**Project Name : Aurora**

**Overview & Vision**  
Project Aurora is an AI-assisted reliability and work-management capability that sits within BHP’s AWS environment in ap-southeast-2 (Sydney). It ingests equipment telemetry, maintenance histories, and incident notes to generate concise digests and proposed next actions for planners and supervisors. The goal is practical: fewer hours scrolling through ticket histories, faster handovers, and higher-quality work orders that reduce unplanned downtime. We use Amazon Bedrock (Claude Sonnet) purely as an advisory layer—recommendations and summaries are presented with source snippets and must be accepted or edited by a human before any action is taken. This is a new digital capability delivered as an application running in our VPC, integrated to CMMS and ITSM platforms via the BHP Integration Platform. The project deliberately avoids autonomous control and any automated decision-making with legal, HR, or safety effect; it’s a copilot for judgment, not a replacement for it.

**Architecture, Product Experience & Operations**  
The service is deployed across separate DEV, UAT, and PROD accounts using ECS Fargate for the application tier, RDS PostgreSQL for operational state, and S3 for curated data; Bedrock endpoints are consumed from the same region with VPC connectivity where supported. EventBridge and step functions handle ingestion and batch transforms, while CloudWatch and Datadog provide observability across logs, traces, and service-level indicators. From a user’s perspective, Aurora appears as a simple web application with SSO via the corporate IdP, presenting an “inbox” of incidents and assets that need attention, a context panel with notable history, and an AI-generated recommendation panel that explains its suggestion and links to the underlying text. The design emphasizes clarity over novelty: large readable typography, keyboard shortcuts for planners, and explicit controls to accept, edit, or discard AI text. Accessibility is a requirement rather than an afterthought, so we target WCAG 2.1 AA, test with screen readers, and support high-contrast views for control rooms. We aim for a 99.5% availability target with multi-AZ database deployments, automatic failover, and a 15-minute RPO; we practice DR table-top exercises twice per year and run monthly chaos tests on non-prod to validate alarms and runbooks. Performance-wise, the product targets sub-3-second median page loads on corporate networks and AI responses within 6–10 seconds, with graceful fallbacks and cached summaries for repeated queries.

**Data, Privacy & Security Posture**  
Most data is equipment-centric, but routine work logs can contain limited personal information (employee name, email, ID, and role). We collect only what is necessary to identify responsible teams and coordinate work; special-category or sensitive personal data is out of scope, and the solution does not monitor individuals or conduct behavioral surveillance. All storage and processing occur in ap-southeast-2: RDS and S3 are encrypted with customer-managed KMS keys; transport uses TLS 1.2+; and non-production data is masked or fully synthetic. Access follows a least-privilege model with role-based permissions, quarterly access reviews, and automatic revocation on role change or departure. Audit events are centralized (CloudTrail plus application audit logs) with retention aligned to records schedules. We publish clear in-product notices describing what the AI does, why it’s helpful, and its limits; the Global Privacy Notice is updated accordingly. We have initiated the Technology Security Assessment, and a pre-production penetration test is scheduled before go-live. For AI specifically, prompts exclude personal attributes, outputs are anchored to visible sources, and every inference captures model, prompt version, and request metadata to aid explainability and post-incident analysis. Vendor contracts explicitly prohibit model training on BHP data and limit access rights strictly to service provision.

**Vendors, Procurement, IP & Governance**  
Delivery support is provided by SouthCross Analytics Pty Ltd under the “Aurora Implementation & Support (BIS-2025)” agreement from 01-Nov-2025 to 31-Oct-2027, with work performed in BHP’s cloud environment and no vendor-hosted production datasets. Access for vendor personnel is time-boxed, audited, and restricted to bastion workflows; non-production uses masked or synthetic data. The engagement sits under Software & Professional Services with a named Supply Specialist and standard BHP terms; a Data Security & Privacy Addendum (DSPA) forms part of the contract. IP developed under this project—prompt templates, integration components, and configuration—vests in BHP, with SBOM generation and open-source governance embedded in CI to prevent Red/Deny components and ensure license compliance. We have engaged Legal for a freedom-to-operate screen, and the team follows a documented Information Protocol for handling confidential materials, reviewed annually and applied to both employees and contractors. Routine governance includes quarterly access recertification, change control through CAB, KPI reviews on summary accuracy and time saved, and a weekly quality session where low-confidence or escalated AI outputs are examined and used to refine prompts.

**Change Management, Success Criteria & Roadmap (non-risk)**  
Adoption matters as much as architecture. We will run short scenario-based training (“plan a shutdown,” “triage a vibration alarm,” “handover in three minutes”) and deploy product champions in each operational area. The early rollout focuses on two pilot sites to validate the value hypothesis: reduce time spent reading incident histories by 30%, increase first-time-right work orders by 15%, and shorten shift handovers by five minutes on average. Feedback is captured directly in the UI, triaged weekly, and turned into backlog items; we’ll maintain a public change log and a lightweight prompt-change governance so planners always know why a recommendation might look different. Sustainability and cost transparency are built in: nightly reports track Bedrock token consumption per team, and the application publishes carbon-aware telemetry (compute and storage estimates) to keep efficiency visible. The forward roadmap explores expansion to recommendations for planned maintenance windows, multi-language UI for global teams, and a guarded “pattern library” for reusable prompts while keeping human approval at the center. None of these roadmap items introduce automated, binding decisions; they focus on speed, clarity, and shared context.

**Implicit Answers Embedded in the Narrative**  
The solution introduces a new technology product and digital process using AI, integrates with third-party systems through the corporate integration layer, and involves a named delivery partner operating under BHP contracts and controls. It processes limited personal information (contact and role data) but excludes sensitive categories and cross-border transfers; all storage and compute remain in Sydney. The vendor does not retain BHP data outside our environment and is contractually barred from using it for training. Security controls cover identity, encryption, network segregation, logging, testing, and non-production masking; privacy controls address transparency, minimization, retention, and access governance. The AI is advisory only with human-in-the-loop review, explainability via source linking, and monitoring for drift and misuse. Availability targets, DR practices, and operational runbooks support reliability without labeling the application as safety-critical. IP is owned by BHP, open-source usage is controlled, and procurement follows standard terms with a DSPA. Together, these choices close out most first- and second-line concerns while keeping the document oriented around how people will actually use the product.