Week 3: Milestones, Benchmarks, and Deliverables Roadmap

Nate Bachmeier

TIM-8190: Computer Science Policy and Strategy

September 19, 2021

Northcentral University

# Milestones, Benchmarks, and Deliverables

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. Its senior leadership team is forming a 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.

## Goals, Scope, and Tenants

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.

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.

Lastly, 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.

# Policy Lifecycle

NCU-F defines specific norms and expectations for introducing, revising, and removing IT policies (see Figure 1). All employees are encouraged to participate in these processes and provide relevant feedback for stakeholders.

Figure 1: Lifecycle Management Process

Diagram

Description automatically generated

## Policy Creation Process

1. IT policies define processes for approaching business challenges (Gartner, 2021). The business enforces that perspective by requiring each policy document to explicitly identify the customer (e.g., internal or external users) and their needs.
2. Next, the authors must explain in two to three paragraphs what methodology lead to these requirements. Ideally, the methodology will include direct customer stories and metrics.
3. The third section enumerates existing policies and their relationship. Those relationships can include standard vocabulary definitions, supersedence, and standard procedures.
4. Fourth, declare the foundational tenants of this new policy (Bryar & Carr, 2021). Each tenant can be a single sentence within a bulleted list. During future debates around the policy’s expectations, the discussion leaders will defer to this list for guidance.
5. Fifth, explain how the mechanisms and frameworks address the business challenges. Additionally, define success criteria and measurements. This section is typically one to three pages in length, never more than five.
6. Lastly, include a Frequently Asked Questions (FAQ) section that addresses common scenarios.

## Policy Storage Process

Next, employees upload the document into NCU-F’s Policy Central Website, a proprietary document management solution built on a NoSQL graph database. The document graph represents the relationships between the documents, similar to many university citation systems. Policy documents initialize to a draft state that is only visible to their working team. This design prevents external teams from accidentally referencing incomplete or unauthorized plans.

## 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, which declares 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 define migration