An IT Service Reporting Framework for Effective Implementation of ITIL Continual Service Improvement Process Conforming to ISO/EC 20000

Mohammad Kajbaf, Negar Madani, Ali Suzanger
ITSM department
Infoamn IT Consulting Co.
Tehran, Iran
{m.kajbaf, n.madani, a.suzangar}@infoamn.com

Shirin Nasher, Mehrdad Kalantarian
Computer Engineering Dept.
Iran University of Science and Technology
Tehran, Iran
{nasher, kalantarian}@vc.iust.ac.ir

Abstract—**In this paper, an IT service reporting framework has been presented to help organizations in implementing IT service improvement process in accordance with ISO/IEC 20000 PDCA-cycle and reporting requirements. It defines six types of reports and includes guidelines for automation of these different types. Afterward, a process for reporting by focusing on defining report templates based on the organization requirements is provided. Proposed report types, process flow, ARCI matrix, and, process integration points as a general IT service reporting framework, helps organizations to organize their communication using reports.**

Keywords-IT service management; continual service improvement; service reporting.

I. INTRODUCTION

A. Service Improvement in Different ITSM Frameworks

Different ITSM frameworks and standards have discussed service measurement and improvement. ISO 20000 requires continual improvement of IT services via the PDCA cycle. It also defines requirements for service reporting to measure, analyze and communicate observations to help improvement of organization activities [1].

The continual service improvement (CSI) is one of the main aspects of ITIL v3; it includes a 7 step process for IT service improvement [2].

The CSI process includes 3 main activities: (1) defining metrics for measurement of activities and service performance; (2) monitoring, measuring, reviewing and reporting defined performance metrics; and, (3) taking corrective actions to improve service performance [3].

In MOF v4, the improvement concept is inherent in the MOF lifecycle, but there is no explicit process or service management function (SMF) in charge. Two management reviews cover measuring performance of IT services and processes, and taking corrective actions: the Policy and Control review and the Operational Health review [4].

In COBIT, the Monitor and Evaluate domain covers reviewing, monitoring and continual improvement of IT services. It includes defining performance indicators and reporting them, acting upon deviations, third-party reviews, and, integrating IT reporting with business reporting [5].

B. Toward an ITSM Management Model

The ITIL® framework is a major source of good practice in IT service management (ITSM) used by organizations worldwide [6]. ITIL defines many policies and key performance indicators (KPI) for different IT services and processes. Although ITIL describes policies and rules for service reporting process in the CSI book [3], it does not clearly define how the process must work.

Organization that are implementing ITIL for the first time, face new challenges. One of them is taking the correct approach in defining performance indicators, and measuring KPIs and reporting them. For most organizations the implementation of true common cross-organizational management processes may be the most difficult aspect of the ITSM project [7]. They need to know how to find which processes are working and which are not.

Keel *at al.* [8] discuss some main challenges in adopting ITSM. It suggests that successful implementation of ITSM strategy relies on the quality of processes.

Keeping sight of return on investment (ROI) and balance, of cost, time and quality is of a very high importance for companies [9]. Lahtela *et al.* [10] suggest an ITSM measurement system to support improvement activities. Lima *et al.* [11] propose a model to quantify IT service quality, to enhance the "Check" phase of PDCA cycle.

In Section II, description of the problem is provided. Main aspects of the provided framework are defined in Section III, and the process flow is presented in Section IV. Section V lists terms and definitions, and Section VI describes future works.

II. DESCRIPTION OF THE PROBLEM

Many problems would arise during implementation of IT security and service management frameworks for customers, especially if they are implementing a business process model for the first time. Employees do not know what they must do, and managers do not know what to expect from them. One of the main areas of ambiguity is the improvement process. By investigating problems in implementing ITSM for customers, we established a reporting structure to decrease ambiguities.

At the first sight, the structure seems like some extra work required from employees. At final steps of the project, all parties can relate their day-to-day activities to concepts they were familiarized with during their ITIL/ISMS classes. For successful implementation, reports must be such that all parties have a common understanding on them.

The proposed service reporting framework is a tool for organizations to clarify their internal communications and simplify defining and monitoring KPIs and metrics, and thus the CSI process. The reporting process helps managers to define clearly what they expect in each activity.

III. IT SERVICE REPORTING FRAMEWORK

Our proposed service reporting framework contains 2 parts. First, a hierarchy of reports for different activities of ITSM is defined. This hierarchy includes six types of reports for different activities of operational, tactical, and strategic types. Then, a Service Reporting process is proposed for defining report templates according to the reporting requirements of the organization. This process could be implemented as a sub-process of ITIL continual service improvement process.

A. Report Types

There are different types of reports in an organization. Some contain low level details of daily observations, while the others are based on high level analysis and contain conclusions required for decision makers. Considering all the activities in the ITIL framework, and by investigating different types of reports communicated internally in our customer companies, six generic types of reports have been identified. Then, they were refined based on the level of activities, the material included in each report, required level of analysis on each and required competency for it.

1) Reporting routine tasks

This category of reports is of operational level, about happenings, successes and failures in on-going daily activities of operation and monitoring type. Audiences include section managers or process owners, whom are accountable for the task. Low amount of analysis is required, and, the report must include patterns, frequencies, time intervals, inconsistencies and extermums in observations. They are often scheduled for small periods of time, from a few times a day up to once in a few weeks.

2) Reporting assigned tasks

This category is of tactical level, about the progress of projects (for teams) or assigned tasks (for persons). These reports are usually in design, development, deployment and implementation activities. Audiences are project or function managers, or the change advisory board (CAB) (in the case of new or change services). They contain some basic analysis on the progress of the project/task, achievements, pitfalls, remained works, estimations, lessons learned, etc. They are always pre-scheduled based on the project/task steps or small periods of times from once in a few days up to once in a few months.

Two types of reports discussed above were about measuring activities in IT processes. The next two types, in contrast, are mostly about IT service measurement.

3) Reporting on events

This type of report is of operational level and is about low level data on events. The data are usually gathered in operation, monitoring and support activities and contain summaries of different types of events in IT services, specially security events, or details of a major/critical event. Detailed data included in reports are defined in the Event Management process.

Audiences are operation and related service managers. In the case of major events, managers of affected services, owners of related monitoring processes, and, the incident manager, are included.

In the case of normal events, summaries and number of different events are included in the report. In the case of major events, descriptions of events, decisions made, activities done, and the results gained, and some calculations on impacts and costs may be required. Normal reports on events are scheduled mostly for small periods of time, from daily up to weekly. Reports on major events are not scheduled but reactive due to the nature of events.

4) Reporting on services

This category is of a tactical level and is about service status data. The included data are gathered and analyzed in monitoring and service management activities. The reports include current and predicted service levels, statistical analysis and trends, user complaints and customer satisfaction measures, measurement of metrics defined in SLAs, OLAs and contracts, and breaches in agreed levels, as well as prediction of required resources and capacities against target levels.

Audiences include service managers and the portfolio, service level and CSI managers, as well as business or external customers about status SLA-signed services. The scheduled periods are of a medium level, from weekly up to once in some months. For business and external customers, reporting schedules are defined in agreements. Out-of-schedule reports may be required due to proactive monitoring or where service level breaches.

5) Reports on review meetings

These reports are of a strategic or tactical level and are produced after review meetings in different phases of IT service management. They always contain summary of discussions, ideas presented by different parties, and details of decisions made, tasks assigned, and further activities/meetings scheduled. Decisions must often be reflected in other types of documents, such as policies, plans, contracts, etc. Therefore, the report must include all required details discussed in the meeting. Report schedules depend on meeting schedules.

Audiences include all attendant parties, as well as, CSI manager, and other relevant IT managers. If decisions include changes to the existing documents, IT services or the infrastructure, the report must be provided to the change manager as well.

The meetings include, but are not restricted to, CAB and emergency CAB (eCAB) meetings, portfolio management meetings, service and technology designers meetings, meetings between development teams, meetings with suppliers and business or external customers, post implementation reviews, non-conformances, etc.

6) Management reports

This category of reports is of strategic level and is about all high level aspects of IT services and ITSM framework. Audiences are top IT and business management officers, the CSI manager, and other parties as defined in the *report template*. Management reports contain analytical data on the performance of IT services, trends, suggestions and

prospects, costs, risks and values, performance and achievements of IT processes and functions according to defined KPIs, demand and market analysis, new methods and technologies, etc. Analysis on business achievements against strategies and objectives or new suggestions may be required.

In summary, this category of reports reflect all the other types of reports to the top IT and business managers. All six types of reports are presented in the table below.

TABLE I.   SUMMARY OF DIFFERENT REPORT TYPE SPECIFICATIONS

Different Report Types				
Report Type	Types of Activities	Types of Audiences	Included Material	Analysis level
Routine Tasks	operational, monitoring	section managers, service owners	happenings, summaries, inconsistencies, observations	low
Assigned Tasks	development, deployment	project/section managers	progress, achievements and pitfalls, learnings	medium
Events	operational, monitoring, support	section managers, service owners	summaries, descriptions, actions done	medium
Service Status	service management, monitoring	service managers, business customers (against SLAs)	service status, statistics, customer satisfaction	high
Review Meetings	management, planning, relationships, development	Top management, design and planning teams, customers	decisions on policies, plans, objectives, strategies, agreements, …	high
ITSM Framework	planning, strategy, service management	Top IT/business managers	measured KPIs, trends, costs and benefits, conclusions	low, medium, high

B. Automation Level

Another factor which can be defined for reports is possibility of using automation tools. Different automatic tools for reporting network and security events and measuring service performance exist. Using these tools for reporting, helps employees in measurement and reporting and decreases human errors. They also ease scheduling of reports. Therefore, we suggest customers to use automated reporting systems, as long as it helps IT personnel in doing their activities at best.

For routine tasks, automated tools are widely present which provide data forms for employees to fill. These tools help employees to generate reports on schedules and usually help to communicate them directly to audiences.

A similar approach for reports on assigned tasks and review meetings could be taken. However it could not cover all aspects of these reports, because they include many analytical data. Therefore, often templates are prepared and rules are defined to fill them.

High levels of automation could be used in event reporting. Different tools for network and security events reporting exist. They automatically gather data and generate reports on their summaries, using different methods like web-services or intelligent agents [12-14].

These tools are often used to provide required data to operators to compose event reports. Therefore, audience of automated event reports is the operator/administrator in charge. In the case of major events, automated systems could alert the incident resolver in charge, the service owner, or event trigger an automated troubleshooting system.

Automated performance measurement systems could be used to gather and analyze service level data and help the report owner in composing the service status reports. they can automatically measure service levels and identify SLA breaches [15-16]. These systems could also alert service manager and person in charge, when a critical service fails.

Reports on ITSM framework are hard to automate. Different systems exist to gather and analyze data, draw charts and even analyze different aspects of a decision and suggest a choice. However, decision making is one of a few activities which still require a human in charge and cannot be fully automated.

Table II demonstrates possibility of using automated tools for each type of report.

TABLE II.   POSSIBILITY OF AUTOMATION IN EACH REPORTING TYPE

Report Type	Possible automation level	Usual type of automation
Routine tasks	Medium	Form-based automation programs
Assigned tasks	Low	Pre-defined templates
Events	High	Automated event notification systems
Service status	Medium	Automated service level measurement
Review meetings	Low	Pre-defined templates
ITSM framework	Low	Pre-defined templates

IV.   IT SERVICE REPORTING PROCESS FLOW AND ACTIVITIES

A detailed discussion of the processes and activities in the Report management process are provided in this section.

A. Service Reporting Policies

Service reporting policies must be clearly defined, and communicated to all IT personnel.

- Each report and report template must have a unique identifier. Reports must contain reference to their report template.
- Report templates should define purpose, audience, person in charge, required metrics and data sources of reports.
- All report templates must be clearly defined, agreed upon by all parties, and recorded in the configuration management database (CMDB). Also, all changes to report templates are subject to change management policies.
- All reports must be generated in time and contain accurate data, according to their report template.

B. Process flow activities

1) Define goals and objectives:

Several reports are prepared and distributed throughout the organizations. However, only the reports prepared based on specific goals and objectives add value to the business and lead to better performance, therefore "what the reports are going to present" and "what they are going to be used for" should be clearly determined in the report template.

This is mainly achieved by reviewing the portfolio and the business policies, rules, goals and objective that refer to reporting requirements and alignment of business and IT. There are three major aspects in reporting:

a) Reactive reports: reports on what has occurred

b) Proactive reports: reports on near breaches

c) Forward reports: reports on scheduled activities

2) Determine scope:

The scope of a report is the section that the report refers to. A report could be prepared for a process, service, activity, section, a specific department or the complete IT organization.

3) Select report types:

Depending on the goal and scope of the report, one or multiple report types are selected. The following steps should be taken for each of the selected report types.

4) Review prior identified requirements:

The prior identified requirements are extracted from the reporting requirements identified in the business and the designing processes such as service level management, availability management, capacity management, information security and service continuity management. These identified requirements are categorized and documented, and will be addressed in the report.

5) Define the measures and metrics

Each identified requirement is studied in order to determine the measures and metrics which present that requirement. These measures and metrics are included in the report.

6) Specify data sources

The value of a report highly depends on the owner and credibility of the evidence that supports its statements and content. Therefore the personnel assigned to prepare the report, the sources, evidence and basics of calculation should be included thoroughly in each report.

7) Review related schedules:

Schedules that refer to major activities or activities which produce or alter a considerable amount of information have a significant impact on report schedules; therefore they should be carefully reviewed and taken into account. These schedules mainly include data gathering schedules, processing schedules, analyzing schedules, management meetings, review meetings, purchase schedules, etc.

8) Specify audience:

Depending on the target audience, the reports are classified in three main categories:

The business category: including the customers, the internal providers such as the business managers and the external providers such as the stakeholders.

The senior IT management category: such as the CSI manager and the business/IT analyst.

The internal IT category: including the middle and low-level management and IT staff such as the service owner, service manager, service level manager, process owner, process manager and etc.

9) Report scheduling:

In order to schedule a report factors determined in the previous steps should be taken into consideration, including the goals and objectives, the report type, the related schedules and the audience.

10) Select communication methods & tools:

Whenever the report is generated by the responsible person, the report should be communicated to the target audiences. The communication may be through the following methods:

- Paper-based hard copies,
- Online soft copies,
- Web-enabled dynamic HTML,
- Real-time portal/dashboard

11) Determine access levels

It is obvious that the reports prepared for the higher level staff should not be accessed by the lower level. However, depending on the organizations rules and policies, some personnel are authorized to access certain reports while their parallel colleagues should not be authorized to access those reports.

12) Review and approve:

Before finalizing the report template, all fields discussed above should be checked and approved. After refining the report template, if necessary, it should be approved by higher authorities such as business, senior or IT management. After approval, the report template must be communicated to the corresponding parties.

The CSI manager or his/her representatives are responsible for monitoring of reports to be generated based on the related report template and to be communicated according to the reporting policies.

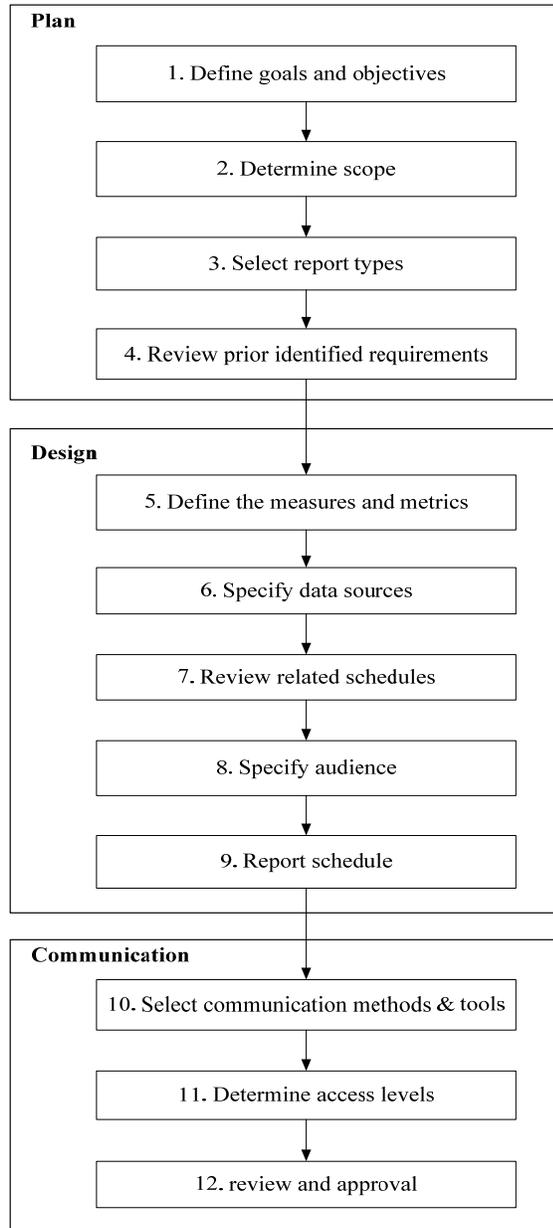Figure 1 demonstrates the complete service reporting process flow.

Plan

1. Define goals and objectives

2. Determine scope

3. Select report types

4. Review prior identified requirements

Design

5. Define the measures and metrics

6. Specify data sources

7. Review related schedules

8. Specify audience

9. Report schedule

Communication

10. Select communication methods & tools

11. Determine access levels

12. review and approval

Figure 1.   Service Reporting Process Flow

C.   Reporting process ARCI matrix

The CSI process owner is the person accountable for service reporting process. IT manager and report owner must cooperate to define right metrics according to business requirements. The information security manager should ensure data flow is in accordance with security policies.

Table III summarizes role of different stakeholders in service reporting process as an ARCI chart.

TABLE III.   SUMMARY OF DIFFERENT REPORT TYPE SPECIFICATIONS

Reporting process activities		CSI manager	CIO	Report	Portfolio	Security	Report
A. Plan							
1	Define goals and objectives	A/R	C		C		C
2	Determine scope	A	C	R			C
3	Select report type	A	C	R			C
4	Review prior identified requirements	A	C	R	C		C
B. Design							
5	Define the measures and metrics	A	C	R			I
6	Specify data sources	A	C	R			C
7	Review related schedules	A	C	R			C
8	Specify audience	A		R			C
9	Report scheduling	A		R			I
C. Communication							
10	Select communication methods	A	C	R			C
11	Determine access levels	A	C	R		C	C
12	Review and approve	A/R		I	C		I
Legend	*A= Accountable, R= Responsible, C = Consulted, I = Informed.*						

D.   Reporting Process Integration Points with other ITIL processes

Here, all documents which are communicated within the proposed service reporting process are listed.

Table IV presents all documents and information from different ITIL processes which are required in the service reporting process.

TABLE IV.   SERVICE REPORTING PROCESS INPUTS

Inputs to reporting process	
Portfolio	-Business and IT rules, policies, goals and objectives -Business report requirements -Business and IT meetings and schedules
Demand	-Demand management requirements for a report -Demand management meetings and schedules
Financial	-Evaluation of reporting costs
SLM	-Service level agreements for the reporting process -SLM requirements for a report
Availability	-Level of availability of each report
Continuity	-The continuity required for providing a report
Security	-The security levels required for each report
Supplier	-Required reports for each supplier
Catalog	-Services available in the organization
Configuration	-CI's available in the organization
Release	-Progress of preparing the report template
Change	-Request for a new report template
Knowledge	-The accuracy of information received

Event	-Event schedules -Events related to inadequate reporting
Incident	-Incidents related to inadequate reporting
Problem	-Problems related to inadequate reporting
Request fulfillment	-The customer report requirements
Access	-The access levels for each report
CSI	-The collected, processed and analyzed data

Table V lists all information generated in the service reporting process.

TABLE V. SERVICE REPORTING PROCESS OUTPUTS

Outputs of reporting process	
Report Template for:	-performance against service level targets; -non-compliance and issues, e.g. against the SLA, security breech; -workload characteristics, e.g. volume, resource utilization; -Performance reporting following major events, e.g. major incidents and changes; -Trend information; -Satisfaction analysis. etc.

E. Service Reporting Process KPIs

- Reduction in the number of issues caused by inadequate reports.
- Improved decision making supported by efficient and effective reporting.
- Decrease gaps between the expected reports and the provided reports.
- Reduction in the number of unauthorized access to reports.
- Increase of relevant information reported to relevant audience.
- Reduced reporting costs.

V. TERMS AND DEFINITIONS:

- *KPI*: Key performance indicators are important metrics and measures used to report on the performance of process, IT service or activity.
- *PIR*: Post implementation review takes place after an activity has been completed and evaluates the success of the activity.
- *ARCI*: A Table that helps defining roles and responsibilities. ARCI stands for Accountable, Responsible, Consulted and Informed.
- *Report template*: A template is defined for each reporting purpose required in the organization. A report template is the result of the report management process.
- *Report designer*: Is a role assigned by the CSI manager which is mainly responsible for preparing the report template.
- *Report owner*: A role responsible for reporting based on the determined and assigned report template.

VI. CONCLUSION AND FUTURE WORK

Measurement and reporting is a key requirement of service improvement, which in turn is required for value creation and success in a competitive market. The proposed reporting framework helps organizations to define reports in a way that eases service improvements.

Many of the proposed concepts could be used for external reports, which are reports on service levels to clients. Further works can be done to classify and clarify external reports. More works are required to identify different types of reports required in different IT process and types of metrics and measures which can be defined for each of them.

REFERENCES

[1] International Standard Institute, "ISO/IEC 20000:2005 Information technology — Service management standard." 2005.

[2] The Office of Government Commerce (OGC), "ITIL Service Management Practices v3 - Core Books", The Stationary Office, UK, 2007

[3] The Office of Government Commerce (OGC), "Service Improvement Book", in ITIL v3 Service Management Practices, The Stationary Office, UK, 2007

[4] Microsoft® Operations Framework v4: Microsoft Publications, 2008.

[5] The IT Governance Institute®, ITGI, "COBIT 4.1 - IT Governance Framework." 2007.

[6] ITIL® V3 : Managing Across the Lifecycle Best Practices: The Art of Service Pty Ltd, 2007.

[7] M. Jantti and K. Kinnunen, "Improving the Software Problem Management Process: A Case Study," in the 13th European Conference on Software Process Improvement, Joensuu, Finland, 2006, pp. 40-49.

[8] A. J. Keel, M. A. Orr, R. R. Hernandez, E. A. Patrocinio, and J. Bouchard, "From a technology-oriented to a service-oriented approach to IT management," IBM Systems Journal, vol. 46, pp. 549-564, 2007.

[9] L. Haber. (2003). How do you measure ITSM success. ITSM Watch, http://www.itsmwatch.com/itil/article.php/3291421/How-Do-You-Measure-ITSM-Success.htm, (Dec 14, 2010).

[10] A. Lahtela, M. Jantti, and J. Kaukola, "Implementing an ITIL-based IT Service Management Measurement System," in Fourth International Conference on Digital Society, St. Maarten, 2010, pp. 249-254.

[11] A. S. Lima, J. N. de Sousa, J. A. Oliveira, J. Sauve, and A. Moura, "Towards business-driven continual service improvement," in Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP, 2010, pp. 95-98.

[12] C. A. Carver, J. M. Hill, J. R. Surdu, and U. W. Pooch, "A methodology for using intelligent agents to provide automated intrusion response," in Proceedings of the 2000 IEEE Workshop on Information Assurance and Security, 2000, pp. 110–116.

[13] K. Nakajima, Y. Kurata, and H. Takeda, "A web-based incident reporting system and multidisciplinary collaborative projects for patient safety in a Japanese hospital," Journal of Quality and Safety in Health Care, vol. 14, p. 123, 2005.

[14] S. Natarajan, A. Harvey, H. Lee, V. Rawat, and L. Pereira, "Technique for providing automatic event notification of changing network conditions to network elements in an adaptive, feedback-based data network," Google Patents, 2003.

[15] T. Fahringer, M. Gerndt, et al., "Knowledge specification for automatic performance analysis, APART Technical Report," vol. FZJ-ZAM-IB-2001-08, FORSCHUNGSZENTRUMJÜLICH GmbH, Zentralinstitut für Angewandte Mathematik, 2001.

[16] A. Sahai, V. Machiraju, M. Sayal, A. Van Moorsel, and F. Casati, "Automated SLA monitoring for web services," Management Technologies for E-Commerce and E-Business Applications, pp. 28-41, 2002.