|  |
| --- |
|  |
| TatakPinoy Inc. |
| MIS 189.2: Service Management |
|  |
| **The Cabs Consultancy Group** |
| **Cruz, Raymond Joseph Nathaniel**  **Gutierrez, Ma. Victoria**  **Lu Chiu, Dave Ericson**  **Tan Stephen Justin**  **Valena, Manolo Luis** |

**September 30, 2013**

|  |
| --- |
|  |

Table of Contents

[Executive Summary 1](#_Toc368251032)

[Assessment of the Company 2](#_Toc368251033)

[Introduction 2](#_Toc368251034)

[Current Situation and Problems 2](#_Toc368251035)

[Proposed Changes 3](#_Toc368251036)

[Service Strategy 3](#_Toc368251037)

[Recommendation 3](#_Toc368251038)

[Service Portfolio Management 4](#_Toc368251039)

[Service Design 4](#_Toc368251040)

[Service Catalog Management 4](#_Toc368251041)

[*Business Service Catalog* 4](#_Toc368251042)

[*Technical Service Catalog* 5](#_Toc368251043)

[Service Level Management 5](#_Toc368251044)

[Capacity Management 6](#_Toc368251045)

[Availability Management 6](#_Toc368251046)

[IT Service Continuity Management 6](#_Toc368251047)

[Information Security Management 7](#_Toc368251048)

[Service Transition 7](#_Toc368251049)

[Service Asset and Configuration Management 7](#_Toc368251050)

[Change Management 8](#_Toc368251051)

[Release and Deployment Management 8](#_Toc368251052)

[Service Validation and Testing 8](#_Toc368251053)

[Knowledge Management 9](#_Toc368251054)

[Service Operations 9](#_Toc368251055)

[Operations Management 9](#_Toc368251056)

[Incident Management 10](#_Toc368251057)

[Problem Management 10](#_Toc368251058)

[Continual Service Improvement 11](#_Toc368251059)

[Roles 11](#_Toc368251060)

[Baseline 11](#_Toc368251061)

[Service Measurement 11](#_Toc368251062)

[Service Reporting 11](#_Toc368251063)

[Service Improvement 11](#_Toc368251064)

[Benefits and Limitations 12](#_Toc368251065)

[Benefits 12](#_Toc368251066)

[Limitations 12](#_Toc368251067)

[Technical Requirements and Other Considerations 13](#_Toc368251068)

# Executive Summary

TatakPinoy Inc. is a Philippine-based manufacturing company engaged in the production and distribution of Filipino products. Currently, there is no real centralized IT department and most of the IT work is distributed among the different departments within the company. The top management is unsatisfied with this, since the promise and value of IT is not fully realized, and decides that a centralized IT department is feasible.

Several departments of TatakPinoy Inc. are having difficulties due to IT-related problems. The Inventory department needs a new vendor for their system since their current incumbent vendor does not satisfy user demands. The Raw Material Planning department’s system is to be integrated with the Inventory department’s system. The Accounting department has a very unstable server for the past 3 months and the Human Resources department has turned off their system temporarily due to the assumption that it has been hacked.

The solution proposed by The Cabs Consultancy Group involves transitioning from separate management of IT-related work and activities into one centralized group, the IT Department. Control of the various IT systems would be handed over to the IT Department and thus centralized servers must be implemented for easier management. Added to that, stricter security measures shall be implemented throughout the company so as to tighten the security and lessen the risk of hacking and compromising or loss of data. Along with these are important BCP or Business Continuity Plans for the departments regarding keeping these servers up and ultimately keeping the business running despite certain events. A DRP or Disaster Recovery Plan would also be set to really ensure business continuity despite such disastrous failures in terms of the system. The IT Department would also cover important service desks for its customers and clients as well as have a maintenance system with regards to making sure that the equipment mentioned along with the plan are well established and maintained.  Moving from there then, we also talk about how the company’s operations with the IT Department would be done as well as ways for them to improve.

This is achieved using the ITIL framework, namely service strategy, design, transition, operation, and continual improvement. We created recommendations for each of the major areas in the creation and managing of a more effective service. The goal of this is to streamline and integrate the internal IT services and processes so that they can be utilized to the fullest and operate with efficiency. By centralizing IT operations, IT costs can be managed more properly and even be reduced. Along with minimizing the problem of the cumbersome costs mentioned in the case, integration of all important data is also within the goals of the project. Keeping all these relevant data intact then through centralizing IT for the company would be more consistent as well as closer for higher management to keep track on so that they may make better decisions for the whole company and their business processes.

# Assessment of the Company

## Introduction

TatakPinoy Inc. is a Philippine-based manufacturing company engaged in the production and distribution of Filipino products. Currently, there is no separate IT department and most of the IT work is distributed among the different departments such as Human Resource, Inventory and Accounting Departments among others. This decentralized management of IT services is because the company purchased different software and made contractual development when they conducted their 3-year computerization program.

## Current Situation and Problems

The company, at least internally, has not been doing well. Various problems exist within TatakPinoy Inc. One problem stated was that the value of some, if not all, IT investments made has not been fully utilized. There have been a lot of programs and software bought over the past few years that haven’t been working well for the different departments. Some of the systems are not implemented well. This results to the slowing down of processes which adds up to the expenses of the company. Below is a list of the departments that have had encountered problems.

* Inventory Department
* Raw Material Planning Department
* Accounting Department
* Human Resource Department

The Inventory Department has issues and errors that are not addressed immediately by the vendor of the software they are currently using. One such issue is that the complaints of the users of the system or program seem to be overlooked by the vendor. Another is that due to the vendor’s lengthy response time, users are too often forced to do manual work such as counting and input of data. Based on the performance of the vendor, the vendor is slothful and is not effective if the company aims to improve the efficiency of the overall performance of its IT-related activities. This led to the decision not to renew the vendor’s contract, forcing the company to canvass for a suitable replacement.

As for the Raw Material Planning Department, it requires input from the Inventory Department to be utilized by their Raw Material Planning System. The process is done by gathering the inventory information printouts produced from the inventory count. The problem lies in the fact that employees have to manually input information found on the printouts into the Raw Material Planning System which takes up a lot of time. Also, this manual process would be vulnerable to human error which can be critical to the company because on the one hand, materials can be over-ordered which can result in degradation of excess stock. On the other, there might not be enough materials ordered which can result to lost transactions.

For the Accounting Department, the system poses a problem to the integrity and completeness of the financial records of the company. This is because of the unstable server being used. The problem increases the possibility of the financial information of the company being lost, which would greatly affect the operations of the company.

As for the Human Resource Department, their system appeared to be hacked or compromised. There have been complaints from the employees that their information has been changed. This poses a problem not only for the employees, but for the whole company itself because critical information of the company may be obtained without consent.

Putting the problems aside, however, the company possesses sufficient amounts of desktop computers for its employees and has already implemented a LAN and a WAN network that can be utilized to the advantage of the company. Some systems of the company also seem to be performing well and are not experiencing any problems such as the Order Shipping and Billing System and the Purchasing System that both currently have no issues.

## Proposed Changes

What the team proposes are the following changes. With the newly established IT Department, all IT-related work would be handed over to them, including the would-be replacement for the current inventory system. This would mean that TatakPinoy Inc. would have to hire IT professionals to handle and manage the department.

Next, because the IT Department will be controlling the systems, software, and networks of the company, we propose a centralized server/s so that management on the part of the IT Department would not be complicated. Also, with a centralized server, data would be consolidated to reduce data inconsistencies.

Lastly, we also recommend an implementation of tighter security within the company. Aside from preserving data integrity, this is also required to prevent unauthorized persons from accessing company data, systems and networks.

## Service Strategy

## Recommendation

As desired by the top management of the company, a separate IT Department is to be established. What we recommend is a centralization of control of the various systems that the different departments are using to improve their IT infrastructure. Using the current decentralized IT of the company as a point of comparison, a centralized IT department will be more efficient in terms of managing company-wide systems and processes, since everything is consolidated in a single location and everything is controlled by the IT Department. This would also promote data integrity and consistency for the company.

A central server then must be acquired and implemented wherein all the programs from the different departments will be connecting to. The rationale of this is that the IT Department will have control and that the data of the company would be consolidated into one single server as opposed to several servers across the company for different departments where duplication of data can compromise data integrity. This would also benefit the IT Department for easier control over the systems.

With regards to the Inventory Department, the group recommends that a new vendor be found immediately to keep the department satisfied and problem-free. Also, the department will be able to operate an efficient inventory system that would satisfy their business needs and negate the qualities that the previous vendor proliferated.The previous vendor’s work ethics were very destructive to the company’s business processes and in effect, overall output effectiveness and efficiency. Applying an IT system and/or protocols would also be in consideration in following the main plan of having a centralized department along with the necessary data to be kept consistent for the main system.

What has to be taken into account regarding finding a new inventory system would be to possibly integrate it with the Raw Materials Planning System. This, according to what the new CIO suggests, would help make the process of the business more efficient. By integrating these two systems, there would be just one instance of input of data into the system and the inventory printouts of the current system can already be dealt away with and in the process, save the company paper costs.

Lastly, what we recommend is for the company to implement better security measures to lessen or totally rule-out the possibility of unauthorized personnel from accessing the systems, the company network and critical information. The company must be provided with multiple security methods so that both internal and external threats are safeguarded from. It is important that the company receives extra protection from malware, which might compromise system security. Having the sufficient amount of security methods implemented will keep the critical information of the company safe and secure leading to the smooth execution of processes.

## Service Portfolio Management

The main objective of Service Portfolio Management is to manage the service portfolio, that which represents the list of services being managed by the service provider. Part of this is to define, analyze and distinguish which services are beneficial for the company and which are not. This helps the company in deciding what services they would offer.

In the case of TatakPinoy Inc., the service provider would be the newly established IT Department and the customers would be the other departments of the company. As stated above, a central server/s would be acquired and implemented so that the IT Department would have control over the various systems, programs and the company network. In line with this, the IT Department must be available and reachable 24/7 for concerns and issues of the departments as well as customers. Maintenance, and in extension upgrades and enhancements, would also be their responsibility as the continual availability and services of the systems is critical to the company. Lastly, General security controls as well as application security controls will be implemented and managed by the IT Department for a multi-level protection mechanism. This would be implemented using employee user accounts which, depending on their roles and positions in the company and their respective departments, would limit access to the systems and programs that they explicitly need for work.

# Service Design

Now that a vision of the changes in TatakPinoy Inc. is presented, a more concrete plan should be laid out for the service details and processes.

## Service Catalog Management

As mentioned earlier, the Service Portfolio includes support and maintenance of systems as well as security controls for the whole operations of the company. This will be maintained and documented by the IT Department for future use as they are also to keep historical data for the catalog of the service.

### *Business Service Catalog*

The business service catalog details all the services that are visible to the customers. It is important that these services are readily available and accessible for the users of the systems. With regards to security, mechanisms will be implemented throughout the different departments of the company. First, biometric fingerprint scanners will be implemented to restrict access to critical departments such as the IT Department, Accounting Department and other areas that the company may require to restrict such as the room where the central servers would be housed. Second, login controls would be implemented on the different computer terminals for the use of the employees. Login mechanisms would also be implemented for accessing the company network as well as for accessing the Internet. Lastly, employees would also need to login to the company systems that they will be using. Each employee would be given a certain level of accessibility within their respective systems (e.g. Top management having more access to certain segments, etc.). This will be made possible by providing the employees with their own user accounts which will be discussed more in detail in the following sections.

As an addition to the login mechanisms, as soon as the user logs in to the company network, a ‘Message of the Day’ window shall appear that will contain company-wide as well as department-specific news and announcements. This is so that all employees will be up-to-date with what is going on with the company and to be notified of any important announcements.

With regards to addressing issues and errors regarding the company systems, FAQ pages will be implemented for self-help, so that employees can resolve their problems they encounter with day-to-day activities. As a second line of support for addressing encountered problems, there would be an internal chat service that directly routes to the IT Department. Employees will be able to contact the IT Department for their concerns and questions through this service. With the assumption that the company has telephone subscriptions, this is also an alternative way to get in contact with the IT Department.

A separate external relations service desk is assumed to already be in place to answer the questions of the customers of TatakPinoy Inc. This is under the HR Department. Further questions that can’t be answered by the HR employees or questions that are too technical may be escalated to upper management or to the IT Department.

### *Technical Service Catalog*

As for the Technical Service Catalog, it will include the support services such as the maintenance of the company systems. Some of the employees in the IT Department will be assigned as part of an internal service desk that will answer all the questions and concerns of the employees of the other departments. Another service would be the handling, updating, and upgrading of the company systems, company hardware and other tools such as Microsoft Office and others.

Aside from the department-specific systems, another part of the Technical Service Catalog is the management and maintenance of the central servers. This is the most crucial part because this is where all the departments’ systems will be connecting to. Constant maintenance is a must so that the servers are running efficiently. Also, backups will be conducted for information security and preservation purposes.

Concerning security, The IT Department will be managing the biometric security accesses. For the login controls, each employee will be given an account which they will be using to log into the computer terminals, the systems, and the company network. Depending on the position and role of a particular user, some parts of the network or some systems won’t be accessible for him. For example, Human Resource Department employees won’t be allowed to access the Inventory Management System, whereas the Purchasing Department will be allowed because of the need.

## Service Level Management

A clear Service Level Agreement must be established between the IT Department and the other departments of TatakPinoy Inc. In this case, the SLA type would be a service-based Service Level Agreement.The need for this SLA arises from the issues of the current processes, which is slow and inefficient and prone to error.

This SLA ensures that the IT Department will deliver on their tasks and duties, which is to support all IT-related work and activity. On their part, they must deliver immediate service, or at an agreed upon response time, and help when asked by the users, something that the vendor of the current inventory system wasn’t able to deliver. This is critical because even a short interruption in the operations of the company can have a great effect.

The IT Department must agree to keep operations running at acceptable levels for all of the departments. Also, the IT Department must monitor their contribution to the company to verify that they are in fact providing benefits. The department must gather feedback from the different departments to adjust appropriately the areas that still need improvement. For instance, if a particular department is experiencing problems with the IT service provided to them by the IT Department, the IT Department should investigate the problems brought up, find solutions for the problems, and then implement the chosen solutions for improvements.

Complaints of the departments should be correctly managed by the IT Department to ensure that they are satisfied. The department must keep its relationship with its customers, the other departments of the company, strong so that better improvements can be made for the overall state of the company.

## Capacity Management

Capacity management deals with the balance between IT resources and the demand for IT services. It is important that the IT department will be able to meet the current and future requirements of the business. The IT department should be able to fully understand the demands that are required of them as of now and be prepared for the possible changes of these demands in the future. It is therefore the responsibility of the IT department to properly and regularly monitor the needs of each of the departments of TatakPinoy Inc.

In efficiently monitoring the needs of each department, the IT Department will be able to anticipate any future changes in their IT needs. Through this, the IT Department will then be able to continuously assess their performance with regard to meeting the IT needs of the different departments and continuously make improvements to their services to be able to meet the changing needs of the departments of the company. This will ensure the capacity of the IT Department to properly utilize its resources and meet future IT business requirements.

## Availability Management

The IT Department must ensure that all services that will be provided for the other departments will be available. In order to keep the services of the IT Department available, it is advantageous to implement proactive activities rather than reactive activities. The market that the company is operating in has a constantly changing environment. There will always be several competitors in the field that will surely improve their processes to keep up with the changing needs of the customers. Upholding this demands a company to keep their internal processes running smoothly and without any long-term interruptions. Therefore, the IT Department of TatakPinoy Inc. must make certain that IT needs and services across all departments of the company are always working properly. It would not be good for the IT Department to wait for the availability of their IT services in the company to deteriorate. Constant evaluation, maintenance and improvement of the services provided must be done.

There will be instances that certain services of the IT Department will be unavailable due to failure. Such things will happen and it is important for the IT Department to respond quickly and effectively to restore the services affected. It would be appropriate for the IT Department to implement IT hardware redundancy to reduce the possibility of the operations of the company from halting. Backup servers can be implemented so that when one or some of the servers in use fail, the IT Department can quickly switch to these backup servers so that downtime would be minimal.

## IT Service Continuity Management

Now this part of the service would need much critical planning if the company wants to be able to fully utilize the systems even if certain events may arise such as disasters and calamities that can potentially compromise and damage the systems. Here, we apply ITSCM or Information Technology Service Continuity Management concepts. First of all, a Business Continuity Plan (BCP) will be in order to assure that the company knows what to do in case disaster strikes in one or more areas of the business. This would include protocols regarding what to do if for example there is fire or an earthquake or if the system is down or being attacked.

If ever such disasters occur wherein damages may entail halting important business processes, there too would be a Disaster Recovery Plan (DRP) as part of the BCP wherein recovering important data would be involved. Referring to ITSCM concepts, the types of recovery plans would be related to the necessity of the speed of recovery with the significance of the departments from a business or operations process perspective. This would range from Intermediate recovery (Warm Standby) to Fast Recovery (Hot Standby).  An example would be how the central servers would require a Fast Recovery while the Raw Material Planning System may be more suited towards an Intermediate Recovery type of recovery plan.

## Information Security Management

For information security purposes, multi-level security mechanisms will be implemented. The first level of security would be physical controls which would include security personnel, backup power supply such as electric generators and UPSs (uninterruptible power supply), surge protection, and fire suppressants.

For access controls, biometric systems will be employed to restrict access to certain areas of the company. The next level of controls would be the login accesses for the computer terminals. Once logged in, users would have to log in again to the network upon the need and again into the systems that they would need to use. For data security, the concepts of minimal privilege (only the required information is accessible to users) and minimal exposure (only users that require the information should have access to the data) will be employed.

Aside from this, backup of the company data will be done. A GFS (Grandfather, Father, Son) scheme can be employed wherein daily backups will be conducted. On weekends, one weekly backup would be done and on month ends, one monthly backup would be conducted. An incremental backup will be used with this scheme wherein only changed data files will be backed up so as to keep in line with capacity management.

Other mechanisms that can be implemented are firewalls to protect the company network. The firewalls will incorporate features such as packet filtering and network address translation (NAT). This will ensure the company network’s protection from internal and external environments.

All security measures will be listed and detailed in the BCP. It will also include measures for disaster prevention and handling and steps for business process recovery to minimize the downtime of the company’s operations should anomalies occur. The BCP is a critical business document and its creation should be a priority of the company.

# Service Transition

With the strategy in place and the design intact, we go about the implementation of the system. In this section, we tackle about transitioning the system into the company and managing this crucial process. The IT Department then would be handling these processes.

## Service Asset and Configuration Management

Now the system would most likely begin keeping Service Lifecycle Configuration Items as it seems that this would be of top priority. The system involves integrating a stronger and more efficient IT system, thus many things in the life cycle would change as a result of this. It is hoped as well that the changes for these would only be minimal, with more emphasis on being more up to date to IT standards.

Another thing to be put into consideration is the Service Capability Assets that the system will yield and seemingly produce to see the project through. Primarily, this shows more on the idea of keeping workforce and service knowledge up to date and efficient with the flow of business. This then would include making sure that functions and processes are indeed working and if certain bottlenecks would be found, they can be solved immediately, especially if it does holds back the company.

The company should also keep in mind all related Service Resource Assets as the system is leaning more towards establishing a better and improved IT infrastructure. This would entail keeping track of the baseline equipment that the company will use in order to apply them in the system. After setting the company standards on the equipment for the significant operations, the IT Department will be responsible for keeping to date necessary hardware or software that is relevant to the systems, if such a need may rise.

After this, definitive Internal and Organizational Configuration Items need to be established. The ideal is that these would not have much changes towards the baseline processes. Having this, the company will have a basis for future activities that can change such as building a new service component or changing or improving processes for efficiency.

## Change Management

With the parameters and kinds of possible dynamic assets known, the IT Department also takes into consideration how to manage change if such needs arise within the service lifecycle and their assets. Within the context of ITIL best practices, change must indeed be managed well to keep it as minimally needed and as effective as possible.

Put into the context here then would be the changes that are most likely to happen. These would include changing hardware, software, and employees. Most of these changes are likely to include emergency changes (hardware/software failure, etc.) or standard changes (software/hardware updates, etc.). Such changes must always be gone through with the IT Department’s upper management before being implemented so as to properly manage and document such changes. All changes revolve around managing requests for change and escalating them accordingly to the important departments (and again, keeping upper management at top priority).

Along with such changes then should include back-up plans in case these changes fall to compromise the system rather than yield the result that was supposedly expected. This is usually to occur when something wrong happens during the change process itself. If all else fails, there is also the important and matching remediation plan which is able to roll back to a process/area’s past status especially if it was relating to hardware/software as well as any important business protocols.

## Release and Deployment Management

Assuming that the various systems of the different departments have their respective servers, it would not be a good idea to have a Big Bang approach for the deployment. Instead, the new design of the company systems, where they will be connecting to central servers, will be run at parallel with the current one so as not to disrupt the daily operations of the company. Little by little then, or using a phased approach, operations will slowly shift to the new centralized systems by first starting with one single department and then to the next until all departments are migrated to the centralized systems. Future updates and changes are expected to also follow this scheme.

## Service Validation and Testing

 Now with applying changes, the IT Department should also apply procedures for validating and testing new and changed services. This is to determine whether the service meets the “fit-for-purpose” and “fit-for-use” aspects which is important for it to be aligned with the service and stay within the conditions as well.

Any service change or new addition for any department would most likely be tested first by acting employees. They will be the most immediate users of such changes, thus it will be up to them to give initial feedback to the changes and new developments. Other feedback would follow from such tests may it be from the customers (e.g. tps involving clients may improve or delay performance, and clients will be first hand to see and prove such improvement or such in value). If such things happen, they would be escalated well to higher management for them to further deliberate what to do along with the professionals for the tasks and changes. This could be done from meetings to surveys depending on how large the change would be and how many the employees affected could be.

         Of course, it would not be enough to determine a service’s fit and efficiency if it were just the employees giving the feedback. Asides from the customers, it may be a good idea to hire professionals on the related fields of the changes to assess and perhaps audit them. Doing so, the IT Department and ultimately the company, could perhaps gain a better and more objective perspective to see better the service’s real fit and alignment to the business process and flow.

## Knowledge Management

 It is very important then that employees and staff are guided well in terms of delivering the service efficiently and understanding the value and data that they get to improve upon. This is the concept of Knowledge management that is to be at work. This is then where all the data and protocols are managed to simulate that progression from data to wisdom for better performance.

Knowledge management here then starts with important protocols and documentation on the services they provide and how to execute the services well. Ideally, this would involve the use of manuals wherein such procedures and explanations would be kept. These then could be taught by veteran employees to other employees to newer employees to carry on and continue the proper handling and execution of the service.

       A proper help desk should also be around to keep customers and clients knowledgeable about the products and services should they want to consult or report problems. This is to be an extension of the customer service should the company decide to extend portions of their IT infrastructure to customers (e.g. e-commerce, etc.). Though it wouldn’t be as technical, it is still very necessary to gain feedback as well at least in areas where repairs and work are needed.

Finally, records should be kept when it comes to Service Validation and Testing. The IT Department should be able to keep this data for further use such as developing a “best practices” document to aid employees into doing what’s best to effectively deliver the services. That document could also serve as some kind of preventive measure as well so that the company knows what not to do in the future so that they can deliver the services as well without having to go through the repeating their mistakes, which is very unproductive.

# Service Operations

## Operations Management

Operations Management is an area concerned with overseeing, designing, and controlling the process of production and redesigning business operations in the production of goods and services. Because all IT-related work and services are being transferred to the IT Department, there will be changes in the processes of the company. This is because the company lacks efficiency and effectiveness, and in addition to that the various problems they encounter in the current process. This slowdown of processes can and will entail additional costs and will also affect the business-side operations.

Within this area of Service Operations, the topic of the service desk is included as it is closest to the day-to-day operations of the company. This service desk would be run by the HR Department and they are to have the necessary databases and have the data needed to be able to see patterns to generate FAQs for customer troubleshooting as well. Service and product queries would be handled by this service desk and other questions that can’t answered can be escalated to upper management of an appropriate department for the specific resolution. A centralized service desk would be more appropriate as to complement the whole need for wanting to have a centralized system.

Now, bulk of operations management then would be in I.T operations management. As the company is going for a centralization of IT, much emphasis would indeed be put here to be able manage the employees well on the daily tasks. This would include being able to run certain tasks that would keep the data flowing and intact from the departments so that business flow would run as constantly and on schedule as possible. The protocols for these would then be maintained by the individual managers of the systems, wherein he or she is responsible for task scheduling and work assignments.

The I.T. operations would be supported and kept running by Technical and Application management. Technical management would include at least enough maintenance experts to be able to maintain the hardware that is around. They would be responsible for keeping track of them and making sure they are running well and as expected. The quality and performance then of the hardware would rely heavily on them. Adding to that, Application management is also important and to be considered with hardware as they would be the ones responsible for making sure the software and applications work as well as updating them. Managing the applications well would mean that hardware would be used to its fullest while still keeping within the range of good working capacity.

## Incident Management

The purpose of incident management is to be able to restore service operations as quickly as possible and to be able to minimize the effects of the incident/s on the business. The implementation of incident management is necessary because it allows the IT Department to be able to properly manage any potential or current disruptions to its services. Being able to properly manage these incidents include activities such as diagnosing the interruptions, efficiently finding solutions to these, and logging these incidents for future reference and prevention.

Incident logging entails that all incidents be logged with a corresponding date and time stamp. The following should be properly logged:

* total number of incidents and breakdown of each incident
* size of the incident backlog
* average time to resolve an incident
* percentage of incidents resolved
* percentage of incidents handled within the agreed upon response time
* the average cost of handling the incident

It is essential that these key metrics be logged by the Service Desk to ensure that history of incidents is available when needed to be referred to and so that correct analysis of incidents and the right course of action may be done for possible prevention in the future.

## Problem Management

For most incidents, the IT Department, and in extension the whole company needs to diagnose the root cause of these and determine solutions to the problems. These solutions are implemented through appropriate control procedures. Information about the problems should also be maintained, in accordance with Event and Incident Management, and specific fixes, solutions and workarounds must be planned out. Contingency plans must also be readily available with reference to Service Continuity.

For the business operations, as mentioned before there is a service desk that will handle all the concerns of the customers. For concerns that cannot be answered, a second line of customer support should be present. In line with that, problem escalation procedures must be defined such as which specific department the problem will be escalated to and the length of time a problem can stay on a certain level. With this, post-problem reports must be logged and recorded for future references.

# Continual Service Improvement

Looking back, we can see that the problem of TatakPinoy Inc. is rooted in the poor performance of some of its departments brought about by various problems. We propose a CSI framework that will bring changes in the IT Department of the company. As the company grows, IT operations will need grow as well and this will be more complex.

## Roles

To implement the framework successfully, a CSI manager must be appointed, who will ensure that the changes brought about by the CSI framework will be adopted and sustained within the company. The CSI manager will be held accountable for the success of the CSI.

Working alongside the CSI managers will be the Service Managers. They manage the development, implementation, evaluation, and ongoing management of new and existing products and services. They are also responsible for developing business case, product line strategy and architecture.

## Baseline

The baseline is an important starting point to highlight improvement areas in the future. Since the IT Department is just newly established, the initial performance of the proposed centralization of IT-related work and activities is to be the baseline. It is important that this is documented for changes that need to be done.

## Service Measurement

For Service Measurements, the IT Department must conduct an overall performance measurement of all IT-related services. It will not be effective to measure individual IT services because the company does not work that way. The company works as a whole, composed of different units working together towards a specific goal and this is why measurements must be done from start to end as one.

## Service Reporting

From the measurements gathered, past performance scores and ratings then can be seen. With that information at hand, the IT Department can then create a comprehensive report that shows what happened and what was done to address this. Also stated in this report should be solutions on how to prevent what happened and how to improve these services and processes in the future.

## Service Improvement

The last step in the 7-Step Improvement Process will be used for the Service Improvement process of CSI. The first six steps are already covered in Service Measurement and Service Reporting. The findings from Service Reporting, especially the solutions and improvements, will be used to formulate and implement corrective actions for the affected IT services.

# Benefits and Limitations

## Benefits

|  |  |
| --- | --- |
| **CHANGES IN THE COMPANY** | **BENEFITS** |
| Centralized IT Department | * A core group that will handle and control all IT-related requirements of every department * Improved IT infrastructure of the company * More efficient and accurate managing of all company-wide systems and processes * More efficient solution generation for all IT-related problems of the company * Reduced operation costs * Increased satisfaction of employees with regard to IT services |
| Centralized Server | * Consolidated data * Reduced data inconsistencies and increased data integrity * Aids in the proper management of the IT department |
| IT Professionals | * Added value to human resources * More defined roles in all things IT-related within the company * Assured competency in managing the centralized IT Department and Server * Faster and more reliable diagnosis and resolution of all IT-related problems |
| Added Security Measures | * Preservation of data integrity * Prevention of unauthorized personnel from accessing any classified data or information of the company * Prevention of loss of critical data or information in case of any disruptions to the company network * Backup of data |
| New Vendor for Inventory System of Warehouse Department | * Faster and more efficient response to issues and problems of the warehouse department * Increased reliability and reduced manual work * Increased satisfaction of warehouse department employees |

## Limitations

* Feedback quality of the IT infrastructure and all its components is not assured. This will depend heavily on the auditors they hire and the level of knowledge of their customers.
* In terms of security, there is no total assurance that the system will be unhackable.
* System failure is possible, even with hardware redundancy
* The centralized IT department may not be on par with expectations of top management

# Technical Requirements and Other Considerations

* We assume that all systems, except for the inventory system, is still capable and appropriate for business
* TatakPinoy Inc. needs to find a new vendor for Inventory System
* the new system should be able to integrate well with the Raw Materials Planning System
* The company needs to acquire new servers to be used as the central servers where all department systems will be connecting to.
* The company needs to hire a network specialist to connect all departments to the central servers and handle the company network
* The company needs to hire capable employees to handle the IT Department.
* The company needs to acquire biometric security systems for physical security controls.
* the IT Department needs to develop and implement login controls (personal workstation, company network, systems)