SPEEDNET

AI Auditor

AI Solutions compliance management

SPEEDNET

New AI Act Reality

Risk Management

Companies must establish, implement, document, and maintain a **risk management system for high-risk AI systems**. This system is required to be a continuous iterative process throughout the entire lifecycle of the AI system, including regular reviews and updates. The process involves identifying and analysing foreseeable risks, evaluating those risks, and adopting appropriate risk management measures to mitigate or eliminate them where feasible.

2.08.2027

Deadline for most companies to install necessary AI Governance processes.

Systematic Testing

High-risk AI systems must undergo testing to ensure they perform consistently and comply with regulatory requirements. This testing should be done throughout the development process and before the AI system is placed on the market.

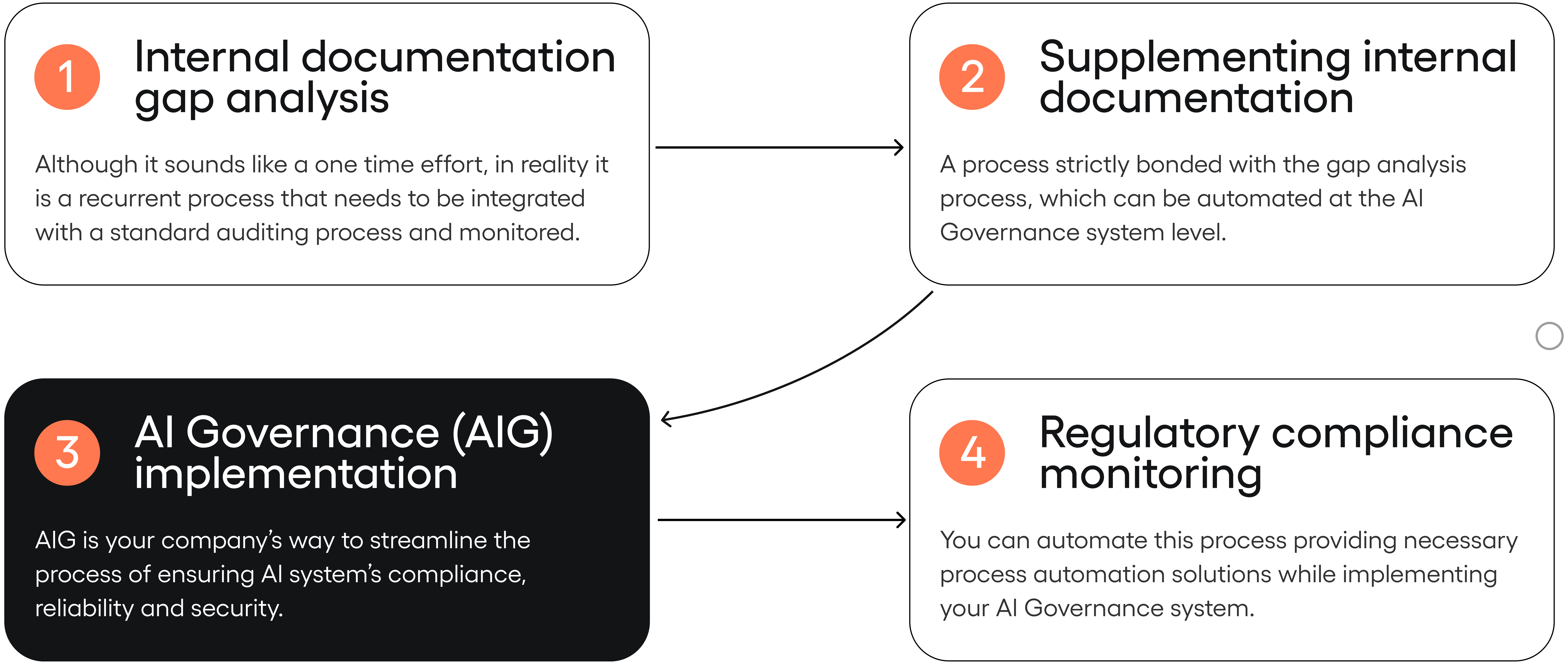
Cybersecurity and Incident Reporting

Companies are also required to ensure an adequate level of cybersecurity protection for AI systems, particularly those with systemic risks. In case of serious incidents, they must track and report these incidents, along with any corrective measures, to the AI Office and relevant national authorities without undue delay

Compliance Integration

For companies already being a subject to other internal risk management regulations under EU law, the AI risk management procedures may be integrated with existing processes to avoid duplication and minimise the administrative burden. This ensures consistency in applying both AI and model regulations.

How to comply?



1 Internal documentation gap analysis

Although it sounds like a one time effort, in reality it is a recurrent process that needs to be integrated with a standard auditing process and monitored.

2 Supplementing internal documentation

A process strictly bonded with the gap analysis process, which can be automated at the AI Governance system level.

3 AI Governance (AIG) implementation

AIG is your company's way to streamline the process of ensuring AI system's compliance, reliability and security.

4 Regulatory compliance monitoring

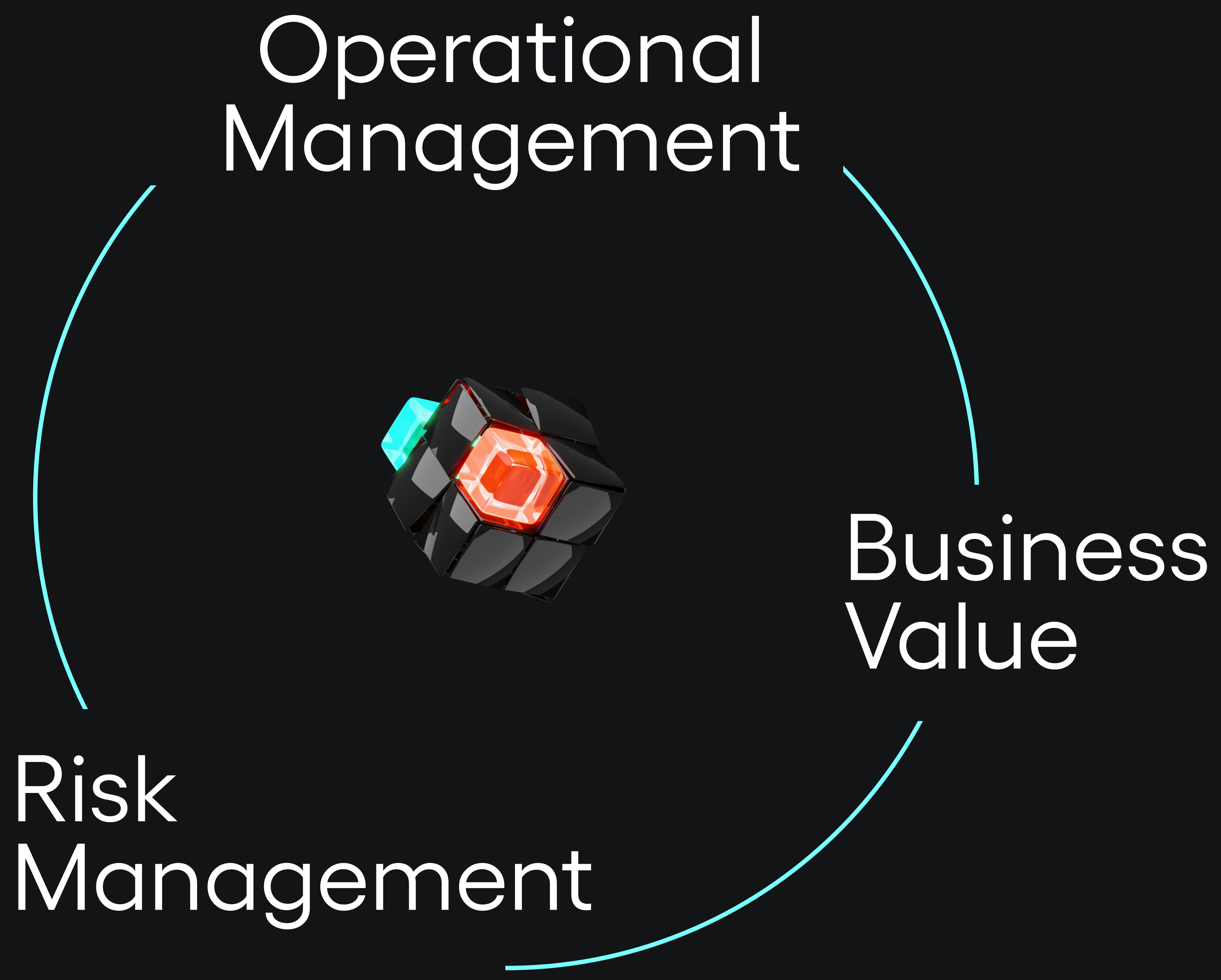
You can automate this process providing necessary process automation solutions while implementing your AI Governance system.

AI Governance

Deployment of AI solutions today is a long pass play.

According to the EU AI Act, European companies must implement comprehensive Ai Governance and risk management processes to comply with the regulation.

Only through thoughtfully implemented, value-driven AI Governance strategy, companies can secure their competitive advantage.

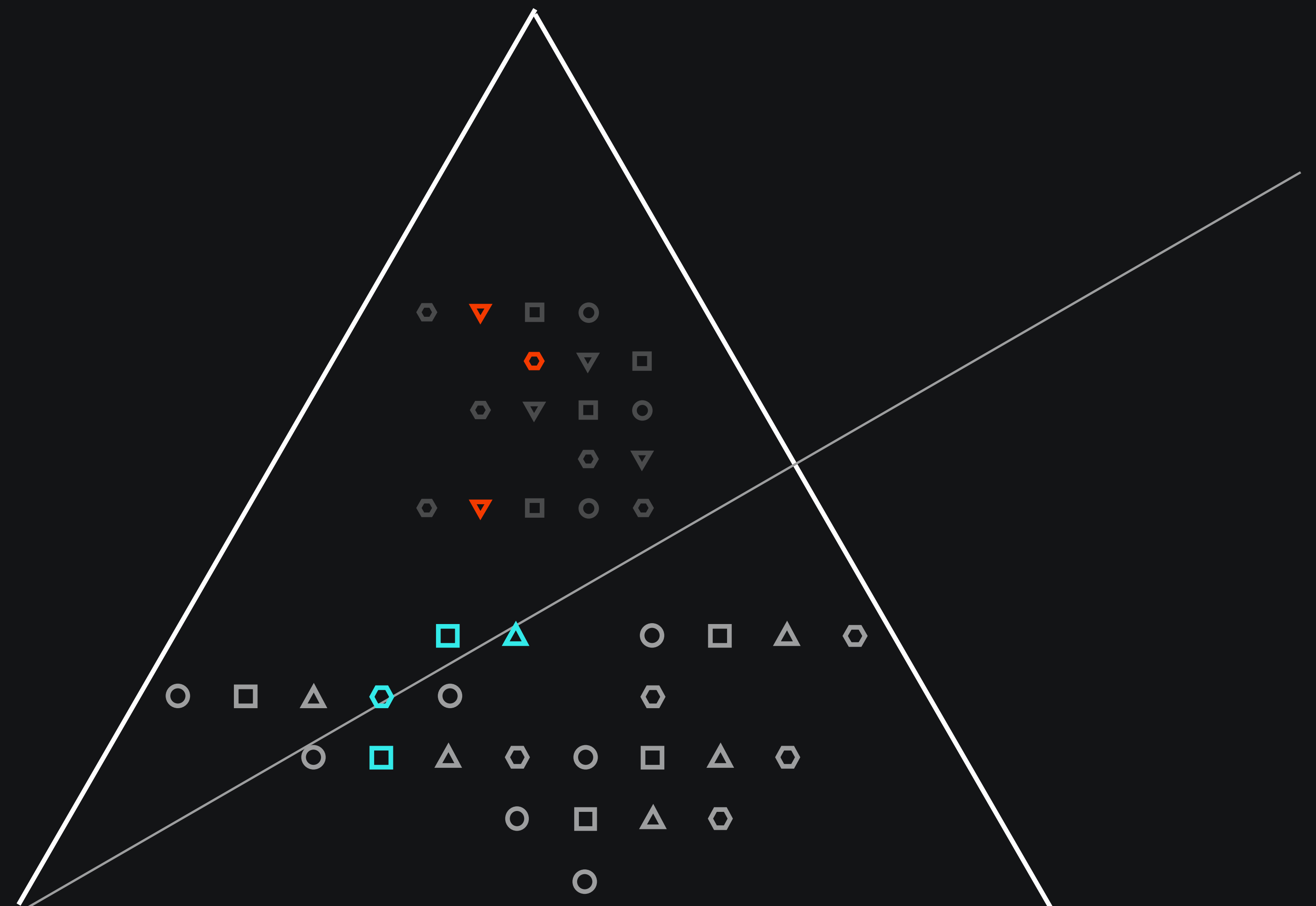


Operational Management

Business Value

Risk Management

Busines
Value



Risk
Mitigation

Cost
Optimisation

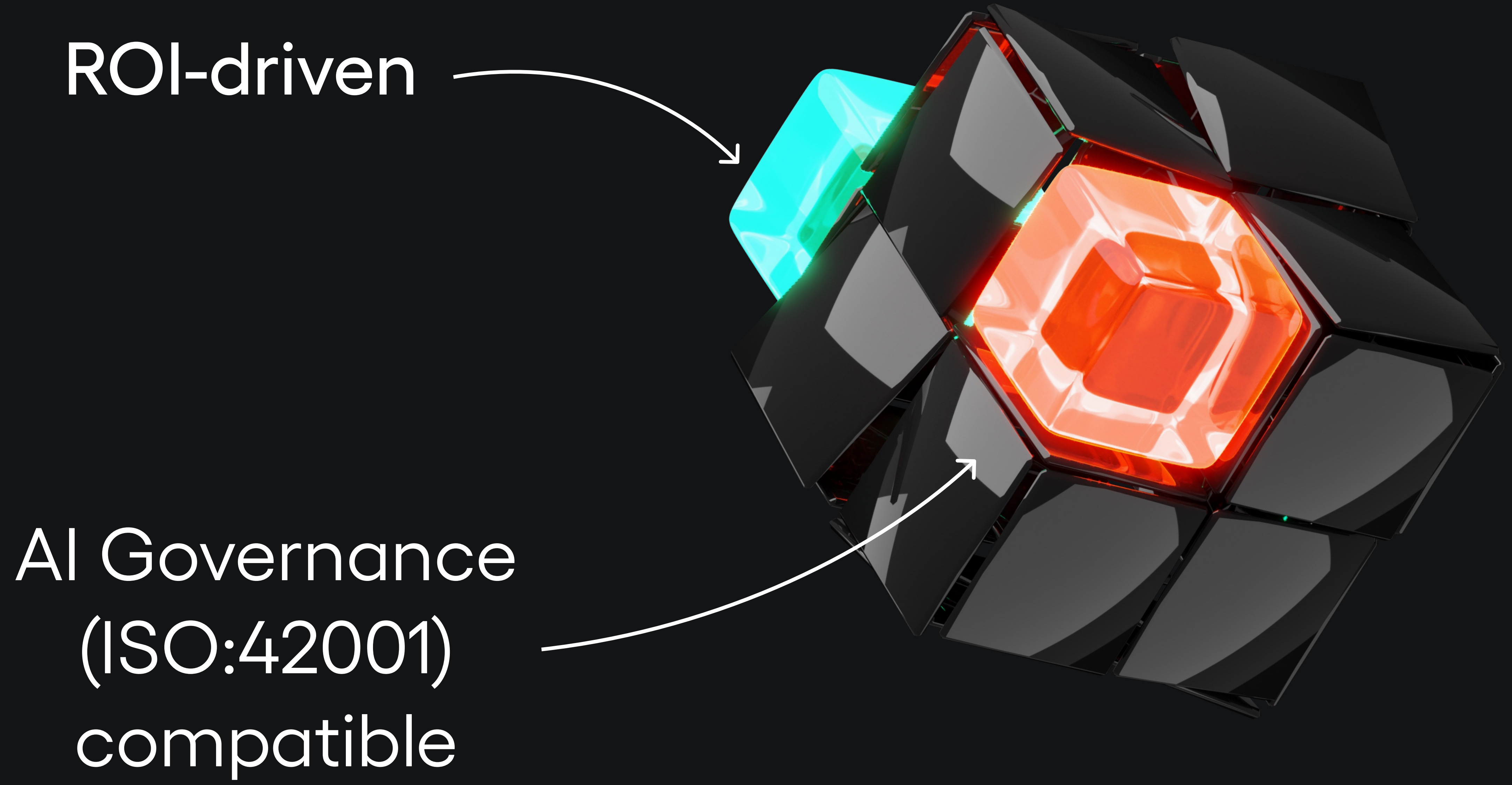
SPEEDNET

What’s AIG-Ready AI Solution?

Develop a bulletproof competitive advantage.

It’s an AIG compliant system with pre-defined risk mitigation strategy for every risk associated with system’s processes, compliant with ISO 42001.

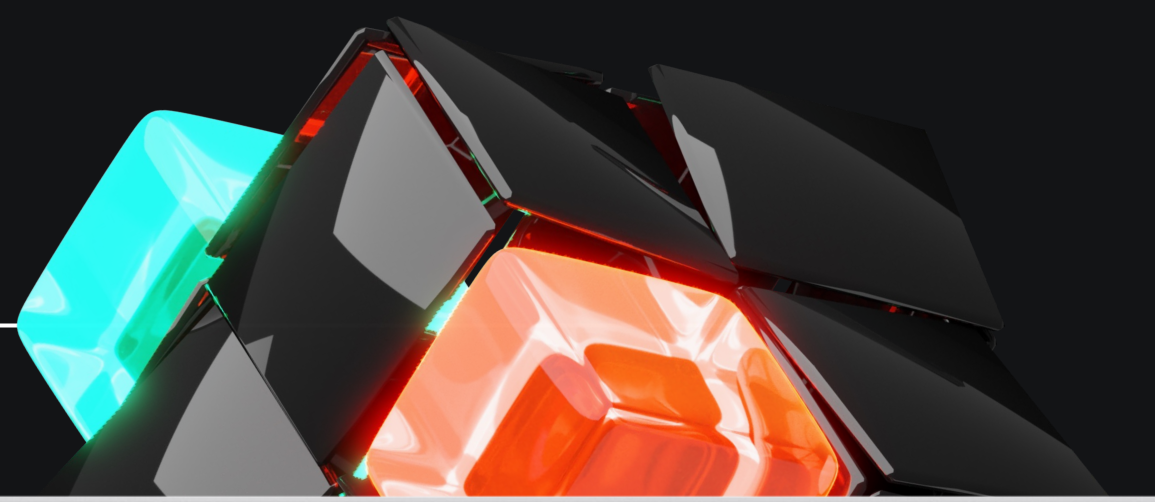
- EU AI Act compliance
- ISO/IEC 42001 compatible
- ROI-driven calculated business objectives
- Fully executable risk management package



ROI-driven

AI Governance (ISO:42001) compatible

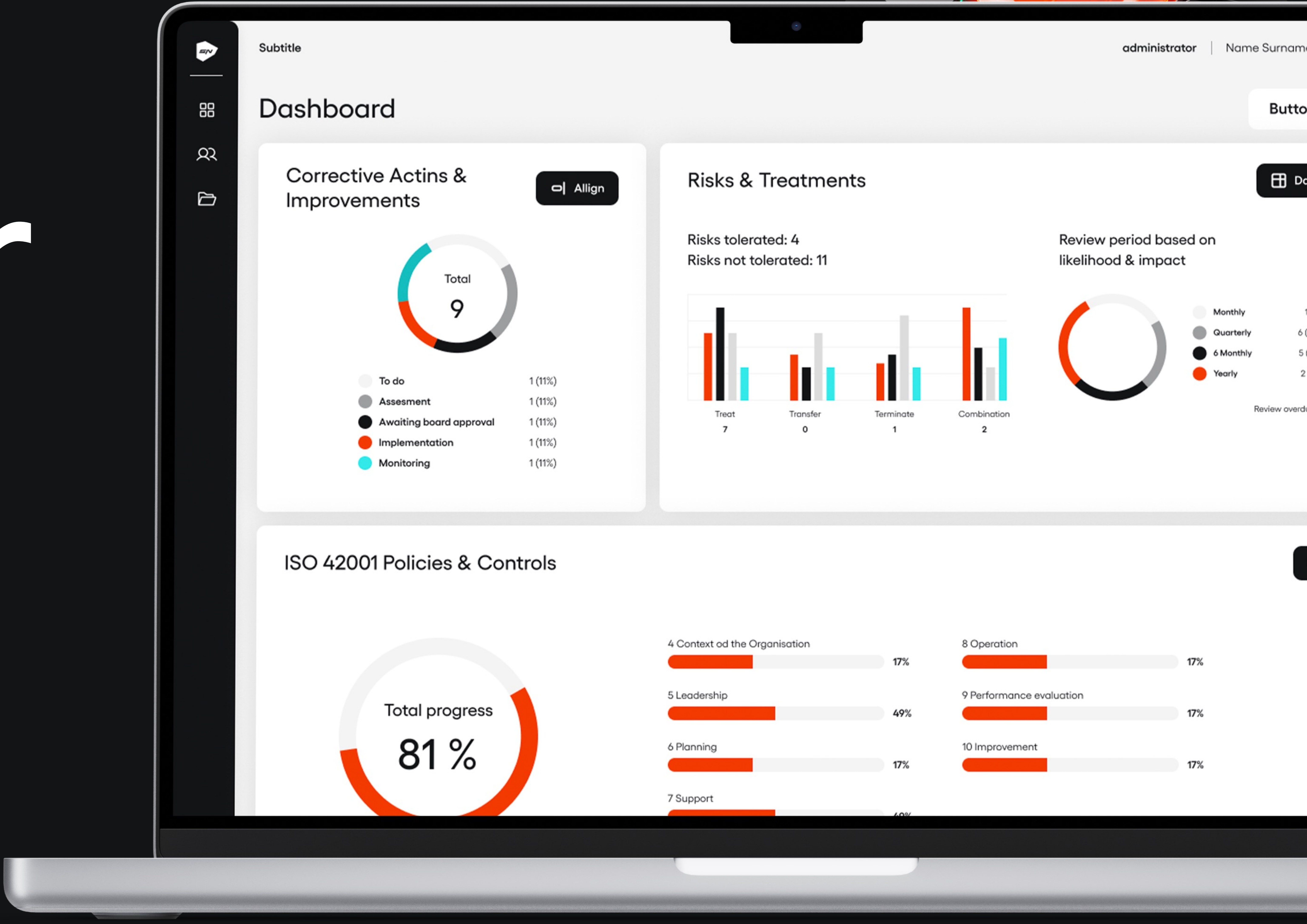
SPEEDNET



AI Auditor

AI Auditor is an AI-based tool that allows for the verification of AI systems' documentation against a defined list of requirements (control package), such as those related to the AI Act regulations. AI Auditor enables analysis, gap identification, and conversation with an AI assistant regarding our AI system in the context of the selected regulations.

ISO:42001:2023 certifiable



Subtitle

administrator | Name Surnam

Dashboard

Corrective Actins & Improvements

	To do	1 (11%)
●	Assesment	1 (11%)
●	Awaiting board approval	1 (11%)
●	Implementation	1 (11%)
●	Monitoring	1 (11%)

Risks & Treatments

Risks tolerated: 4
Risks not tolerated: 11

Review period based on likelihood & impact

ISO 42001 Policies & Controls

Total progress 81 %

4 Context od the Organisation	17%
5 Leadership	49%
6 Planning	17%
7 Support	49%
8 Operation	17%
9 Performance evaluation	17%
10 Improvement	17%

How Does It Work?

Imagine you are an IT System Auditor in a large bank. Your task is to make sure, a new AI System (for example: credit scoring AI assistant) is compliant with legal regulations and your internal AI Governance policies.

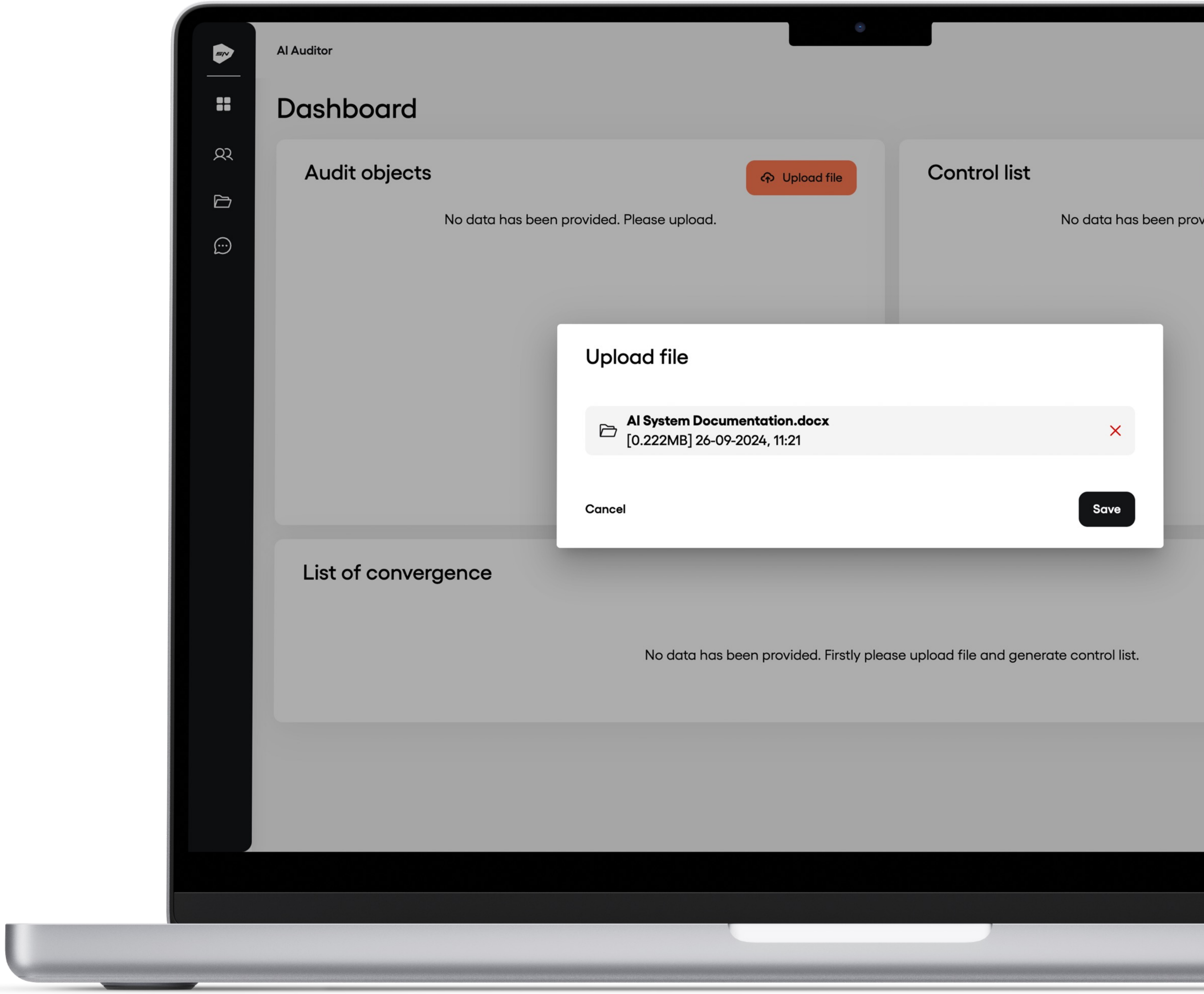
You need to:

1. Identify gaps and inconsistencies in documentation
2. Solve problems related to gaps
3. Update documentation and certify compliance

Audit Object

1. Documentation upload

- First thing you need to do is to upload an **Audit Object** - System's data including information that will allow you to verify whether the System is compliant. Documentation (especially that of AI Systems) should have consistent form and include pre-defined Control Package elements.
- Control Package is a collection of "checkpoints" - requirements that allows your company to monitor risks and compliance associated with AI systems. Your Control Package should have it's own standard and the best standard you can use is **ISO:42001**.
- AI Auditor processes PDF and .docx files.



AI Auditor

Dashboard

Audit objects

No data has been provided. Please upload.

Control list

No data has been prov

Upload file

AI System Documentation.docx
[0.222MB] 26-09-2024, 11:21

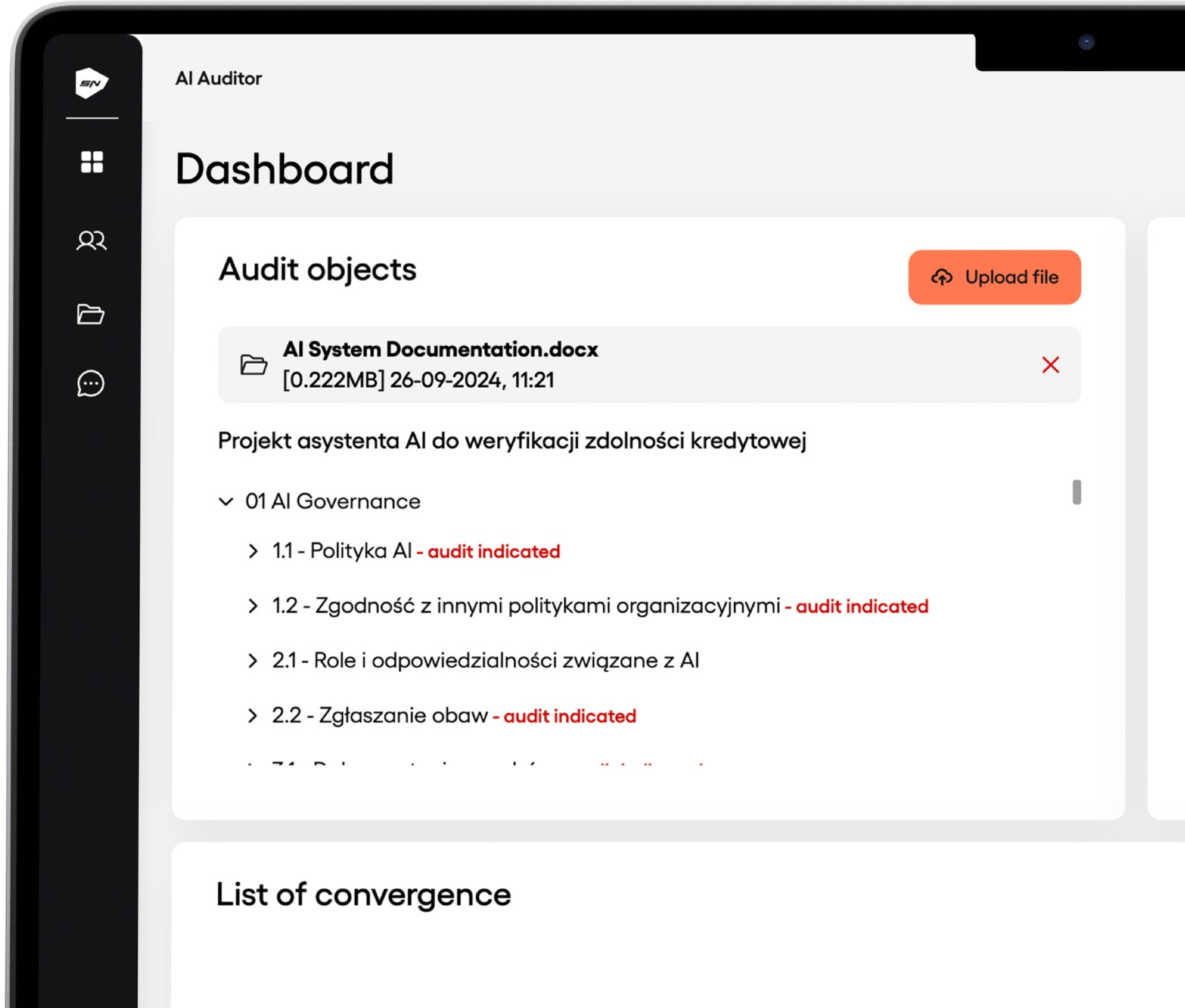
List of convergence

No data has been provided. Firstly please upload file and generate control list.

Object Analysis

2. Data processing & risk flagging

- Once you upload the documentation, Auditor will analyse it to understand it’s structure and look for necessary information.
- When the risk detection module identifies potential risks, it flags suspicious areas potentially requiring your attention.



AI Auditor

Dashboard

Audit objects

Upload file

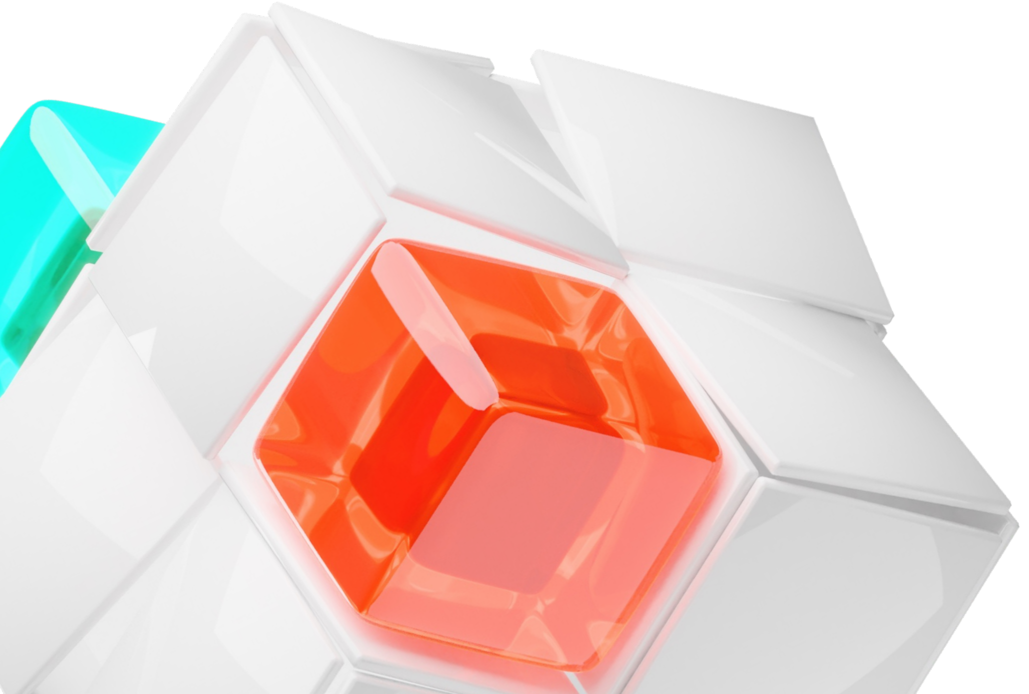
AI System Documentation.docx
[0.222MB] 26-09-2024, 11:21

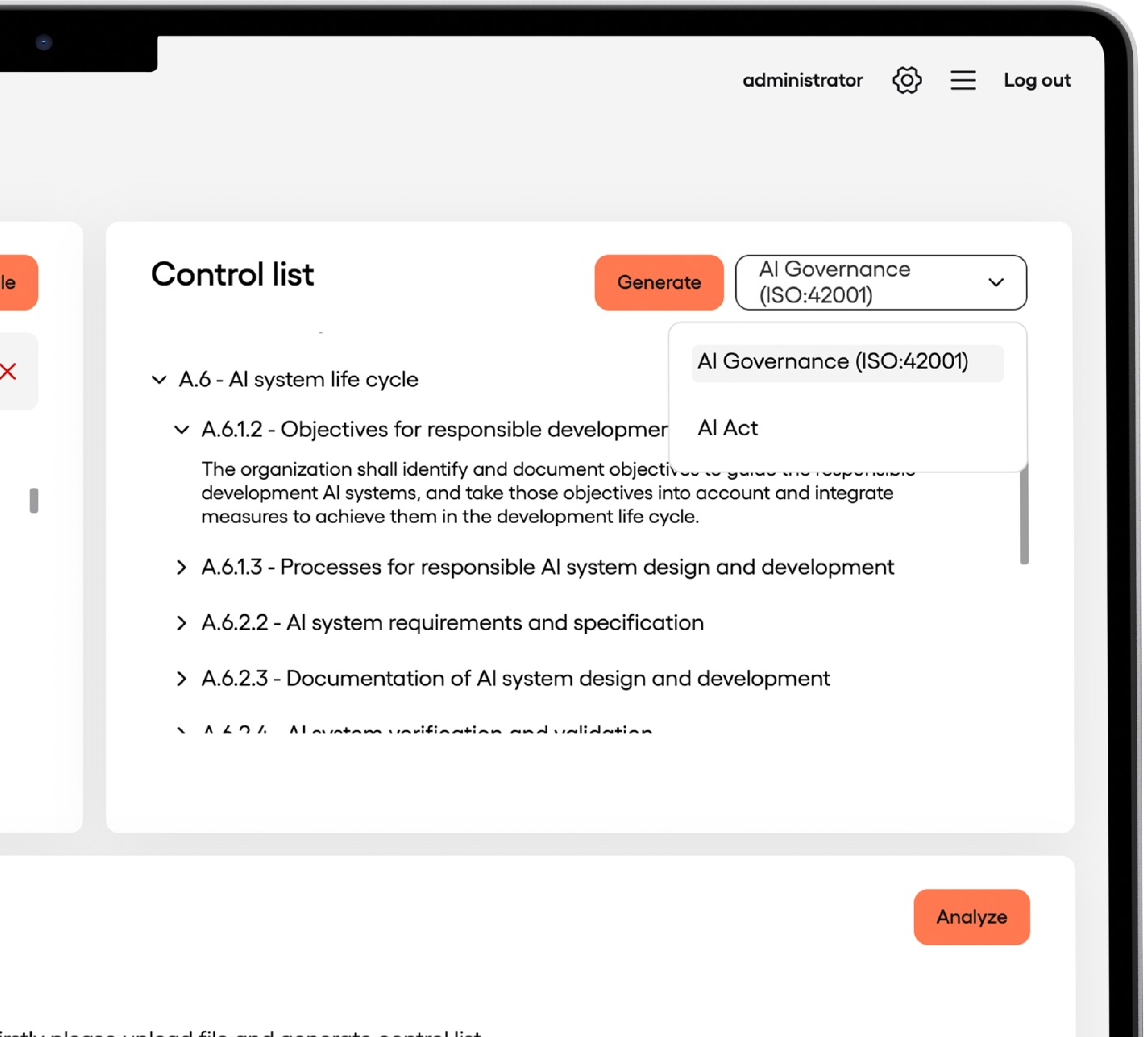
Projekt asystenta AI do weryfikacji zdolności kredytowej

01 AI Governance

- 1.1 - Polityka AI - audit indicated
- 1.2 - Zgodność z innymi politykami organizacyjnymi - audit indicated
- 2.1 - Role i odpowiedzialności związane z AI
- 2.2 - Zgłaszanie obaw - audit indicated

List of convergence





Control list

- A.6 - AI system life cycle
  - A.6.1.2 - Objectives for responsible developmer

    The organization shall identify and document objectives to guide the responsible development AI systems, and take those objectives into account and integrate measures to achieve them in the development life cycle.
  - A.6.1.3 - Processes for responsible AI system design and development
  - A.6.2.2 - AI system requirements and specification
  - A.6.2.3 - Documentation of AI system design and development
  - A.6.2.4 - AI system verification and validation

irstly please upload file and generate control list

Control List

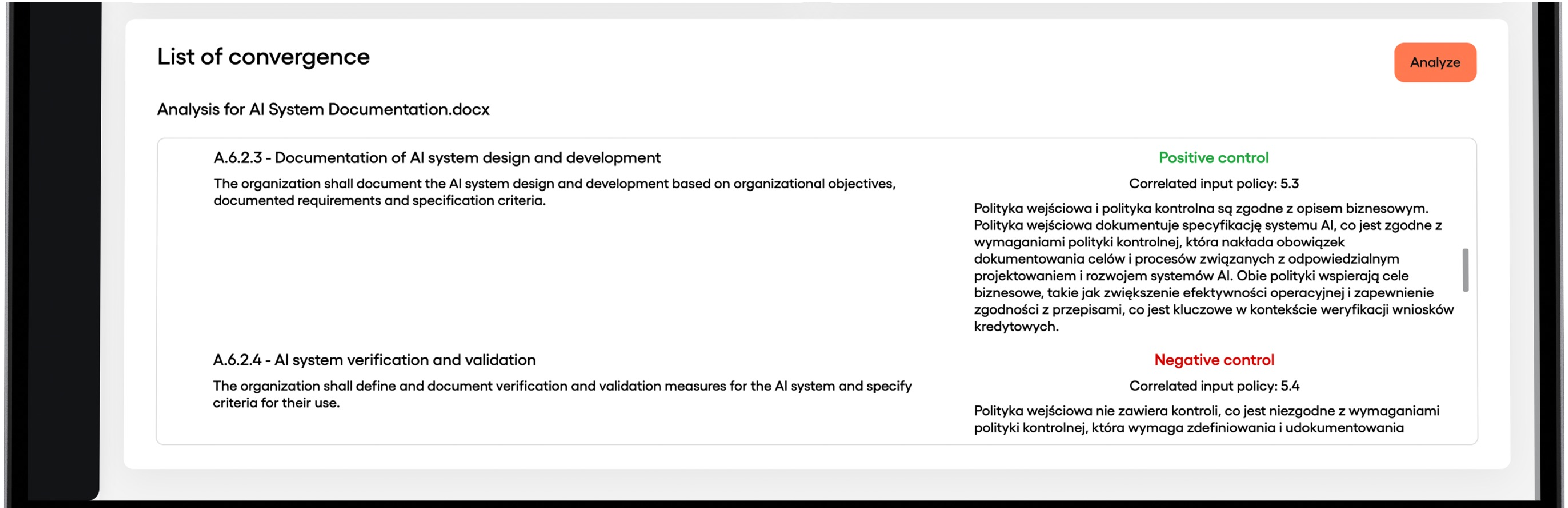
3. Control List generation

- Once your object has been analysed, you need something to reference its contents and compare it to the requirements.
- The reference is nothing else than the pre-defined Control List (Package), which should be defined for all AI Systems according to your internal AI Governance policies. An AI Governance Control List can be based on the ISO:42001:2023 standard.
- By clicking ‘Generate’ AI Auditor generates a pre-defined Control List according to your needs. It can be anything: AI Act, AI Governance policies, DORA, GDPR etc.

Compliance Analysis

4. Compliance Control Analysis

- Next thing your AI Auditor will do is searching for appropriate information regarding compliance conditions in the documentation according to Control List.
- List elements are marked as either positive or negate, if the system meets or doesn't meet their criteria. If the Object doesn't provide enough data, Auditor will mark the element for manual verification.
- The tool provides contextual information about flagged errors, helping auditors understand why a particular area was flagged.



List of convergence

Analysis for AI System Documentation.docx

A.6.2.3 - Documentation of AI system design and development

The organization shall document the AI system design and development based on organizational objectives, documented requirements and specification criteria.

Positive control

Correlated input policy: 5.3

Polityka wejściowa i polityka kontrolna są zgodne z opisem biznesowym. Polityka wejściowa dokumentuje specyfikację systemu AI, co jest zgodne z wymaganiami polityki kontrolnej, która nakłada obowiązek dokumentowania celów i procesów związanych z odpowiedzialnym projektowaniem i rozwojem systemów AI. Obie polityki wspierają cele biznesowe, takie jak zwiększenie efektywności operacyjnej i zapewnienie zgodności z przepisami, co jest kluczowe w kontekście weryfikacji wniosków kredytowych.

A.6.2.4 - AI system verification and validation

The organization shall define and document verification and validation measures for the AI system and specify criteria for their use.

Negative control

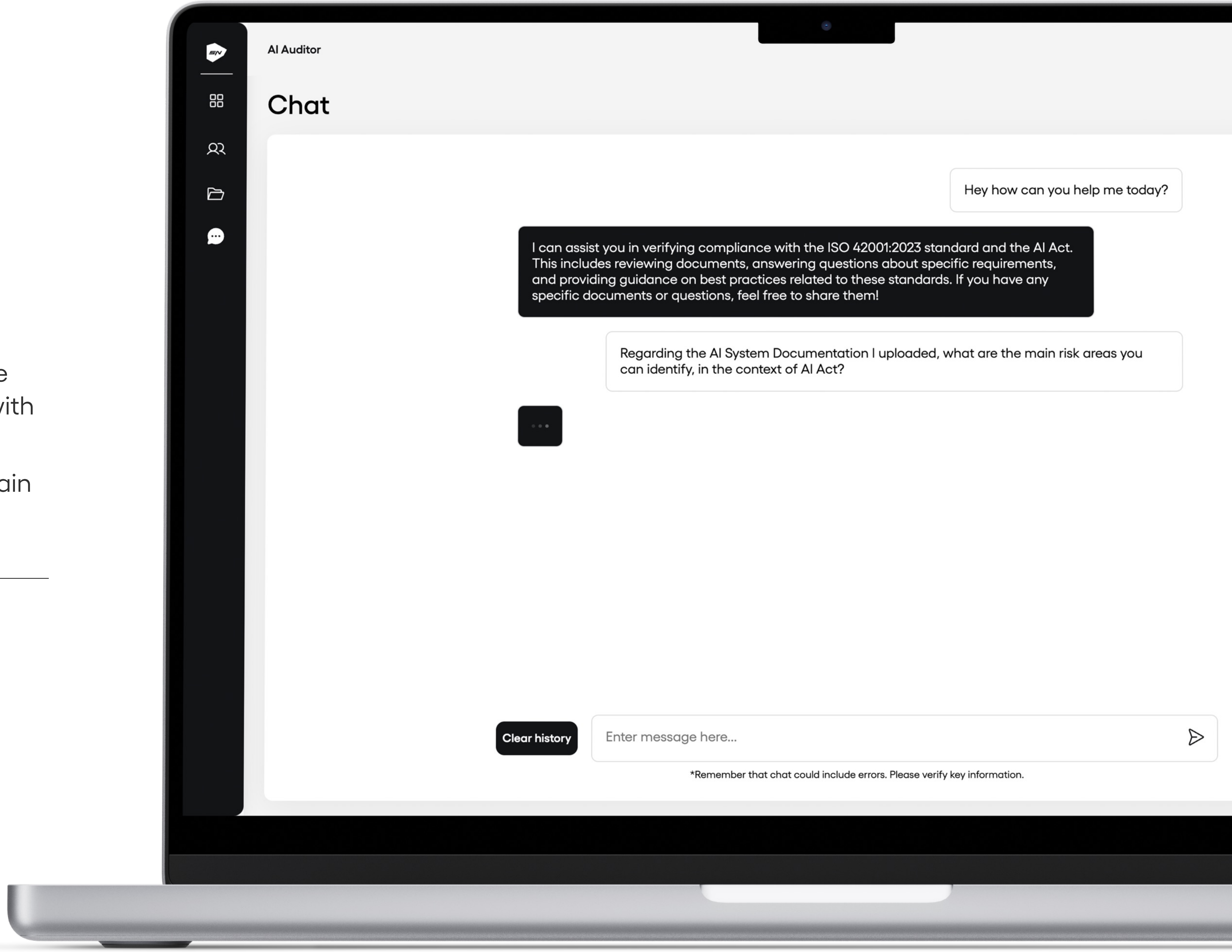
Correlated input policy: 5.4

Polityka wejściowa nie zawiera kontroli, co jest niezgodne z wymaganiami polityki kontrolnej, która wymaga zdefiniowania i udokumentowania

Compliance Assistant

5. Compliance & Risk database chat

- Your responsibility is to detect and minimise risks associated with the System. If you don't know how to approach certain risk associated with an analysed Object - you can ask Auditor's Assistant.
- The Assistant is trained to understand any legal and regulatory domain important to you. AI Act, ISO, DORA, GDPR - you can ask anything related to these regulations. For example:

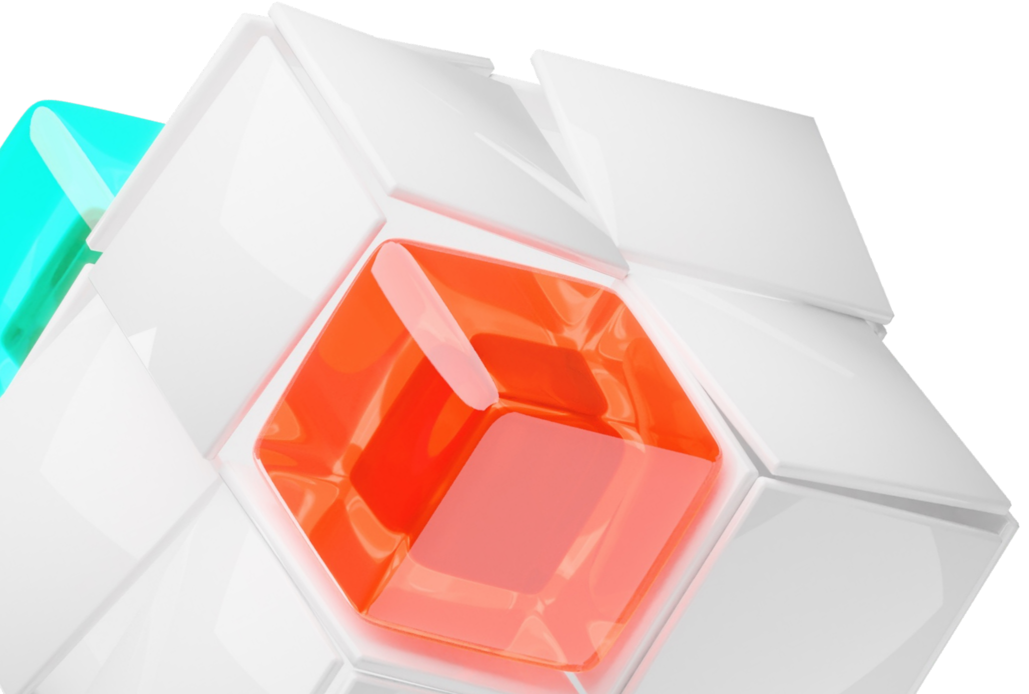


Hey how can you help me today?

I can assist you in verifying compliance with the ISO 42001:2023 standard and the AI Act. This includes reviewing documents, answering questions about specific requirements, and providing guidance on best practices related to these standards. If you have any specific documents or questions, feel free to share them!

Regarding the AI System Documentation I uploaded, what are the main risk areas you can identify, in the context of AI Act?

*Remember that chat could include errors. Please verify key information.

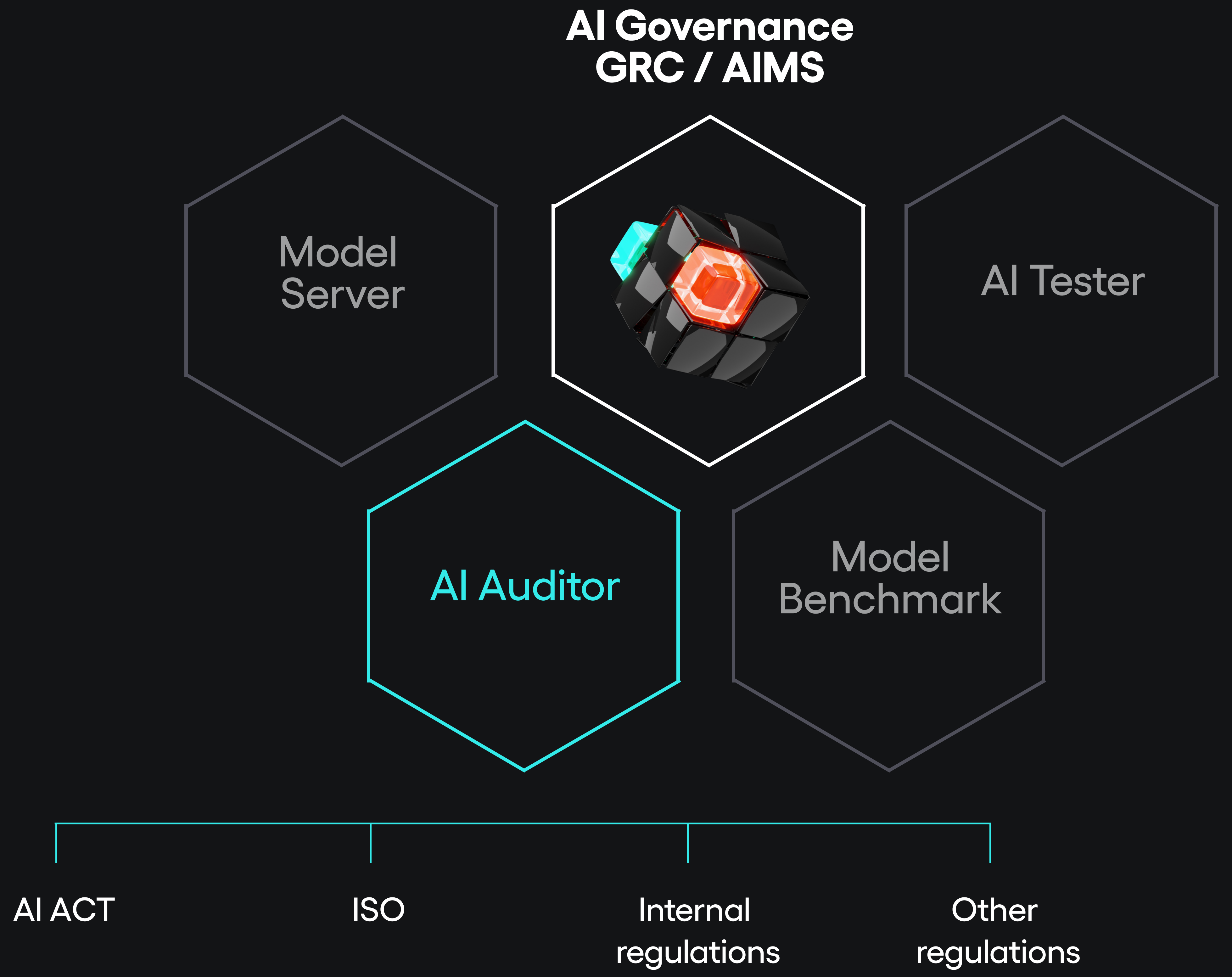


AI Auditor as a part of GRC

Key element on the way to implement AI Governance GRC

AI Auditor, in addition to being an excellent tool for any bank auditor, also fulfills its primary function as a key module of the GRC system tailored for AI Governance. This agent allows for the automation of the compliance verification process for high-risk/restricted-risk systems and objects in accordance with the AI Act, internal regulations, KNF guidelines, ISO, and any legal or regulatory documents. Integrating it with the AI Governance system enables risk identification and assessment at any time, without the need to go through the costly process of a full audit.

Implementing the AI Auditor tool can be an excellent first step towards building and deploying a complete GRC system that addresses AI Governance tasks.



How do we implement AI Auditor?

Every AI Auditor is unique. We provide you a custom solution tailored to your needs.

1. Verification of your auditing process
2. Solution adaptation
3. Implementation

Delivery Process

Speednet

Business Analyst

AI Solutions Architect

Client

Risk Management Department Stakeholders

1 We map the company's current risk management processes. We define the **business requirements for the tool**. We conduct an assessment of the risk of implementing the Auditor, identifying gaps in the scope of regulations and project feasibility conditions in such a way that the tool is compatible with ISO:42001 and the company's vision of AI Governance development.

example

Objective:
Compliance of the AI-supported AML process when collecting financial transaction data, including amounts, recipients, senders, transaction locations, as well as historical data on customer transaction behaviour.

Requirement related to ISO:42001:2023:
In the context of the identified risks, ISO 42001:2023 would require the company to conduct a detailed analysis of the impact of AI misinterpretation on audit results and implement appropriate controls, such as manual verification of critical decisions or additional model testing to minimise the risk of errors.

An example of such a requirement could be the obligation to implement oversight mechanisms that ensure that critical AI decisions are subject to manual verification by appropriately trained personnel, which minimises the risk of negative consequences resulting from AI misinterpretation.

Delivery Process

Business Analyst

AI Solutions Architect

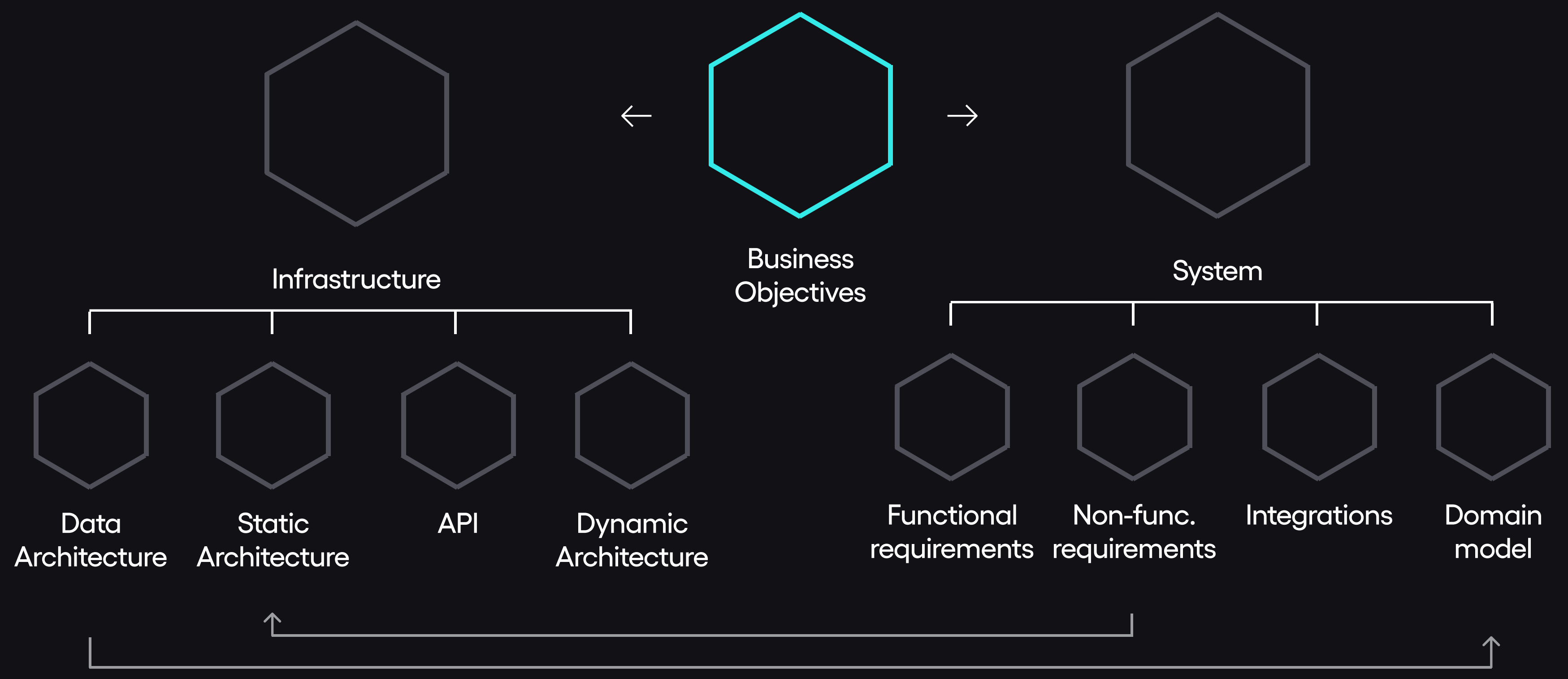
Software Developers

Speednet

Client

IT Department Stakeholders

2 Based on the defined Business Objectives and the conducted feasibility assessment with established feasibility conditions, the **High-Level Architecture** concept is created.



example

Example of
High Level Architecture (PDF)

Download →

1. Introduction
    - 1.1 Project background and purpose
    - 1.2 Glossary of terms
    - 1.3 Recipients and document goal
2. Scope of the project
    - 2.1 High level conceptual/architecture overview
    - 2.2 Business Process perspective & mapping
3. Use Case diagrams
4. Functional requirements
    - 4.1 System functions with description
    - 4.2 Integration specification
        - 4.2.1 Identified IT systems in the processes
        - 4.2.2 Identification of SPOCs
5. Non-functional requirements

Delivery Process

Business Analyst

UX/UI Designer

Client

Speednet

3 Created diagrams of Business Processes and Functional Requirements allow us to create high-level **User Stories**. Our UX/UI Designer uses them to create mockups to visualise the most critical functionalities.

example

DESCRIPTION

As a registered user, I want to be able to log into the application to access all functionalities.

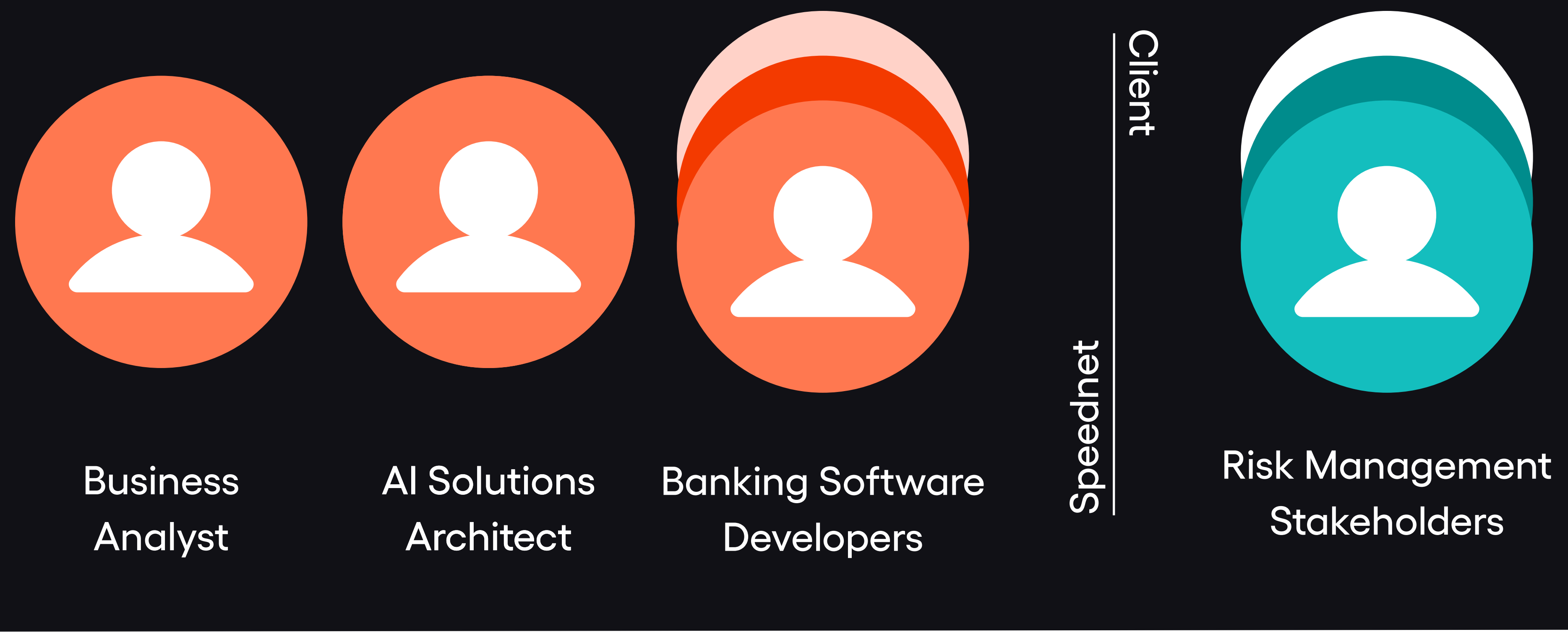
INPUT CONDITIONS

The user has logged out of the application - not logged in.

1. Logging in is done by phone number and SMS code
2. The form displays an input for entering the phone number
3. Clicking on the input displays the system numeric keypad
4. In the input "Phone number" you can enter up to 9 digits
5. CTA "Send activation code" activates after entering 9 characters in the input
6. After entering the phone number, an SMS code is sent to the indicated number
7. SMS content: Activation code for ABC application is: <SMS code>.
8. The user enters the SMS code, after which logging into the application takes place
9. Functionality meets the requirements of WCAG

SPEEDNET

Delivery Process



4 In the final step, we provide our offer with detailed **Project Cost Estimation** and **Delivery Plan**. Once you decide to move forward, we start implementation.

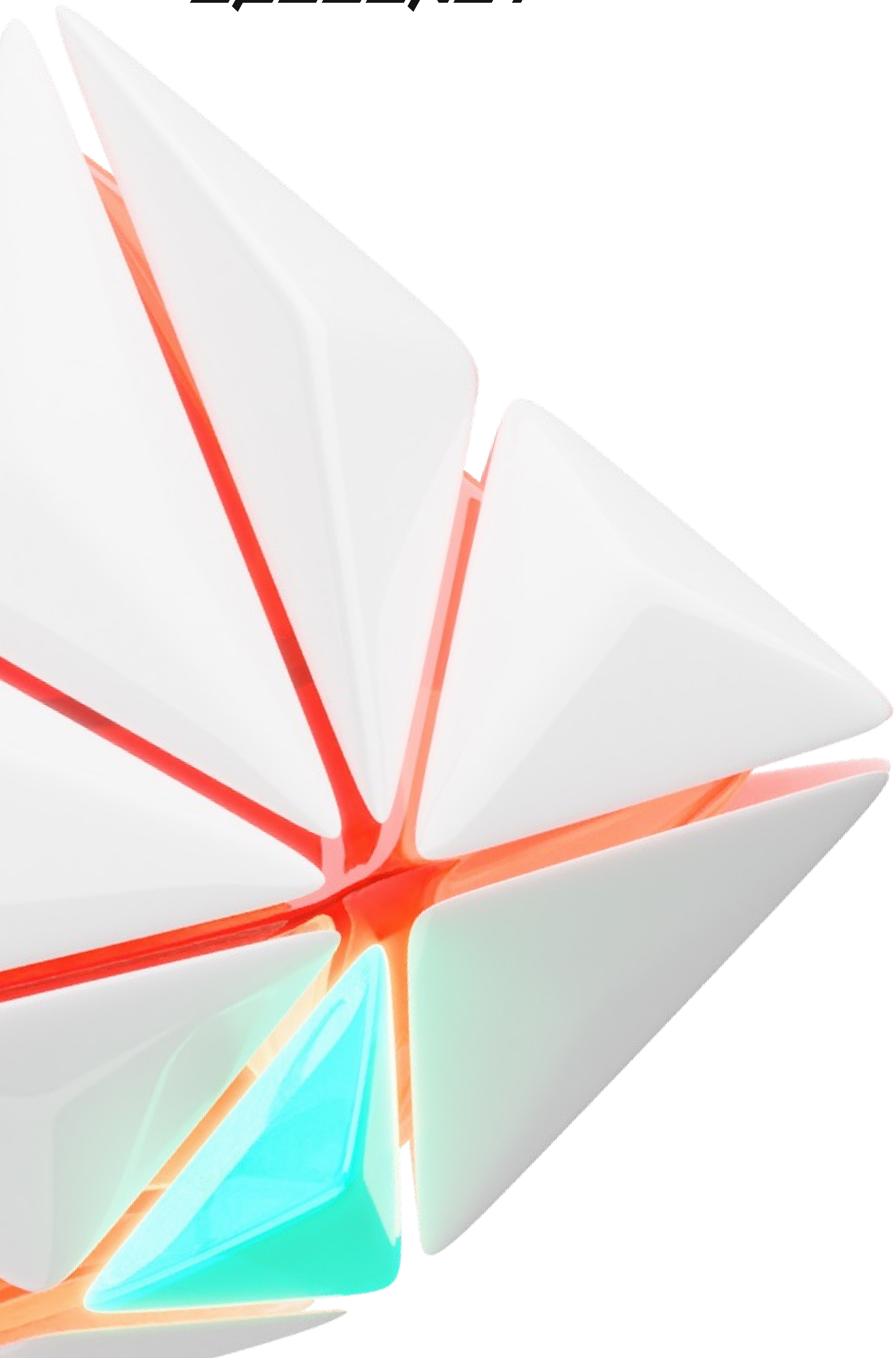
example

See Sample Cost Estimation*

SAMPLE PRICING →

*Cost Estimation depends on various factors that are to be determined on early stage of implementation.

SPEEDNET



What’s next?

Talk to us about your AI Governance!

Tymoteusz Olszewski
AI Strategy Manager

tymoteusz.olszewski@speednet.pl
+48 794 783 335

in Let’s talk →

Our website