proactively collect and review experience gained from the use of AI systems they **place on the market** or **put into service** for the purpose of identifying any need to immediately apply any necessary corrective or preventive actions;

(9) (7) The testing of the high-risk AI systems shall be performed, as appropriate, at any point in time throughout the development process, and, in any event, prior to the placing on the market or the putting into service. Testing shall be made against preliminarily defined **metrics** and **probabilistic thresholds** that are appropriate to the intended purpose of the high-risk AI system.

(61) (1) The **post-market monitoring system** shall actively and systematically collect, document and analyse relevant data provided by users or collected through other sources on the performance of high-risk AI systems throughout their lifetime, and allow the provider to evaluate the continuous compliance of AI systems with the requirements set out in Title III, Chapter 2.

(61) (2) Providers shall establish and document a **post-market monitoring system** in a manner that is proportionate to the **nature** of the artificial intelligence technologies and the **risks** of the high-risk AI system.

(61) (3) The **post-market monitoring system** shall be based on a post-market monitoring plan. The post-market monitoring plan shall be part of the technical documentation referred to in Annex IV. The Commission shall adopt an implementing act laying down detailed provisions establishing a template for the post-market monitoring plan and the list of elements to be included in the plan.

(61) (4) For high-risk AI systems covered by the legal acts referred to in Annex II, where a **post-market monitoring system** and plan is already established under that legislation, the elements described in paragraphs 1, 2 and 3 shall be integrated into that system and plan as appropriate.

Risk Management System

Develop and maintain a comprehensive risk management system for high-risk AI systems, including its implementation and documentation, as mandated by the EU AI Act.

Recital

(42) To mitigate the risks from high-risk AI systems placed or otherwise put into service on the Union market for users and affected persons, certain mandatory requirements should apply, taking into account the intended purpose of the use of the system and according to the risk management system to be established by the provider.

(46) Having information on how high-risk AI systems have been developed and how they perform throughout their lifecycle is essential to verify compliance with the requirements under this Regulation. This requires keeping records and the availability of a technical documentation, containing information which is necessary to assess the compliance of the AI system with the relevant requirements. Such information should include the general characteristics, capabilities and limitations of the system, algorithms, data, training, testing and validation processes used as well as documentation on the relevant risk management system. The technical documentation should be kept up to date.

Article

(9) (1) A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems.

(9) (2) The risk management system shall consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating. It shall comprise the following steps:

(9) (2) (a) identification and analysis of the known and foreseeable risks associated with each high-risk AI system;

(9) (2) (b) estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse;

(9) (2) (c) evaluation of other possibly arising risks based on the analysis of data gathered from the post-market monitoring system referred to in Article 61;

(9) (2) (d) adoption of suitable risk management measures in accordance with the provisions of the following paragraphs.

(9) (3) The risk management measures referred to in paragraph 2, point (d) shall give due consideration to the effects and possible interactions resulting from the combined application of the requirements set out in this Chapter 2. They shall take into account the generally acknowledged state of the art, including as reflected in relevant harmonised standards or common specifications.

(9) (4) The risk management measures referred to in paragraph 2, point (d) shall be such that any residual risk associated with each hazard as well as the overall residual risk of the high-risk AI systems is judged acceptable, provided that the high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse. Those residual risks shall be communicated to the user.

In identifying the most appropriate risk management measures, the following shall be ensured:

(9) (4) (a) elimination or reduction of risks as far as possible through adequate design and development;

(9) (4) (b) where appropriate, implementation of adequate mitigation and control measures in relation to risks that cannot be eliminated;

(9) (4) (c) provision of adequate information pursuant to Article 13, in particular as regards the risks referred to in paragraph 2, point (b) of this Article, and, where appropriate, training to users.

(9) (4) In eliminating or reducing risks related to the use of the high-risk AI system, due consideration shall be given to the technical knowledge, experience, education, training to be expected by the user and the environment in which the system is intended to be used.

(9) (5) High-risk AI systems shall be tested for the purposes of identifying the most appropriate risk management measures. Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and they are in compliance with the requirements set out in this Chapter.

(9) (6) Testing procedures shall be suitable to achieve the intended purpose of the AI system and do not need to go beyond what is necessary to achieve that purpose.

(9) (7) The testing of the high-risk AI systems shall be performed, as appropriate, at any point in time throughout the development process, and, in any event, prior to the placing on the market or the putting into service. Testing shall be made against preliminarily defined metrics and probabilistic thresholds that are appropriate to the intended purpose of the high-risk AI system.

(9) (8) When implementing the risk management system described in paragraphs 1 to 7, specific consideration shall be given to whether the high-risk AI system is likely to be accessed by or have an impact on children.

(9) (9) For credit institutions regulated by Directive 2013/36/EU, the aspects described in paragraphs 1 to 8 shall be part of the risk management procedures established by those institutions pursuant to Article 74 of that Directive.

Appendix C: Frequently Asked Questions (FAQs)

1. What is Orthrus?

Orthrus is a regtech tool designed to assist users in complying with the EU AI Act. It helps identify AI systems, classify their risks, generate risk reports, and monitor them after deployment.

2. What are the system requirements for Orthrus?

Orthrus operates on a range of systems. It typically requires a standard computer with an up-to-date web browser and a stable internet connection. Detailed requirements can be found in the "Getting Started" section of the manual.

3. How do I configure regulatory rules in Orthrus?

Configuring regulatory rules involves defining the specific criteria and standards you want Orthrus to use when assessing AI system compliance. This can be done in the "Regulatory Compliance" section of the tool.

4. What should I do if I encounter an issue with Orthrus?

If you face problems while using Orthrus, consult the "Troubleshooting" section of this manual, which provides solutions to common issues. If the problem persists, please reach out to our technical support team.

5. How often is Orthrus updated?

Orthrus is regularly updated to enhance its features and ensure compliance with evolving regulations. The "Updates and Maintenance" section contains details on the update process and frequency.

6. What kind of training resources are available for Orthrus users?

Orthrus offers various training resources, including workshops, online tutorials, and certification programs. These can be found in the "Training and Resources" section.

7. How can I provide feedback or suggestions for improvement?

Your feedback is valuable. Please use the designated channels within Orthrus to share your thoughts and suggestions. A dedicated "Feedback and Improvement" section in this manual guides you through the process.

8. How can I access the Glossary of Terms in this manual?

The Glossary of Terms is located in "Appendix A." It provides clear definitions of key terms used throughout the Orthrus manual.

9. Where can I find detailed information on the EU AI Act?

References to the EU AI Act and additional regulatory compliance resources are listed in "Appendix B: Regulatory Compliance References." This section provides a wealth of information and sources.

10. Is there a certification program available for Orthrus users?

Yes, Orthrus offers a certification program. Details on how to enroll and what the certification entails are available in the "Training and Resources" section.

These frequently asked questions are designed to assist users in navigating Orthrus effectively and resolving common queries. If you have further questions or require more detailed information, please refer to the relevant sections of the manual or contact our support team.