Week 4: Design an IT Policy Control Framework

Nate Bachmeier

TIM-8190: Computer Science Policy and Strategy

September 5, 2021

Northcentral University

# Design an IT Policy Control Framework

NCU-F is a large-sized enterprise within the Banking-as-a-Service (BaaS) industry. The business predominately grows through acquisitions, and this has caused the company to have inconsistent standards between business units. This situation creates challenges for teams to collaborate and share solutions. The business has established a central task force to define Information Technology and Communication (IT&C) policies and build the missing cohesion.

Next, the organization must adopt a policy control framework. Leaders approach this situation by combining existing frameworks, such as COBIT, ITIL, COSO, CMMI, and FAIR (Lindros, 2017). These industry-standard frameworks assist project teams in implementing their artifacts using a secure, reliable, and maintainable process. However, using only engineering-centric frameworks is potentially too narrow. Many projects span different teams, role families, and organizations (e.g., vendors, consultants, and partners). NCU-F must address these issues and limitations by formally declaring its project artifacts like charters, mandates, and roadmaps (Bonnal & Rauser, 2017). When documents explicitly declare universal agreements across the direction and appropriate guardrails, it unifies team communication. Business professionals can then efficiently map the guiding decisions to their role and team-specific operating models.

# Naming Standards

## Business Problem

Enterprise organizations like NCU-F can easily own hundreds of thousands to millions of resources. Historically, individual business units set naming schemas and deferred enforcement to their operations teams. This strategy enables more autonomy and flexibility in exchange for less organizational consistency. However, it is challenging to discover, monitor, and react to operational issues without naming conventions and standards. For example, central alert rules must explicitly support the various permutations, manifesting complexity throughout the systems management lifecycle.

## Rejected Solutions

Nevertheless, renaming every object is prohibitively expensive. The business could embark upon prolonged migration that seeks to reach a point of eventual consistency. During the transition phase, department leaders prioritize shared resources over internal implementation details. For instance, the edge router into the Credit team’s app must be discoverable by all NCU-F personal. In contrast, a smaller cohort must interact with traffic policies within the Credit team’s private subnets. Since the team size directly impacts its ability to support a custom vocabulary, this dimension forms a natural sorting order.

## Accepted Solution

However, the time to reach organizational consistency can become too costly as well. The operational and engineering teams will surely encounter feature regression risk, and the customer will not see any direct value. Furthermore, the hybrid state will disrupt the existing team vocabularies and cause unnecessary pain. NCU-F wants to avoid these scenarios and is willing to accept the technical debt. This decision pushes the organization toward standardizing the metadata associated with the various resources (Harper, 2019). That metadata can reside within Enterprise Resource Management Systems (ERMS), which meets the discovery and monitoring requirements. Additionally, third-party tools exist for bulk importing resources and enabling version control capabilities.

## Resource Hierarchy

NCU-F requires business units to record their resources within the central ERMS database. The database utilizes a hierarchical structure with strict rules where resource definitions can reside (Table 1). For instance, all routers exist under the namespace /devices/routers, and all workstations follow the format /domain policies/workstations.

Table 1: Resource Hierarchy

|  |  |  |
| --- | --- | --- |
| **Category** | **Subcategory** | **Subcategory** |
| Telecommunication | Devices | Phones VOIP |
| Policies |  |
| Control |  |
| Network Device | Devices | Switches |
| Routers |
| Policies | QoS |
| Security |
| Domain Policies | Servers | Baseline |
| Web |
| Application |
| Database |
| Workstation | Windows |
| Mac |
| Certificates | PKI |
| Metadata Management | Core | EMRS |
| NCU-F | Importers |
| ComplianceCheckers |
| Data Management | Identity | Service Principals |
| Account Principals |
| Foreign Principals |
| Encryption | Minimum |
| Business Unit Name |
| Retention | Minimum |
| Business Unit Name |
| Design Requirements | Engineering | Coding Standards |
| Incident Response | Procedures |
| Reporting Templates |
| Program Management | Document Templates |
| Release Management | Procedures |
| Reporting Templates |
| Quality Assurance | Test Procedures |

## Mandatory Tags

After declaring the resource, operations staff must add several resource-type specific mandatory tags (Table 2). Optionally, the team can include arbitrary additional tags to align with legacy asset management processes. Data validation processes periodically assess the metadata and report inaccurate or incomplete information. It is the responsibility of the owning team to remediate the issue promptly.

Table 2: Required Resource Metadata

|  |  |
| --- | --- |
| Tag Name | Description |
| ncu:name | The friendly resource name |
| ncu:department | The business unit that owns the resource |
| ncu:cost-center | The business that is responsible for expenses |
| ncu:app | The resource’s primary application |
| ncu:location:geo | The geographic region where this resource resides |
| ncu:location:building | The building where this resource resides |

# Categorization Process

When