Week 7: Design an IT Policy Implementation Plan

Nate Bachmeier

TIM-8190: Computer Science Policy and Strategy

October 17, 2021

Northcentral University

# Design an IT Policy Implementation Plan

## Executive Summary

NCU-F specializes in Banking-as-a-Service and payment processing services across North America, Europe, and Asia. The organization has ten thousand employees that serve over a million customers. Those customers rely on the business for several integral capabilities, such as facilitating online purchases and enabling friends to send one another money. NCU-F also offers mortgage services, investment specializations, checking and savings accounts, and personal loans. Over the last decade, the organization has seen aggressive expansion through acquisitions. While this strategy enables the business to reach new markets and deliver customer value quickly, it also led to a fragmented technology platform. For instance, customers must maintain multiple distinct profiles and cannot easily navigate between the various products. Additionally, NCU-F is inefficiently utilizing its resources as many business units are recreating similar solutions to the same problems. The senior leadership team wants to improve upon these issues through IT Governance.

# Strategic Goals and Alignment

The organization cannot provide the best-in-class user experience until it changes its IT Governance model. Only through a strategic alignment between the information systems and business goals can NCU-F present a unified product suite for its customers (Iyamu, 2015).

NCU-F’s governance model requires mechanisms and processes to enforce consistency, standardization, and choose the best-in-company implementations. These controls must foster intellectual (e.g., planning and infrastructure) and social (e.g., shared understanding) alignment across the organization (Ping-Ju, Straub, & Liang, 2015). When team members understand the desired end-state, they can more efficiently plan and prioritize work. It also removes design choices that would not align with business goals.

## Establishing an IT Steering Committee

The senior leadership team must create an IT steering committee that collectively agrees on the organizational patterns and practices. This group requires executive sponsorship to ensure decisions carry weight. When the committee identifies high-value work, such as centralizing customer identity, there must be processes to appoint a Single-Thread Leader (STL) (Bryar & Carr, 2021). An STL is a project owner who manages the goal’s lifecycle, governance, and stakeholder communication. This owner should not work on multiple goals in parallel, as it introduces project risk.

While the IT steering committee(s) establish patterns and practices, it would be unrealistic to assume complete uniformity. For example, the savings and checking business unit runs on Windows and .NET versus the personal loan features are written in Perl. Requiring that one group rewrites their implementation would be both challenging and a poor return on investment. Instead, the committee must focus on interoperability and code portability through industry standard patterns. For instance, each product should have an Application Programming Interface (API) that supports RESTful methods (Representational State Transfer protocol).

## Auditing IT Investments

Another expectation of the IT steering committee is to audit investments into IT resources (Ali, Green, & Robb, 2015). Many businesses like NCU-F purchase technology widgets to address challenges and introduce new capabilities. However, these widgets can fall to the wayside as new paradigms appear. For instance, most enterprise data centers have an Apache Hadoop cluster because the platform provides high-available and elasticity. Managing these environments is challenging, which gave rise to Kubernetes. Eventually, something cloud-native will supersede Kubernetes. Each application migration comes with costs and reliability risks. Businesses must be cognizant of these trade-offs and understand the reasons not to embrace new technologies blindly.

## Impact of Developing Policies, Standards, and Procedures

The business must strategically decide which governance policies to enforce versus recommend. When the organization mandates a shift in direction, it creates additional work and deprioritizes competing efforts. One approach is defining maturity levels and target groups, then slowly raising expectations on specific critical resources first. For instance, a recent outgate with the Identity Services highlights its criticality, making it a candidate for targeted investments. These changes could include policies that reduce Domain controller utilization through data caching requirements.

NCU-F must also devise plans for removing technical debt and implementing standards across the platform. That standardization enables the company to move faster with greater consistency. However, the business must be cognizant of the current business cycle since paying down debt also implies fewer new features. Without an adequate volume of improvements, the customer’s experience becomes stale and fails to meet expectations.

Furthermore, formalizing organizational procedures such as disaster recovery and incident management will pay dividends later. For instance, the initial release of the trading platform stores customer data across eight different storage technologies. This approach decouples the implementation between microsystems and promotes engineering efficiency. However, end-users do not care. Instead, they want a consistent system state that withstands an individual server or partition failure.

# Milestones, Benchmarks, and Deliverables

The task force is responsible for establishing the Technical Communities, overseeing initial staffing, and reviewing abstract community decisions (see Table 1). Each community consists of subject matter experts that own a cross-cutting concern (e.g., networking or security).

Table 1: Projected Timeline

|  |  |  |
| --- | --- | --- |
| Milestone | Duration | Core Deliverable / Objective |
| Identify the technical Communities | 30 days | Provide a list of cross-cutting concerns areas, owning program manager, and executive sponsor |
| Staff the Communities | 90 days | Each community will document specific eligibility requirements. Existing IT staff will join relevant communities |
| Assess Community State (Forming) | 90 days | Each community will inventory the state of their areas and prioritize standards |
| Implement Changes (Storming) | 365 days | Each community will review the backlog and execute the highest priority tasks |
| Enter Maintenance Mode (Norming) | \* | Each community will complete periodic area assessments and submit recommendations to the task force |

The task force’s charter defines procedures, mechanisms, and frameworks across the IT policies lifecycle. This lifecycle includes specific events such as creating, storing, approving, modifying, and retiring policies. Additionally, the group seeks to centralize relevant artifacts in a discoverable repository. Those artifacts must encompass Standard Operating Procedures and controls throughout demand, execution, and performance management (Selig, 2016). Upon project completion, employees can promptly identify any relevant governance models.

Second, the task force also seeks to balance consistency with business unit agility. When organizations put technology before the products and services, it prevents resources from delivering on the corporate mission and delighting customers (Ali, Green, & Robb, 2015). Therefore, new policies must enable the organization to make more strategic and efficient investments.

Third, there are infinite business challenges, and the task force cannot predict every future scenario. Senior leaders have the authority to grant exceptions and propose policy modifications as necessary. Documentation must exist for those decisions so the task force can periodically assess broader course corrections.

These requirements and constraints will cause different communities to modernize at varying rates. For example, the business currently maintains over a dozen web frameworks utilizing multiple conflicting patterns. Resolving these challenges will take additional *storming* time before the group transitioning into the *norming* phase. The organization can accelerate these timelines by increasing investments or permitting lower policy maturity levels.

# Control Framework

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

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 2). For instance, all routers exist under the namespace /devices/routers, and all workstations follow the format /domain policies/workstations.

Table 2: 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 3). 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 3: 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 |

# Stakeholder Responsibility

NCU-F’s senior leadership team owns forming the task force to define Information Technology (IT) policies that enable the Business Units to collaborate more efficiently. This team has stakeholders from the major divisions, executive sponsors, and legal representatives.

## Policy Approval Process

The task force delegates many day-to-day decisions to internal Technical Communities. Each community owns a specific cross-cutting concern (e.g., disaster recovery) and self-manages any enrollment criteria that govern membership eligibility. Community members are responsible for reviewing new policy requests, debating ambiguity with existing policies, and proposing technical guidance. Employees can define new technical communities by submitting requests to the task force oversight committee.

Employees that want to create a new policy must identify an appropriate community to vet their document. The community will assign one or two reviewers to iterate the proposal until it adheres to internal standards during this process. After the reviewers approve the document, the authors can request that their policy is globally visible within Policy Central. Typically, the community leaders promote the new concept through appropriate media (e.g., email group). Suppose the reviewers do not support the change. In that case, the authors can optionally escalate to the community’s program manager or executive stakeholder.

## Policy Revision Process

Within Policy Central, all documents contain version metadata. Employees can submit minor updates as an addendum, declaring any applicability criteria and discussions leading to the change. Major revisions must declare a new policy document and repeat the adoption process. This new policy document can initialize as a “copy, paste, edit” of the previous version. Either approach requires approval through the owning Technical Community.

## Policy Deprecation Process

Many policies become deprecated due to external changes in the business strategy. When these situations occur, the Technical Community must submit a migration plan to their executive sponsor. This plan must include procedures to identify the migration’s scope, mechanisms for communicating status, and any potential risks from migrating. Lastly, there must be a section that details any reasons *not* to deprecate and migrate. After agreeing on the new direction, the Policy Central document’s status becomes either deprecated or superseded.

# Communication or Training Plan

NCU-F is a large-scale enterprise with ten thousand employees working across several global financial services. The business requires policies and procedures that enable its staff and customers to raise support issues and discover standard solutions. Information Technology can serve those experiences using self-service portals into knowledge databases. When answers are not available, those same systems can escalate requests to product support networks.

# Tiered Support Networks

Tiered-Support Network provides the structural model to scale-out support across broad enterprise environments and even multi-organizational situations.

Figure 1: Tiered-Support Network

Diagram

Description automatically generated

## Support Model

Without sufficient scalability, the support network becomes prohibitively expensive. One approach to meeting this requirement is through a two pyramid structure (Figure 1). The top inverted pyramid represents members of the product engineering role-family, versus the bottom, consists of the support role-family. Under this model, support tickets flow up and solutions down. The business receives a strong economic incentive to address issues at the bottom of the structure, as the higher levels require specialized resources. Since the customer must first traverse through multiple generalists, each layer has a compounding cost effect.

## Support Pyramid

For example, a customer wants to integrate their business process with one of NCU-F’s web services. When customers can quickly discover that information from a blog or wiki, the business must only pay content hosting fees. Otherwise, the request escalates to support staff which must first route the ticket to the least costly junior technicians. After the junior fails to address the issue, they can escalate it to a more experienced peer for review. If the support team requires further assistance, there must be communication channels for escalating to program management. After discovering the solution, the business has an incentive to document the procedure within the knowledge base to minimize future investigational costs.

Specific divisions within NCU-F, like the central DevOps engineering team, have dozens of area owners, creating routing challenges. This situation might necessitate multiple PM-to-PM switching. NCU-F should proactively configure Incident Management software like PagerDuty, or a similar Software-as-a-Service (SaaS) solution. These systems accelerate the search for on-call staff and improve the customer experience through lower time to mitigate.

## Engineering Pyramid

The support PM must then contact the area owner PM on the relevant engineering team. For instance, this specific customer wants to ingest market data from the Trading Platform. In this case, the Trading PM will ask the Engineering Manager for a solution. Unless the manager can resolve the matter, it must escalate to a service engineer. The engineers must halt inflight work and context switch, introducing risks to existing timelines and commitments.

## External Support

Suppose the engineering team cannot mitigate the issue. In that case, the process begins anew with the external vendor or partner. Those third-party providers have similar economic constraints, which forces them into these stacked pyramid structures. This consistency includes knowledge databases, support channels, and customer access to the service team. However, there can be specific scenarios that are not resolvable. In these situations, both the engineering and support program managers need to agree on an appropriate response. Responses can include adding to the backlog, proposing workarounds, among other stopgaps. Lastly, reporting must inform the executive leadership of any business impact to approve future investments into the problem.

# Leadership Involvement