Deliverable 13 Under ICT Strategy and Action Plan
Consulting Services

Report (ver. 1.0.0) on

ITIL Version 3 Implementation Guide

Project Id: 035

Submitted To:
Local Government Engineering Division (LGED)

Submitted By:

Technohaven Company Ltd.
70 Green Road, Fattah Plaza, 9th floor, Dhaka-1205
Tel: +(880-2)-964-1266, Mob: +(880-17)-1500-8917
e-Mail: mailbox@technohaven.com

ITIL Version 3 Implementation Guide

Project ID: 035

Revision History

Ver. No	Date of Release	Prepared By	Prepared Date	Reviewed By	Review Date	List of changes from Previous Version
1.0.0	13-01-2019	S. M. Saifuddin	08-01-2019	Md. Delwar Hossain	10-01-2019	

Approved By: Habibullah Neyamul Karim
Approved Date: 13-01-2019

Table of Contents

1 Introduction

IT Infrastructure Library (ITIL) provides a framework of Best Practice guidance for IT Service Management and since its creation, ITIL has grown to become the most widely accepted approach to IT Service Management in the world.

This compact guide has been designed as an introductory overview for anyone who has an interest in or a need to understand more about the objectives, content and coverage of ITIL. Whilst this guide provides an overview, full details can be found in the actual ITIL publications themselves.

This guide describes the key principles of IT Service Management and provides a high-level overview of each of the core publications within ITIL.

1.1 Scope of Implementing ITIL

Service management is a planned and conscious means of building and managing support structure to meet business and service objectives – moving from chaos to control, from fire-fighting to fusion.

IT Service Management organizations can be structured as per the ITIL recommendations, which defines its scope based on four major functions (Service Desk, Technical Management, Application Management and IT Operations Management). It also attributes its importance for standard roles to any task and activity for good ITSM effort.

Lifecycle Phases	Process
Service Strategy	Service Strategy Service Portfolio Management Demand Management Financial Management
Service Design	Service Catalogue Management Service Level Management Availability Management Capacity Management Service Continuity Management IT Security Management Supplier Management
Service Transition	Change Management Service Asset and Configuration Management Release and Deployment Management Transition Planning and Support Service Validation and Testing Evaluation Knowledge Management
Service Operation	Incident Management

Lifecycle Phases	Process
	Problem Management Event Management Service Request Fulfillment Access Management
Continual Service Improvement	The seven steps improvement process

Processes listed above under all the lifecycles are important and they all are interrelated with their measurable purposes. All processes are bound together with continual Service Improvement. ITIL stresses on improvising the available processes with best practices with need.

1.2 Dependencies

Service Operation includes the execution of all ongoing activities required to deliver and support services. The interdependency of Service Operation includes:

The services themselves: Any activity that forms part of a service is included in Service Operation, whether it is performed by the Service Provider, an external supplier or the user or customer of that service

Service Management processes: The ongoing management and execution of many Service Management processes are performed in Service Operation, even though a number of ITIL processes (such as Change and Capacity Management) originate at the Service Design or Service Transition stage of the Service Lifecycle, they are in use continually in Service Operation. Some processes are not included specifically in Service Operation, such as Strategy Definition, the actual design process itself. These processes focus more on longer-term planning and improvement activities, which are outside the direct dependency of Service Operation; however, Service Operation provides input and influences these regularly as part of the lifecycle of Service Management.

Technology: All services require some form of technology to deliver them. Managing this technology is not a separate issue, but an integral part of the management of the services themselves. Therefore a large part of this publication is concerned with the management of the infrastructure used to deliver services.

People: Regardless of what services, processes and technology are managed, they are all about people. It is people who drive the demand for the organization's services and products and it is people who decide how this will be done. Ultimately, it is people who manage the technology, processes and services. Failure to recognize this will result (and has resulted) in the failure of Service Management projects.

ITIL emphasizes more on People as they can be either service providers, service enablers or Consumers of the service, Training people based on the role and requirements is the key for success. Processes another important factor which has impact on success on any framework, Processes need to be defined precisely aligning with business needs and should be measurable.

Technologies more key factor which enables all the measurable to be more efficient and effective. Various tools and service delivery platforms play important role in service delivery and improvements of the same.

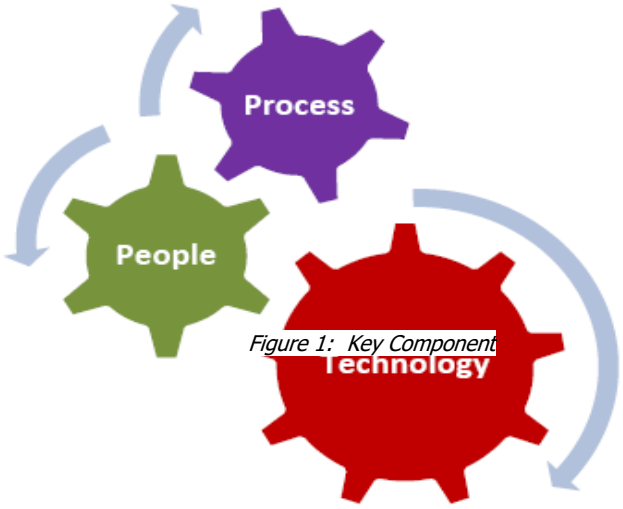


Figure 1: Key Component

Hence understanding these dependencies and making them more adaptive is the key for successful adoption of the framework, yes we need to believe in rule Adapt Improvise and Overcome. In other words it's all about implementing new processes which would bring value to the business in long run and putting the processes in operation and trying to optimize the value to the business through cycle of Implement, Operate and Optimize.

1.3 Overview of Particular Components

Service Operations is the phase in the ITSM Lifecycle that is responsible for 'business-as-usual' activities.

Service Operation can be viewed as the 'factory' of IT. This implies a closer focus on the day-to-day activities and infrastructure that are used to deliver services. However, this publication is based on the understanding that the overriding purpose of Service Operation is to deliver and support services. Management of the infrastructure and the operational activities must always support this purpose.

Well planned and implemented processes will be to no avail if the day-to-day operation of those processes is not properly conducted, controlled and managed. Nor will service improvements be possible if day-to-day activities to monitor performance, assess metrics and gather data are not systematically conducted during Service Operation.

Service Operation staff should have in place processes and support tools to allow them to have an overall view of Service Operation and delivery (rather than just the separate

components, such as hardware, software applications and networks, that make up the end-to-end service from a business perspective) and to detect any threats or failures to service quality.

As services may be provided, in whole or in part, by one or more partner/supplier organizations, the Service Operation view of end-to-end service must be extended to encompass external aspects of service provision – and where necessary shared or interfacing processes and tools are needed to manage cross-organizational workflows.

2 ITIL Framework in LGED Context

2.1 Why ITIL V3

ITIL v3 is the third version of the Information Technology Infrastructure Library, a globally recognized collection of best practices for managing information technology (IT).

It will help the government IT departments in LGED to establish a framework for best practices. While ITIL v2 remained strongly focused on basic IT operations, ITIL v3 emphasizes the concept that IT is a service that supports business goals.

The ITIL v3 framework is more emphasis into the following five sections:

- ITIL service strategy - specifies that each stage of the service lifecycle must stay focused upon the business case, with defined business goals, requirements and service management principles.
- ITIL service design - provides guidance for the production and maintenance of IT policies, architectures and documents.
- ITIL service transition - focuses upon change management role and release practices, providing guidance and process activities for transitioning services into the business environment.
- ITIL service operation - focuses upon delivery and control process activities based on a selection of service support and service delivery control points.
- ITIL continual service improvement - focuses upon the process elements involved in identifying and introducing service management improvements, as well as issues surrounding service retirement.

2.2 ITIL Service Support

Service Support is one of two disciplines comprising IT Service Management. It encompasses the support processes necessary to ensure service quality. These processes manage problems and changes in the IT Infrastructure and are more control-oriented than technical in nature.

The major processes in this area are:

(i) Incident Management
(ii) Problem Management
(iii) Configuration Management
(iv) Release Management
(v) Change Management

Incident Management:

Why has incident management?

Incident management is highly visible to the organization, and it is therefore easier to demonstrate its value than in most areas of service operation. For this reason, incident management is often one of the first processes to be implemented in service management projects. The added benefit of doing this is that incident management can be used to highlight other areas that need attention, thereby providing a justification for implementing other ITIL processes.

The objectives of incident management

To restore normal service operation as quickly as possible and minimize the adverse impact of the Incident on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

Normal service operation is defined here as service operation within Service Level Agreement limits.

The scope of incident management

Incident management includes any event which disrupts, or which could disrupt, a service. This includes events which are communicated directly by users, either through the Service Desk or through an interface from event management to incident management tools.

Incidents can also be reported and/or logged by technical staff (if, for example, they notice something untoward with a hardware or network component they may report or log an incident and refer it to the Service Desk). This does not mean, however, that all events are Incidents. Many classes of event are not related to disruptions at all, but are indicators of normal operation or are simply informational.

The value to the organization of incident management

- The ability to detect and resolve Incidents which results in lower downtime for the organization, which in turn means higher availability of the service.
- The ability to align IT activity to real time business priorities. This is because incident management includes the capability to identify business priorities and dynamically allocate resources as necessary.

- The ability to identify potential improvements to services. This happens as a result of understanding what constitutes an incident and also from being in contact with the activities of business operational staff.
- The Service Desk can, during its handling of incidents, identify additional service or training requirements found in IT or the business.

The activities of incident management

Incident identification and logging (Service Desk responsibility)

- Record basic details of the incident
- Alert specialist support group(s) as necessary

Categorization, prioritization and initial diagnosis

- Categories incidents
- Assign impact and urgency, and thereby define priority
- Match against known errors and problems
- Inform problem management of the existence of new problems and of unmatched or multiple incidents
- Assess related configuration details (daily verification)
- Provide initial support (assess Incident details, find quick resolution)
- Close the incident or route it to a specialist support group, and inform the user(s)

Investigation and diagnosis

- Assess the incident details
- Collect and analyze all related information, and resolve, (including any work around) or route to online support
- Escalate (functionally or hierarchically) where necessary

Resolution and recover

- Resolve the incident using the solution/work around or, alternatively, raise a request for change (RFC) (including a check for resolution)
- Take recovery action

Incident closure (Service Desk responsibility)

- When the Incident has been resolved, the Service Desk should ensure that:

a. Details of the action taken to resolve the incident are concise and readable
b. Classification is complete and accurate according to root cause
c. Resolution/action is agreed with the customer – verbally or, preferably, by email or in writing

- All details applicable to the incident are recorded, such that:

a. The customer/user is satisfied
b. Cost center project codes are allocated
c. The time spent on the incident is recorded
d. The person, date and time of closure are recorded

Note – service requests and major incidents have their own process
The incident management process diagram

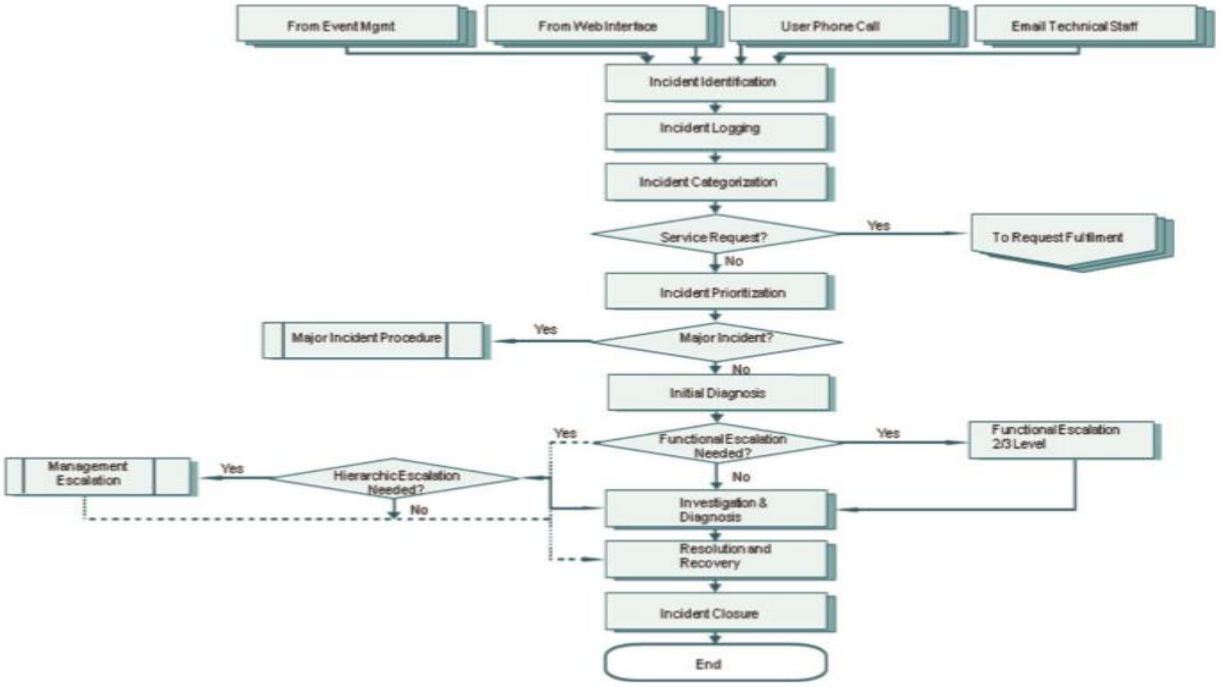


Fig: Incident & Problem Process Diagram

The terminology of incident management:

Incident- unplanned interruption to or reduction in quality of IT service

Functional escalation – escalation across IT to subject matter experts

Hierarchical escalation – involves more senior levels of management – usually for decision making

Work around – a temporary fix for the incident

A major incident – an Incident which has high impact on the organization and for which a separate process exists

Problem management

Why has problem management?

Failure to halt the recurrence of incidents or understand the root cause of major incidents leads to lost time, loss of productivity and frustrated users.

Effective problem management halts the recurrence of incidents and has benefits to the individual and the organization as a whole as it improves availability (up time) and user productivity.

The objectives of problem management

The objective of problem management is to minimize the adverse impact of incidents and problems on the business that are caused by errors within the IT infrastructure, and to prevent recurrence of incidents related to these errors.

The scope of problem management

Problem management includes the activities required to diagnose the root cause of incidents and to determine the resolution to the problems. It is also responsible for ensuring that the resolution is implemented through the appropriate control procedures (change management).

Problem management will also maintain information about problems and the appropriate work around and resolutions, so that the organization is able to reduce the number and impact of Incidents over time. In this respect problem management has a strong interface with knowledge management, and tools such as the Known Error Database will be used for both. The Known Error Database is a hugely effective tool at the Service Desk and is used in early resolution of incidents.

Although incident and problem management are separate processes, they are closely related and will typically use the same tools, and may use similar categorization, impact and priority coding systems. This will ensure effective communication when dealing with related incidents and problems.

The value to the organization of problem management

Problem management works together with incident management and change management to ensure that IT service availability and quality are increased.

When incidents are resolved, information about the resolution is recorded. Over time, this information is used to speed up the resolution time and identify permanent solutions, reducing the number and resolution time of incidents. This results in less down time and less disruption to business critical systems.

Additional value from problem management is derived from the following:

- Higher availability of IT services

- Higher productivity of business and IT staff
- Reduced expenditure on work around or fixes that do not work
- Reduction in cost of effort in firefighting or resolving repeat incidents

The activities of problem management

Problem Management consists of two major processes:

- Reactive problem management – generally executed as part of service operation
- Proactive problem management – initiated in service operation, but generally driven as part of continual service improvement

The reactive activities are:

Problem detection and problem logging

- Use incident guidelines for problem identification
- Other processes (e.g. availability, security) could log problems prior to incident occurring

Problem categorization and prioritization

- Categories the problem by IT functional area
- Assess urgency and impact to assign priority

Problem investigation and diagnosis

- Assign to IT functional area for further investigation

Workarounds and raising a known error record

- In cases where a work around is found, it is important that the problem record remains open, and details of the work around are documented within the problem record

- As soon as the diagnosis is complete, and particularly where a work around has been found (even though it may not be a permanent resolution), a known error record must be raised and placed in the Known Error Database, so that, if further incidents or problems arise, they can be identified and the service restored more quickly

Problem resolution

- Problem record closed when known error located and work around identified

Problem closure

- Problem record closed when known error located and work around identified

The proactive activities are:

Major problem review and errors detected in the development environment

After every major problem, and while memories are still fresh, a review should be conducted to learn any lessons for the future. Specifically the review should examine:

- Those things that were done correctly
- Those things that were done wrongly
- What could be done better in the future
- How to prevent recurrence
- Whether there has been any third party responsibility and whether follow up actions are needed

Such reviews can be used as part of training and awareness activities for staff – any lessons learned should be documented in appropriate procedures, working instructions, diagnostic scripts or known error records.

Tracking and monitoring

The Service Desk Manager owns/is accountable for ALL incidents. Tracking and monitoring takes place throughout all of the other activities.

Trend analysis

- Review reports from other processes (e.g. incident management, availability management, change management)
- Identify recurring problems or training opportunities.

Targeting preventative action

- Perform a cost benefit analysis of all costs associated with prevention.
- Target specific areas taking up most attention.

The terminology of problem management

Problem – unknown, underlying cause of incident(s)

Known error – known, underlying cause of incident(s) and a work around identified

Work around – temporary resolution

Proactive problem management – removal of current/potential errors before they cause problems.

Configuration Management

Why have configuration Management?

Configuration management (CM) is a systems engineering process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life.

What is the objective of configuration management?

The Objectives of Configuration Management: The fundamental purpose of Configuration Management (CM) is to establish and maintain the integrity and control of system components and elements throughout a project's life cycle or during the ongoing operation and management of an ICT Unit.

The Scope of Configuration Management

Configuration Management covers the identification, recording, and reporting of IT components, including their versions, constituent components and relationships. Items that should be under the control of Configuration Management include hardware, software and associated documentation.

Given the definition above, it should be clear that Configuration management is not synonymous with Asset Management, although the two disciplines are related. Asset Management is a recognized accountancy process that includes depreciation accounting. Asset Management systems maintain details on assets above a certain value, their business unit and their location. Configuration Management also maintains relationships between assets, which Asset Management usually does not. Some organizations start with Asset Management and then move on to Configuration Management.

The basic activities of Configuration Management are as follows:

- **Planning:** Planning and defining the purpose, scope, objectives, policies and procedures, and the organizational and technical context, for Configuration Management.

- **Identification:** Selecting and identifying the configuration structures for all the infrastructure's CIs, including their 'owner', their interrelationships and configuration documentation. It includes allocating identifiers and version numbers for CIs, labeling each item, and entering it on the Configuration management database (CMDB).

- **Control:** Ensuring that only authorized and identifiable CIs are accepted and recorded, from receipt to disposal. It ensures that no CI is added, modified, replaced or removed without appropriate controlling documentation, e.g. an approved Change request, and an updated specification.

- **Status accounting:** The reporting of all current and historical data concerned with each CI throughout its life cycle. This enables Changes to CIs and their records to be traceable, e.g. tracking the status of a CI as it changes from one state to another for instance 'under development', 'being tested', 'live', or 'withdrawn'.

- **Verification and audit:** A series of reviews and audits that verify the physical existence of CIs and check that they are correctly recorded in the Configuration management system.

Configuration Management interfaces directly with systems development, testing, Change Management and Release Management to incorporate new and updated product deliverables. Control should be passed from the project or supplier to the service provider at the scheduled time with accurate configuration records.

2.3 ITIL Service Delivery

ITIL Service Delivery defines the business of IT—and it's one of two disciplines that comprise ITIL Service Management.

But what is ITIL Service Delivery? And why is it important?

Service Delivery is much like it sounds: it's the delivery of an IT service to a customer. Done well, Service Delivery brings the business and IT together to benefit the company as a whole—eliminating the detrimental "Us-versus-Them" mindset.

This is important because it performs a service the customer cannot do—and provides great value. Service Delivery should foster a corporate behavior for responsible use of IT services while maximizing corporate profits.

Effective Service Delivery processes should:

- Clearly define the content of IT services
- Clearly define the roles and responsibilities of customers (those who pay for the services), users (those who use the services), and service providers
- Set expectations of service quality, availability, and timeliness

Services need to be tailored to meet the specific business needs of the customer at a price they can afford. By establishing clear Service Delivery processes, you can easily figure out how to provision services with the right mix of internal staff/resources and external vendors.

Being able to measure results of services is key to Service Delivery, too. Meaningful metrics can be used to drive continuous service improvement.

Any effective Service Delivery strategy is comprised of five key components:

- Service level management
- Financial management for IT services
- Capacity management
- Availability management
- IT service continuity management

Service Level Management:

Service level management (SLM) is arguably the most important set of processes within the ITIL framework.

SLM processes define IT and business roles and responsibilities. This is important for establishing clear goals for Service Delivery. And clear goals make it easy to measure and report on success factors.

Why use them? They ensure that the business receives appropriate levels of service at a reasonable cost.

Here's how SLM processes provide the framework to:

- Define services
- Provide levels of service needed to support the agreed-upon processes
- Develop and satisfy service level agreements (SLAs) and operational level agreements (OLAs)
- Outline costs for the services developed

Gathering and storing historical performance data helps the SLM team set the customary levels of service that the business is currently experiencing. With this data in hand, the SLM team can then work with the business to ensure services are efficient and cost-effective—while satisfying business needs.

You could put a lot of work of your own team in creating an SLM process strategy. Or, you could harness the power of IT service optimization software—like Team Quest's—to easily develop effective SLM processes.

Plus, IT service optimization software can be used to determine the additional infrastructure resources required, as well as the costs associated with those changes. Next-level performance data and reporting tools can even be used to monitor service performance and alert the team to adverse trends and/or problems.

Financial Management of IT Service:

Financial Management for IT is one of five components in the ITIL Service Delivery area. It determines the costs of services and provides financial accounting support to ensure expenditures fall within approved plans and that funds are well-spent.

The role of Financial Management varies depending upon the view of IT within the company. Some companies view IT as an expense center, some as a profit center, and some as a cost-recovery center. However, in all cases, Financial Management supports the "business" of IT.

Financial Management activities include:

- Providing oversight of all IT expenditures
- Ensuring funds are available for planned events
- Providing detailed financial information for proposed initiatives
- Influencing the use of IT assets to maximize the return on IT investments through chargeback systems
- Tracking current expenditures against the budget

WHY SHOULD I IMPLEMENT FINANCIAL MANAGEMENT?

Financial Management processes allow you to:

- Plan and predict IT expenditures required to maintain or improve services
- Ensure expenditures fall within approved plan guidelines and that money is well-spent
- Assist senior management in understanding the ongoing total cost of a proposed IT initiative
- Promote a better understanding of the costs associated with providing specific services
- Foster an environment of control to ensure IT services are effectively and efficiently used

Financial Management has close ties to Service Level Management, Capacity Management, and Configuration Management areas, as well as the Corporate Finance Department.

Team Quest Surveyor can enable IT organizations to generate chargeback reports directly from the tracking data and avoid adding a second separate system for billing. The business can easily match its bills to the original data, avoiding questions and concerns about incongruence and potential errors associated with having a separate billing system.

Team Quest Surveyor can give you the ability to automate reports against historical data and track actual usage to your technology plan. You can use Team Quest Predictor to easily prepare reports that visually show how trends are impacting your plans today and on into the future.

Team Quest tools support Financial Management by:

- Enabling IT organizations to generate chargeback reports directly from the tracking data and avoid adding a second, separate system for billing.
- Allowing business units to easily match bills to the original data, avoiding questions and concerns about incongruence and potential errors associated with having a separate billing system.
- Automating reports against historical data.
- Tracking actual usage to your technology plan.
- Providing the ability to prepare reports that visually show any deviation and how it impacts both your plan today and predicts the impact for the rest of the year.

As with all major projects, proper planning is the key. Team Quest recommends following these steps for implementing ITIL Financial Management for IT:

1. Gather the data.

Identify a finance manager with substantial IT knowledge to ensure proper oversight of IT expenditures and assign additional staff as required. The team must perform several duties:

- Perform a current-state assessment, using either a consultant or self-assessment checklists, to discover where and to what extent Financial Management work is being performed today.
- Inventory tools and software currently used for budget, accounting and chargeback systems.
- Perform a gap analysis to reveal areas that require process improvements, training or software.

2. Build the plan.

The implementation plan should:

- Establish the three major components of Financial Management - people, processes and tools.
- Outline the costs necessary to sustain the new organization and build a preliminary budget.
- Determine where the financial manager is located in the organization, ideally reporting directly to the CIO or IT Director.
- Describe workflow, including data inputs, information outputs, and work processes.
- Identify and train the people who will perform the work.

- Identify any necessary work to acquire, consolidate and/or implement financial management tools.

Be sure to communicate the organization and its processes to the rest of the company, preferably through your internal corporate communications team.

Once the project plan and budget are complete, they should be submitted for approval.

3. Execute the plan

You will want to execute the project plan in a series of steps:

- Assign the staff.
- Document and publish the processes. This is an important step that will likely take considerable time during initial implementation.
- Acquire and implement the tools. Ideally, a single tool would be used to provide the data and reporting necessary for accurate reporting of service performance.
- Build the accounting and budgeting framework. Use existing budget as a starting point and adjust it as needed based on the new structure. Obtain invoices, staffing expenses, travel, supply, vendor services and depreciation schedules and use as input. Establish a financial calendar to specify when regular analyses and review points will take place.
- Identify, define and implement chargeback systems. Gather and analyze usage data to confirm original estimates and allocations, establish rates, and finalize reporting.
- Define metrics to measure success. Be sure to tie your metrics to business value, not technical measures. Metrics should be few in number, yet succinct and to the point. Most FM metrics will be related to financial performance.
- Build training materials and execute the training plan. Develop the training materials based on the processes you drafted and test staff members to ensure retention.
- Implement reporting and exception processes and procedures. Two types of reporting are necessary. High-level reporting, used to keep management informed, often takes the form of a dashboard, using colors to depict service quality. Be sure to report both current status and how it is trending. The second type of reporting is more detailed for use by the FM team to identify problematic service areas.

4. Initiate the ongoing work of Financial Management

Begin work to automate and produce financial reports. Be sure the reports alert the FM team when financial targets are threatened and when substantial changes in user behavior occur.

5. Perform post-implementation review.

Document lessons learned and identify any changes that should be made to the process to facilitate future process migrations. Perform a post-implementation audit 6-12 months after

completion to determine if the new processes are being adhered to and if you're getting expected results.

Capacity Management:

Capacity management is the practice of right-sizing IT resources to meet current and future needs. It's also one of five areas of ITIL Service Delivery.

Effective capacity management is proactive, not reactive. Those doing well at capacity management make sure that business and service needs are met with a minimum of IT resources.

What Things Are Included in Capacity Management?

There is plenty of IT tasks that fall under the umbrella of capacity management.

Here are some of them:

- Monitor, analyze, and optimize IT resource utilization
- Manage demand for computing resources (this requires an understanding of business priorities)
- Create a model of infrastructure performance to understand future resource needs
- Right-size applications to make sure service levels can be met (without overdoing it)
- Store capacity data
- Produce a capacity plan that covers current use, forecasted needs, and support costs for new applications/releases
- Build the annual infrastructure growth plan with input from other teams

Why Should I Implement Capacity Management?

Capacity management is critical to keeping IT costs down and quality of service up.

Most organizations use it to:

- Get more out of existing IT resources
- Improve IT cost per service unit positions
- Fine-tune applications and infrastructure components
- Improve performance, reduce consumption, and delay upgrades
- Eliminate redundant work
- Ensure consistent reporting
- Provision capacity efficiently
- Make informed business decisions using timely capacity and related cost information

- Provide insight into total cost of ownership (TCO) of IT upgrades and initiatives
- Predict future use based on growth levels
- Uncover bottlenecks with enough time to stop them before service is affected

Capacity management teams also have close ties to ITIL service level management and financial management areas.

In fact, capacity management processes lead to more thorough service level and associated financial information for the business. And this helps business leaders make more informed decisions.

Where Do I Start?

Capacity management is often the starting point for an ITIL Service Delivery initiative.

Here's why. It offers quick, early wins. And these typically create enough cost savings to fund the remainder of your ITIL project. In our experience, such savings are typically in the millions of dollars.

Plus, recovering implementation costs and showing success keeps the project afloat. (This also encourages upper management to stay the course and reduces resistance in your organization.)

5 Steps to Successful Capacity Management

As with all major projects, proper planning is key. If you're looking to get your project off the ground, here are the five steps you should take.

1. Gather the Data

To plan for where your capacity is going, you need to know where you're at. That's why it's important to identify a capacity manager and form a capacity management team.

This team can then:

- Develop a mission, including desired end-state goals, processes and responsibilities
- Assess the current state of capacity management
- Evaluate existing capacity management skills of the IT staff
- Take inventory of tools and software currently used for monitoring, capacity planning, performance management, and chargeback
- Collect budget details for capacity management work
- Perform a gap analysis to reveal areas that require process improvements, training, or software

2. Build the Plan

Next, you'll need a plan for implementing capacity management.

Typically, your plan should:

- Establish the three major components of capacity management (people, processes, and tools)
- Outline the necessary costs and build a preliminary budget.
- Determine where capacity management should be placed in the organization
- Decide on either a formal, centralized capacity management team OR a matrixes organization
- Establish workflow, including data inputs, information outputs, and work processes
- Allocate sufficient time for training
- Identify any necessary work to acquire, consolidate, and/or implement capacity and performance tools

Once you have your plan (and budget) in place, you can submit it for approval.

3. Execute the Plan

Ready to act on your capacity management plan? Here's what you'll need to do.

Your first step in executing the plan is to build the team. This includes determining the size of the team and writing job descriptions complete with position names, salary grades, and skill requirements.

Next, you'll need to document and publish the processes. This is usually a lot of work. But it is important minimize the impact of a disruption on day-to-day activities.

Processes usually cover:

- Performance management
- Capacity planning
- Modeling
- Performance data collection, storage, and reporting
- New application and major upgrade sizing

Then you'll need to acquire and implement the appropriate tools.

These tools can usually do the following:

- Infrastructure monitoring
- Data collection
- Automated reporting
- Analytics
- Modeling

Your next task is to implement metrics for success. But be sure to tie your metrics to business value (not just technical measures). That's what your upper management team wants to see.

Finally, you must build the training materials and execute the training plan. The better your staff understands the work and the processes, the greater your chances for success.

4. Open for Business

Once you've executed on your plan, you'll want to focus on managing performance. And a key part of managing is measuring.

For starters, choose a visible (but not so complex) area to measure. Typically, this will be a low-risk problem with wide visibility and significant benefit to the company.

Plan to gather at least 30 days of historical performance data before developing any trends or models. Start with simple, platform-specific capacity planning. Then work your way to end-to-end application transaction and business processes.

5. Review After Implementation

After capacity management is going full steam at your organization, it's time to take a step back and assess.

List the lessons you've learned. And identify any changes that should be made to the process in the future.

We recommend performing a post-implementation audit after 6–12 months. This should give you plenty of time and data to determine what's working and if there's anything you can improve.

Need more help along the way? Check out Getting Started: A Manager's Guide to Implementing Capacity Management.

Continuity Management:

IT service continuity management (ITSCM) helps you develop IT infrastructure recovery plans. This helps support overall business continuity management (BCM) plans and timeframes. IT service continuity management is also one of five components of ITIL service delivery.

IT service continuity management as disaster control plan (DCP), disaster recovery planning (DRP), or simply disaster recovery (DR). Whatever term you prefer, ITSCM is critical to developing infrastructure recovery plans.

IT team should work closely with business continuity management (BCM) departments. The goal of this collaboration is to ensure plans and alternative service options are in place—before a serious business outage or service disruptions.

Why Implement IT Service Continuity Management?

ITSCM processes are a must if you want to prepare your business—and IT department—for disasters of any kind.

Done well, ITSCM processes should:

- Minimize disruptions in IT services
- Reduce costs associated with disaster recovery
- Prioritize the recovery of IT services in the event of a disaster

5 Common IT Service Continuity Management Activities

Your IT service continuity management plans will vary based on your region. Your potential disaster recovery plans may need to account for earthquakes, floods, hurricanes, tornadoes, and/or terrorist activities.

1. Conduct a Business Impact Analysis

A business impact analysis will help you determine potential issues and recovery requirements. You should work with BCM and service level management (SLM) teams on it.

You can use predictive analytics to simulate a disaster scenario—and understand how it will impact your business. Software (like Team Quest Predictor) can help you do this—and predict your recovery needs.

2. Take a Risk Assessment

Taking a risk assessment will help you:

- Assess risks
- Determine costs to mitigate those risks
- Prioritize which recovery plans to develop

3. Translate Your Requirements

Do you know your recovery requirements?

If you don't, your top priority is to gather data that shows IT resource usage for each application or service.

If you do… Great, then you can translate them into your infrastructure and data storage requirements.

4. Test Backup and Recovery Plans

Doing what-if analysis can help you determine service performance on back-up servers.

So put your backup and recovery plans to the test. Implement them and test them on your infrastructure.

Be sure to experiment with various business continuity options. For example, test out consolidating and moving work to different servers.

Make sure they work. This may also include negotiating and signing contracts for alternate sites.

5. Review Your Plans

Once you've settled on a disaster recovery plan, you can't just sit back. You need to review it periodically to make sure it stays effective as your infrastructure and environment changes.

As you review and refine your plans, be sure to experiment with multiple scenarios. That's the best way to determine what resources you need to meet your business unit goals.

Put ITSCM Into Practice

It's time to ITSCM into practice. Learn how IT risk mitigation solutions can help you do it. The right solution should help you meet SLAs, prevent outages, and protect your revenue (and reputation).

Availability Management:

ITIL availability management is used to ensure application systems stay available. This usually means making sure everything is up for use under the conditions of service level agreements (SLAs).

Availability management is also a part of the ITIL service delivery framework.

To do this, the availability management team reviews business process availability requirements. Then, they make sure the most cost-effective contingency plans are in place. These plans are tested on a regular basis to make sure your business needs are met.

For example, you may have 30-minute or less recovery requirements for your online ordering systems. You may need to provision these with infrastructure components that add redundancy (but make it easier to recover).

On the flip side, you may have a 5-day recovery period for less important (and non-customer-facing systems). This means you'll need less expensive infrastructure for these systems than for your ordering systems.

Availability management also plays a lead role in component failure impact analysis (CFIA) and service outage analysis (SOA) initiatives. Typically, the available management team determines the cause of the problem. Next, they analyze any related trends. Finally, they take the next steps to ensure service availability meets SLAs.

Why Should I Implement Availability Management?

There are plenty of good reasons to implement ITIL availability management.

For starters, it's essential for making sure services are available for use during the timeframes specified in SLAs.

Availability management is also helpful for making sure services are provisioned on the right infrastructure for their needs. This ensures you avoid unnecessary costs. You wouldn't want to provision services with longer recovery times on more expensive high availability platforms.

Another great way to use availability management is to identify and correct issues—before they impact service.

Availability management processes go hand-in-hand with the other four areas of ITIL service delivery. In fact, it's often used as a support for service level management, capacity management, IT service continuity management, and incident management.

How to Do Availability Management

Performance management software goes a long way to helping you get ITIL availability management implemented at your organization.

For instance, you can use capacity prediction software to perform what-if analysis. This type of analysis involves running multiple scenarios to show the impact of certain decisions. What-if analysis is a great way to determine the performance levels needed to meet your business goals. You can even track and report on these metrics on an ongoing basis.

You can also use infrastructure monitoring software to keep an eye on availability across your systems. You'll get detailed diagnostic capabilities, so you can quickly determine the probable cause of an outage. Plus, you'll find out how to keep an outage from happening again. You can even capture historical data, so you'll be able to report on trends over time.

This type of monitoring makes it easier to predict potential issues and address them before they become problems.

If you need more reporting, you can enlist performance management software. This takes the effort out of reporting by automatically publishing reports with availability metrics across your systems. You can customize them for different audiences, too.

3 Implementing ITIL

The implementation and management of quality IT services that meet the needs of the business. IT service management is performed by IT service providers through an appropriate mix of people, process and information technology.

Process

A process is a structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs.

Function

A function is defined by ITIL as a team or group of people and the other resources or tools that are used to carry out a process or process activities

There are some pre-requisites that should be met before starting an ITIL project. First, we will need at least one person devoted to the project management and coordination of the implementation. You will also need a Service Desk to act as an IT interface. Finally, you will need an ITSM tool. Remember, however, that your processes should drive the tool and not the other way around. The tool can often offer guidance on best practice but should not restrict your efforts. The high level areas in an ITIL implementation are:

I) Map out your current processes

II) GAP analysis

III) Plan and create a roadmap

IV) Implement, communicate and measure

V) Continual improvements

3.1 Getting Started

There is no set way of where to start implementing ITIL; however the best way is to look for areas of the business that needs solutions and start there. Implementing ITIL in a "big bang" approach rarely works. This is due to the fact that it is not only a cultural change; it is also major process and workflow overhaul. This is difficult to do effectively in a "big bang" approach.

3.2 Service Definition

A service is a means of delivering value to customers by facilitating outcomes customers want to achieve, but without the ownership of specific costs and risks.

3.3 Introducing ITIL Roles and Owners

Service Strategy

Business Relationship Manager

- The Business Relationship Manager is responsible for maintaining a positive relationship with customers, identifying customer needs and ensuring that the service provider is able to meet these needs with an appropriate catalogue of services.
- The Business Relationship Manager works closely with the Service Level Manager.
- The Business Relationship Manager has been introduced as a new role in ITIL 2011.

Demand Manager

- The role Demand Manager has been introduced in ITIL 2011 to perform the activities in the Demand Management process.
- The Demand Manager is responsible for understanding, anticipating and influencing customer demand for services.

- The Demand Manager works with capacity management to ensure that the service provider has sufficient capacity to meet the required demand.

Financial Manager

- The Financial Manager is responsible for managing an IT service provider's budgeting, accounting and charging requirements.

IT Steering Group (ISG)

- The IT Steering Group (ISG) sets the direction and strategy for IT Services. It includes members of senior management from business and IT.
- The ISG reviews the business and IT strategies in order to make sure that they are aligned.
- It also sets priorities of service development programs/ projects.

Service Portfolio Manager

- The Service Portfolio Manager decides on a strategy to serve customers in cooperation with the IT Steering Group, and develops the service provider's offerings and capabilities.

Service Strategy Manager

- The Service Strategy Manager supports the IT Steering Group in producing and maintaining the service provider's strategy.
- This role is also responsible for communicating and implementing the service strategy.
- The Service Strategy Manager has been introduced as a new role in ITIL 2011.

Service Design

Applications Analyst

- The Applications Analyst is an Application Management role which manages applications throughout their lifecycle.
- There is typically one Applications Analyst or team of analysts for every key application.
- This role plays an important part in the application-related aspects of designing, testing, operating and improving IT services.
- It is also responsible for developing the skills required to operate the applications required to deliver IT services.

Availability Manager

- The Availability Manager is responsible for defining, analyzing, planning, measuring and improving all aspects of the availability of IT services.
- He is responsible for ensuring that all IT infrastructure, processes, tools, roles etc. are appropriate for the agreed service level targets for availability.

Capacity Manager

- The Capacity Manager is responsible for ensuring that services and infrastructure are able to deliver the agreed capacity and performance targets in a cost effective and timely manner.
- He considers all resources required to deliver the service, and plans for short, medium and long term business requirements.

Compliance Manager

- The Compliance Manager's responsibility is to ensure that standards and guidelines are followed, or that proper, consistent accounting or other practices are being employed.
- This includes making sure that external legal requirements are fulfilled.

Enterprise Architect

- The Enterprise Architect is responsible for maintaining the Enterprise Architecture (EA), a description of the essential components of a business, including their interrelationships.
- Bigger organizations may opt to introduce specialist EA roles like Business Architect, Application Architect, Information Architect, or Infrastructure Architect.

Information Security Manager

- The Information Security Manager is responsible for ensuring the confidentiality, integrity and availability of an organization’s assets, information, data and IT services.
- He is usually involved in an organizational approach to Security Management which has a wider scope than the IT service provider, and includes handling of paper, building access, phone calls etc., for the entire organization.

IT Service Continuity Manager

- The IT Service Continuity Manager is responsible for managing risks that could seriously impact IT services.

- He ensures that the IT service provider can provide minimum agreed service levels in cases of disaster, by reducing the risk to an acceptable level and planning for the recovery of IT services.

Risk Manager

- The Risk Manager is responsible for identifying, assessing and controlling risks.
- This includes analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats.

Service Catalogue Manager

- The Service Catalogue Manager is responsible for maintaining the Service Catalogue, ensuring that all information within the Service Catalogue is accurate and up-to-date.

Service Design Manager

- The Service Design Manager is responsible for producing quality, secure and resilient designs for new or improved services.
- This includes producing and maintaining all design documentation.

Service Level Manager

- The Service Level Manager is responsible for negotiating Service Level Agreements and ensuring that these are met.
- He makes sure that all IT Service Management processes, Operational Level Agreements and Underpinning Contracts are appropriate for the agreed service level targets.
- The Service Level Manager also monitors and reports on service levels.

Service Owner

- The Service Owner is responsible for delivering a particular service within the agreed service levels.
- Typically, he acts as the counterpart of the Service Level Manager when negotiating Operational Level Agreements (OLAs).
- Often, the Service Owner will lead a team of technical specialists or an internal support unit.

Supplier Manager

- The Supplier Manager is responsible for ensuring that value for money is obtained from all suppliers.

- He makes sure that contracts with suppliers support the needs of the business, and that all suppliers meet their contractual commitments.

Technical Analyst

- The Technical Analyst is a Technical Management role which provides technical expertise and support for the management of the IT infrastructure.
- There is typically one Technical Analyst or team of analysts for every key technology area.
- This role plays an important part in the technical aspects of designing, testing, operating and improving IT services.
- It is also responsible for developing the skills required to operate the IT infrastructure.

Service Transition

Application Developer

- The Application Developer is responsible for making available applications and systems which provide the required functionality for IT services.
- This includes the development and maintenance of custom applications as well as the customization of products from software vendors.

Change Advisory Board (CAB)

- A group of people that advises the Change Manager in the assessment, prioritization and scheduling of Changes.
- This board is usually made up of representatives from all areas within the IT organization, the business, and third parties such as suppliers.

Change Manager

- The Change Manager controls the lifecycle of all Changes.
- His primary objective is to enable beneficial Changes to be made, with minimum disruption to IT services.
- For important Changes, the Change Manager will refer the authorization of Changes to the Change Advisory Board (CAB).

Configuration Manager

- The Configuration Manager is responsible for maintaining information about Configuration Items required to deliver IT services.
- To this end he maintains a logical model, containing the components of the IT infrastructure (CIs) and their associations.

Emergency Change Advisory Board (ECAB)

- A sub-set of the Change Advisory Board who makes decisions about high impact Emergency Changes.
- Membership of the ECAB may be decided at the time a meeting is called, and depends on the nature of the Emergency Change.

Knowledge Manager

- The Knowledge Manager ensures that the IT organization is able to gather, analyze, store and share knowledge and information.
- His primary goal is to improve efficiency by reducing the need to rediscover knowledge.

Project Manager

- The Project Manager is responsible for planning and coordinating the resources to deploy a major Release within the predicted cost, time and quality estimates.

Release Manager

- The Release Manager is responsible for planning and controlling the movement of Releases to test and live environments.
- His primary objective is to ensure that the integrity of the live environment is protected and that the correct components are released.

Test Manager

- The Test Manager ensures that deployed Releases and the resulting services meet customer expectations, and verifies that IT operations is able to support the new service

Service Operation

1st Level Support

- The responsibility of 1st Level Support is to register and classify received Incidents and to undertake an immediate effort in order to restore a failed IT service as quickly as possible.
- If no ad-hoc solution can be achieved, 1st Level Support will transfer the Incident to expert technical support groups (2nd Level Support).
- 1st Level Support also processes Service Requests and keeps users informed about their Incidents' status at agreed intervals.

2nd Level Support

- 2nd Level Support takes over Incidents which cannot be solved immediately with the means of 1st Level Support.
- If necessary, it will request external support, e.g. from software or hardware manufacturers.
- The aim is to restore a failed IT Service as quickly as possible.
- If no solution can be found, the 2nd Level Support passes on the Incident to Problem Management.

3rd Level Support

- 3rd Level Support is typically located at hardware or software manufacturers (third-party suppliers).
- Its services are requested by 2nd Level Support if required for solving an Incident.
- The aim is to restore a failed IT Service as quickly as possible.

Access Manager

- The Access Manager grants authorized users the right to use a service, while preventing access to non-authorized users.
- The Access Manager essentially executes policies defined in Information Security Management.

Facilities Manager

- The Facilities Manager is responsible for managing the physical environment where the IT infrastructure is located.
- This includes all aspects of managing the physical environment, for example power and cooling, building access management, and environmental monitoring.

Incident Manager

- The Incident Manager is responsible for the effective implementation of the Incident Management process and carries out the corresponding reporting.
- He represents the first stage of escalation for Incidents, should these not be resolvable within the agreed Service Levels.

IT Operations Manager

- An IT Operations Manager will be needed to take overall responsibility for a number of Service Operation activities.

- For instance, this role will ensure that all day-to-day operational activities are carried out in a timely and reliable way.

IT Operator

- IT Operators are the staff who perform the day-to-day operational activities.
- Typical responsibilities include: Performing backups, ensuring that scheduled jobs are performed, installing standard equipment in the data center.

Major Incident Team

- A dynamically established team of IT managers and technical experts, usually under the leadership of the Incident Manager, formulated to concentrate on the resolution of a Major Incident.

Problem Manager

- The Problem Manager is responsible for managing the lifecycle of all Problems.
- His primary objectives are to prevent Incidents from happening, and to minimize the impact of Incidents that cannot be prevented.
- To this purpose he maintains information about Known Errors and Workarounds.

Service Request Fulfillment Group

- Service Request Fulfillment Groups specialize on the fulfillment of certain types of Service Requests.
- Typically, 1st Level Support will process simpler requests, while others are forwarded to the specialized Fulfillment Groups

Continual Service Improvement

CSI Manager

- The Continual Service Improvement (CSI) Manager is responsible for managing improvements to IT Service Management processes and IT services.
- He will continually measure the performance of the service provider and design improvements to processes, services and infrastructure in order to increase efficiency, effectiveness, and cost effectiveness.

Process Architect

- The Process Architect is responsible for maintaining the Process Architecture (part of the Enterprise Architecture), coordinating all changes to processes and making sure that all processes cooperate in a seamless way.

- This role often also supports all parties involved in managing and improving processes, in particular the Process Owners. Some organizations combine this role with the Enterprise Architect role.

Process Owner

- A role responsible for ensuring that a process is fit for purpose.
- The Process Owner's responsibilities include sponsorship, design, and continual improvement of the process and its metrics.
- In larger organizations there might be separate Process Owner and Process Manager Roles, where the Process Manager has responsibility for the operational management of a process.

3.4 GAP Analysis

ITIL describes a gap analysis in the Continual Service Improvement (CSI) Book:

"A gap analysis is a business assessment tool enabling an organization to compare where it is currently and where it wants to go in the future."

Before a gap analysis can be undertaken, the organization must clearly understand its long-term vision with respect to the subject of the gap analysis. The scope of a gap analysis also needs to be clearly defined. An organization might conduct a gap analysis on their overall organizational processes and IT capabilities, or they might focus a gap analysis on some aspects of their business operations and processes. Additionally, a gap analysis could be focused on overall information technology or some aspect of information technology, such as a tool implementation.

ITIL does not come with a scale to help identify the extent to which an organization adheres to the best practice. Many different scales have been used though. Most commonly, a scale that resembles a CMMI scale is used. This scale shows levels from 1 to 5, with level 1 being low maturity and level 5 representing high maturity.

Finally, the conclusions of a gap analysis must describe how much effort is required in terms of time, money, and human resources to achieve the vision.

3.5 Planning of New Process

A model is needed to be identified before planning a process to ensure the Successful factor of implementing ITIL in organizations.

Today many organizations spend a lot of money in ITIL implementation projects and fail. A maturity model will solve this problem as it will allow not only assessing the level of ITIL in organizations but also will guide them and will tell them what they miss or need to achieve the level they want

The main goal is to design a model that provides a roadmap to help the organizations in ITIL implementation, in a correct way and avoiding errors that already made other organizations failed and collapsed. For that we need to accomplish a few objectives:

Global vision of ITIL: The study of ITIL is essential to realize a good work, understand the process, dependencies, relation, goals, etc. Only with a good knowledge of ITIL it is possible to design a model to evaluate it.

- **Processes dependencies**: The processes dependencies are important to understand which process should be implemented, when, with which other process, how high, etc. Therefore a dependencies map should be done.

- **Study maturity models**: Comparing existing maturity models is an important goal in order to identify the most reliable model(s).

- **Choose the right maturity models**: Select the advantages of each maturity model studied to design a good maturity model that could be applied to ITIL.

- **Mapping processes**: Mapping the processes between the maturity model(s) selected and ITIL to identify the relevant goals and practices of the model(s).

- **Design staged model**: Based on the model(s) selected, on dependencies map and on the mapping of processes made before, design a staged model leveling the processes with coherence.

- **Create questionnaire for the largest number of ITIL processes**: After identifying the processes of the selected models that correspond to each ITIL process a questionnaire for each process should be created and leveled by a maturity scale. If possible test each questionnaire in organizations.

- **Design continuous model**: After creating a questionnaire for each ITIL process, collect them all and design the continuous model

- **Assess organizations**: With the questionnaires we'll be able to assess organizations and get results in order to demonstrate the potential of the designed maturity model.

- **Results**: Collect the results of the several assessments performed, get a conclusion and improve the model.

3.6 Process Control

A coherent strategy for process control not only helps to assess whether the objectives followed with the ITIL introduction are achieved, but also has long-term benefits, in that it delivers the necessary data for a continuous process improvement.

How to decide whether a process "runs well" or not? Objective criteria (quality measurements, also known as Key Performance Indicators or KPIs) must be determined for this purpose.

Only then, when it is clear which quality measurements a process must achieve, can its inner details be confi-dently designed with these goals in mind.

Determine the Process Owners

Successful management of a process depends on Process Owners who identify themselves closely with their task, and who are sufficiently empowered and equipped with the necessary means.

It is therefore important to have the Process Owners (being the ones responsible for running the processes after their implementation) as active participants in the implementation project, so they should be named at an early stage.

In most cases, the selection of Process Owners is rather straightforward (the Problem Manager will, for example, be the owner of the Problem Management process).

Define ITIL Metrics and Measurement Procedures

Process Owners use objective quality criteria to assess whether their processes are running "well". This puts them in a position to decide upon the need for process improvements.

The first step when selecting suitable ITIL KPIs (see Fig. 1: ITIL metrics - examples) must always be to decide upon the overall objectives of a process, e.g. a high first-resolution rate at the Service Desk. With these objectives in mind, it will be possible to select KPIs which are suitable to measure a successful process execution.

There are also quantitative measures, which are used by the Process Owner to steer the resources within a process (e.g. the number of Incidents received by the Service Desk over the course of time).

Which KPIs are eventually chosen is dependent, amongst other things, upon the available possibilities for their measurement. Ideally, KPIs can be computed automatically, e. g. via a Service Desk system. The measurement procedures defined here are therefore also requirements for the systems to be implemented.

These KPIs were taken from the ITIL recommendations; they have been in some parts supplemented with elements from COBIT. Where necessary, further suggestions for KPIs are available in several books on IT Service Management.

Process control should not be about setting up as extensive an arsenal of KPIs as possible: Practice has proven that an over-complex structure of measures creates a disproportionate amount of effort, gains little acceptance, and after a short period, is no longer applied. Rather, few significant measures should be defined so that KPI measurement and reporting may be executed with a justifiable amount of time and effort.

Set KPI targets

Target values for the KPIs define "success" in an objective way and set goals for the Process Owner. It must be noted, however, that target values (like first-time resolution rates) cannot be easily transferred from business to business without precaution.

It is recommendable not to define fixed KPI targets initially, but to merely select suitable KPIs and start measuring. Once a statistically significant number of measurement results are present after a certain time there will be a more solid base for setting targets.

Define the Reporting Procedures

Reporting on process quality is the final element within process control. Reporting procedures must be defined, specifying which KPIs are reported in which form to particular recipients.

3.7 Implementation Road MAP

The aim of the roadmap is to provide an overview of how the implementation will be executed. In order to create the roadmap, each of the actions needs be reviewed and classified by the time and effort for completion. A good method is to use time frames in the ITIL implementations such as:

ITSM Implementation Roadmap that will identify key streams of activities, key phases within each stream, high level deliverables and benefits that each stream should deliver. Few overarching elements should be considered:

- Grouping the necessary activities into project work streams combined to form an ITSM program
- Scheduling activities based on the business priorities to establish the quick wins and disseminate these to the business
- Ensuring there is adequate integration between work streams and the necessary governance in place

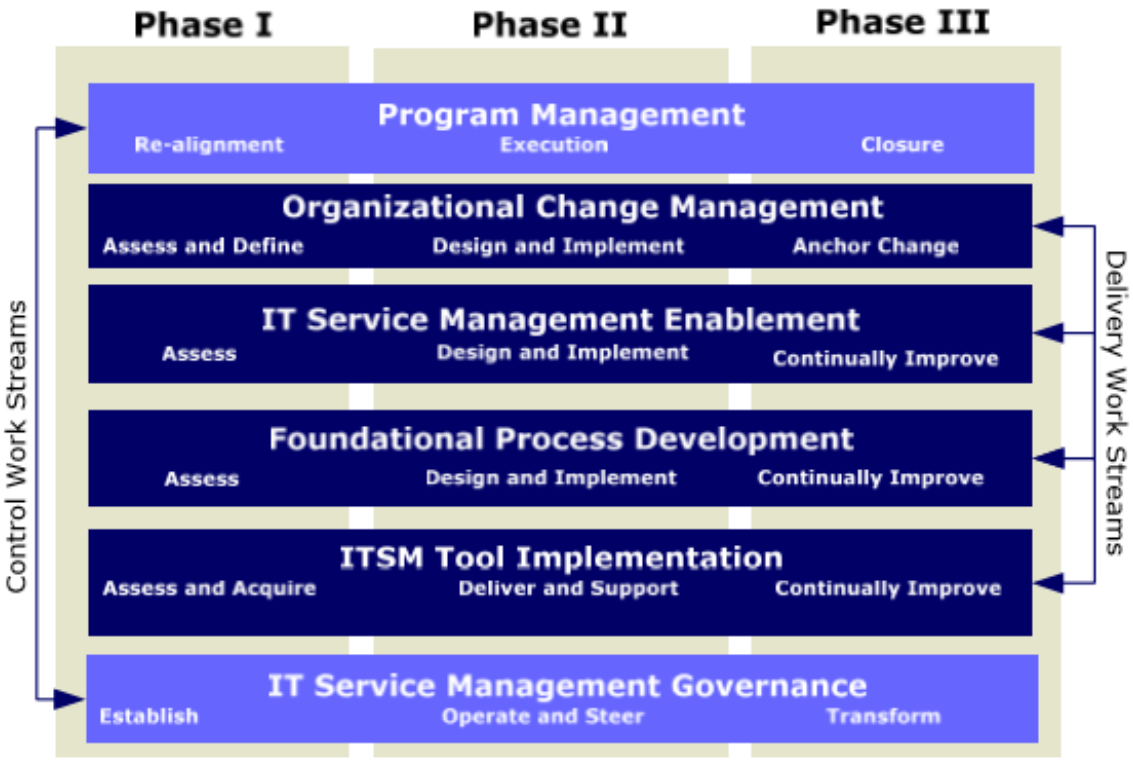


Fig: Roadmap of ITIL Implementation

3.8 Implementation of ITIL Process

Environment

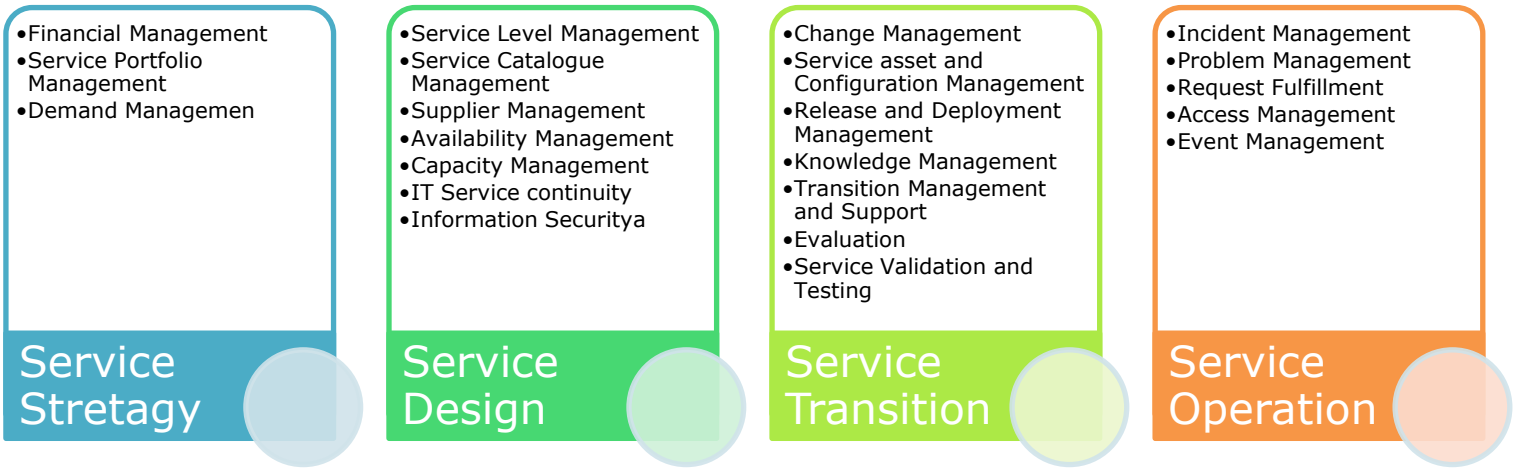
The main motivation for the implementation and consequent certification in the IT Services Management is given by the demand on the contract renewal with the unique client in the segment of the company LGED.

The other motivations are:

- Search for better practices in the market;
- Greater participation in restrict market niche;
- Increase the quality and the reliability in services provision;
- Improve the management of contracts with suppliers and partners.

Preparation

Once the certification is decided for, the managerial group carries out a meeting to define the implementation strategy of the due standard, as described by Figure Service Management Process.



The ISO/IEC 20000 implementation process was performed in fourteen months, with high investment, and consisted of:

- Define and approve the scope: A standard and certification scope of work is initially defined and submitted for prior approval by the certifying organization. The team is defined by the managerial body according to the profile of each member. There is a periodic videoconference between the consultant and the project coordination committee for the implementation of the next steps of the process.
- Elaborate and approve project plan: A plan is create by the committee aided by the hired consulting and approved by the areas managers of LGED;
- Evaluate the current practices: Comparison with the quality management system (ISO 9001) implemented and consistent in the company;
- Compare practices with ISO 20000: A comparison between the requirements of ISO 20000 and ISO 9001 is performed; Elaboration of Service Level Agreement with the client; External Support Agreement with suppliers and Operational Level Agreement among internal areas. Thus integrating a partnership in the implementation of a better provision of remote support services;
- Document and evaluate the differences (gap analysis): An electronic spreadsheet with the analysis of what the company which is already certified in the ISO 9001 needs to achieve the ISO/IEC 20000. The requirements are found in the referred standards.
- Elaborate Action Plan: An action plan is elaborated for the carrying out of the committee;
- Train teams in ITIL: Training and certification in ITIL V.3 for the managerial body, standard implementation committee and the operational body of the organization; Training on interpretation of the standards ISO/IEC 20000 and ISO/27002 for the committee and the managerial body;
- Define and implement the management system: Review the ISO 9001 documents with the inclusion of IT Management and elaboration of new ones, taking into account the

structure of the internal processes of LGED. The list of the current documents can be consulted in Attachment I of this research;

- In order to manage the incidents and problems, The choice for such tool was due to the fact that it works with the ITIL Service Management standard and it allows changes according to client's requirement;
- Implement ITIL processes: Initiate the application of the documents and adjust; formation of a change committee, composed by the Senior Executive, the Change Manager and the representatives from the units;
- Train in management system processes: Carry out awareness event for the whole organization in the revised/new documents made available in the documents management;
- Perform Internal Audit: Between November 3rd and 5th, 2018, to check the implementation of the requirements of the due standard.
- Perform External Pre-Audit: Between December 26th and 27th, 2018, by the Certification organization.
- Perform External Final Audit: Between January 21st and 22nd, 2019, by the Certification organization. Such activity lasted 2 days and no nonconformities or observations were registered;
- Get a recommendation: The certifying organization delivered the indication letter, once the certification could only be delivered within a one month. This way, there was no need for a follow-up audit, which consists of a verification of the treatment of the inconsistencies found in the certification audit and its closure;
- Get the ISO 20000 certification: The certificate was delivered to the LGED thirty days after the recommendation, when the company was formally declared certified on ISO/IEC 20000, ITIL. From that moment on, the news was made public to the press, clients and suppliers, and so were the benefits resulting from such achievement.

Figure- Service Management Process shows the internal processes structure of the LGED, which consists of the relation between the corporate and commercial processes, integrated management, integration aid which support the whole organization and the specific Contact Center (IT Remote Support) process of the LGED(unit) so the Operation area may perform the users' support service and comply/surpass the client's satisfaction level.

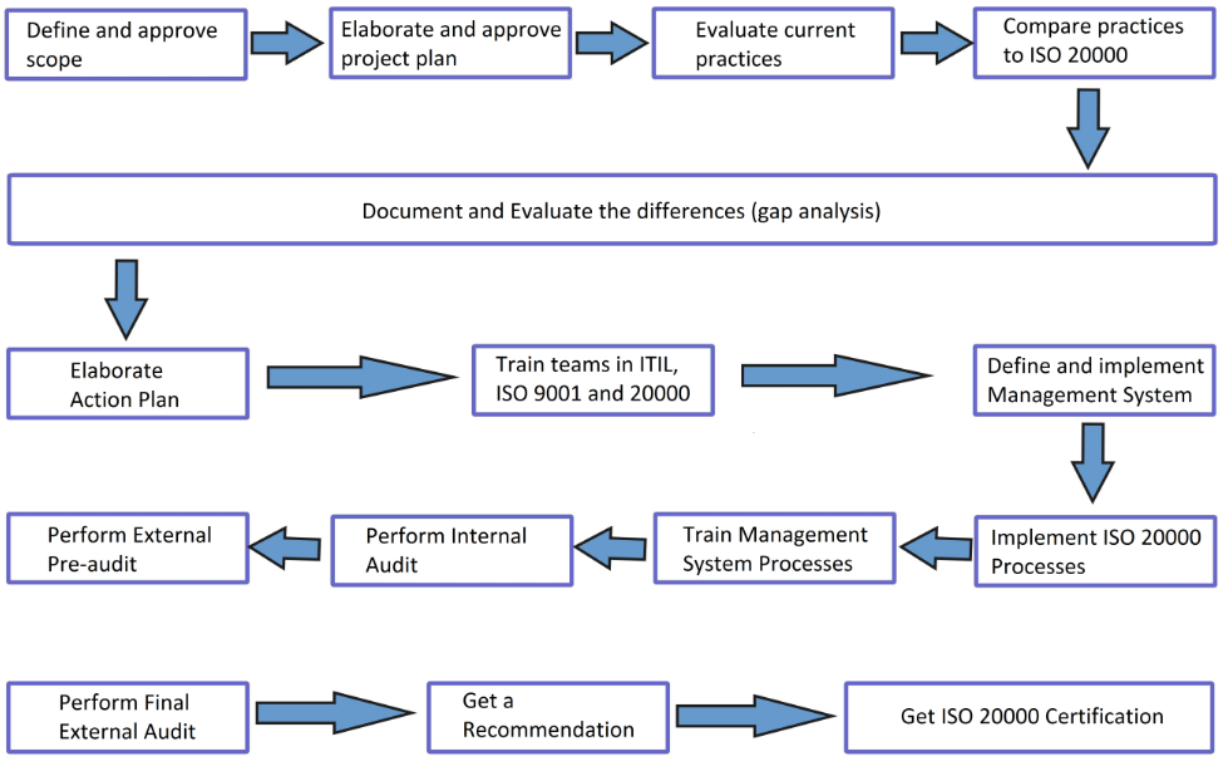


Fig- ITIL Implementation Process

Continuous improvement process: the company LGED kept its ITIL committee reducing only its meetings periodicity from weekly to twice a month. This way maintaining the management system of the IT services implemented and searching for the continuous improvement of its result to the client's view.

3.9 Time Frame

ITIL Project Implementation Time Table

T-ask	In Charge	Start Date	End Date
Identify the service structure Identify the structure of Business service Identify the structure of supporting services			
Select ITIL Roles and Determine Role Owners Identify the ITIL roles for the processes to be introduced Determine the role owners			
Define Process Structure Analyze as-is processes Define the to-be process structure Define the process interfaces			
Establish Process Control			

T-ask	In Charge	Start Date	End Date
Determine the process owners Define KPIs and measurement procedures Define reporting procedures			
Design Processes in Detail Define detailed activity sequences			
Implement Processes and System Identify system requirements Select system(s) to support the to-be processes Implement system(s) Implement to-be processes			
Train IT Staff and Customers Train IT staff involved in running the new processes Inform and instruct users (customers)			
Project Closure			

4 ITIL V3 Publications for LGED

4.1 Service Strategy

Service Strategy is depicted as residing at the center of the ITIL model, as it directly influences all other phases of the Service Lifecycle. The objective of Service Strategy volume is to help organizations understand the fundamental premise of IT Service Management, where the customer is the focus, and IT delivers value to them in the form of value-adding services. The goal of the volume is to help IT organizations establish themselves as IT Service Management organizations, and therefore become a strategic asset to their businesses. The discussion within the book includes review of IT Service Management as a Practice, definition of an IT service, value, concepts of utility, warranty, market spaces, service strategy fundamentals, service structures, types of service providers and current types of service sourcing.

This volume also describes a number of processes that relate to, enable or enhance development of Service Strategies, namely:

- Service Strategy process, including:
  - Defining the Market
  - Developing the offerings
  - Developing Strategic Assets
  - Preparing for execution
- Service Economic processes, namely:
  - Financial Management, including Return on Investment

- Service Portfolio Management
- Demand Management.

4.2 Service Design

The second volume in the ITIL library and the second phase in the ITIL Service Lifecycle describe the process of designing new and improved IT Services, and associated and enabling IT processes. This volume introduces the concept of the Service Design package – a set of detailed blueprints required for building a new, or changed IT service. Specific processes discussed in the Service Design volume include the following:

- Service Catalogue Management
- Service Level Management
- Service Availability Management
- Service Capacity Management
- Security Management
- IT Service Continuity Management

4.3 Service Transition

Service Transition is the third volume in the ITIL library, and also marks the third phase of the Service Lifecycle. It provides guidance on how to successfully transition newly designed ITservices and IT processes into operation.

The guidance includes a number of processes critical to successful transitions:

Service Transition Planning and Support

- Change Management
- Service Asset and Configuration Management
- Release and Deployment Management
- Service Validation and Testing
- Evaluation
- Knowledge Management

4.4 Service Operation

Service Operation is the fourth volume of the ITIL library and represents the fourth sequential phase of Service Lifecycle. It focuses on operations, which are key in effective and efficient

delivery of IT Services. Most industry experts agree that IT operations is the most essential phase in the Service Lifecycle, as it is in this phase that all the previous work, from strategy to design and transition gets realized and delivered to clients. The guidance in this volume includes the following:

- Event Management
- Incident Management
- Request Fulfillment
- Problem Management
- Access Management

4.5 Continual Service Improvement

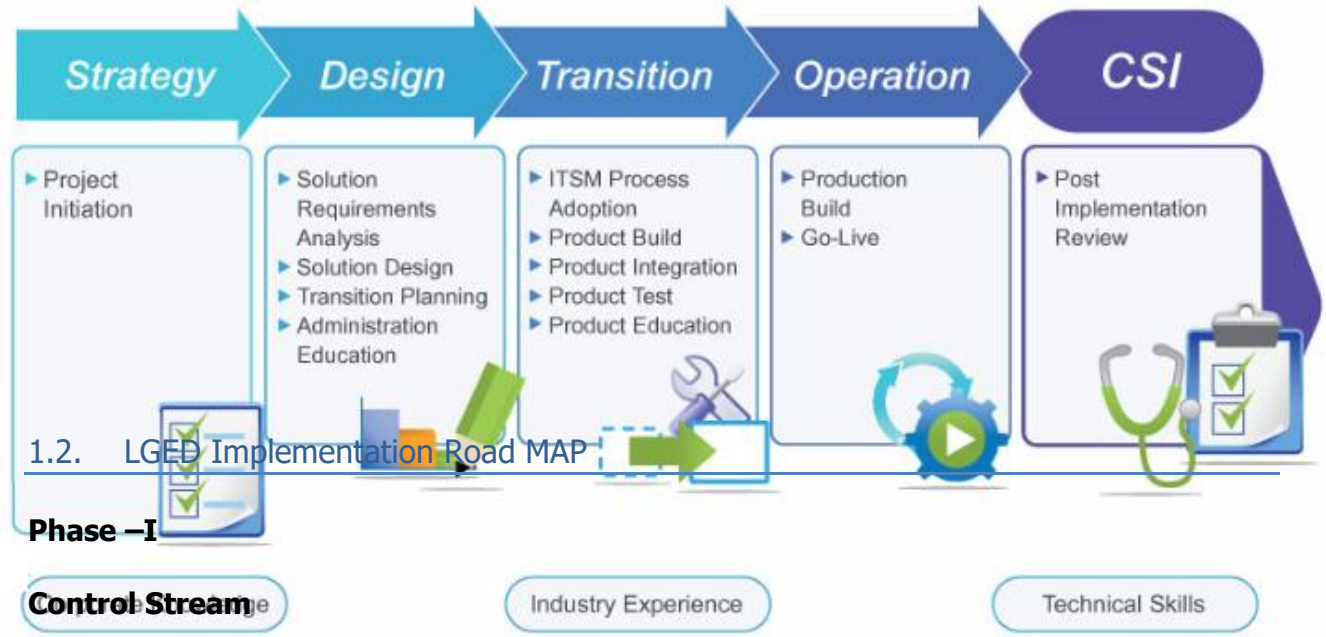
Continual Service Improvement (CSI) is the final volume of the core ITIL library. It is NOT considered to be the fifth phase in the Service Lifecycle, as continual improvement is assumed to take place at every stage of the Service Lifecycle. CSI volume is heavily inspired by the teachings and practices of W. Edwards Deming, a famous American statistician, professor and consultant who is credited for development of numerous improvement methodologies such as the Total Quality Management (TQM), 12 Step Continual Improvement Models, Deming Cycle and others. The guidance in the CSI volume includes the following processes:

- The 7-Step Improvement Process
- Service Reporting
- Service Measurement
- Return on Investment for CSI
- Service Level Management

5 Recommendations

- ✓ IT service management will be a prerequisite for demonstrating business value. Success requires commitment and perseverance.
- ✓ IT service management requires fundamental cultural and behavioral change. Pay careful attention to organizational change management issues.
- ✓ Success in IT service management is based on repeatable processes. Use ITIL as the basis for IT operational processes and then focus on continually improving them.
- ✓ Seek opportunities to learn from and copy best-practice processes. Adopt a Capability Maturity Model approach to progressively build process competency

5.1 LGED ITIL Implementation Model



1.2. LGED Implementation Road MAP

Phase –I

Control Stream

1. **Program Management:**

   The Program Management stream establishes the appropriate project and program controls, leads the selection of program staff, and will establish the funding model. The ongoing operations of the Program Management work stream will be to manage the other work streams and ensure that projects are integrated, on budget, in scope and are being delivered on schedule. This stream will monitor and manage all of the interdependencies between the various streams and the dependencies on external initiatives.

   It is through this stream that the ITSM Program ensures the appropriate level of discipline is applied.

   Deliverables:

- ✓ Detailed Program Plan, as per an organization PMO standards and guidelines
- ✓ Project Charter
- ✓ Risk and Issue Logs
- ✓ Exception Reports and other Management Products
- ✓ Stage Gate Process
- ✓ Funding Model
- ✓ Program Team staffing recommendation
- ✓ Program Team expectations document
- ✓ Ongoing management of the program

2. IT Service Management Governance Stream:

The IT Service Management Governance work stream has two aspects:

One is to initially establish IT Service Management governance and the second is the ongoing operations of the IT Service Management governance. The ongoing operations of IT Service Management governance will govern the work streams and ensure there are appropriate controls in place with clear ownership and accountability. This stream will play a vital role in approving changes to the program plan where required, providing an independent channel and steering committee to resolve any conflicts around design or the approach to implementing the various components of the IT Service Management solution, and provide the business-aware, final decision making authority to resolve strategic issues that affect the program and/or the business to minimize the chance of delay.

Deliverables:

- ✓ IT Service Management Governance Assessment Report
- ✓ IT Service Management Steering Committee Terms of Reference document
- ✓ IT Service Management Performance Management competencies framework document
- ✓ IT Service Management Operational Governance design
- ✓ Communication of Steering Committee commitment
- ✓ Decisions as necessary
- ✓ Transition plans from IT Service Management Program steering committee to Service Review Committee

Phase – II

Delivery Stream:

1. **Organizational Change Management Stream**

The Organizational Change Management stream will initially be focused on developing the foundational elements required for a successful transformational initiative. A significant amount of implementation time and effort should be spent on effective organizational communication and change activities to ensure the organization is informed, ready and willing for the changes being proposed. This work stream will focus on building and then implementing the necessary tools such as the Management of Change strategy, communication strategy to ensure information sharing is embedded into the project and that progressive stakeholder engagement is achieved this stream will ensure that activities required to anchor the change after the project elements are over are properly identified and performed.

Deliverables:

- ✓ Actionable Communication Plan
- ✓ Stakeholder Management Plan
- ✓ Actionable Training Plan
- ✓ Future Organizational Operating Strategy
- ✓ Communication of Executive commitment
- ✓ Outputs of the Communication Plan
- ✓ Outputs of the Training Plan
- ✓ Outputs of the Organizational Operating Strategy
- ✓ Training in anticipation of deployment of processes and tools
- ✓ Ongoing and Sustained Organizational Commitment:
    - Top Driven
    - Middle Management Supported and Enforced
    - Enthusiastic adoption by IT staff members Benefits

2. **IT Service Management Enablement**

The IT Service Management Enablement work stream initially focuses on defining and documenting the IT services offered to the business. Further, it starts to build the understanding of the underlying components and devices that support delivery of IT services to facilitate capacity, availability and continuity planning. As part of documenting the services that an IT organization provides, cost and demand should be identified and activities undertaken to understand these costs and demand levers. During the latter phases of this work stream, processes will be implemented to help the

organization better manage and report on IT services provided. Ultimately, this stream is the whole reason for pursuing IT Service Management.

Deliverables:

- ✓ Service Portfolio Framework
- ✓ Documented Services – IT Service Catalogue
- ✓ Continual Service Improvement (CSI) process documentation
  - o CSI process implementation
- ✓ Financial and Demand Management process documentation
  - o Financial and Demand Management process implementation
- ✓ Service Level Management process documentation
  - o Service Level Management process implementation
- ✓ Service Catalogue Management process documentation
  - o Service Catalogue Management process implementation
- ✓ Availability Management process documentation
  - o Availability Management process implementation
- ✓ Capacity Management process documentation
  - o Capacity Management process implementation
- ✓ Service Continuity Management process documentation
  - o Service Continuity Management process implementation
- ✓ Knowledge Management process documentation
  - o Knowledge Management process implementation
- ✓ Improvement plans for documented services

3. Foundational Process Development

The focus of the Foundational Process Development work stream is to design and implement the Service Support processes based on ITIL best practices. This stream aims to build the capabilities of the IT organization to operate as an internal services provider, gradually building the processes to define and support an integrated and automated (where possible) controlled process environment.

Deliverables:

- ✓ Process Maturity Baseline
- ✓ Incident and Request Fulfillment process documentation
  - o Incident and Request Fulfillment process implementation
- ✓ Configuration Management process documentation

- Configuration Management process implementation

- ✓ Asset management process documentation
  - Asset management process implementation
- ✓ Change Management process documentation
  - Change Management process implementation
- ✓ Release Management process documentation
  - Release Management process implementation
- ✓ Problem Management process documentation
  - Problem Management process implementation
- ✓ Process Maturity Reassessment
- ✓ Improvements and modifications as necessary

4. IT Service Management Tool Implementation

IT Service Management Tool Implementation is a work stream to implement a new Service Management tool within an organization. The long term plan should be to use a selected tool as an integrated IT Service Management toolset for all the processes and functions – Service Desk, Change, Asset, and the Configuration Management Database (CMDB).

Deliverables:

- ✓ Incident Management module
- ✓ CMDB Data architecture
- ✓ Service Desk module deployment (Supports Incident, Request, and Problem Management)
- ✓ Change Management module deployment
- ✓ Asset Management module deployment
- ✓ CMDB deployment
- ✓ Analytics and Reporting
- ✓ Improvements and modifications as necessary

6 Budget and Post Implementation Review

Scope of Work	Activities	Resources	Cost (BDT)
Project Planning	- Kickoff meeting - Defining the scope with business - Roles, responsibilities and accountabilities - Design and mapping - Communications		95,000.00
Assessment &Gap Analysis	- Overview and Training - Discover and Review Background Information - Stakeholder Interviews - Draft Gap Analysis and Presentation - Complete Final Deliverables		1,060,000.00
Process Design & Implementation	- Design and document, Comprehensive of: o Policies, Process and Templates o Roles, Responsibilities, Metrics and Reporting - Process definition and workflow review - Coordination of customize procedures specific to business and support group - Final planning based on the project roadmap		2,040,000.00
Result Review &Documentation	- Acceptance and selection of process owner and Mangers - Project roadmap review - Process templates review - Documentations review and screening - Post project review		850,000.00

Scope of Work	Activities	Resources	Cost (BDT)
	- Assess human element - Review effectiveness and efficiency - Prepare review reports		
Internal Audit	- Cycles of Internal Audit - Identification of Non-conformities (NC's) - Remediation suggestions for Gaps identified - Remediation coordination - Division wise self-audit coordination - Final Audit related articles & evidences arrangement and final readiness - Disaster Recovery Plan		660,000.00
Training and Developing	- Define group(s) for training - Send training invitation - Prepare training venue - Prepare training materials - Perform training - Create training records form training		680,000.00
Handover and Takeover	- Project documents - Final Audit report with recommendation and remediation - Training Documents/materials - Development documents and - Certification		85,000.00
Certification	- Finalize internal & external audit - Complete certification		340,000.00
Project Closer and contingency	- Achievement of the project's objectives - Performance against plan (estimated time and costs		7,50,000.00

Scope of Work	Activities	Resources	Cost (BDT)
	- versus actual) - Statistics on issues raised and changes made - Total impact of changes approved - Lessons learned and recommendations - Post project review plan		
Total Cost of ITIL Implementation			**6,560,000.00**

Acronyms and Abbreviation

CCB	Change Control Board
CFMA	Component Failure Impact Analysis
CM	Configuration Management
CR	Change Request
DR	Disaster Recovery
ePMS	Electronic Project Monitoring System
ICT	Information and Communication Technology
IDSS	Integrated Decision Support System
IRA	ICT Roadmap and Action-plan
ISG	IT Steering Group
ITIL	IT Infrastructure Library
LGED	Local Government Engineering Department
MIS	Management Information System
NOC	Network Operation Centre
OLA	Operational Level Agreements
PM&E	Project Monitoring & Evaluation Unit
PMIS	Personnel Management Information System
PMS	Progress Monitoring System
RTIP-II	Second Rural Transport Improvement Project
SLA	Service Level Agreement
SLM	Service Level Management
UAT	User Acceptance Test
uFMS	Uniform Financial Management System