USING THE ITIL STANDARD FOR MORE EFFECTIVE IT DEPARTMENT MANAGEMENT AT A MODERN COMPANY

Luiza BRZOZOWICZ, Marek KĘSEK

Summary: Maintaining modern management support systems requires the organisation of a properly operating IT department. Particularly at mining companies, where not just production processes are supported but also staff safety, the correct operation of this department is a priority. Currently, IT is strictly connected with or even forms a part of the core business of many organisations at which intangible products cannot exist without information technology. IT service management constitutes a set of interdependent processes which assure the quality of IT services provided to the rest of the organisation. What helps in IT service management is the ITIL methodology, i.e. the Information Technology Infrastructure Library. This is a set of documents containing guidelines on how to organise the processes of service provision by the IT. This article presents the application of the ITIL methodology at an enterprise in order to improve the understanding of IT processes by the management staff, to raise the effectiveness and productivity while simultaneously reducing costs.

Keywords: decision support systems, information technology, ITIL standard, IT department, IT services, management, enterprise.

1. Introduction

Modern management support systems feature modules which make it possible to consider information about previous activities of the enterprise when making decisions for the future. This is particularly important at large companies, where the quantity of data collected necessitates the application of special analysis techniques. The Department of Industrial Economics and Management of the AGH University of Science and Technology carries out research aimed at developing an integrated system supporting the management of a modern mine. This system would use a knowledge base founded on reasoning rules generated from data recorded by companies.

The majority of conceptual and programming work load needed to build such a system is devoted to studying the development of algorithms making use of state-of-the-art scientific achievements and analysing the possibility of integrating existing software. However, the real conditions of operating the system within an enterprise cannot be ignored. IT system operation, implementation and maintenance is the job of the IT Department.

Looking back, IT departments used to have to deal with the entire organisation and their duties also used to include training and helping the staff. As time passed, IT started supporting almost every facet of business. As IT covered more and more forms of business, it was used more and more intensively to get a better insight into the operations conducted. Management Information Systems, Business Intelligence, data warehouses and data mining have become an indispensable part of enterprise operation and everyday tools of managers.

Currently IT is strictly connected with or is even a part of the core business of many organisations. Examples include banks, publishing houses, insurance companies and exchanges, whose dematerialised products cannot exist without the IT.

The growing complexity of IT and organisations' dependence on it has led to a situation in which business and IT can no longer be seen as independent. Many organisations now have a Chief Information Officer (CIO) as part of top management, and he/she plays the role both of a manager of technology, and of business, but this role is really about combining these two functions [1].

2. What is the ITIL standard?

IT service management is supported by the ITIL methodology, i.e. the Information Technology Infrastructure Library. This is a set of documents containing guidelines on how to organise the processes of IT service provision.

It represents the most widely accepted approach to IT Service Management in the world, and has become the undisputable global standard in this field. ITIL's roots go back to late 1980s, when a set of documents laying down the standards of providing IT services to UK government agencies was drawn up. The standards laid down in them turned out to be flexible and suitable for other sectors as well (industry, education, finance). 1991 saw the establishment of the IT Service Management Forum, a non-profit organisation promoting the ITIL philosophy. Last year, ITSMF opened its Polish branch, supported by companies like HP, IBM and others. These and other companies confirmed ITIL as the official methodology for IT services [2].

ITIL defined a coherent map of processes, relationships, roles, key terms and measures which has been generally adopted by the IT industry. It also introduced a service culture in IT organisations. In Poland, this industry is also following the path charted by the more mature markets of Western Europe and the US.

ITIL offers a wide set of best practices developed by the public sector and private companies from all over the world, which are universally followed as well as actively supported by training and exam centres, IT service providers, in-house IT departments, vendors of tools for IT, customers and users of IT services and consultancies.

ITIL represents a set of comprehensive recommendations from the IT sector which became the starting point for an international IT service management standard – ISO/IEC 20000 Service Management.

In late May 2007, another update of the standard was published, marked ITIL V3, which has brought about a 5 new publications that demonstrates the complete lifecycle of an IT service [3].

The ITIL philosophy is based on providing and managing IT services through processes. The ITIL skeleton defines management processes, their inputs and outputs as well as links and the responsibility scope. Currently, the set of ITIL publications authorised by the ITSMF comprises 40 literature items describing primarily the best practice in implementing process-oriented IT service management which ensures long-term cost reduction, service quality improvement, customer satisfaction and allows one to obtain an ISO certificate from the 9000-2000 group [2].

Following ITIL guidelines mainly means:

- Reducing costs – managing IT as though it were the business;
- Communication – a common concept of the IT world and a communication structure;

- Customer relationships – focusing on business benefits (looking at IT through the eyes of the business);
- Quality management – continuous organisation improvement.

The ITIL process model provides a holistic view of IT and structures the entire organisation, not just its selected parts. As a result, it makes the concepts coherent [3].

3. Principles of_ ITIL application

ITIL describes best practice in IT service management which should be used to draw up detailed procedures and instructions adjusted to the specific nature of services provided by the company implementing the former.

Guidelines from the ITIL library chart the directions of action to improve IT department effectiveness. They point out the most common errors, explain how to avoid them, suggest solutions which have successfully worked out at many other organisations. One should not look within ITIL for specific procedures and instructions ready for application at any organisation. No methodology could provide these, as the specific nature of every company's operation makes them impossible.

ITIL cannot be implemented, because it is not a tool. ITIL is a series of guidelines that are valuable – due to being tested in practice – and precise and which will help develop procedures and instructions necessary for the correct operation of every organisation. ITIL calls this the 'adopt and adapt' approach.

The ITIL process model provides a comprehensive description of the entire IT organisation. However, deciding to transpose it in its entirety in one go and adopting it for the purposes of the organisation is a recipe for disaster. This area is too broad for a project like this to succeed. Consequently, the process has to be split into stages, keeping in mind the strong relationships between individual areas, as implementing one process in isolation from the entire model makes little sense either [3].

4. Applying ITIL standard processes at an enterprise.

The enterprise at which the ITIL standard is being implemented provides operational leasing, i.e. services consisting in leasing car fleets and managing them. Its staff of around 60 manage over 6000 vehicles. As the core business of the company consists in long-term leases, is main goal is to keep long-term customer loyalty by ensuring high service quality, flexibility, outstanding offers and long-term expertise in the Car Fleet Management (CFM) sector.

The organisational structure of the company is made up of six main departments whose directors, just as the internal auditor, report straight to the director general. The IT department manages the ICT infrastructure, security, technical support for users, new IT solution implementations, reporting, IT system deployment. This department is split into two teams:

- Support team – responsible for managing the ICT infrastructure (network, hardware, software, licenses, fixed-line/mobile phones) and for the Help Desk providing technical support to users (incident, change and problem management).
- Development team – in charge of deploying new IT solutions.

The service life cycle, in accordance with the ITIL process model presented on the authorised ITSMF website, is made up of 5 stages, each of which contains the processes listed below:

1. Service strategy;
2. Service design;
3. Service transition;
4. Service operation;
5. Continual service improvement.

Below, the individual processes are discussed, and their implementation and practical usage in a service company are described. As the ITIL methodology has been present in the Polish market for only a short time while the company is classified as an SME (small and medium enterprises), there are elements or processes which have not been used in practice, some have been modified, while the implementation plan is only being formulated for some others.

1) **The service strategy** is used by the IT service provider to define its own strategy and methods of operating in accordance with it. The ideal situation for the IT department is when it forms an organisationally and financially isolated unit, i.e. an external IT service provider (a company within a company). Then Service Level Agreements (SLAs) are signed with regard to service provision and they regulate the level of IT services provided by way of the price to be paid by the supported departments (customers of the IT department). Unfortunately, such a situation is only found at large enterprises.

   In our service company , which is a small/medium enterprise, the IT department operates along the same principles as the remaining departments. In this situation, service portfolio management has a financial nature and is mainly limited to managing a predefined budget which is split into current expenses and investments.

   Before planning investment projects for the following year, the IT Department Manager collects information on hardware or applications needed by other departments. The cost of these services as well as the financial capability of the company are established and a decision is made on the planned expenditure and specific projects for the following year.

   One of the key tasks of the IT Department Manager is to manage finances, i.e. control that the budget allocated to this department is not exceeded. This is done in three complimentary ways:

   - Financial reports – monthly tables of expenditure on IT department work and purchases, confronted with budget assumptions. This way, expenditure is controlled on a current basis and if significant variances are detected, quick reaction is possible. In addition, such financial reports help plan the budget for the following year.
   - Purchase requisition – if the IT department is to incur capital expenses, i.e. buy a computer or a printer, a Purchase Requisition must first be received. The Requisition may be in writing or by e-mail and may be submitted only by managers of specific departments. At the end of the month, the director analyses the IT budget situation and a decision is taken on the quantity and type of purchases.
   - Change implementation – if the company needs to change the existing IT solutions or deploy new ones, the IT Department receives a “Change Request”. Based on the

assumptions and the description of the final product contained in the Request, the cost and the labour outlay is estimated, and then, together with the expected benefit, it forms the grounds for taking a decision on the legitimacy and the date of implementing the project.

2) **Service design** consists not just in designing new services, but also in modifying existing ones. In this process, the level of provided services should be defined, described in detail as well as approved by both the service provider and the buyer. An agreement, written or verbal, should detail the type of services, their quality, availability, downtime, and give a usability warranty. Obviously such agreements are rarely used at smaller companies, so they can be replaced with a Service Catalogue, which also serves as a single, coherent source of information on the services provided. This requires specifically defining all the services provided by the IT department and their related processes, splitting them into business and technical categories and determining the required support the IT staff provide for them. This is a very useful tool for people working for this department, as it clearly tells them what their duties are. They can thus avoid many misunderstandings with other staff, who frequently ask IT specialists for help in using software like MS Excel or fixing office equipment like shredders, which has little to do with their real responsibilities.

When designing services, particular attention should be paid to information security. This process usually forms an element of the Security Management process within the whole organisation and also covers paper document handling, facility access control and telephone connections.

At the company discussed here, the Security Policy covers several areas:

- Network (technical) security – mainly associated with using the Internet. To avoid possible intrusions from the network, antivirus software as well as security updates for the Windows environment or the MS Office software suite are applied. In addition, the company uses its own applications which continuously monitor Internet use by the employees and send notifications to the IT department when a threat appears.
- Information newsletters – every employees is regularly informed, electronically or in writing, of the current security rules, changes to company security policy or rules of using all IT programs and the Internet. He/she then has to review such a notification and acknowledge that he/she agrees to it.
- Rights – data access is secured in two ways. Firstly, only IT department staff can access the server room. In every instance, they must sign the guest list, fillingin their personal details, the entry and exit time. The second way consists in making data confidential. Obviously, only company employees have access to applications and information after an electronic account is first sets up on the appropriate server and approved by IT staff. There are specific level of access to documents, for example access for all employees, for employees of a given department or for department managers.
- In addition, there are three types of network folders: assigned to a department, e.g. Administration; specialised, topical, e.g. Contracts; and shared, i.e. generally accessible. Such folders are accessible to a limited number of users, and this access is based on read/write rights granted by the owner of the folder, usually the manager of the department from which the data stored in that folder originates.
- Defined controls – these are predefined regular controls aimed at the regular verification of data security. Every IT department employee is assigned specific

controls of selected IT areas, and after completing them he/she executes a report and sends it to the manager.

- External Security Audit – as the company is a member of a multinational corporation, the parent corporation board imposes guidelines about corporate operations, including data security, on the branches in various countries. Then, once a year, an external audit is carried out to check the level of data security, and if the adopted criteria are not met, it specifies what is to be improved or changed.
- Recovery procedure – this is to protect data from being lost as a result of a failure, a natural disaster or an attack from the Internet. Data from disk drives is archived and stored on external storage media kept outside company offices. Data is backed up at defined intervals. The frequency of those backups complies with the adopted corporate security policy which balances the cost of making and keeping the backups with the duration and scope of data recovery demanded by the business, which is one week in the case analysed here.

Data security is strictly connected with the continuity management of IT services. In case of a crisis, the company must have a plan of how to recover core business as soon as possible, including computers, systems, the network, applications, data warehouses, telecom hardware, the environment, technical support and the Service Desk.

Drawing up the IT service continuity plan consists of several stages:

1. Selecting scenarios – determining events which may compromise company operations and for some of them, for example the most probable ones (a flood, a fire, an Internet attack), formulating an overall plan of recovering the company's operations.
2. Service list – a list is drawn up of processes, services and applications which must be recovered for the company to be able to operate. Then, two parameters are established:
   - RTO (Recovery Time Objective) – this is the time counted from the incident within which the service is to be recovered, e.g. within 24h or 48h;
   - RPO (Recovery Point Objective) – specifies how much data (since when) should be recovered, i.e. how often the Backup Procedure is repeated. In practice this is equal to the range of data the company can afford to lose.
3. Plan – the last step is to develop the procedure for recovering IT services and company operations. The plan should be divided into stages, e.g. the first 24h, 48h, 72h, 1 week, and it should defined which services will be recovered at subsequent stages, as well as what steps are to be taken for this purpose.
4. Control – during the year, tests and simulations of executing ITSCM procedures should be run to check their practicability and to remedy possible errors.

3) Service transition prepares the IT service provider to commission a new or a modified service and provide it in accordance with the SLA agreement. It includes planning all stages and coordinating resources required at those stages. As part of it, the risk of failure during activities associated with commissioning the service is identified, managed and controlled as well. A new service can be planned using a form containing some basic questions: Who is the author of the idea? What is the reason or business requirement for deploying the new service? What is its scope? Advantages and benefits of deploying it? The cost of creating, launching and operating it? Then a group of several people, preferably management staff, take a decision and if the new service is accepted, it is put on the Project List and transferred to the IT department, which deals with planning it and preparing for its deployment.

After the launch of the new service is accepted, the next stage is change management. This consists in the detailed planning of launch stages so that after the service is launched its negative impact on the remaining applications is minimised and the company's core business is not interfered with. Changes can be divided into three types:

- Normal – changes described above, requested e.g. using the form. These concern company development, i.e. launching large format services which gain the status of a Project, and whose planning and launch requires a lot of work.
- Standard, or preauthorised – these are requested by authorised persons (usually department managers) and concern known and formalised procedures. Instances include the preparation of a work station for a new employee, setting up an e-mail account, granting access rights.
- Emergency – analysed outside the queue and most frequently related to the work of the IT department, such as the risk of failure, a threat to network or server security.

Companies usually provide many different services for whose handling several or even over a dozen applications are used. In this situation, the Knowledge Management process is a useful tool. This tool is to improve the productivity of IT services by reducing the need to regain knowledge and assure that the appropriate persons have the appropriate knowledge at the right time to provide and support the services needed by the business.

In practice, the Knowledge Management process mainly boils down to recording tried and tested solutions in the form of procedures allowing IT department staff to quickly and efficiently deal with an incident or problem that has arisen, identify the request as a 'Known Error', install or configure a given application or system. All such instructions are recorded in shared files split by the area they concern or the type of application supported and are published on a server dedicated to IT department staff. As a result of such procedures, if a failure occurs, the step by step way of proceeding is known. An IT Knowledge Base thus compiled is supplemented with instructions from external service or software providers supplied in case problems appear.

Additionally, end users are provided, within a distinguished directory, with a set of user guides for individual systems or applications which every new employee has the duty to learn.

4) Service operation coordinates and executes actions necessary to provide the business with IT services at the agreed level. It is responsible for managing the IT systems and infrastructure used to provide and support services.

Processes supporting service operation in the production environment are as follows:

- *Incident management* – acts as a fire-fighter to restore the IT service for the users as soon as possible, minimising the negative impact of the incident on the operation of business processes. An incident means any event which is not a part of the regular operation of the service and which causes or may cause an interruption in the provision of, or reduce the quality of the IT service (e.g. a printer failure, delays in delivering e-mails). Incidents are frequently detected by the Event Management process or are notified directly by users who contact the provider using the Service Desk function. Incident management quickly and effectively cures failure symptoms by using standard workarounds. The analysis of root causes of the failure and remedying them is the job of the Problem Management process.
- *Problem management* – its purpose is to prevent incidents from happening and to minimise the impact of those that cannot be prevented. A problem means an

incident or a group of incidents for which there is no ready solution and whose remedying requires analytical activities to be undertaken and/or a project to be implemented (e.g. a frequently occurring error in a given application, repeating erroneous invoice printouts). When it is impossible to remedy the notified incident immediately, it is reclassified as a 'Problem' and then subjected to a joint analysis by the IT department, which may result in: 1) finding a quick fix and implementing it; 2) finding a solution which, alas, requires a 'Change' (an order whose fulfilment requires changing a configuration, a procedure or another element of the IT infrastructure, for instance adding a new functionality to an application) or a 'Project' (a job which requires a complex approach, such as the analysis, execution, implementation and testing, for instance reconfiguring the telephone switchboard). Then its cost and labour requirement is determined, and the project may be accepted and added to the project list, or rejected, e.g. because the cost is too high and it is then classified as a 'Known Error'; 3) the problem cannot be solved, e.g. because the suitable technology is not available, so it is classified as a 'Known Error' straight away.

- *Request fulfilment* – allows users to request standard IT services and receive them, obtain information on the services provided and their maintenance procedures. In practice, requests mean all notifications of users which are not classified as incidents or problems, i.e. are not associated with failures. These may be enquiries about the provided services, procedures, orders and user complaints.
- *Event management* – an event is understood as a change of the status that is material for managing configuration elements or IT services. It is not equivalent to monitoring, but is dependent on monitoring. Event management generates and detects notifications while monitoring checks the status of components, even if no event has occurred. In practice, events occur at a company in addition to incidents and problems. They may have the nature of a message or a notification and concern non-standard changes occurring in the IT structure which require reacting to and taking the appropriate steps. They are executed by special programs which continuously monitor the condition of the network, its configuration and components, or by a user. Two main types of events can be distinguished:
  1. Notifications from the antivirus system whose job is to completely secure servers and users' PCs both from malware and from attempted attacks from the network;
  2. Notifications from WSUS (Windows Server Update Services), which is a system of automatic updates that install necessary software on servers and users' PCs, both for security reasons and to improve application running.
- *Access right management* – allows authorised users to access IT services, data or other resources. This process comprises identity and rights verification, granting access to services, access recording and logging, deleting and changing rights when the status or role changes. The first step the company has taken to ensure security and prevent unauthorised access was to introduce physical restrictions. The data centre is a separate, air conditioned room housing servers, which only IT department staff can enter. The entrance is secured with a reader of access control passes which are registered to individuals, so it is precisely known who and when entered and left the room. The room is fitted with a special alarm system which texts a mobile phone in case of a break-in, flooding, a fire, excessive temperature,

a power failure (although there is an emergency backup system providing uninterrupted power supply for at least 40 minutes).

The management of access rights necessary to use the company system was split into several areas: access to the corporate network, access to network folders, access to business applications. For security reasons, it is not allowed to use a Wi-Fi network within the company premises while access to the local corporate network is only possible from within the offices, after a user account is created and linked with at least one group or department. Access to network folders is based on a folder list containing: folder content description, its purpose, physical location, people in charge (owner, administrator), set of users using the folder, information on access and limits. Folder owners must be department managers assigned to a given folder depending on the purpose or contents of the shared folder. There are two access levels possible: read or write. The request for creating access must be authorised and made by the owner of the folder. Access to applications is based on defined Application Sheets containing: the general operation description, persons in charge of the application (owner, administrator, experts), technical installation and configuration specifications, purchase and licence information, list of users with the history of access rights granted to them, a log of changes to application functionalities, a rights approval log. The list of rights is created independently for every application and rights are changed at the user level. The application owner is the manager of the department most concerned with the application due to its purpose or contents. Only he/she can order an account to be opened in the application. He/she is also responsible for granting rights, access changes, freezing or closing accounts.

5) **Continual service improvement** serves to evaluate and improve the quality of IT services, the general maturity within the service lifecycle and the related processes.

The objectives of Continuous Service Improvement are as follows:

- Review, analysis and recommendations of improvement opportunities at every stage of IT service provision;
- Control and analysis of results achieved;
- Identification and implementation of specific activities to raise the IT service quality as well as the productivity and effectiveness of service management processes;
- Improving the cost efficiency of delivering IT services with no deterioration in customer satisfaction;
- Ensuring the use of the appropriate quality management methods to support service improvement activities.

The greatest problem at a company is the use of an excessive number of applications which cause a lot of difficulties in the communication between departments, in integrating data between applications and in the management of IT services by IT support. Creating one coherent database for all programs used at the company and available to all employees should be the management's first step to raise productivity and improve the quality of services provided by the IT department. All applications would still be used for their basic functions, as the purchase and deployment of new ones would not represent cost-effective investment, but the information contained in them would be kept in a single database, so that it could be utilised in reports, analyses and projections.

What could be very helpful would be to apply a database consistent with the OLAP Cube, as very many requests to the IT department concern reports and executing

analyses. The OLAP cube is a structure that stores data in a way resembling multi-dimensional spread sheets. It allows manipulating and analysing data from different perspectives (in various dimensions, e.g. financial figures can be analysed according to the service, price, time, city, type of income and cost). Obviously, rolling out such a complex database would initially cause a lot of problems to employees. It is probable, however, that in the longer term and after the appropriate training has been given, the use of a multi-dimensional, coherent database could bring down the number of requests concerning applications, as a result of which IT department staff could devote more of their time to, for instance, company development. In addition, the effectiveness and productivity of employees would rise as a result of improvements in the information exchange between departments or the execution of analyses or reports.

However, creating a multi-dimensional database would be just a single step solving only one current problem, whereas the more effective operation of the enterprise requires the continuous improvement of processes running in it and the constant improvement in the quality of services provided.

A good solution could be to start regular meetings of all department managers or of employees who have extensive knowledge of a given area or a lot of experience. This team would analyse processes running within the enterprise, think about the opportunities and ways of improving them, estimate the cost and the risk of introducing changes as well as set the directions and the priorities of innovative activities.

5. Final conclusions

IT service management constitutes a set of interdependent processes which assure the quality of IT services provided to the rest of the organisation. Its main goals include:

- Providing IT services to the customer;
- Aligning IT services with the organisation's goal;
- Drawing up and managing cost-effective agreements for IT service provision.

Strategic IT applications consist in the information systems operated at the company, which directly contribute to gaining a competitive advantage on the market, and technological solutions supporting the formulation, implementation and modification of the strategy.

The ITIL methodology helps manage IT services. It consists of a set of documents containing guidelines on how to organise the processes of service provision by the IT.

The ITIL standard divides IT processes taking place within the enterprise into five areas:

- Service strategy;
- Service design;
- Service transition;
- Service operation;
- Continual service improvement.

The analysis of IT processes running within the enterprise in the light of the ITIL methodology allows the following benefits of using the ITIL to be distinguished:

- Aligning IT strategies and IT services provided with the organisation's goals and strategy;
- Using IT to raise the effectiveness and productivity of the organisation’s operations as a result of automating repetitive tasks and processes and improving the communication and information exchange between departments and employees;

- Raising the innovation of the enterprise, leading in turn to achieving competitive advantage on the market;
- Reducing costs by managing IT as though it were a business;
- Using information technology for the continuous improvement of the enterprise operations and services provided;
- Structuring the processes and tasks of the IT department makes them understandable to other employees and the management of the enterprise, thus improving communication between IT and business.

References

1. De Sutter J.: IT Potęga technologii informatycznych. Wydawnictwo VIZJA Press & IT, Warszawa, 2007.
2. Łagowski J.: ITIL – Zarządzanie usługami IT poprzez procesy". XI Konferencja PLOUG, 2005, http://www.ploug.org.pl/konf_05/materialy/pdf/07.pdf, 25.09.2011.
3. IT Service Management, http://itsm.itlife.pl (http://itsm.itlife.pl), 16.09.2011.

Research financed with state budget funds for science in 2010-2013 as research project N N524 468939

Luiza BRZOZOWICZ, M.Sc., Eng.
Student, AGH University of Science and Technology, Krakow
Department of Industrial Economics and Management
AGH University of Science and Technology, Krakow
30-059 Kraków, Al.. Mickiewicza 30
e-mail: lbrzozow@o2.pl

Marek KĘSEK, Ph.D., Eng.
Department of Industrial Economics and Management
AGH University of Science and Technology, Krakow
30-059 Kraków, Al. Mickiewicza 30
(+4812) 617 20 77
e-mail: kesek@agh.edu.pl