Product Requirements Document (PRD): Aegis Risk Platform

Version: 3.0 (Intelligent Platform Edition)
Date: October 26, 2023
Author: Cybersecurity Expert (AI Consultant)
Status: Final Blueprint

1. Introduction & Vision

1.1. Overview

Aegis is an intelligent Software-as-a-Service (SaaS) web application designed to streamline, automate, and centralize an organization's cybersecurity risk management lifecycle. By intelligently mapping CIS Controls to the NIST CSF, integrating with key security tools, and leveraging Large Language Models (LLMs), Aegis empowers security teams to move beyond manual processes and focus on high-impact strategic decisions.

1.2. Vision Statement

To be the most intuitive and powerful platform for operationalizing cybersecurity risk management, transforming it from a compliance chore into a proactive, threat-informed, and AI-assisted program.

2. Target Audience & User Personas

- **Persona 1: The CISO / Security Director:** Needs high-level, business-aligned risk reporting and budget justification.
- **Persona 2: The Cybersecurity Analyst / GRC Specialist:** Needs to perform detailed assessments, track remediation, and manage evidence efficiently.
- **Persona 3: The IT Manager / System Owner:** Needs clear, actionable tasks and a simple interface to provide evidence.
- **Persona 4: The Internal/External Auditor:** Needs an efficient way to review controls and audit trails.

3. Core Features & Workflow

The platform is built on a four-stage workflow: **Assess, Analyze, Mitigate, Report**, with dashboards and AI woven throughout.

3.1. Dashboards: The Personalized Command Center

The dashboard is not a single, static page but a dynamic, role-based command center designed to translate raw data into targeted insights. It is the most critical component for making the platform's data actionable.

- **The CISO Cockpit View:** A strategic command center showing high-level, aggregated metrics.
  - **Widgets:** Risk Posture Trend (line graph), NIST CSF Maturity (radar chart), Overall Risk Heatmap, and Mitigation ROI.
  - **Answers:** "How safe are we, where should we invest, and are my programs working?"
- **The Analyst Workbench View:** A tactical workload manager guiding daily activities.
  - **Widgets:** "My Open Tasks" queue, calendar of upcoming assessments, feed of recent high-risk findings from integrations, and a queue for evidence awaiting review.

    - **Answers:** "What do I need to work on right now, and what's coming next?"
- **The System Owner Inbox View:** A simple, non-cluttered to-do list for non-security staff.
    - **Widgets:** "My Assigned Remediation Tasks," "My Controls for Attestation," and clear, red-flagged "Overdue Items" alerts.
    - **Answers:** "What does the security team need from me?"

3.2. Module 1: Assessment

- **Asset Management:** Centralized inventory of all organizational assets.
- **Integrated Frameworks:** Pre-loaded NIST CSF and CIS Controls with editable mappings.
- **LLM-Powered Evidence Analysis:** When evidence (e.g., a policy PDF) is uploaded, the LLM scans the document and summarizes the specific sections relevant to the control being assessed. This drastically reduces manual reading time.
- **LLM-Powered Narrative Generation:** Based on the analyzed evidence, the platform suggests a first draft of the "Control Narrative," shifting the analyst's work from writing to reviewing and editing.

3.3. Module 2: Analysis

- **Risk Register:** A central, dynamic repository of all identified risks.
- **Risk Calculation:** Configurable matrix for calculating inherent and residual risk scores.
- **LLM-Powered Risk Statement Generation:** The LLM uses technical details (from scans), asset context, and threat intelligence (from OpenCTI) to automatically generate a formal, business-impact-oriented risk statement, ensuring consistency and clarity.

3.4. Module 3: Mitigation

- **Plan of Action & Milestones (POA&M):** Generate structured POA&Ms for accepted risks.
- **Task Management & Workflow:** Kanban-style board to track remediation tasks.
- **LLM-Powered Remediation Suggestions:** For a given risk, the LLM can propose a high-level, step-by-step remediation plan, providing an actionable starting point for the assigned system owner.

3.5. Module 4: Reporting

- **Template & Custom Reports:** One-click and custom reports for compliance, maturity, and risk.
- **LLM-Powered Executive Summary Generation:** The CISO can auto-generate a business-centric narrative for leadership. The LLM analyzes key metrics (risk scores, mitigation progress, top risks) and produces a concise summary suitable for a board-level audience.

4. Design & User Experience (UX/UI)

- **Aesthetic:** Clean, professional, modern, with available dark and light modes.
- **Color Palette:** Neutral base with a striking **gradient accent color** for primary actions and visualizations.
- **Animations:** Smooth page transitions, subtle interactive animations, and animated data visualizations to create a fluid and engaging experience.

5. Technical Requirements

- **Authentication:** Exclusively via **OAuth 2.0 / OIDC**, with first-class support for **Microsoft Entra ID**.
- **Backend:** Python (Django/FastAPI) or Node.js (NestJS) with a PostgreSQL database.
- **Frontend: React (with Next.js)** for the core dynamic application and **Astro** for fast, content-heavy static sites (marketing, blog, documentation).
- **Integrations:** API-first architecture with native connectors for:
  - **Vulnerability Management (OpenVAS):** To automate evidence collection for CIS Control 7 and flag technical risks.
  - **Cyber Threat Intelligence (OpenCTI):** To enrich risk analysis and inform likelihood scoring with real-world threat data.
- **LLM Integration:** Secure API calls to a foundational model provider (e.g., Azure OpenAI Service, Google AI Platform) with carefully engineered prompts to perform the specific automation tasks outlined in Section 3.

6. Lifecycle Management & Auditability

- **Implementation Tracking:** Detailed tasks with assignees, due dates, statuses, and a complete history of comments and attached artifacts.
- **Review & Approval Workflow:** A formal review gate (`Awaiting Review`) with an approval/rejection mechanism and mandatory feedback, all logged in an immutable audit trail.
- **Integrated Documentation:** The platform acts as a central evidence hub, linking policies and procedures directly to the controls they satisfy.
- **Process Oversight Reporting:** Reports on the health of the risk program itself, including overdue tasks, review bottlenecks, and controls with missing evidence.

7. Success Metrics

- **Adoption:** Monthly Active Users (MAU), number of assessments created.
- **Efficiency:** Reduction in time to complete a full assessment cycle (measured before and after LLM feature adoption).
- **Engagement:** Percentage of high-risk items with an active mitigation plan.
- **Value & User Satisfaction:** Number of executive reports generated; Net Promoter Score (NPS) with specific questions on the usefulness of dashboards and AI features.