# Aegis Risk Management Platform: Complete Documentation

## 1. Executive Summary

### 1.1. Platform Overview and Business Value

The Aegis Risk Management Platform is a comprehensive, enterprise-grade cybersecurity solution that provides a centralized system for managing risks, tracking assets, and automating security assessments. By integrating advanced AI capabilities, Aegis streamlines risk management workflows, enhances decision-making, and reduces the manual effort required to maintain a strong security posture. The platform’s business value lies in its ability to provide a real-time, unified view of risk, enabling organizations to proactively address threats, ensure compliance, and align security initiatives with business objectives.

### 1.2. Key Features and Capabilities

Aegis offers a robust set of features, including: - **Centralized Risk Register**: A unified system for tracking and managing all identified risks. - **Asset Management**: A complete inventory of organizational assets with categorization and ownership. - **AI-Powered Analysis**: Automated evidence review, risk statement generation, and compliance reporting. - **Multi-LLM Support**: Integration with over 14 LLM providers, including OpenAI, Google Gemini, and Anthropic Claude. - **Role-Based Dashboards**: Tailored views for CISOs, analysts, and system owners. - **External Integrations**: Seamless connections with OpenVAS, OpenCTI, and Microsoft Entra ID.

### 1.3. Target User Personas and Use Cases

Aegis is designed for a range of cybersecurity professionals: - **CISO/Security Director**: Gains a high-level view of the organization’s risk posture for strategic decision-making. - **Cybersecurity Analyst/GRC Specialist**: Utilizes the Analyst Workbench for day-to-day risk assessment and evidence management. - **IT Manager/System Owner**: Manages assigned tasks and attests to security controls through a dedicated inbox. - **Internal/External Auditor**: Accesses a comprehensive audit trail and verifies compliance evidence.

### 1.4. ROI and Efficiency Benefits

Aegis delivers a strong return on investment by: - **Reducing Manual Effort**: Automating repetitive tasks such as evidence analysis and report generation. - **Improving Efficiency**: Streamlining risk management workflows and providing a single source of truth. - **Enhancing Accuracy**: Leveraging AI to ensure consistent and accurate risk assessments. - **Accelerating Compliance**: Simplifying audit preparations and providing a clear view of compliance status.

## 2. Complete Deployment Guide

### 2.1. System Requirements and Prerequisites

* **OS**: Linux, macOS, or Windows (with WSL2)
* **RAM**: 16GB+ recommended
* **Storage**: 20GB+ free space
* **CPU**: 4+ cores recommended
* **Software**: Docker and Docker Compose

### 2.2. Docker Deployment Instructions

1. **Clone the Repository**:

* git clone <repository-url>  
  cd aegis-platform

1. **Configure Environment**:

* cp .env.example .env  
  nano .env

1. **Deploy**:

* chmod +x deploy.sh  
  ./deploy.sh

### 2.3. Environment Configuration

The .env file contains over 150 configuration variables. Key settings include: - **Security**: SECRET\_KEY, JWT\_SECRET\_KEY - **Database**: POSTGRES\_PASSWORD - **AI Providers**: OPENAI\_API\_KEY, AZURE\_OPENAI\_API\_KEY - **Integrations**: OPENVAS\_HOST, OPENCTI\_URL, AZURE\_CLIENT\_ID

### 2.4. Database Setup

The platform uses a PostgreSQL database, which is automatically initialized during the Docker deployment. To connect manually:

docker exec -it aegis-db psql -U aegis\_user -d aegis\_db

### 2.5. Security and Hardening

* **Change Default Credentials**: Update all default keys and passwords.
* **Network Security**: Use a reverse proxy and enable HTTPS.
* **File Permissions**: Secure the .env file with chmod 600 .env.
* **Regular Updates**: Keep all software components up to date.

## 3. Multi-LLM Provider Configuration

### 3.1. Supported Providers

Aegis supports over 14 LLM providers, including: - **Cloud**: OpenAI, Azure OpenAI, Google Gemini, Anthropic Claude - **Aggregation**: LiteLLM, OpenRouter, Together AI - **Local**: Ollama, LM Studio, Text Generation WebUI

### 3.2. Configuration Examples

Enable and configure providers in the .env file: - **OpenAI**: bash ENABLE\_OPENAI=true OPENAI\_API\_KEY=sk-your-api-key - **Azure OpenAI**: bash ENABLE\_AZURE\_OPENAI=true AZURE\_OPENAI\_API\_KEY=your-key - **Ollama**: bash ENABLE\_OLLAMA=true OLLAMA\_BASE\_URL=http://localhost:11434

### 3.3. Advanced Features

* **Failover**: Automatically switches to a backup provider if the primary fails.
* **Cost Optimization**: Tracks and manages costs across different providers.
* **Performance Monitoring**: Monitors the health and performance of all enabled providers.

## 4. User Guides by Persona

### 4.1. CISO/Security Director

The CISO Cockpit provides an executive-level view of the organization’s risk posture, including key metrics, risk trends, and compliance status.

### 4.2. Cybersecurity Analyst/GRC Specialist

The Analyst Workbench is the primary interface for managing risks, conducting assessments, and reviewing evidence. It includes a task management system to track remediation efforts.

### 4.3. IT Manager/System Owner

The System Owner Inbox displays all assigned tasks and control attestation requests, allowing system owners to upload evidence and confirm compliance.

### 4.4. Internal/External Auditor

Auditors have read-only access to the platform’s audit trail, evidence repository, and compliance reports, enabling them to verify controls and validate assessments.

## 5. Technical Architecture

### 5.1. System Architecture

* **Backend**: FastAPI with a modular, service-oriented architecture.
* **Frontend**: React + TypeScript for a responsive and modern user interface.
* **Database**: PostgreSQL for robust and reliable data storage.
* **Authentication**: JWT with optional integration with Microsoft Entra ID.

### 5.2. Database Schema

The database schema is fully normalized and includes tables for assets, risks, controls, evidence, and users. Alembic is used for database migrations.

### 5.3. API Documentation

A comprehensive REST API reference is available at http://localhost:8000/docs after deployment.

## 6. Configuration Reference

### 6.1. Environment Variables

The .env file contains over 150 variables for customizing the platform, including settings for the database, AI providers, and external integrations.

### 6.2. Framework Configuration

Aegis supports NIST CSF and CIS Controls out of the box, with options to configure and customize the risk matrix and assessment workflows.

## 7. Administration Guide

### 7.1. User Management

User roles and permissions can be managed through the admin interface, allowing for granular control over access to different platform features.

### 7.2. System Monitoring

The platform includes health check endpoints and comprehensive logging to monitor system performance and troubleshoot issues.

### 7.3. Backup and Recovery

Database backups can be created using the pg\_dump command, and a restore procedure is available for disaster recovery.

## 8. API Documentation

### 8.1. REST API Reference

The complete REST API documentation is generated using Swagger and is accessible at http://localhost:8000/docs after deployment.

### 8.2. Authentication

The API uses JWT for authentication, with an optional OAuth 2.0 integration for Microsoft Entra ID.

## 9. Security and Compliance

### 9.1. Security Hardening

A detailed security checklist is provided in the deployment guide, covering everything from changing default credentials to configuring a reverse proxy.

### 9.2. GDPR/Privacy

The platform includes features to support GDPR compliance, such as data retention policies and comprehensive audit trails.

### 9.3. SOX Compliance

Aegis helps organizations meet SOX requirements by providing a clear and auditable record of risk management activities.

## 10. Troubleshooting and Support

### 10.1. Common Issues

The deployment guide includes a troubleshooting section that covers common issues such as port conflicts and permission errors.

### 10.2. Support

For additional support, please refer to the community forums or contact the support team.