Week 1: Develop a Knowledge Transfer Program

Nate Bachmeier

TIM-8190: Computer Science Policy and Strategy

October 10, 2021

Northcentral University

# Develop a Knowledge Transfer Program

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.

# Preparing Contingency Plans

NCU-F leverages organizational structure to route support tickets to the correct business contacts, though this model still contains threats. The business must also consider procedures for revising the plan, incident responses, and emergency communication.

## Identify Threats

The two-pyramid system enables cross-organizational communication and the routing of support issues. However, it also has specific implementation challenges due to internal drivers, external circumstances, and goal validity changes (Morgan & Dale, 2013)(Table 1). NCU-F must mitigate these situations through IT Investment Governance (Ali, Green, & Robb, 2015). Within the investment governance policies, a balance between reducing technical debt and adding more customer value. Additionally, the business must make investments into employees’ careers and the central knowledge repositories quality.

Table 1: Example Threats

|  |  |
| --- | --- |
| Change Type | Example |
| External Circumstance | Staff members leave the company |
| Internal Circumstance | Knowledge database integrity declines |
| Goal No Longer Valid | Improving feature performance after its deprecation (wasteful investment) |
| Business Case No Longer Valid | Continuing to innovate on dying platforms (Windows Mobile) |

For instance, many IT professionals change their roles and responsibilities every two to five years (High & Passerini, 2014). This high-churn rate can leave knowledge gaps within the pyramid because the experts no longer work at NCU-F. Recovering that information requires tasking non-experts to learn reverse-engineer those systems and make educated guesses. Without the full context, the engineer could regress the application behavior or give incorrect answers. External partners and vendors sell support licenses for proprietary applications. However, this approach is expensive because the custom work is challenging to scale versus standard COTS (Commercial Off The Shelf) support. Furthermore, the security and compliance teams require strict background checks before external staff can begin, introducing more delays.

Suppose the knowledge database’s integrity declines and sections are no longer trusted. These situations originate through stale documentation and poor versioning systems. What should Alice do after finding two conflicting documents in Confluence? How can she reconcile the actual state? Worse, an implementation team invests weeks into planning a cross-product integration, only to uncovers that the procedure is wrong. After enough occurrences, customers lose trust in the database, leading to premature escalations and competing solutions.

## Revising the Plan

Plans are in-valuable, though almost always wrong. Without a plan, the organization cannot uniformly move, leading to inefficient corralling between business units. These events can originate from a 2x2 matrix of knowns and unknown elements (Morgan & Dale, 2013). There are virtually unlimited unknown factors that will influence a project plan (e.g., COVID). It would be impractical to include every risk, so project sponsors must focus on known aspects and implement agile planning (Corral, Sillitti, & Succi, 2013). This design methodology asks participants to identify the continuously assess the business value of a given task.

When prioritization changes occur, the business must leverage existing communication channels between the various divisions. For example, suppose a knowledge database becomes untrusted. In that case, there needs to be a conversation about the cost-to-restore, the database’s perceived future value, and alternative solutions. This approach steers NCU-F toward making appropriate investments that improve its customers’ and employees’ experience.

## Incident Severity Considerations

The appropriate response to an incident directly correlates with the severity of the issue (Table 1). Consider the difference between an offline production system and general inquiry. During a service outage, merchants cannot complete their customer’s transactions which can have a long-term brand impact on NCU-F. The organization must drop everything and restore continuity promptly. Meanwhile, senior leaders must prepare communications with their more prominent customers and social media outlets. In contrast, the Severity-5 issue has a constrained blast radius, which an area leader can resolve at worse.

Table 2: Incident Severity Definitions

|  |  |  |
| --- | --- | --- |
| Level | Description | Response Service Level Objective (SLO) |
| 1 | Production system severely impaired | Real-time (<5 mins) |
| 2 | Production system degraded | Within 15 to 30 minutes |
| 3 | Non-Production workload impaired | Within 60 to 120 minutes |
| 4 | Upcoming initiative assistance | Within 1 to 2 business days |
| 5 | New requests and general inquires | Within 3 to 5 business days |

Specific incidents are beyond the control of corporate governance. During the 2020 Pandemic Lockdown, businesses worldwide closed their doors overnight, catching even the most prepared organizations off-guard (Hou, 2020). If the Lockdown occurred before the ubiquitous access to public clouds and Software-as-a-Service (SaaS), the work environment would be very challenging. Instead, executive leadership could ensure continuity through IT investments in VPN (Virtual Private Networking) services and remote collaboration tooling. Though, products can only solve part of the problem.

Additionally, managers could no longer walk down the hall and knock on doors. They had to adapt to directing products with more trust and less visibility into individuals’ behavior. With KPI (Key Performance Indicator) tracking across the direct reports, leaders can partially mitigate these risks. Afterward, the manager can assess the degree of performance degregation and form an appropriate response.

## Incident Handling and Response Policy

All software systems and human processes are bound to eventually fail. When these events occur, there needs to be a response policy that carries the initial detection through resolution and into an improvement phase (Figure 2). It is critical to avoid blaming individuals or teams during this phase and instead focus on the criteria that trigger the failure. Ideally, the discovery comes from service telemetry or automated test cases versus a customer complaint. Whatever the origin, the incident response team must promptly confirm the issue and mitigate the service impairment. This action could include sophisticated patching thru imperfect machine reboot strategies. Then the area owners must uncover the issue’s root cause using a Correction of Errors (CoE) or alternative postmortem procedure. Lastly, the owners must create new controls that prevent the situation from reoccurring.

Figure 2: Incident Response Policy

## Emergency Communication Strategy