

Building a Governance-First Enterprise CMDB for a Large Energy Utility Organization

The Customer's Challenge

A large energy organization needed to build an enterprise CMDB capable of supporting thousands of infrastructure assets, services, and relationships under strict governance and security requirements. Configuration data was scattered across numerous tools, including SCCM, Intune, VMware, Red Hat Satellite, SolarWinds, and Nokia platforms. This limited visibility into how infrastructure supported business services. Ownership and governance were inconsistent, and highly sensitive Tier-0 resources couldn't be discovered directly due to security policies. Without consistent standards, lifecycle controls, and authoritative data sources, a sustainable CMDB would have been difficult to achieve.

Windward Solution

Building on a pre-engagement assessment of the organization's ServiceNow CMDB program, Windward developed a future-state design and a four-phase roadmap to CMDB maturity that guided the engagement. The team took a governance-first approach, establishing standards, lifecycle controls, and ownership models before large-scale population began. Discovery requirements were defined across all major infrastructure domains, with Service Graph Connectors prioritized for authoritative data intake. For sensitive Tier-0 assets, Windward created a controlled process using approved integration or manual governance workflows, so these resources could be represented in the CMDB without compromising security.

Results Achieved



Trusted CI Baseline: Roughly 60,000 CIs populated across principal classes from six live integrations.



Faster Troubleshooting: Linux server details available directly in ServiceNow, saving an estimated 10+ minutes per incident.



Reduced Handle Time: Help desk agents instantly identify a caller's device without asking for serial numbers.



Fewer Unnecessary Escalations: Scheduled patching windows are visible, so planned downtime isn't mistaken for an outage.



End-to-End Service Visibility: Service mapping reveals dependencies and related incidents, reducing reliance on tribal knowledge.



Sustained Data Quality: Automated retirement policies, health dashboards, and audit logs keep records accurate and current.



Secure Tier-0 Handling: Sensitive data protected behind approval-based access controls rather than excluded entirely.



Scalable Foundation: Documented standards and governance provide a repeatable blueprint for onboarding future data sources.