Asset Management & CMDB Design

Cybersecurity Governance Case Study

Scenario

Oscorp engaged KPMG to perform a cybersecurity internal audit as part of a newly established three-year internal audit program. During KPMG's first cybersecurity audit, a major finding identified weaknesses in Oscorp's asset management practices. Specifically, Oscorp lacks a centralized, accurate, and up-to-date configuration management database (CMDB) and currently relies on a single spreadsheet with ad-hoc asset information.

Problem Statement

Without a reliable asset inventory, Oscorp has limited visibility into the systems supporting its business operations. This gap increases cybersecurity risk, limits the effectiveness of security controls, and makes it difficult to perform vulnerability management, incident response, and audit activities. Oscorp requested guidance on how to design a structured process to capture assets and maintain an accurate CMDB.

Objective

Design a scalable and auditable asset management process that improves visibility into IT assets, supports cybersecurity controls, and aligns with governance and risk management expectations.

Recommended Asset Management Process

Asset Identification and Ownership

Oscorp should begin by identifying all asset types across the organization, including hardware, software, cloud resources, and data assets. Each asset should be assigned a clear business

and technical owner responsible for its accuracy and maintenance. Ownership accountability ensures assets are reviewed, updated, and retired appropriately throughout their lifecycle.

Asset Classification and Criticality

Once identified, assets should be classified based on their business function, data sensitivity, and criticality to operations. Understanding asset criticality allows Oscorp to prioritize security controls and focus protection efforts on systems that pose the greatest risk if compromised.

Centralized CMDB Implementation

Oscorp should replace the existing spreadsheet with a centralized CMDB solution that supports standardized asset attributes. At a minimum, each asset record should include ownership, asset type, location, business function, classification, lifecycle status, and last review date. Standardization improves consistency and ensures the CMDB can be reliably used for audits and security assessments.

Ongoing Maintenance and Governance

To keep the CMDB accurate, asset updates should be embedded into existing IT processes such as change management, system provisioning, and decommissioning. Periodic asset reviews should be conducted to validate accuracy and completeness. Clear governance procedures should define who is responsible for maintaining the CMDB and how often reviews occur.

Security and Risk Alignment

A well-maintained CMDB enables Oscorp to strengthen its cybersecurity posture by supporting vulnerability management, incident response, and risk assessments. Accurate asset data allows security teams to quickly identify affected systems during incidents and prioritize remediation efforts based on business impact.

Conclusion

By implementing a formal asset management process supported by a centralized CMDB, Oscorp can improve asset visibility, reduce cybersecurity risk, and address the audit findings identified by KPMG. This approach strengthens governance, supports security operations, and positions the organization for more effective future audits.