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 |

# IT Policy Categorization Process

The business must support categorizing future policies in a flexible yet maintainable manner. NCU-F implements a straightforward categorization process, specifically to discourage over-engineering. Its workflow consists of four steps mainly, selecting the domain, scenario, resource type, and criticality (Figure 1).

Figure 1: Categorization Process

After identifying the appropriate tuple, the policy author(s) must work with the Technical Community that owns the relevant domain and scenario. Since community members are the defacto subject matter experts, they are most qualified to choose controls. Those controls must encompass quality planning, activity organization & coordination, training, validation, and continuous improvement (Botezatu, Pirnau, & Carp Ciocardia, 2019). While the owners have general autonomy, they must adhere to the corporate IT charters and mandates. The corporate guardrails include standards for many cross-cutting concerns, such as security and compliance.

# Business Drivers and Performance Monitoring

## Executive Summary

NCU-F cannot deliver the best customer experience with the richest feature set because its internal processes are inefficient. These inefficiencies stem from internal roadblocks that prevent collaboration and cross-team communication. For instance, the business maintains multiple Customer Relationship Management (CRM) systems that cannot integrate. Consistently these conflicts are a byproduct of inconsistent team standards and procedures. Instead, the task force wants to maintain policy controls across a resource-specific hierarchy. Additionally, the task force owns documenting the corporate direction and guardrails. Technical Communities are responsible for maintaining elements of the hierarchy and enforcing quality controls.

After implementing this model, the senior leadership can set the vision and monitor the progress. Meanwhile, delegating responsibility to area experts ensures an appropriate level of flexibility and adequate controls exist. When conflicting or competing requirements arise, the community can swarm on the issue and be empowered to decide. This structure will remove roadblocks and promote cross-organizational collaboration.

## Performance Measurements

Program managers are responsible for reporting progress regarding their team’s ability to collaborate effectively. For instance, how often did the Credit team assist the Savings team? NCU-F recommends that each team automate collecting quantitative metrics either daily or weekly. These statistics generally originate from Issue Tracking and Management (ITM) systems (e.g., Jira or ServiceNow). Additionally, team leaders publish monthly qualitative information encompassing high-lights, low-lights, blockers, and upcoming initiatives. The data and stories should collectively tell an accurate accounting of status and business challenges. If the performance data suggests that two teams are not communicating, or worse, on conflicting paths, the senior leadership can intervene.

Measuring collaboration rates is essential, as it confirms the health of input variables, though customers only care about output results (Bryar & Carr, 2021). Program managers must also report on updates to project scope, schedule, budget, performance, issues, risks, and general notifications (Martinelli & Dragan, 2016). When a correlation between inputs and outputs does not occur, it signals issues with the control framework. This situation presents an opportunity for senior leadership to dive deep and examine any process issues.

## Reporting System

NCU-F chose to buy-versus-build their reporting system because creating such as service is outside its core competencies (e.g., financial products). Team members periodically submit updates to the ERMS, Issue Tracking, and Status Reporting databases (see Figure 2). Next, an Extract-Transform-Load (ETL) process queries these discrete systems and performs minor data aggregations. Then the results flow into a relational database that holds Key Performance Indicator (KPI) metrics. Lastly, Tableau, a dashboarding solution, reads those metrics and displays the information in charts and graphs.

Effective dashboards should tell a story succinctly, and avoid overwhelming the viewers with too much information (Tufte, 1983). Maintaining this balance requires working with the stakeholders to understand their needs. This behavior should create empathy and deeper collaborations which further promote engagement (Cahyadi & Prananto, 2015). Dashboard authors must also remain cognizant that different audiences will value specific content. For instance, the security and localization teams have distinct requirements. Mixing those needs on the same canvas will only lead to confusion.

Figure 2: Reporting System

Diagram

Description automatically generated