2009

IT Service Management Review (ITSMr)

Prepared by Guillaume FRESNEL (Service Delivery Manager)

for IN2P3 Villeurbanne

Version 1.6

IN2P3

Institut national de physique nucléaire et de physique des particules

Revision Control

Name	Date	Version	Reason
Guillaume FRESNEL	01/06/09	1.0	Creation of the document
Guillaume FRESNEL	25/06/09	1.1	Mistakes correction + new incident management information flow simplified schema
Guillaume FRESNEL	07/07/09	1.2	Wording Correction from Colin Willies
Guillaume FRESNEL	07/07/09	1.3	Correction from Gilles Breton
Guillaume FRESNEL	27/07/09	1.4	Correction from Oscar Carolan and Cynthia Baloula
Guillaume FRESNEL	31/07/09	1.5	Remarks from Core ITIL (mails)
Guillaume FRESNEL	05/08/09	1.6	Remarks from Core ITIL (conference call)

TABLE OF CONTENTS

1. Introduction

All companies are wrestling with IT complexity and driving to develop simplification strategies to become more efficient. Dell's Premier ProSupport suite entitles customers to annual Service Management benchmarking and roadmap assistance for building successful ITIL-based Continuous Service Improvement programs.

Dell's Information Technology Service Management Review (ITSMr) leverages the best practices laid out in the IT Infrastructure Library (ITIL®) and The Capability Maturity Model® (CMM) and is intended to tie into your IT Simplification strategy. ITIL® is a methodology that applies the science of management to IT infrastructures (set of best practices, based on a common language). It is vendor independent and provides guidance across the breadth of IT infrastructure, development and operations. The CMM is a framework for business process improvement.

Dell's review concentrates on assessing four processes against the ITIL® framework as they relate to the enterprise environment (Incident, Problem, Change, and Configuration Management). There is also an examination of the Service Desk function using information obtained during the participant interviews.

The current assessment is based on version 3.0 of ITIL.

1.1. Participant to the survey

The IN2P3 Villeurbanne IT Department survey participation rate was 92% for the interview and 59% for the web survey. The first interviews were defined with 8 IT members. Following those first sessions, we enlarge the scope of the assessment to the overall IT service (12 people). Most of the interviews had been done onsite and recorded, the rest were done by phone.

Participants communicated openly about the inherent strengths and challenges faced by the IN2P3 Villeurbanne IT staff as they make every effort to meet very high expectations in a rapidly changing environment.

Name	Role	Online Survey	Interview
Micael Gonzalez	Administrator	Yes	Yes
Catherine Biscarat	End User	Yes	Yes
Mattieu Puel	Administrator	Yes	Yes
Jérôme Bernier	Team Manager	Yes	Yes
Yannick Perret	Administrator	Yes	Yes
Fabio Hernandez	Director	Yes	Yes
Pierre Larrieu	Purchase Manager	No	Yes
Philippe Olivero	Service operation Manager	No	Yes
Dominique Boutigny	Director	No	No
Marc Chiumento	Service Infrastructure Manager	Yes	Yes
Laurent Caillat	Network Manager	Yes	Yes
Marc Delaunay	Storage Manager + CSO	No	Yes

1.2. CMMI assessment score

Aggregate ITSMr Responses:

INCIDENT MANAGEMENT

CC-IN2P3 Self Assessment Score = 2.4

DELL Assessment = 1.95

PROBLEM MANAGEMENT

CC-IN2P3 Self Assessment Score = 2.66

DELL Assessment = 1.88

CHANGE MANAGEMENT

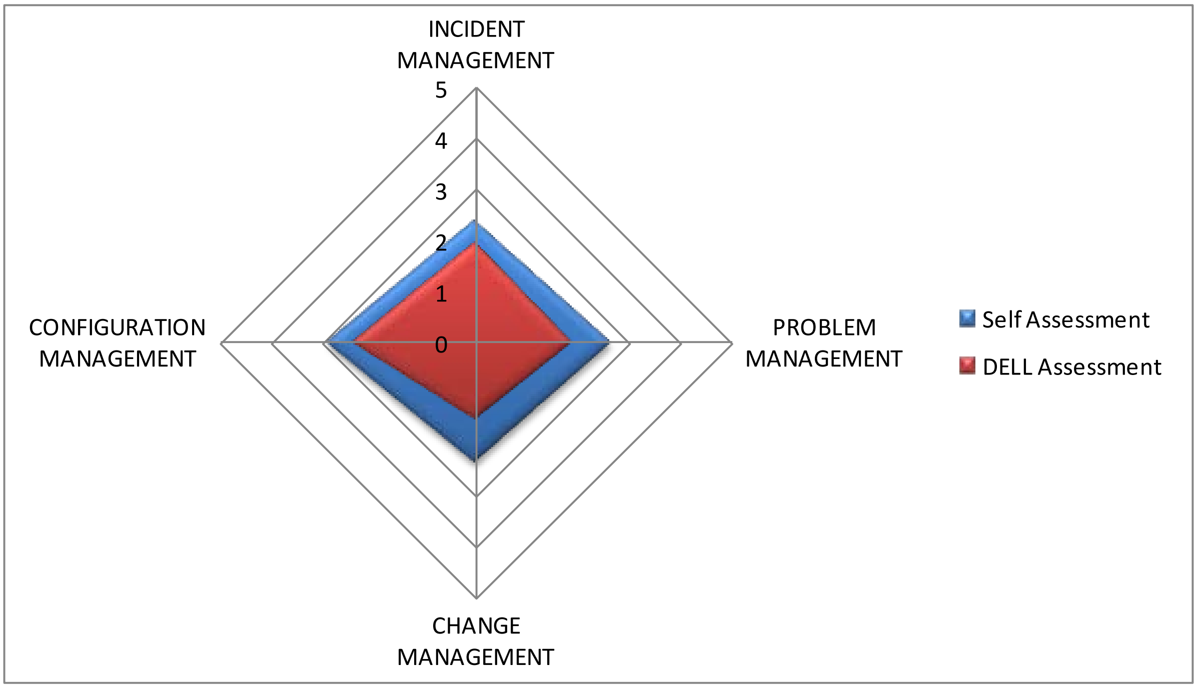
CC-IN2P3 Self Assessment Score = 2.36

DELL Assessment = 1.5

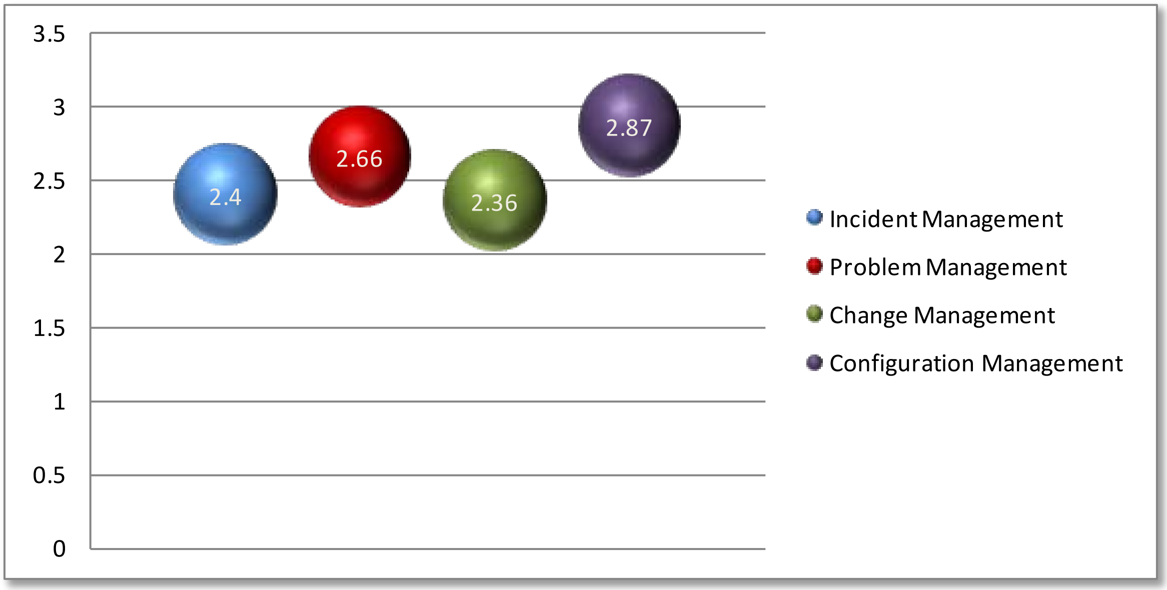
CONFIGURATION MANAGEMENT

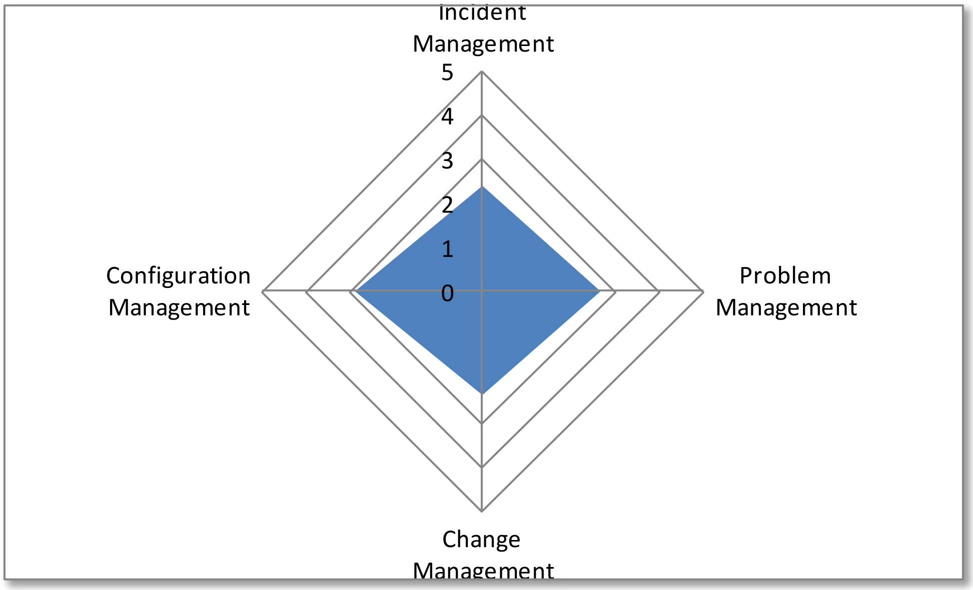
CC-IN2P3 Self Assessment Score = 2.88

DELL Assessment = 2.38

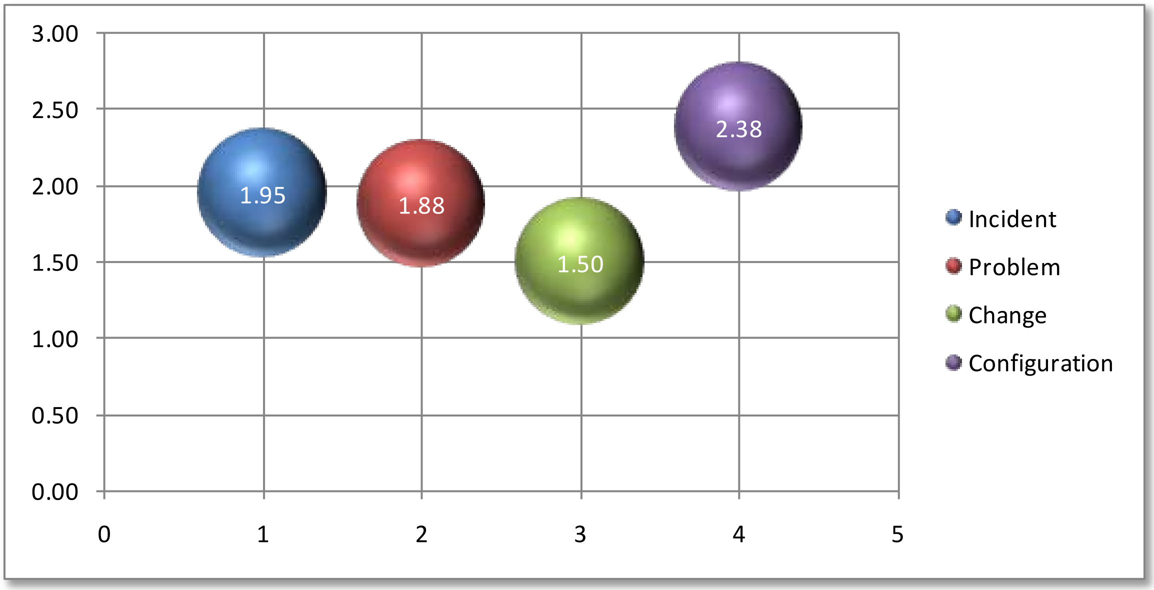


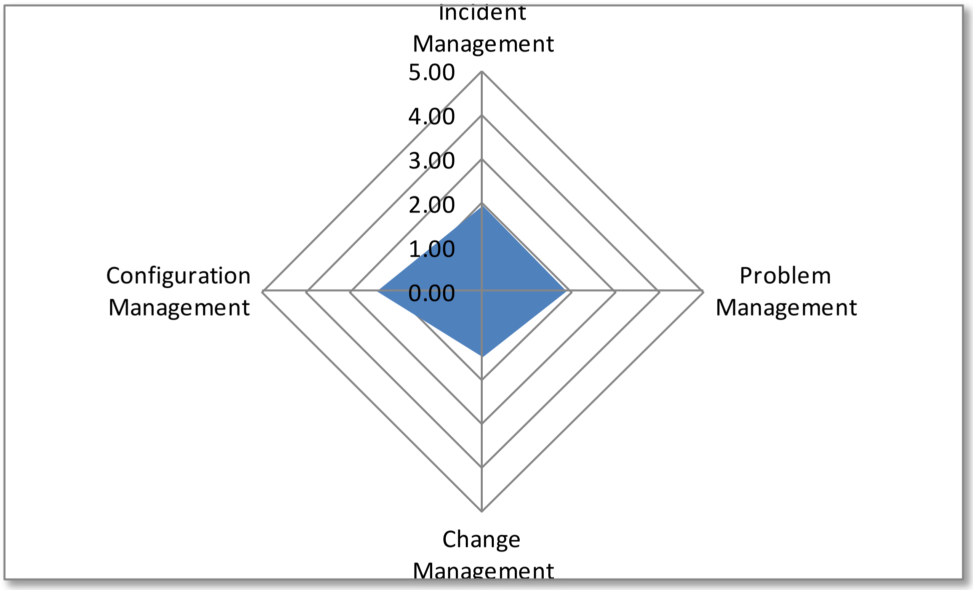
1.3. CMMI CC-IN2P3 Self Assessment Score





1.4. CMMI DELL Assessment Score





2. The Dell IT Service Management Review

Dell's IT Service Management Review was conducted via online assessments, face to face and phone interviews and provides a snapshot of your IT organization's perceived CMMI® capability level. This estimate is based on CMMI® level definitions and a comparison against industry-standard best practices and is intended to tie into your IT Simplification strategy.

This report contains an overview of ITIL® best practice for selected process areas, the results of the assessment, and some relevant first steps and challenges to consider when planning an ITSM implementation.

2.1. What is ITIL®?

Information Technology Infrastructure Library (ITIL®) was developed in the early 1980's by the British Office of Government Commerce (OGC) to realize a more cost effective and efficient use of the UK's IT expenditures. ITIL® Version 3 is a comprehensive and dynamic framework based on five books that provide guidance and a cohesive structure to IT Service Design and Operation. ITIL® is a public domain framework providing a common language with which the business and IT Service staff can effectively communicate and coordinate services that support the business mission.

ITIL® is the foundation for BSI 15000:2000 and the international standard for IT Service Management (ITSM). ITIL® is vendor agnostic and descriptive, not prescriptive approach to IT Service provision in direct support of business goals and objectives

Why adopt an IT Simplification approach?

Dell advocates true simplification of IT that transforms innovation from a lofty ideal into a daily business practice. This requires the deliberate design of services that provide relevant and effective business outcomes and the supporting processes. Within Service Strategy, IT Services are seen as a revenue-stream enabler and a source of competitive advantage.

The business does not focus on the needs of IT – they focus on what the business requires from IT: adaptive, efficient and effective IT Services. Once a service is negotiated between the business and IT, Service Management provides guidance for designing dynamic processes, procedures and roles that are responsive to a changing business environment.

Good processes are designed to support the objectives of the business and:

- outcomes can be audited and tracked, providing data for workload and forensic reporting
- codify and instill organizational discipline, avoiding out-of-process behavior
- clarify organizational boundaries and roles, linking individuals with the work roles they fill
- capture organizational knowledge through a well-maintained central knowledge base
- avoid duplication of effort, enhancing efficiency and avoidance of acting at cross-purposes
- support focused continuous process improvement with built-in assessment and improvement mechanisms
- shift focus from people to processes and helps drive down costs
- allows for a more complete business perspective of IT operations

Necessity versus Intentional Process Design

IT processes have traditionally evolved by necessity, rather than as an intentional and continually improved design. If IT Operations are a reaction to, or independent of, business objectives then strategic and tactical alignment of the two organizations can be problematic. This can lead to an inefficient allocation of resources and the pursuit of IT goals that are no longer supportive of business.

2.2. Assessment Expectations

Management welcomed an IT Simplification approach to service and process review. Senior executives are tasked with maximizing the value of the IT organization while minimizing (for example, Personnel). Current managers hoped that the assessment would reveal how taxed their current staff is in barely meeting the SLA's set forth by the organization.

Senior management expressed interest in revealing a set of recommendations and starting points to optimize IT processes.

2.3. Assessment Methodology

The assessment was setup in 2 main activities:

- Online survey: Participants answered approximately 75 questions regarding four IT process areas which were devised to extract a measure of the *perceived* level of maturity for the four ITIL® processes to be examined (Incident, Problem, Change and Configuration Management).
- Interview via phone or face to face : to draw detailed information about internal processes and communications at IN2P3 Villeurbanne.

Participant's answers were averaged and the results correspond to points on a scale based on the Capability Maturity Model Integration (CMMI®). Each question in the IT Service Management review had five possible answers relating to the *perceived* state of the organization's processes (referred to APPENDIX A: CMMI Capability Levels) .

Those activities provided a double evaluation one based on multiple auto-evaluations which were concatenated in one CMMI notation, one based on the global evaluation of the SDM. The methodology provides a set of comparison between the IN2P3 Villeurbanne individual perceptions and a global external evaluation (DELL SDM).

Intelligent people often disagree on where an organization currently fits along the maturity continuum. There is often a difference of opinion on how process improvement efforts are viewed between those who handle tactical issues (technicians and SME's) and those who are responsible for strategic direction. By incorporating many opinions from all levels of the IT organization, the average perception can be more appropriately assessed.

At the beginning of an ITSM effort, prior to widespread ITIL® training, many of the answers to questions on an assessment often do not exactly match the intent of the question that were asked. This understanding gap should improve as the ITSM effort unfolds.

2.4. ITIL® Process Assessment Scope

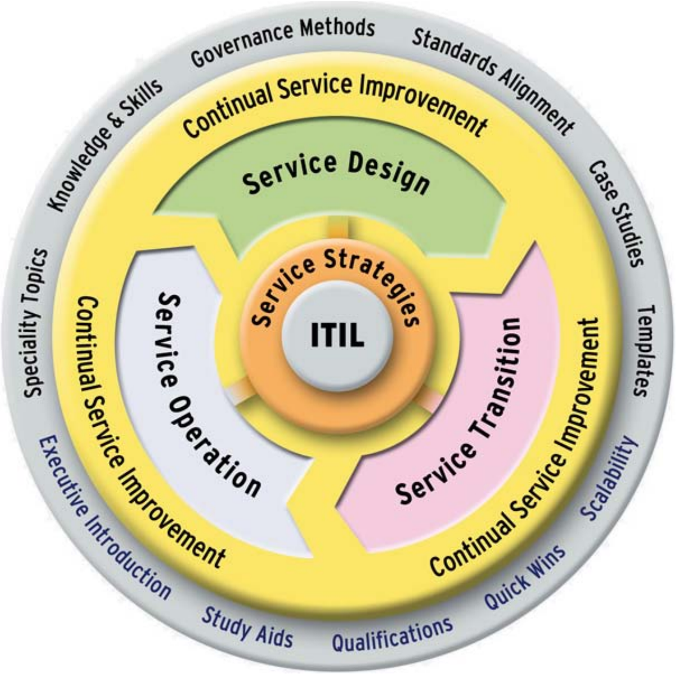
ITIL® V3 published by the Office of Government Commerce, in the UK, consists of five books: Service Strategy, Service Design, Service Transition, Service Operations and Continuous Service Improvement; providing a framework for the strategic design of IT Operations throughout the IT lifecycle. The foundation of this framework is built around several critical processes, which are the subject of this review: Incident Management, Problem Management, Change and Configuration Management.

From the information gathered, inferences are made as to the adequacy of the Service Desk function and the ability for IT Operations to respond to changes within the business and the IT environment.

The IT Service Management review is not an all-inclusive prescription for ITSM implementation (as this requires a much more intimate knowledge of the IN2P3 Villeurbanne IT environment), but concentrates on benchmarking process maturity of current practices. Some “first steps” for process improvement are also offered.

All the ITIL® processes are dynamically interactive, in that each process receives inputs from, and provides outputs to, all the other processes. This structure provides scalable processes and closed-loop feedback mechanisms. Processes can then be improved in an iterative ‘generate, test and improve” manner.

2.5. ITIL® Framework Processes and Components



Process	Goal
Incident Management (Service Operations)	The goal of ***incident*** management is to restore standard service functionality as quickly as possible, while minimizing undesirable impact to productive business operations. Incidents are managed throughout the full lifecycle (from initial trouble ticket through to customer resolution by the Service Desk. Documentation is standardized to enhance business intelligence/reporting.
Problem Management (Service Operations)	*A **problem*** is often identified because of identifying multiple incidents exhibiting common symptoms. The goal of this process is to resolve the root cause of recurring Incidents, minimize the impact on the business and to prevent future related incidents. Many problems are the result of errant changes released into the environment.
Change Management (Service Operations)	The goal of ***Change Management*** is to minimize the impact of change-related incidents and to improve the effectiveness of day-to-day operations. A formal and strictly enforced Change Management process is a protective wall between potentially damaging Changes and the Live production environment.
Configuration Management	To provide a logical model of the infrastructure or a service by identifying, controlling, maintaining, and verifying the versions of Configuration Items ***and the relationships between them***. These are stored in the ***Configuration Management Database*** (CMDB). A CMDB also includes all documentation: project and change plans, process manuals, procedures, and SLA's.

3. IN2P3 Villeurbanne – Facts, Figures, IT Structure, Goals and Objectives

3.1. Facts, Figures, Goals and Objectives

CNRS Facts and Figures

The Centre National de la Recherche Scientifique (National Center for Scientific Research) is a government-funded research organization, under the administrative authority of France's Ministry of Research.

Founded in 1939 by governmental decree, CNRS has the following missions:

- To evaluate and carry out all research capable of advancing knowledge and bringing social, cultural, and economic benefits for society
- To contribute to the application and promotion of research results
- To develop scientific information
- To support research training
- To participate in the analysis of the national and international scientific climate and its potential for evolution in order to develop a national policy

IN2P3 Facts and Figures

The IN2P3 is an institute of the CNRS (French National Center of Scientific Research). This department manages the nuclear and particles physics areas.

IN2P3 Computing Centre of Villeurbanne

Funded by the National Centre for Scientific Research (CNRS) and the Atomic Energy Commission (CEA/DSM/Dapnia), it has provided computing services for more than two decades to several “experiments” in the fields of nuclear physics, particle physics and astroparticle physics.

Experiments of the Large Electron Positron (LEP) collider, and more recently DZero and Babar, are examples of major users of the centre. Since the early 2000s it has also provided computing services to research institutions in the field of biomedical applications.

CC-IN2P3 has set up and operates a Tier-1 centre to process data from the four Large Hadron Collider (LHC) “experiments”. It is planned to eventually contribute about 9% of the total worldwide Tier-1 computing capacity for ALICE, 13% for ATLAS, 10% for CMS and 27% for LHCb.

Becoming an LHC Computing Grid (LCG) Tier-1 centre means many changes to the site. A major upgrade of the cooling and power infrastructure of the centre's computer room is scheduled for the second half of 2006. This will enable it to host the data-processing equipment that is essential for the LHC “experiments” and for other scientific “experiments” that the centre will continue to support in the coming years. A second machine room in a new building is planned to extend the site's capacity by 2009.

A dedicated optical network circuit that links CC-IN2P3 and CERN at 10 Gbit/s has been in operation since early 2006. It is being used to validate the data-exchange infrastructure for LHC “experiments” in the context of the LCG project. Data transfer rates of 250 MB/s have been demonstrated between CERN and CC-IN2P3. This circuit, along with the site's links to the national and international networks, are operated by RENATER, the French telecoms network for research and education.

Work has also begun to upgrade the disk- and tape-based data storage and the computing infrastructure of the centre to the levels required for the LCG project. The new Grid components at the site are being integrated progressively into the production-level procedures, with the aim of reaching a high quality of continuous service by the time LHC starts.

CC-IN2P3 has been actively involved in Grid activities since Datagrid, the first European-level Grid project. It also contributes to Enabling Grids for E-sciencE (EGEE), both as a regional operations centre for France and as the developer and operator of the EGEE central daily operations portal.

The LCG, like other large-scale projects, is both a major technological push and a significant human enterprise. In the year of the 20th anniversary since CC-IN2P3 moved from Paris to Lyons, its staff are working hard to meet the challenges presented by the LHC over the coming years.

To ensure their ability as high-end computing provider, the CC-IN2P3 are continually investing in new technology as :

- large Storage solutions
- large backup solutions
- HPCC : High Performance Computing Cluster (currently a solution of 1000 DELL PE1950)

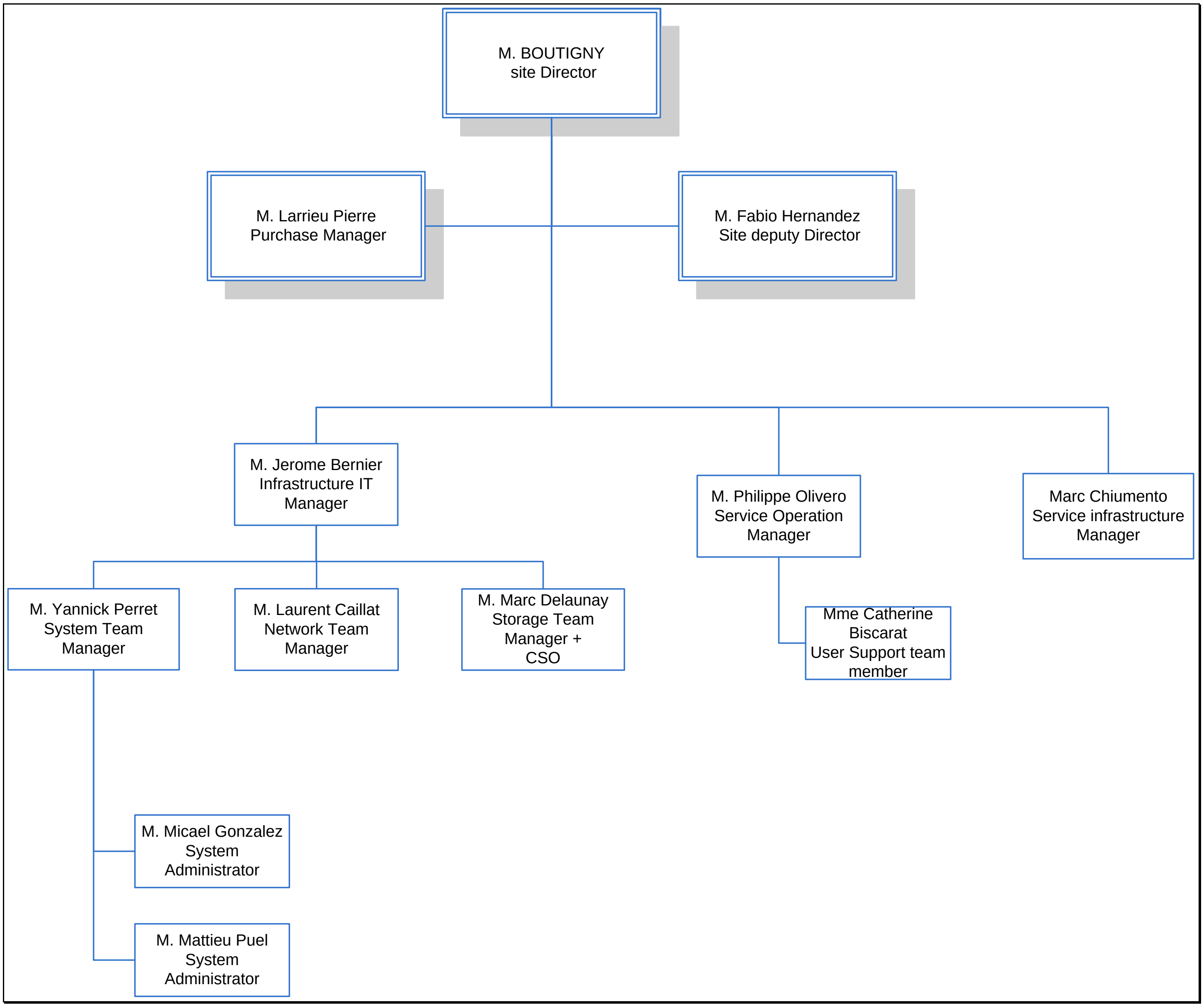
In regards of the main goals of the CC-IN2P3, two of the main KPI (Key Performance Indicator) are the :

- availability in term of MIBS par period of time
- volume allocated to the “experiments”.

One of the main challenges that the CC-IN2P3 encounters is power, cooling and floorspace limitation. The main actions and projects which are currently running to solve this issue are:

- Reduce the power, cooling consumption of current solutions
- Reduce the floor space usage of current solutions
- Design and creation of a new dataroom.

3.2. IT Structure

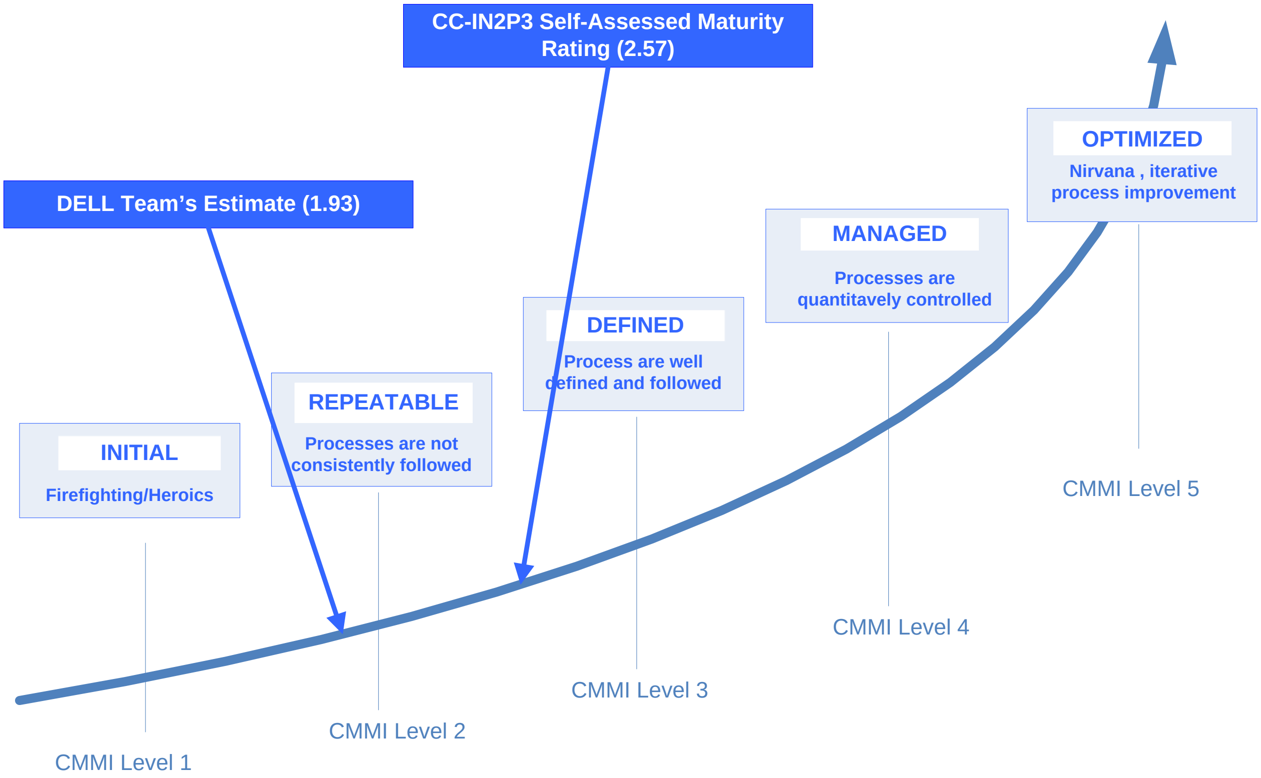


4. Assessment Observations

Participants said that the outcomes generated by your IT organization are successful due partly to these elements:

- IN2P3 Villeurbanne delivers results and complex solutions in sensitive environments
- IN2P3 Villeurbanne's people are very competent and are capable of producing acceptable IT outcomes even if ITSM processes are incomplete and not universally adhered-to
- IN2P3 Villeurbanne's management is aware of the opportunities that exist for process improvement and have already begun examining process improvement practices and tools
- Service Desk Functions and Incident Management are organizational strengths

Participant's survey responses suggest that there is room for improvement in each of the support processes. Overall, IN2P3 Villeurbanne IT perceived maturity scored at CMMI level 2. The Dell team's observations place IN2P3 Villeurbanne IT between CMMI level 1 and CMMI level 2 based on the interviews with the participants.


CC-IN2P3 Self-Assessed Maturity Rating (2.57)
DELL Team's Estimate (1.93)
OPTIMIZED
Nirvana , iterative process improvement
MANAGED
Processes are quantitavely controlled
DEFINED
Process are well defined and followed
REPEATABLE
Processes are not consistently followed
INITIAL
Firefighting/Heroics
CMMI Level 5
CMMI Level 4
CMMI Level 3
CMMI Level 2
CMMI Level 1

CMMI® Level	Description
1 = Initial	**1 = No formal process exists; issues are resolved on an ad-hoc basis**
2 = Repeatable	**2 = A process exists but is not consistently employed**
3 = Defined	**3 = A formal process exists BUT controls and/or audit trails are not adequate**
4 = Managed	**4 = A formal process exists AND better controls are in development**

5 = Optimizing	**5 = A formal process exists and is followed; mature controls and audit trails** ***Based on participants perceived level of maturity**

The IT Service Management Review team was able to interview with 11 people ranging from directors to the technicians who handle incident resolution. Participants communicated openly about the inherent strengths and challenges faced by IN2P3 Villeurbanne IT staff as they strive to meet very high expectations in a de-centralized environment.

Participating staff commented that IN2P3 Villeurbanne’ support model is more “people-based, rather than process-based” indicating a lower maturity. In most environments we have examined, inadequate process structures usually lead to visible service gaps and less than stellar customer satisfaction. In IN2P3 Villeurbanne’’ case, the quality of the handpicked staff who resolves incidents and initiate changes to some extent helps mitigate any process maturity needs.

It is, however, common for IT organizations like IN2P3 Villeurbanne to evolve over time by necessity, rather than through holistic and intentional design especially due to the center history, unequal process awareness and strong independence and autonomy of the internal resources. Some processes and procedures are being utilized with inadequate communication between the various IT functional groups. These sites can experience significant service interruptions and put additional workload and pressure on technical staff. The efficiency and effectiveness of operations often is not moving toward an optimized state. In addition, business intelligence is usually inadequate, making it complicate and unclear to request or substantiate expenditures for additional staffing personnel or material technology investments.

CC-IN2P3 has many tools and processes. The people are well trained and know their roles and functions. It appears that there is a lack of common building will between teams. Based on interview feedback, they have the necessary tools and knowledge to improve their maturity with regards to CMMI. They must define a role of quality/ITIL manager who will define the cross-function usage of what is already in place. Few steps are necessary to grow above a CMMI second level and approach the third.

Based on these discussions, IN2P3 Villeurbanne may have a significant opportunity to enhance bi-directional communications between the technical staff and senior management.

4.1. Overall IT strategy vision

An IT service strategy determines which services are required to support business goals and objectives. Business and IT management must carefully discern which initiatives offer the highest business value while ensuring the availability of necessary resources and the commitment to deliver on the investment.

A successful service strategy will ensure that:

- IT goals are aligned to business goals.
- Annual IT initiatives that support business goals have been identified.
- There is agreement on both the strategy and a corresponding plan for achieving the goals and initiatives.
- The strategy is assessed against business outcomes.
- Opportunities for improvement are identified.

The culture of the organization is a main issue to be taken into account during organizational change, because organizational change could support an implementation, and it can also lead to resistance. For that reason the organizational culture should be managed in order to avoid problems like resistance. Therefore the entire staff must be aware, understand and keep informed about the overall strategy with regards to his goal, his measurements (Key Performance Indicators: KPIs), risks and impacts. In this way, you can ensure that your organization is fully involved in the company objectives.

Participants from the technical staff told us that:

- The global strategy and KPIs (Key Performance Indicator) are not well-known by everybody.
- Some team member are interested in getting more information about the global strategy of the CC-IN2P3 (long term view).

Management told us that:

- The management has a quite similar vision of the strategy and often presented the same KPIs.
- The management is aware that the strategy is not well-known by everybody,
- Some of the managers think that there are not enough KPIs.
- Recruitment is based on feedback from the managers. Metrics are not used as a decision-making tool.
- There is no formal process to enroll and train a new hire. Usually the team is a mentor for him.

Information shared globally:

- Each interviewed person was able to describe correctly his role in his structure.
- The CC-IN2P3 strategy is completely linked to the needs of the main “experiments”.
- Main parts of the communication are transparent for the end user:
    - logs in the ticket tool are fully visible
    - main communications are done on the CC-website. http://cc.in2p3.fr/cc_accueil.php3?lang=en
- KPIs are published on the website and on displays in the physical entrance of the CC-IN2P3 site.
- Some studies are performed to gather the necessary information in regards of KPIs and the strategy (ex: evaluation of the cooling and power consumption).

4.2. People, Processes and Products

Process framework analysis looks at how the various components of an IT infrastructure (the inputs) contribute to the effectiveness of IT operations (the outputs). In general, these components can be broken down into three categories: People, Process and Technology.

People: are the agents that provide support within the IT environment.

> ***Survey participants said that people are the dominant component in IN2P3 Villeurbanne current operational model. Tribal knowledge and a focused work ethic are credited as the keystone of IT's support model. People are also handling the Technology as they are developing most of the tools they are using.***

Processes: are sets of structured procedures and activities designed to accomplish specific objectives and include the roles, responsibilities, tools and management controls required to deliver reliable, appropriate and satisfactory outcomes. These processes form the operational context within which People support the IT organizations users and customers.

> ***IN2P3 Villeurbanne IT staff almost unanimously pointed out that the processes in place are incomplete, not universally accepted and possibly bypassed. Process gaps have been mitigated by extraordinary effort from individuals. The direction board are currently interested in investing more in the process with regards to their activities and knowledge.***

Products (Technology): These are the hardware and software components within the infrastructure.

> ***Due to the nature of IN2P3 Villeurbanne' mission and the criticality of achieving successful outcomes, participants described their technology infrastructure as consistent and well-designed.***
>
> ***Many different tools are used but only the incident tool and the CC-IN2P2 website are common to all the functions (teams). There is no clear will to align tools and processes inside the organization.***

4.3. Inherent Risks

Whenever operational success depends too much on people rather than process, there are inherent risks that:

- people will leave the organization and take critical knowledge with them
- people will act unknowingly at cross-purposes, slow down progress and cause service degradation or outages
- people will become overburdened under heavy load and abandon the processes that are in place

IN2P3 Villeurbanne may mitigate these risks by devising, implementing and improving ITSM processes that provide for consistency and continuity. In addition, people possessing important technical knowledge should be encouraged to populate a centralized Knowledgebase (KB) to make their expertise available to others. Many organizations we have examined have succeeded in building substantial KB material quickly by making a contest out of the effort. SME's and technical personnel were challenged to compete amongst themselves for the highest number of complete and adequate KB items.

Summary:

Currently, IN2P3 Villeurbanne reliance on individual skills rather than on process for the successful execution of organization objectives is indicative of a CMMI maturity rating between Level 1 and Level 2 (see maturity definitions in appendix A). There is significant opportunity to inject consistency and continuity with more focused, followed and enforced IT processes which would lead toward a CMMI maturity rating of 3 (a good intermediate goal for CC-IN2P3).

4.4. Individual Process Explanations and Discoveries

4.4.1. Incident Management

CC-IN2P3's self assessment score	**2.4**
DELL Assessment score	**1.95**

4.4.1.1. Discoveries

CC-IN2P3 support model is highly dependent on the individual heroics of many talented people. In such an environment, there are opportunities for workarounds.

A common incident tool (except for infrastructure) is present. It is strong enough to provide correct handling of the incident following the ITIL methodology. People are not using the Incident tools for all their incidents. The parameters and options are not well-known (priority, status, metrics …). It generates report based on different incident metrics. Unfortunately, few people are using them. There is Therefore is no traceability and decisions cannot be taken on facts.

CC-IN2P3 uses a help desk (user support) in their environment to provide support rather than a Service Desk model as suggested by ITILV3. Incidents arrive at the Help Desk in multiple ways (email and web), but users are still contacting technical resources directly, bypassing the processes in place and thwarting appropriate prioritization by business impact and urgency.

There is opportunity for more consistent incident documentation to provide better business intelligence and forensic data. Multiple knowledge databases exist in each team and have different purposes. It is important to regroup them in one main knowledge base that experts can populate with regards to help desk usage.

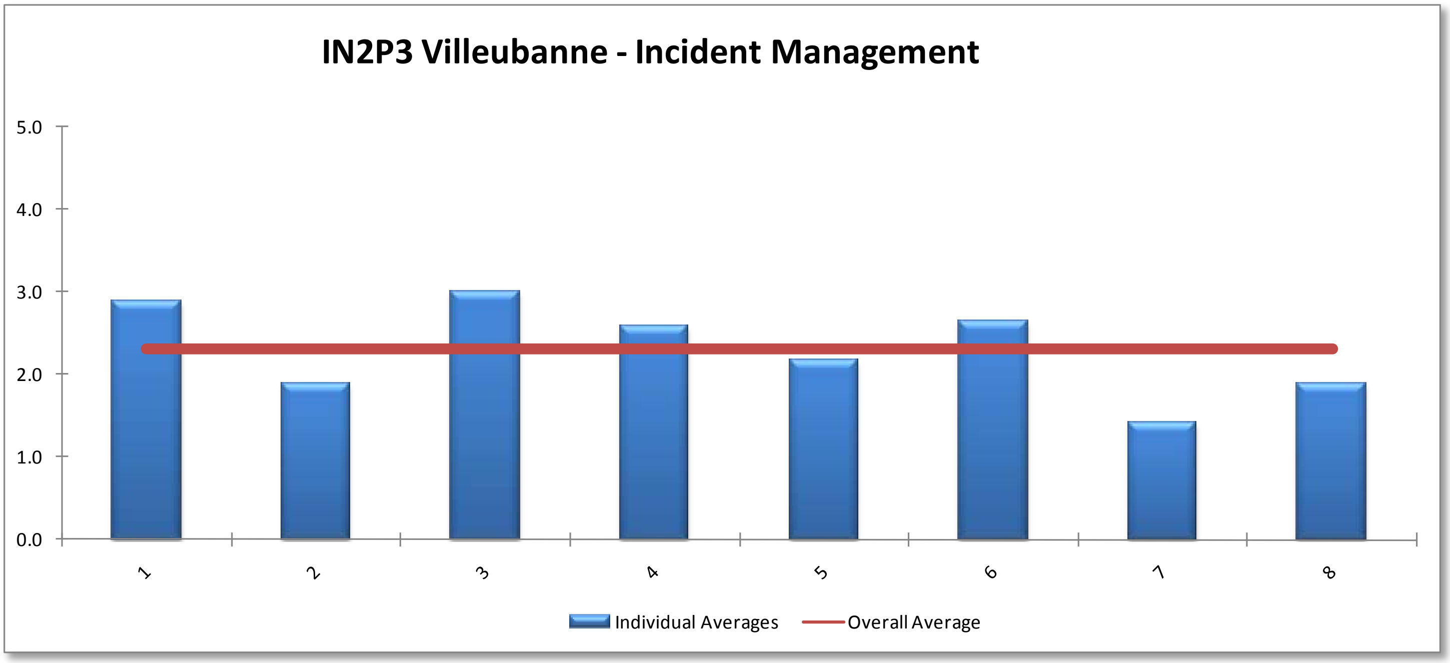
Incidents are assigned to a technician but are not actively managed by Help Desk personnel throughout their lifecycle (closures are done by the last assigned technician and not by the help-desk). This can lead to incidents languishing due to lack of oversight and misrouting and can cause additional risk to the live environment and to customer confidence in IT.

There is no existence of assignment processes for ticketing. Only the appreciation of the incident and the understanding of the different functions by the owner are used in the evaluation of an assignment.

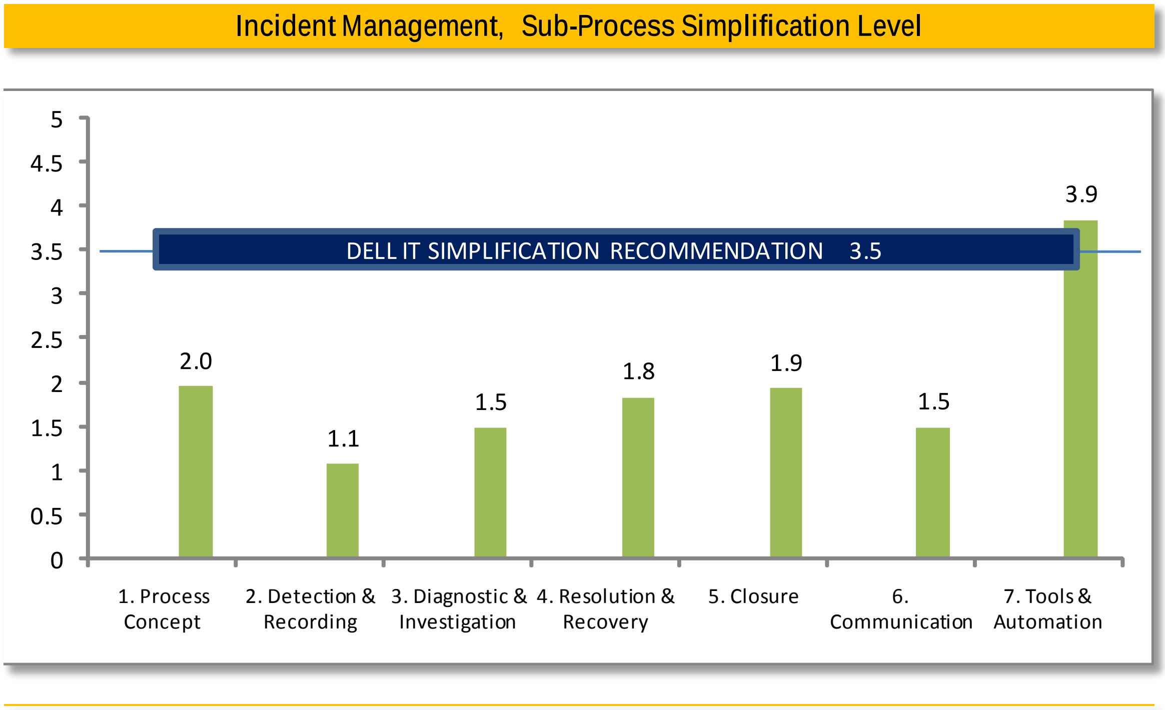
As logs and incident closures are left to the judgment of case owner without clear recommendations, it can lead to misinterpretation and dissatisfaction from the end user (experiments).

Changes released into the environment should be communicated to all Help Desk staff in a Forward Schedule of Changes (FSC) so that all can be aware of the potential for Problems related to an errant change.

4.4.1.2. Participant Survey Results – Incident Management



4.4.1.3. DELL Assessment Results – Incident Management



4.4.1.4. What Participants told us about Incident Management

Management feedbacks

- Some managers advised that the time spent in incident management is not the main part of the specialists daily job.
- Few of the managers are aware about the metrics that the current incident management tool can provide and were less able to explain the formula for the definition of each metric. Only two of them seem to take care of metric reports No one seems to really perform a periodic analysis of them (no knowledge of the current statistics).
- Important incidents are scrubbed by the site management during the weekly meeting. Those incidents are followed by a post incident report by mail.
- Management provided examples of escalation to the board of directors which shows that the ticket owner are not involved or measured on the quality (issue on case logging due to incorrect language).
- Management encountered some issues with regards to the weak handover between specialist on an incident (assignment between teams or during out of office period).
- There is no satisfaction survey but there is a specific meeting every year to gather experience feedback. This meeting has 2 limitations:
  - it doesn't provide a quantified evaluation (notation) which can be used as baseline for future comparisons.
  - it doesn't take care of all the experiences (small experiences are not represented).
- To complete the knowledge database, some teams are naming a champion who will populate the database. But this processes is sporadic and not duplicated globally in the organization.
- Concerning the ISO process, a QMS (Quality Management System) is not implemented. Therefore there is not one repository which contains all the written procedures and processes with a validation process for publishing and expiration date on documents.
- Some team managers are checking the incident queue (it is not a process with a frequency) to avoid forgotten incident in the ticketing tool. For most of them, user support has the mission to check if cases are still opened.
- Important incidents are scrubbed by the site management committee during weekly meeting. Those incidents are followed by a post incident report by mail. In this case, the incident priority can change in regards of the business impact. The business impact is only analyzed on important incident and/or escalated incident to the site direction.
- When an “Experiment” (end user) reminds the owner of the ticket, the “user support“are not automatically informed for follow-up.
- Only one of the interviewed teams (service operation) said that they are using a dashboard to follow events, incidents and problem solutions.
- SLAs only exists with regards to the safety of the site (lift, …).

Technician feedbacks

- Team members confirmed that they relieve direct calls about incidents or requests. In this case, nobody logs a ticket in the incident management tool for traceability.
- user support is sometime used to translate the specific language of experiences for technical teams.(ex: ATLAS). This point shown that the user support should be involved in the ticket closure as their awareness of the experiences is superior.
- Few of them are aware about the current metrics in regards of an incident and no one seems to use them. Metrics must be checked to improve the quality of the follow-up.
- Those Interviewed described four limitations in the incident management tool:
  - During the sequence of the first ticket opening, the system sends a mail requesting to go on the website and create an account. It seems that this manipulation could perturb some end user.
  - the system doesn't take care of the CC in the opening mail. Hence if a CC contact must act on or follow a ticket, he will not be informed of the ticket follow up.
  - The incident management tool cannot provide the necessary details to measure the time passed in each function. And then afterwards take corrective action. The time measurement is based on last owner before the closure.
  - There are two fields in the tools: one for the assignment, one for the measurement. It means that if the field used for the measurement is not filled right, it could influence the metric of another team.
- The CC-IN2P3 is currently working to develop more processes. One of the reasons for this investment is the feeling that ticket follow-up differs between resources (some incident can stay open longer with some people)..
- The incident management tool can generate messages to inform about long incidents.

- On incidents linked to the function “System Administration”, the administrators evaluate that 60% of the incidents are handle by user support and 40% by the System team. This evaluation is not based on clear metrics but with manual checks of the incident management tool queue.
- Some technicians are using the user support FAQ but it is not a usual process.
- Admin systems prefers to create small tools easy to maintain than a large complex one for all functions.
- Without sign of life from the experience end user, the ticket owner can take the decision to close the ticket.

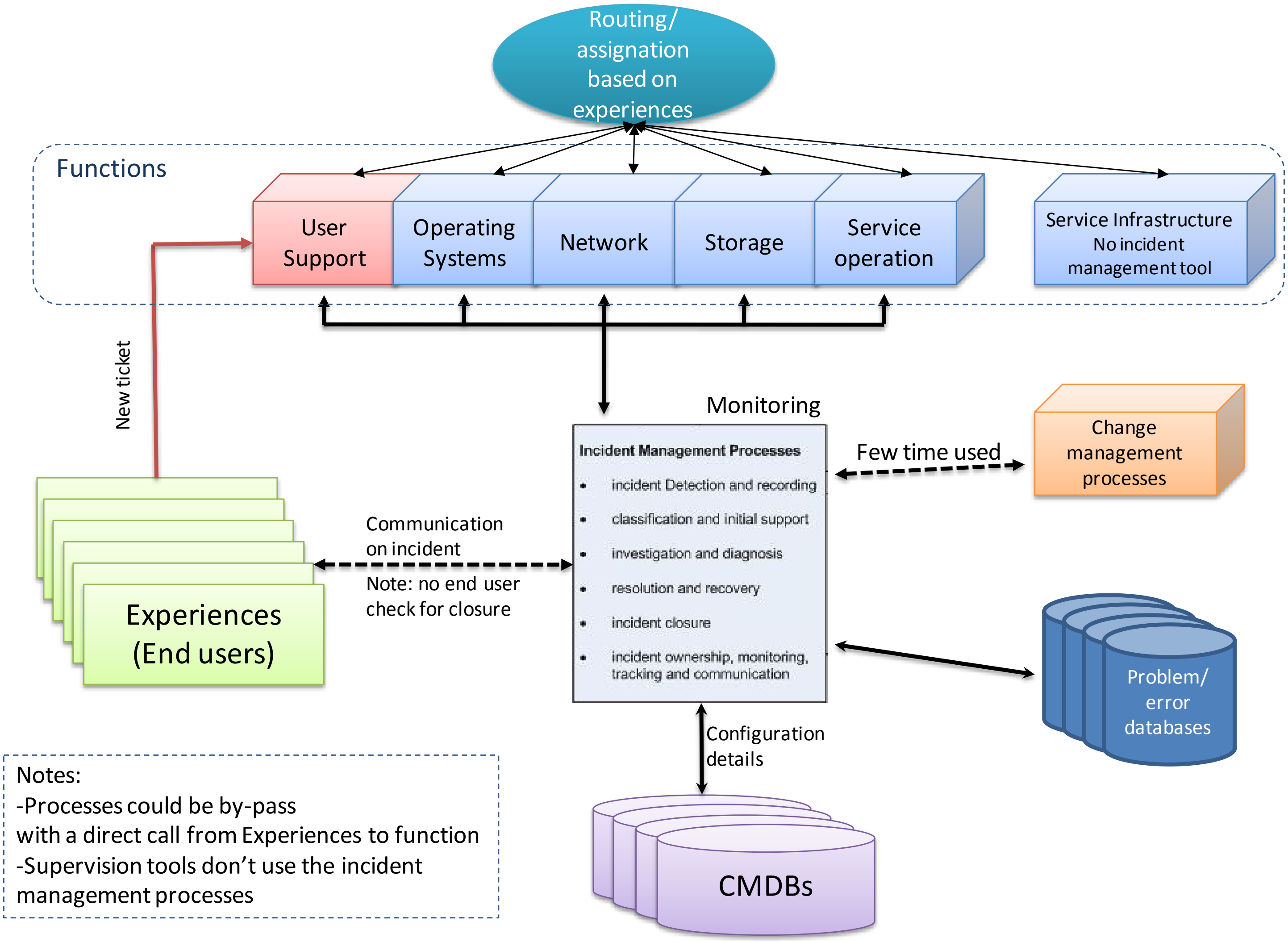
Common feedbacks

- There is one incident management tool used by all the team except the Infrastructure (which means that Infrastructure team accepts that they lose or miss some incidents).
- user support is equivalent to the service desk in ITIL. There are primary level of assignment for each ticket.
- user support is divided between main “experiments”. There is only one person for the other small “experiments” (support general). This organization promotes the main “experiments”.
- The end user (“experiments”) use either mail or the website to log an incident (tool zoobs).
- Functional escalation: The user support and teams do not use defined procedures to assign a ticket between them. Hence one of the difficulties is to get a clear vision of the perimeter and skills of each team.
- Assignments are based on alias with a group behind avoiding any assignment to a single person.
- Each team has its own knowledge database based on different criteria (FAQ for User Support, forum for admin system …). Most of the Interviewed persons confirmed that it is quite easy to find a document with the tools.
- There is no known written procedure about the ticket handling convention.
- A global knowledge database and resolution procedure are currently generated in regards of the on-call process. This database is not used for daily incident management but it is accessible for everybody involved in incident management.
- The end user can track incident status and contents via the web site. Logs are completely transparent.
- There is no official hierarchical procedure for escalation. If an incident is highlighted (processes undefined), the weekly director board meeting will handle it.
- All those interviewed confirmed that no tickets are lost once it is recorded in the incident management tool.
- Some tickets can be forgotten until the user or user support management reactivates them. Most of those interviewed have encountered forgotten tickets which can be up to one month old.
- There is no SLA except for the new contract with the LHC (resolution and engagement time). LHC SLAs are still in test and validation period..Only the User Support and Service Operation responded that they are aware of and implicated by the objectives defined as the SLAs. SLA must be known and committed to by all functions.
- In the incident management tool, the last owner closes the ticket. ITIL advises that the ticket should be closed by the service desk to ensure complete check-up of customer satisfaction and resolution.
- The closure of a ticket is not based on user feedback but on an assessment of the resolution of the issue by the ticket owner. If the problem is not solved or the end user is not satisfied after the closure, he can reopen the ticket.
- communication with end users is mainly based on the ticket logs and at times by a call. The priority field in the incident tool must be used a decision trigger between written and oral communication (High priority= call, low priority= written)
- logs are completely available for the end user who can generate a communication issue when comments are not politically correct.
- There are 3 priority levels. By default, the second level is selected. There are no criteria to define priority. If a user wants to modify it, he has an account in the incident management tool via the website, therefore the priorities are often used. Most of those interviewed do not take them into consideration.
- The incident management tool can be circumvented by a direct call to a specialist. In this case, most of the time the specialist doesn’t use the incident management processes. This kind of workaround influences the metrics and statistics. Therefore metrics could be corrupted, generate wrong assumptions and become a factor in future decisions which can negatively affect processes.
- There are no products/solutions in service which are not supervised. The main part of the supervision was developed specifically for current solutions in service and seems really accurate. Most of the time, incidents proactively opened via supervision are not associated to a incident ticket.
- The incident management tool seems to provide the usual functions for this kind of product (status, assignment, statistics …).
- The status can differentiate between closed (acceptation from all the parties to close the incident) and resolved (the incident is solved but we are waiting a final approval for closing). Currently CC-IN2P3 doesn’t perform this kind of differentiation which could be a factor of information for improvement.

- The quality of incident management seems to depend more on owner involvement than a formal process.
- Each experiment is represented by one main contact named Caesar. Caesar receives information about the service and how to use it. CC-IN2P3 can escalade to Caesar on an incident with regards to an end user interaction.
- Proactive actions are performed based on:
    - follow-up of bugs fixed or security corrections
    - analysis of the events from supervision
- Everybody answered that the Incident Management Processes are mainly based on People. Few processes exist but are not shared between functions. The Products are correct but are not used at their full potential except for supervision which is complete but not integrated in the ticketing system. Products are fully developed by People therefore depends on People.

4.4.1.5 Incident Management call flow

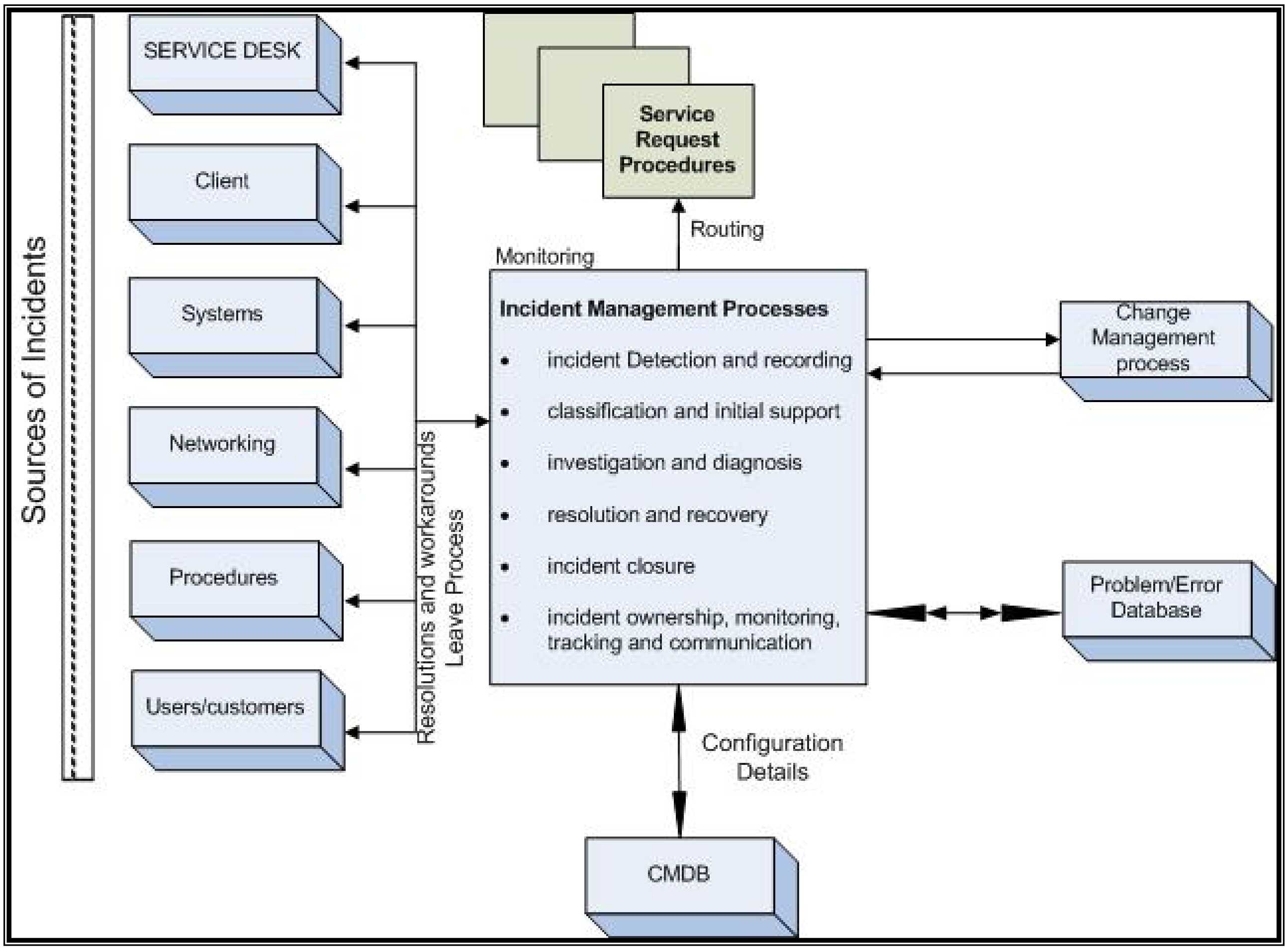
Incident Management Information flow (simplified vision)


Routing/ assignation based on experiences
Functions
User Support
Operating Systems
Network
Storage
Service operation
Service Infrastructure
No incident management tool
New ticket
Monitoring
Incident Management Processes
incident Detection and recording
classification and initial support
investigation and diagnosis
resolution and recovery
incident closure
incident ownership, monitoring, tracking and communication
Few time used
Change management processes
Communication on incident
Note: no end user check for closure
Experiences (End users)
Problem/ error databases
Configuration details
CMDBs
Notes:
-Processes could be by-pass with a direct call from Experiences to function
-Supervision tools don't use the incident management processes

4.4.1.6. Incident Management Recommendations

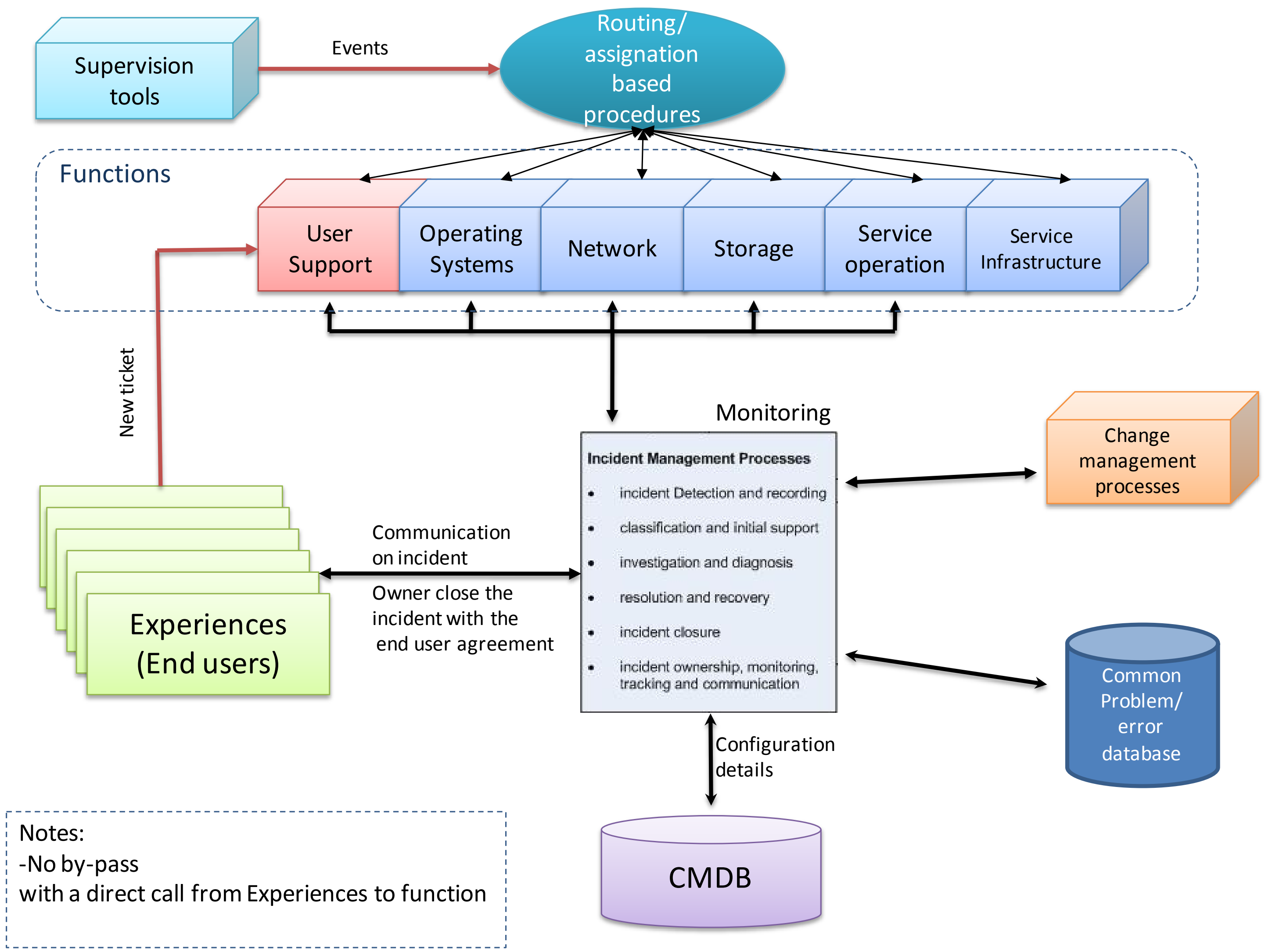
- Integrate incident management with other processes (Problem, Change and Configuration) and the Service Desk
- Introduce customer surveys to understand their perception of the Incident Management process to get direct feedback to initiate improvement in Customer Experience (CE)
- Negotiate, enforce, monitor and report well-defined SLA's (an important feedback and adjustment metric)
- Enforce case logging, documentation, SLA standards by implementing a random case audit process
- Introduce metrics as First Time Fix or Time to Resolve to evaluate the performance and define the areas of improvement.
- Formalize processes on incident logging by introducing templates for uniform logging to drive efficiency, consistency and provide historical data for business intelligence
- Document how the incident management tool work with best practices and also assignment processes.
- Regroup all the different knowledge database into one common database. Use the expertise of your functional champion to populate the knowledge (problem/error) database and provide necessary information to quickly close most of incidents at user support level and then reduce resolution time and specialist workload.
- Encourage and introduce incentive programs to publish and maintain articles in the Knowledgebase to minimize duplication of effort and incorrect information
- Define an Incident Manager role in the organization. One of his first role will be to:
  - Limit possible workarounds
  - Define clear path for escalations.
  - Define clear assignation processes between team.
- Close incidents at the help desk level to ensuring the correction answer to the end user (close the loop). Help desk must get a clear feedback from the end user before closing the case.
- Changes released into the environment should be communicated to all Help Desk staff in a Forward Schedule of Changes (FSC) so that all can be aware of the potential for Problems related to an errant change.
- Recommendations must be done to incident management user about the case logging. Some contents of the cases must be scrubbed to ensure the global consistency of the overall incident logs and then ensure the end user satisfactions.

Example of Incident Management Information Flow (ITIL pratices)



Sources of Incidents
SERVICE DESK
Client
Systems
Networking
Procedures
Users/customers
Resolutions and workarounds
Leave Process
Service Request Procedures
Routing
Monitoring
Incident Management Processes
• incident Detection and recording
• classification and initial support
• investigation and diagnosis
• resolution and recovery
• incident closure
• incident ownership, monitoring, tracking and communication
Change Management process
Problem/Error Database
Configuration Details
CMDB

Potential future Incident Management Information Flow for CC-IN2P3



Incident Management Processes

- incident Detection and recording
- classification and initial support
- investigation and diagnosis
- resolution and recovery
- incident closure
- incident ownership, monitoring, tracking and communication

Notes:
-No by-pass
with a direct call from Experiences to function

4.4.2. Service Desk

The Service Desk is not part of this Assessment. however, based on the different feedbacks and interviews, the DELL auditor defined that the current Score with CCMI of CC-IN2P3 is 2,14

4.4.2.1. Service Desk Definition

Tasks include handling incidents and requests, and providing an interface for other ITSM processes.

- Single Point of Contact (SPOC) and not necessarily the First Point of Contact (FPOC)
- There is a single point of entry and exit
- Easier for Customers
- Data Integrity
- Communication channel is streamlined

The primary *functions* of the Service Desk are:

- Incident Control: life cycle management of all Service Requests
- Communication: keeping the customer informed of progress and advising on workarounds

The Service Desk function is known under various names .

- *Call Center*: main emphasis on professionally handling large call volumes of telephone-based transactions
- *Help Desk*: manage, co-ordinate and resolve incidents as quickly as possible
- *Service Desk*: not only handles incidents, problems and questions but also provides an interface for other activities such as change requests, maintenance contracts, software licenses, service level management, configuration management, availability management, Financial Management and IT Services Continuity Management

The three *types* of structure that can be considered are:

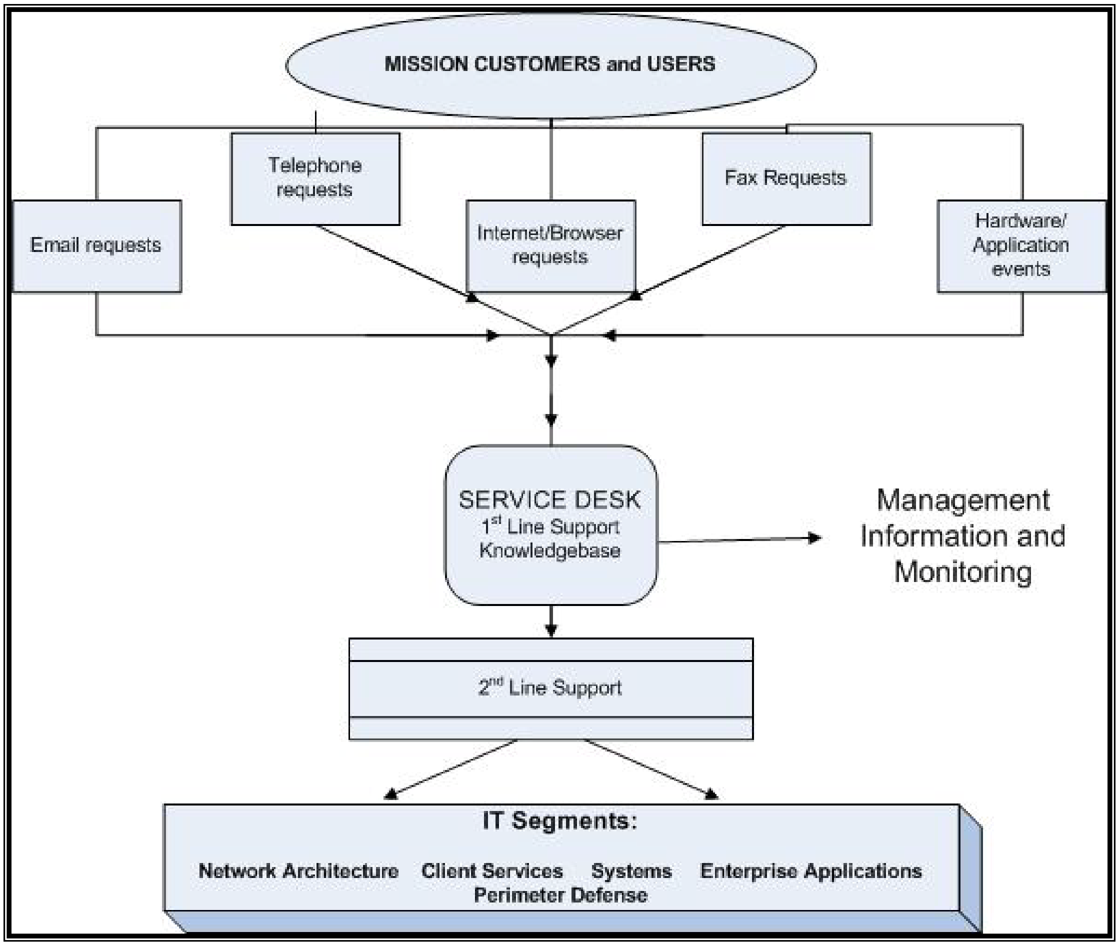
- *Local Service Desk*: to meet local business needs - is practical only until multiple locations requiring support services are involved
- *Central Service Desk*: for organizations having multiple locations - reduces operational costs and improves usage of available resources
- *Virtual Service Desk*: for organizations having multi-country locations - can be situated and accessed from anywhere in the world due to advances in network performance and telecommunications, reducing operational costs and improving usage of available resources

4.4.2.2. Service Desk Recommandation

Service Desk / Help Desk Recommandations

- Make Service Desk as the single point of contact for users to serve as the face of IN2P3 Villeurbanne IT; all minor issues should be resolved at this level to serve as first screening layer to minimize direct calls, emails and walk-ups to analysts
- Create a policy to drive all incidents through the Service Desk with prioritization based on business impact and urgency
- Track incidents and resolutions in a single database (which symbolically resides in the CMBD defined later in configuration management)
- Cross train personnel on key technology areas and applications (skills transfer taught by Subject Matter Expert)
- Create an initiative to get all the tribal knowledge incorporated in a centrally available Knowledge Base
- Update the CMDB with all information about configuration before closing events (incidents)
- Introduce common tools accessible and known by the entire organization with population processes and access right
- Introduce dropdown selections within closing root cause criteria (provides better reporting and trend analysis)
- Measure call flow into Service Desk staff to provide ongoing information about workload
- Strive to make help desk staff more efficient through process improvements garnered from experience, metric measurement and communication with other process owners and users
- Enforce accountability for consistent incident management processes with random Case Audits
- Establish an end user, customer satisfaction survey, to include help desk technicians and system engineers
- Establish a schedule for reviewing Help Desk processes and procedures for effectiveness

ITIL version of the Service Desk Flowchart



4.4.3. Problem Management

CC-IN2P3's self assessment score	2.66
DELL Assessment score	1.88

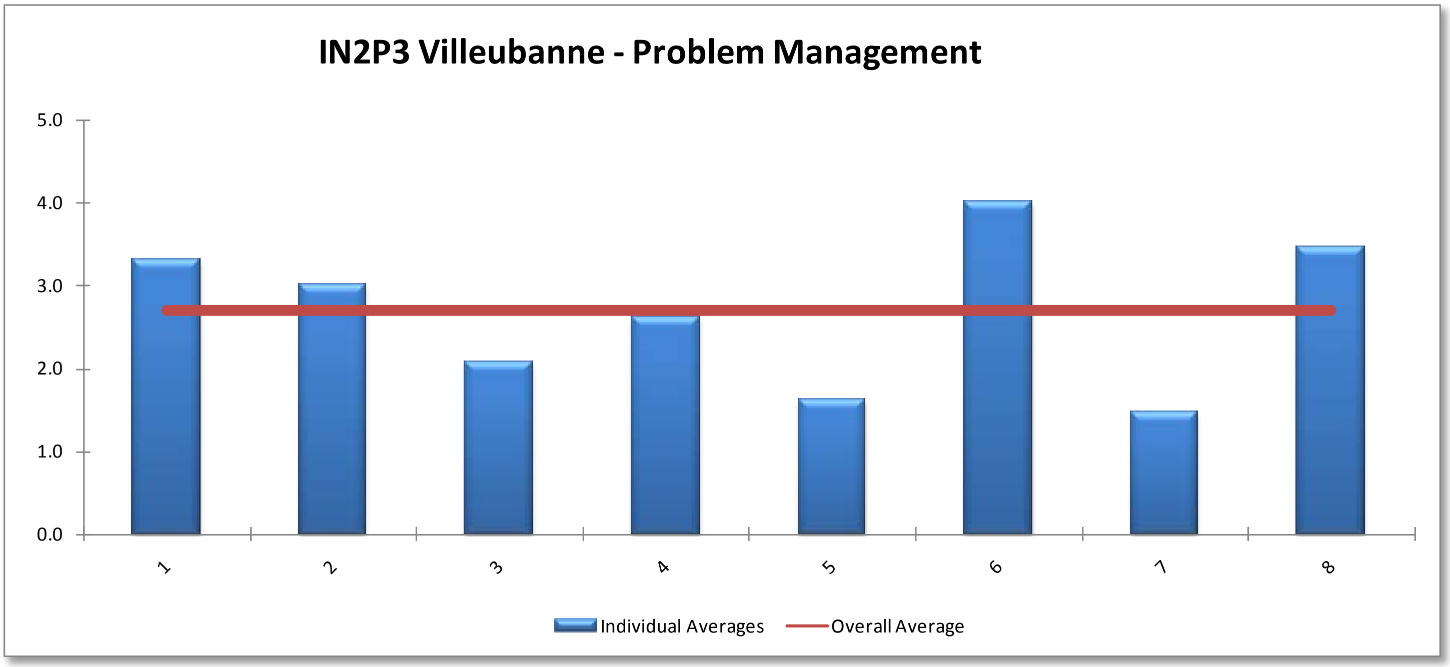
4.4.3.1. Discoveries

IN2P3 Villeurbanne does not have a formal Problem Management process in place and relies on individual technicians' experience and initiative. The incident management system, Rabbit, has limited capability for identifying problems as they arise. IN2P3 Villeurbanne does not have incidents and problem clearly differentiated, so there is a potential risk that errant changes can cause unrecognized repeating, risk-bearing incidents as the result of changes. The Help Desk functions are not effectively integrated with Change Management and there is no consistent Forward Schedule of Changes distributed to alert Help Desk personnel. This can negatively impact Incident control, reporting and logging functions. Unidentified problems can lead to significant incident churn, and the associated workload, as well as greater risk that changes made to the environment will risk degradation of the services IT is responsible for providing for the customer.

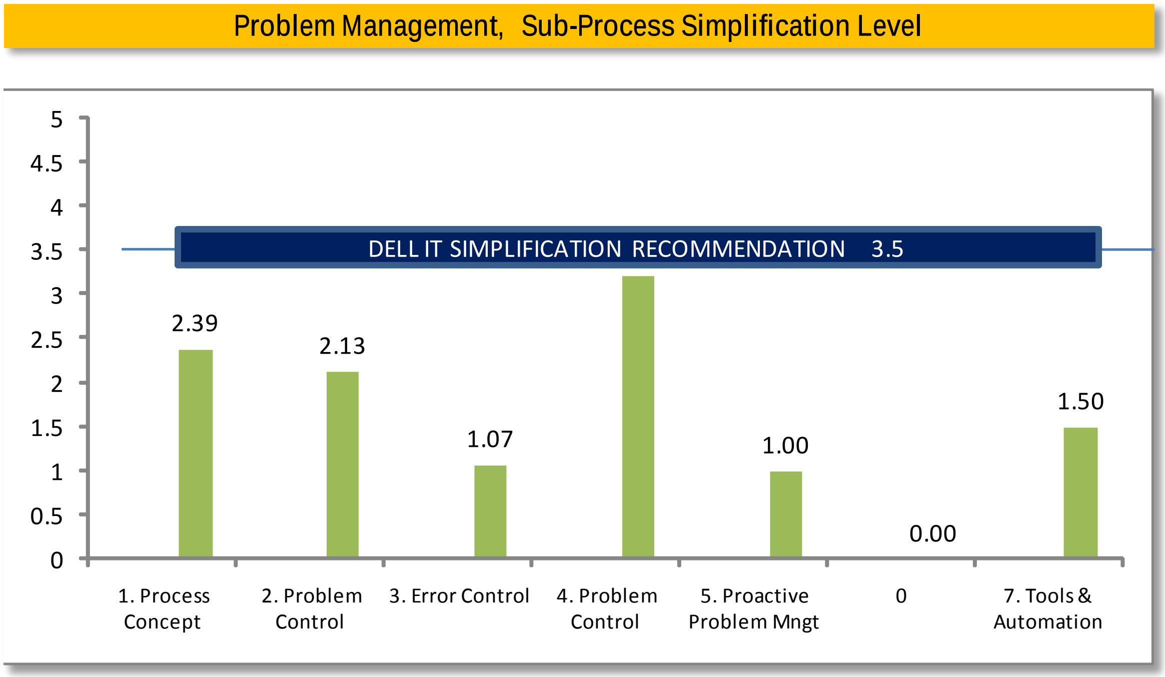
Only Problems with high visibility are handled by the board of directors. The only exception to this rule is Service Operations where there is periodic meeting to evaluate past and current issues and then define solutions and possible common or additional causes.

A defined troubleshooting methodology is missing. Only experience and brainstorming are used without guidelines which increases the time to resolve and the risk to partially solve all causes.

4.4.3.2. Participant Survey Results – Problem Management



4.4.3.3. DELL Assessment Results – Incident Management



4.4.3.4. What Participants told us about Problem Management

Management feedbacks

- important problems, are handled by management using a brainstorming process but it is not formal.
- communication is not normalized. It really depends on who is doing it.
- The weekly management committee has the role of scrubbing important incidents (only incidents with high visibility)..

Technician feedbacks

- User Group provided one example where a meeting solved a problem with an incorrect initial identification. This problem was solved during a meeting which was dedicated to follow any subjects around specific projects . Therefore we can conclude that a periodic follow-up meeting can improve the resolution of recurrent or complex issues.
- Owner teams inform the other functions about recurrent issues often by mail and some teams document important issues in a Word document.

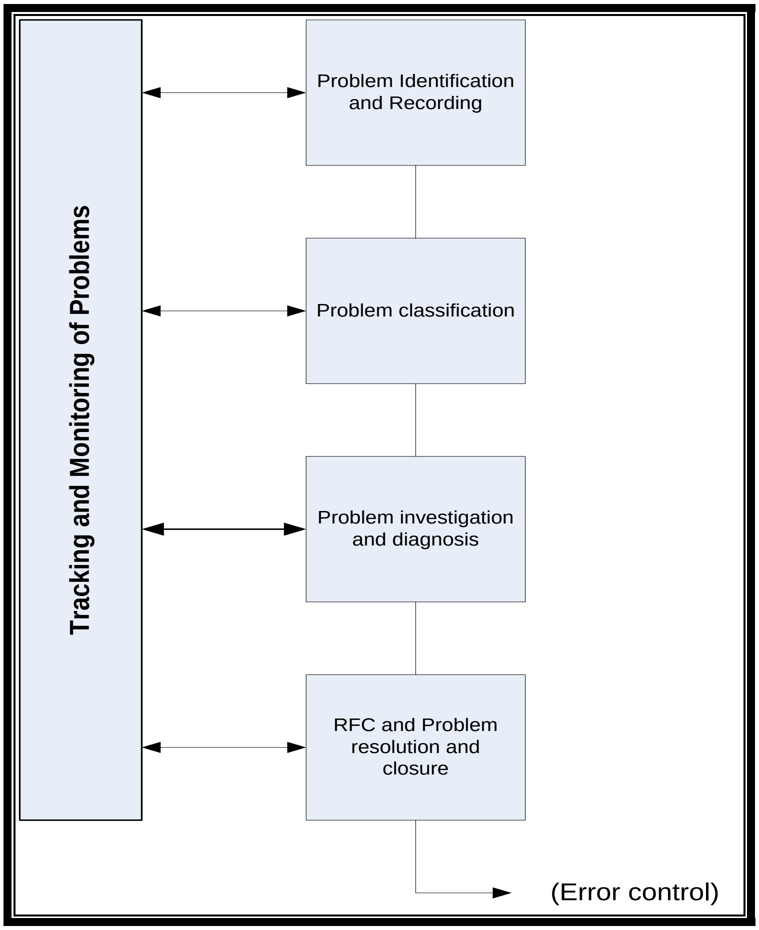
Common feedbacks

- There is no periodic meeting to analyze multiple problems and define one root cause. Only on the LHC project, the Service Operation and some teams participate in a weekly AT Grid Meeting where they discuss recent incidents. One person is designated to handle all the ELog (trace of problems) and try to define correlation.
- There is no accurate process to identify, analyze, document and then create an RFC (Request For Change). Usually it depends of the type of the complexity of the issue and management exposure to it.
- communication on problems to the other functions or experiments is based on mail and/or messages left on the CC-IN2P3 website.
- There is no troubleshooting methodology and no meeting defined specifically in case of long incident with all involved resources between functions. however, within a function, administrators generate a natural communication between them and take the time to explore solutions among them. The lack of troubleshooting methodology is covered by the experience/skills of the resources.
- There is no metric summary or report with statistics to follow and analyze trends at posteriori.
- problem management is more based on the strong experience and skills of the team than on a formal methodology. The majority of those interviewed think that the People are the fundamental pillar for Problem Management. Processes are not written and Products are often not implemented.
- People use various forums (jabber) to communicate between them and then exchange information about issues or subjects. This tools seems to be used more by the System team as it was the only team that talked about this.

4.4.3.5. Problem Management Recommendations

- Train staff using Problem identification and resolution methodology. Define a Facilitator who is a specialist in the methodology and can be used during unsolved problems.
- Create a plan to implement an adequate Problem Management process with complete Service Desk, incident, and Change Management process integration model
- Create a documented audit and analysis trail within the CMDB to support management reporting, business intelligence, problem recognition and resolution
- Implement a problem categorization and prioritization function to prioritize known problems for resolution within the Change Management process
- Create, monitor and manage a Problem database alongside the Service Desk's Knowledgebase
- Empower the appropriate individuals to mine the CMDB for problems and develop opportunities for improvement
- Survey users and other relevant stakeholders to assure that problems are effectively resolved and make enhancements to the KB based on user feedbacks
- Improve the metrics in regards to evaluation, measurement and improvement (Metrics: Change Success Rate, Reason to Improve …)
- Define a Problem Manager role in the organization
- Problem Manager will take the lead on periodic meeting across teams and organization to review past and current issues and then define common causes

Problem Management (ITIL pratices)


Tracking and Monitoring of Problems
Problem Identification and Recording
Problem classification
Problem investigation and diagnosis
RFC and Problem resolution and closure
(Error control)

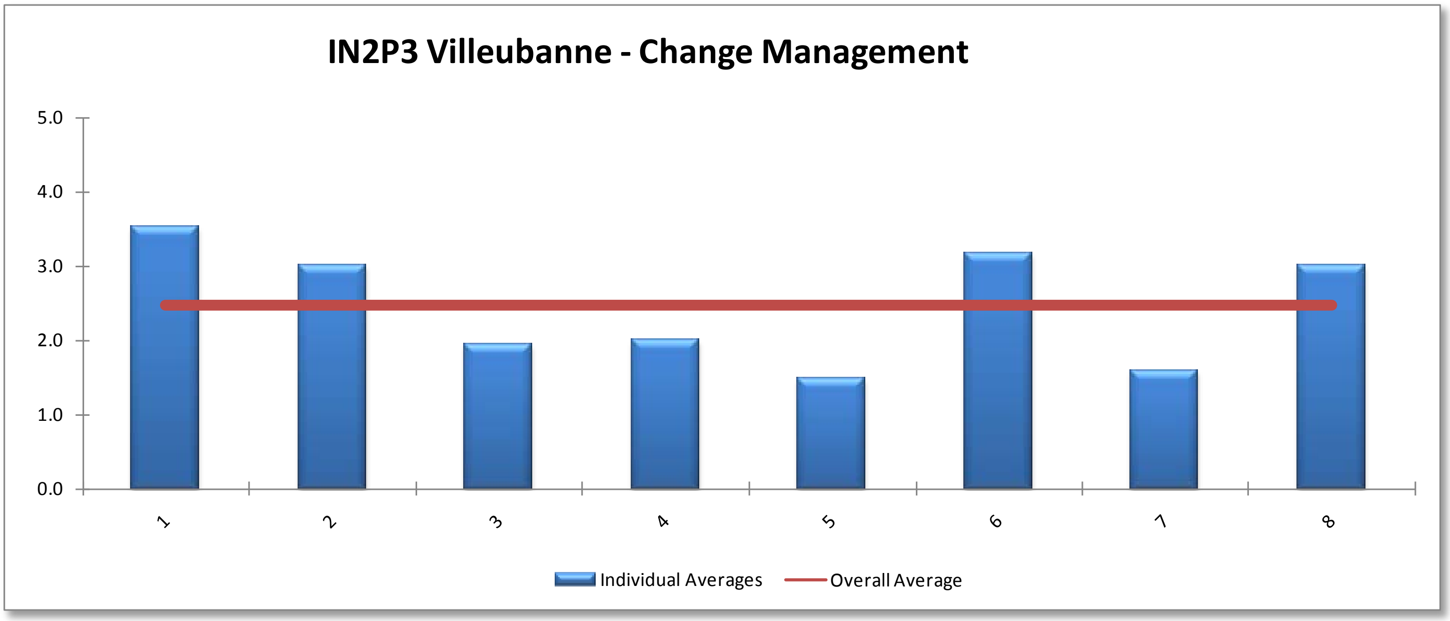
4.4.4. Change Management

CC-IN2P3's self assessment score	**2.36**
DELL Assessment score	**1.50**

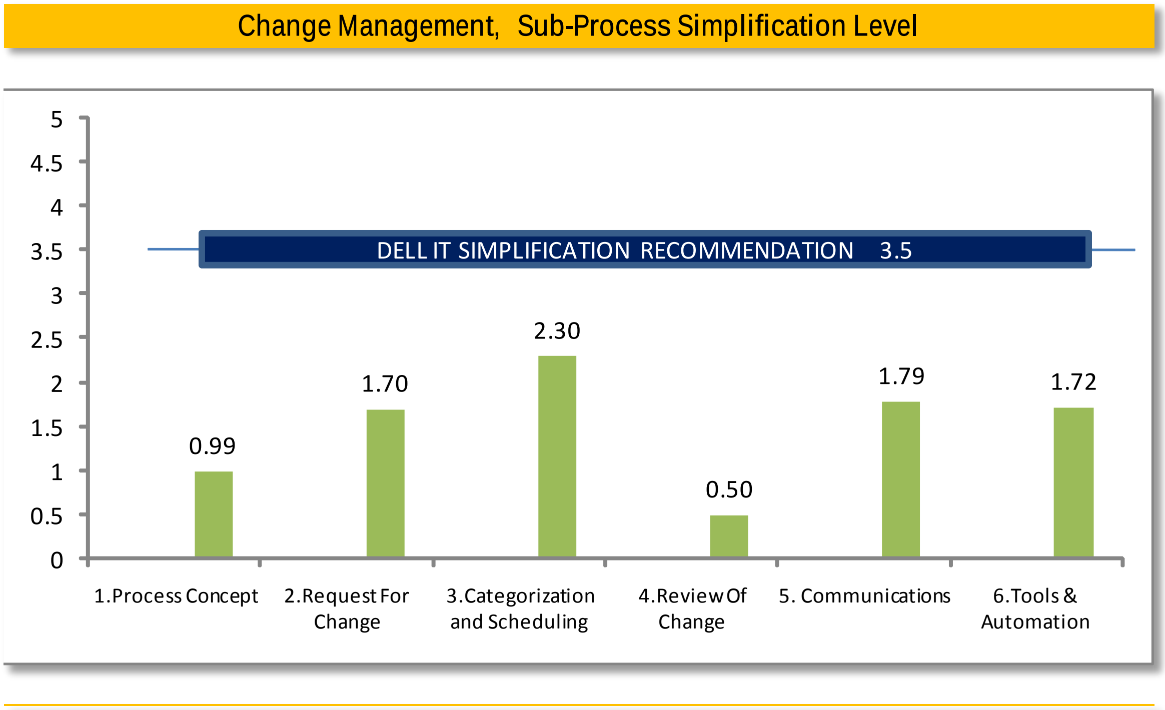
4.4.4.1. Discoveries

Because there is no consistent, common and formal process for change control (only main maintenance windows and important project are monitored),, CC-IN2P3 experiences unplanned service disruptions. The organization has attempted to respond to this by scheduling initiative based (vs. process based) stakeholder meetings to evaluate limited critical changes but not always based on urgency and priority. When they do meet, they follow a reasonably structured process that involves, testing critical changes, notifying the help desk of the change and so on. CC-IN2P3 would benefit by evaluating this ad-hoc process for effectiveness then installing a clearly defined Change Advisory Board that met regularly to evaluate RFCs based on urgency and priority, put all changes through the appropriate release management and had change notification policies in place.

4.4.4.2. Participant Survey Results – Change Management



4.4.4.3. DELL Assessment Results – Incident Management



4.4.4.4. What Participants told us about Change Management

Management feedbacks

- The board of directors is the main authorization body for important changes.
- There is a logbook system where each team can record information and changes with regards to their activity.
- With regards to the type of maintenance, the service operation has formal timelines to inform end users.
- On safety management, the infrastructure team follows each change and document them.
- management thinks that the IT organization is well-balanced between stability and adaptability.

Technician feedbacks

- CC-IN2P3 encountered some issues during the last maintenance week-end with regards to some missed synchronizations in the change.
- There is no back-out plan defined before a change but interviewed people continually work to keep backup and restoration points available.
- Team members think that the IT organization is more adaptive than stable.
- The system team is working to create a robot which can handle changes on servers.
- For important changes, there is a migration committee which has the goal of defining implementation methodology.

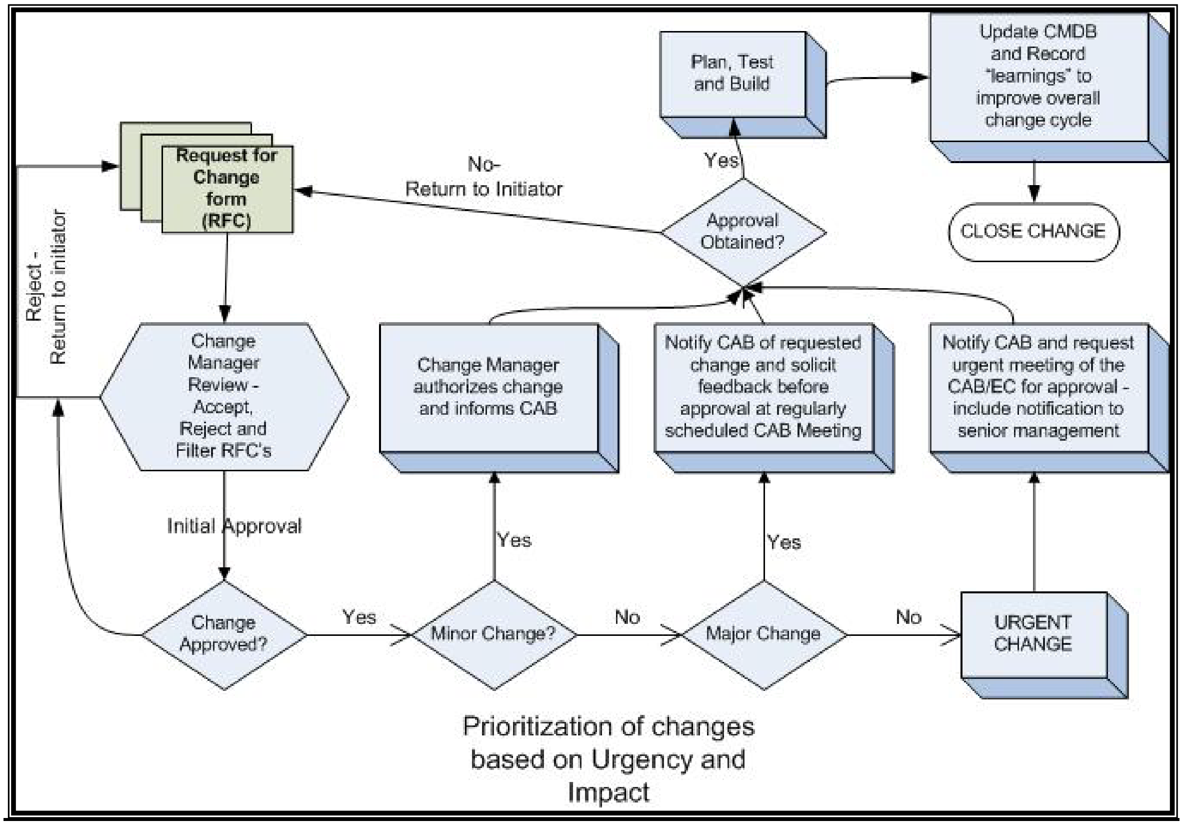
Common feedbacks

- CC-IN2P3 applies a change methodology during main projects.
- There is no methodology for change following incident or problem resolutions:
- During an incident the administrators take the decision themselves to apply a change with regards to their knowledge of the environment.
- For other changes, the decision is taken by the Team Manager or the Team Leader (except important change decisions taken during the management board)"
- There is no Change Advisory Board (CAB) to check all the change and no Change Manager to authorize (Only one interviewed person said that they have something similar to a CAB in their team)
- There are 4 main maintenance windows (complete shutdown) for the site. The project manager for each maintenance lists all the changes. This list usually doesn't contain changes with regards to past incidents.
- change management activities don’t use a control methodology.
- Most of those interviewed think that the organization is more based on People. There is Process on main projects and a few Products (basic tools such as spreadsheet).
- Example: Issue during the last Maintenance Windows because the Infrastructure team planed an intervention on the second Power Circuit during a shutdown of the first.

4.4.4.5. Change Management Recommendations

- Regroup all changes in one common list. This list needs to contain all changes with regards to the application in continual service improvement and for future corrections based on incident learning. Each change must be qualified on urgency and impact criteria.
- Form a Change Advisory Board (CAB) of business owners and stakeholders that meets consistently to review changes that have been submitted through prearranged methods such as an RFP. Ensure there is a process in place for emergency changes.
- Define a Change Manager role in the organization
- Document and communicate all methods and procedures from beginning to end and enforce those procedures.
- Document all Requests for Change (RFC's) in a CMDB and filter RFC's for completeness, quality or duplication so there is a record of changes available for forensic reporting.
- Align with vendors to include changes required by critical patches and updates
- Make a requirement that all changes be submitted to release management and appropriately tested in lab environments before implementing them in production
- Define and report on Key Performance Indicators (KPI's) so that the success of a change can be measured
- Create a clear audit trail of all changes by documenting KPI's, change revisions, and feedback in the CMDB
- Set up a Continual Service Improvement (CSI) process & survey customers to learn to improve future updates
- Perform irregular audits to check for staff compliance to change management standards and report on results so improvements can be measured and celebrated
- List all your changes in one main document where you will classify changes by impact and priority (urgent or not). The list will be follow by the CAB who will validate each change with a global correlation and propose a calendar to apply them (low impact can be directly apply and high impact must be plan during the next maintenance windows . Notes: CAB is not the authority who authorize the change. Only the Change manager can do that.
- It is important to be able to track how many changes create an incident in the future (metric named "Change Success Rate"). This information will be key to evaluate the quality of your change processes. Usually between 20% and 35% of changes generate an incident. Organization well prepare can lower this statistic to 5%.

Change Management (RFC) (ITIL pratices)


Plan, Test and Build
Update CMDB and Record "learnings" to improve overall change cycle
Request for Change form (RFC)
No- Return to Initiator
Yes
Approval Obtained?
CLOSE CHANGE
Reject - Return to initiator
Change Manager Review - Accept, Reject and Filter RFC's
Change Manager authorizes change and informs CAB
Notify CAB of requested change and solicit feedback before approval at regularly scheduled CAB Meeting
Notify CAB and request urgent meeting of the CAB/EC for approval - include notification to senior management
Initial Approval
Yes
Yes
Change Approved?
Yes
Minor Change?
No
Major Change
No
URGENT CHANGE
Prioritization of changes based on Urgency and Impact

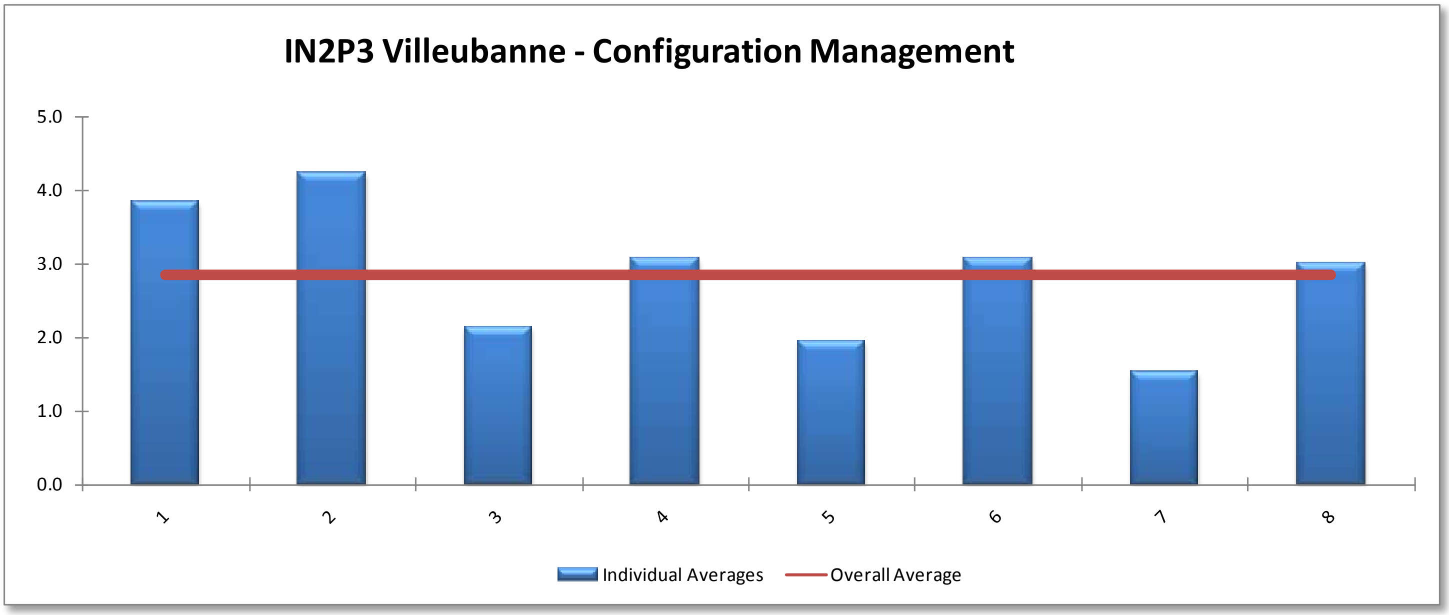
4.4.5. Configuration Management

LA Dept of Revenue's self assessment score	2.88
ITSM Review Team Assessment score	2.38

4.4.5.1. Discoveries

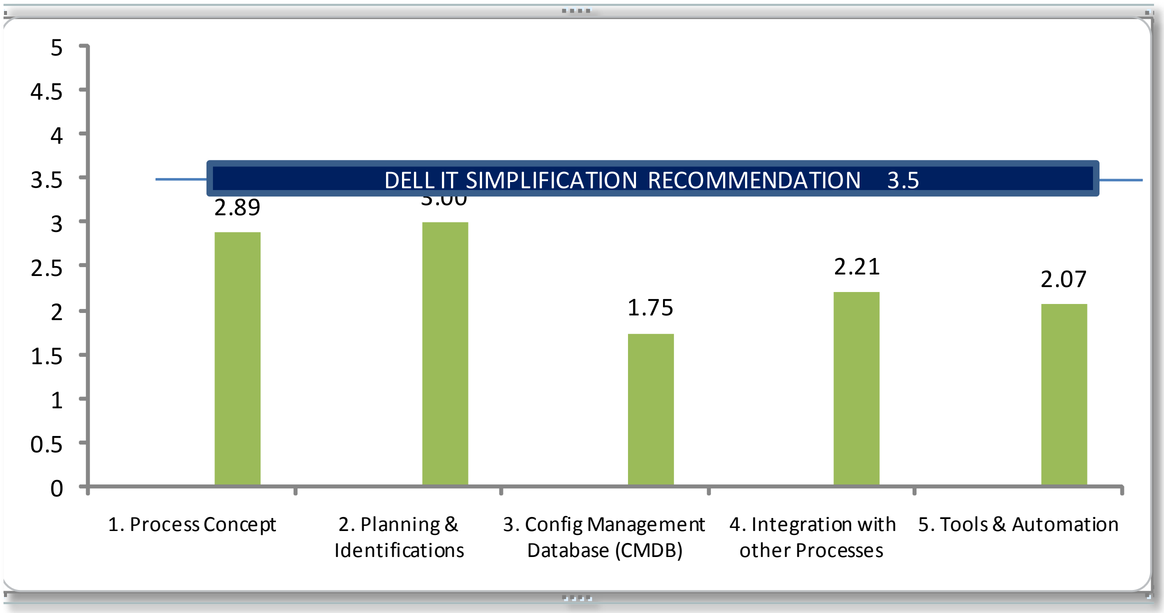
Attempts have been made to document IT assets. Most of the configuration details and assets are documented in spreadsheets or on SharePoint or dedicated tools. Several systems are in place; inventory spreadsheets and system information exist at system admin, departmental, group or team level. These documentation initiatives are not centrally controlled in terms of content or frequency of updating. Links between Configuration Items are not present and this doesn't help for future correlations. Not all the teams are always documented the different release and reasons for change which could generate issues during a back-out. However all information are available from dedicated tools or spreadsheet with guarantying to follow up and future control. But the lack of globalization of tools are limiting the vision at a team level.

4.4.5.2. Participant Survey Results – Configuration Management



4.4.5.3. DELL Assessment Results – Incident Management

Configuration Management, Sub-Process Simplification Level



4.4.5.4. What Participants told us about Configuration Management

Management feedbacks

- No feedbacks only common to Management

Technician feedbacks

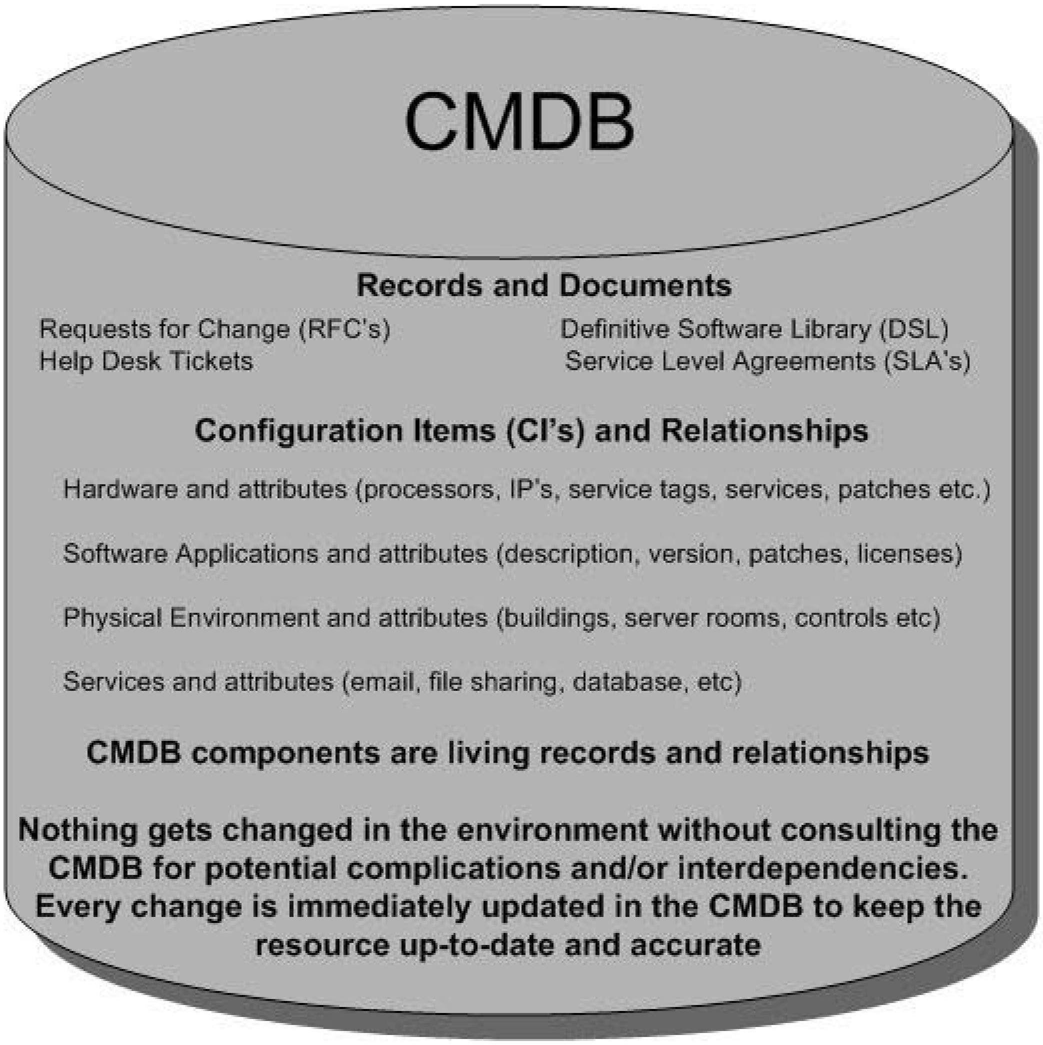
- The system team has a database which contains all the release notes with regards to past changes.
- The Network team records the history of the network device configuration on a central SharePoint but it is not periodic (human request).

Common feedbacks

- Each team has his own inventory of assets and licenses (excel file, database).
- There is no correlation between each inventory.
- IN2P3 is currently performing a global inventory of assets with deeper information on consumption, cooling …
- Some licenses are followed but not all.
- Most of those interviewed indicated that People and Products are the main pillars of the change management.
- On Laptops and desktops, it is difficult to follow the licenses and gather the local information as a part of CC-IN2P3 reinstalls their operating Systems themselves without agents.
- On Laptops and desktops, the life cycle of each product is followed (order number, age, …)

4.4.5.5. Configuration Management Recommendations

- Merge all the current databases and spreadsheets in one main tool for the entire organization.
- Evaluate the discrete systems already in place and see where they can be leveraged into one effective system to Implement, define and expand a Configuration Management Database (CMDB) that identifies and records configurations items and their relationships to the underpinning IT services.
- Start with a high-level scope and then modify gradually as changes are made to the environment. Each time a change is made, make sure the CMDB is modified thus using the change process to help drive accuracy of the CMDB.
- Establish a single point of ownership and accountability for the CMDB
- Implement an audit schedule for checking CMDB data against the physical environment to ensure and verify accuracy of the CMDB
- Document rules for making changes to the CMDB, communicate and enforce them.
- Integrate the CMDB with the other core IT processes, especially Incident and Change Management to ensure on-going changes continue to be documented.



CMDB

Records and Documents

Requests for Change (RFC's)
Help Desk Tickets
Definitive Software Library (DSL)
Service Level Agreements (SLA's)

Configuration Items (CI's) and Relationships

Hardware and attributes (processors, IP's, service tags, services, patches etc.)

Software Applications and attributes (description, version, patches, licenses)

Physical Environment and attributes (buildings, server rooms, controls etc)

Services and attributes (email, file sharing, database, etc)

CMDB components are living records and relationships

Nothing gets changed in the environment without consulting the CMDB for potential complications and/or interdependencies. Every change is immediately updated in the CMDB to keep the resource up-to-date and accurate

5. General recommendations

5.1. First Steps

- Fund and require ITIL Foundations training for all full-time IT personnel
- Participate in a Service Definition Workshop and/or Dell ITSM Executive Briefing
- Strengthen internal communications with regular informal "brown bags" to discuss any new initiatives, strategy, KPIs, challenges or communication disconnects
- Use this assessment as a starting place for discussing and planning a path forward, implementing continuous process improvement and a movement toward ITSM best practices
- Perform a yearly follow up ITMSr Assessment to gauge process improvement
- Embed a "generate, test and improve" framework into your process set.

5.2. Continuous Service Improvement Recommendations

Disclaimer: **While ITSM frameworks are very useful for conceptualizing an idealized IT Service environment, they are NOT a set of requirements to be implemented 'into'. These concepts are a tool for guidance and can be used as templates when the business case deems it appropriate and pragmatic to do so.**

Establishing a Continuous Process Improvement program to support IN2P3 Villeurbanne business mission built around ITIL®/ITSM best practices requires more than just an executive decision to implement change.

ITSM requires that all personnel within the IT environment speak and think in a common language. Process design and control requires a culture change - a well-defined break with out-of-process behavior and unidirectional modes of communication in favor of multi-directional information flow, new and deliberate processes and ways of getting things done.

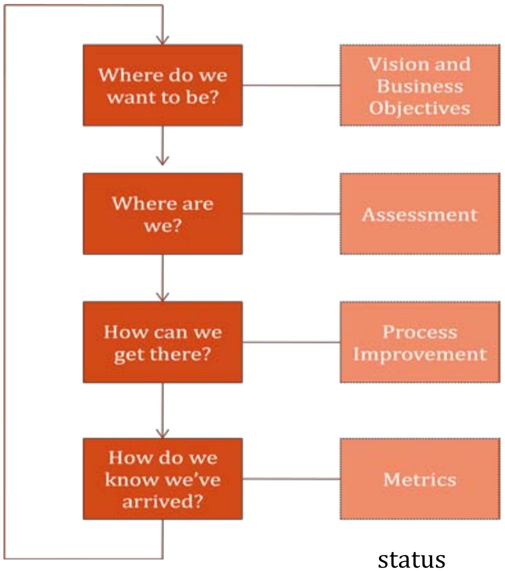
IT staff and stakeholders must be onboard with the program and agree to participate wholeheartedly to the extent possible. All involved should achieve understanding of the ITSM/ITIL® framework and the interdependency of the ITIL® Service Support processes. Even further, all IT agents should understand how their role fits into the bigger picture.

Without a clear and fully embraced program, the effort will fail and eventually fissile out. Done properly, the effort has a better likelihood of igniting centers of innovation and embedding processes that maximize mission objectives and a more efficient and effective use of material, effort and manpower.

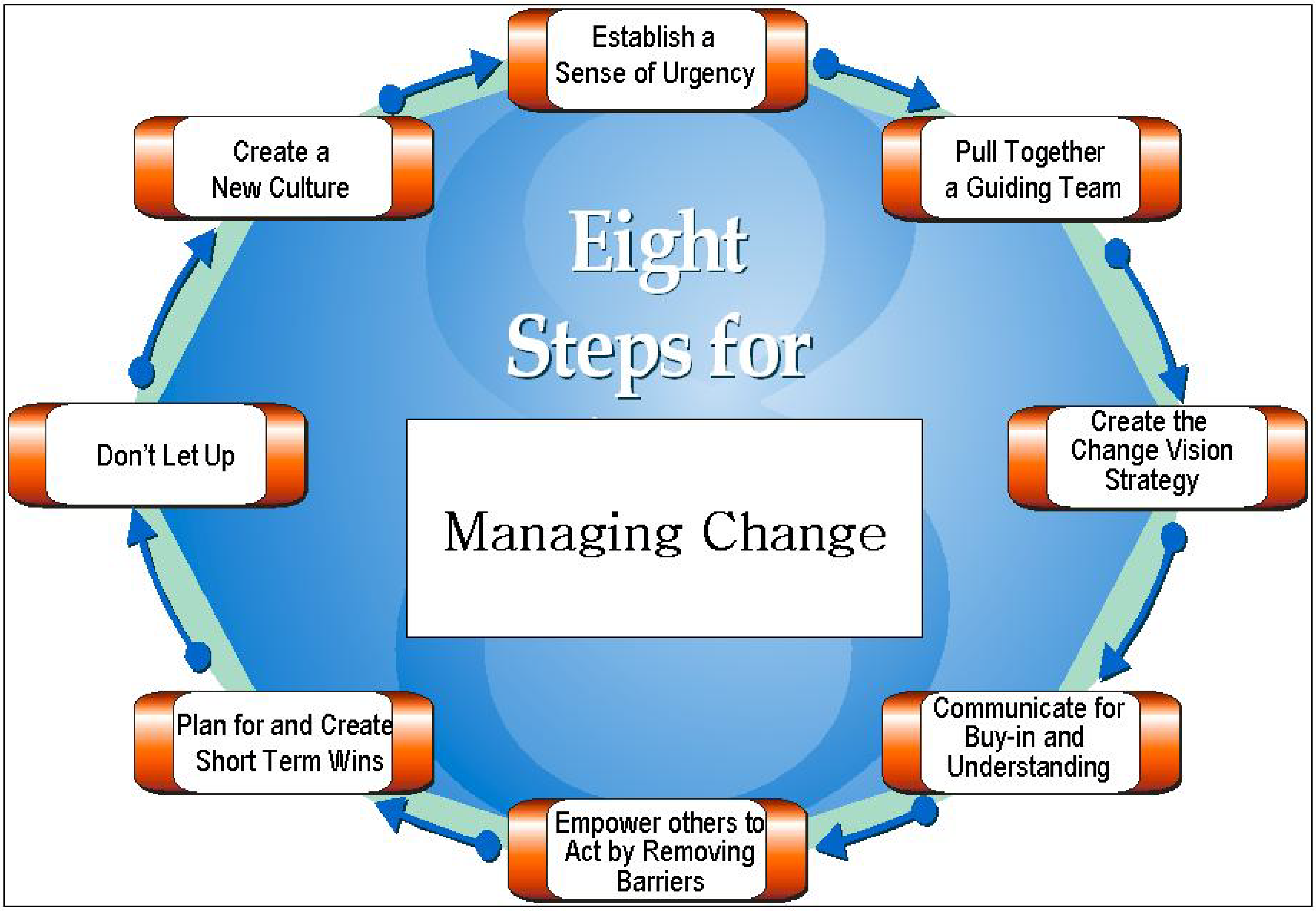
Implementing Best Practices - Potential Complications:

- Executive management buy-in is an absolute pre-requisite for a successful ITSM effort
- Many ITSM process implementation efforts are sidetracked by overly aggressive time frames. Trying to make too many improvements at once can lead to frustration (objectives are not met and/or too many complications arise). It is better to achieve a few "small wins" and proceed in phases to build confidence in the program
- Getting started can take a while and require significant effort because the implementation of best practices requires a change of culture within the organization
- If process structure mistakenly becomes the objective, rather than the optimized business outcomes, the service quality may be adversely affected; procedures can become bureaucratic obstacles that people learn to avoid
- A solid understanding of how committing to new processes and how success is going to be measured is necessary for success with process change and control
- Leaving the development of process structures to a group of specialists may isolate them from the rest of the organization and set out on a direction that is not acceptable to other departments
- If there is insufficient investment in tools, the processes will not do justice and service may not be improved
- CMDB development requires many tentacles and dynamic feedback loops from the entire process spectrum. Many organizations have asset management tools in place that they mistakenly confuse for a complete CMDB (of which asset management is only a subset)

Create a Cultural Environment for Process Control and Improvement s



- Provide training for IT Staff on ITIL® Best Practice Methods to produce ITSM champions throughout the organization so everyone will be speaking a common language
- Create a organizational focus on a Continuous Process Improvement program
- Create a clearly communicated and highly interactive readiness for change:
  - Establish a sense of urgency
  - Pull together a guiding team
  - Develop the change vision strategy
  - Communicate clearly and widely to achieve unanimous buy-in and understanding
  - Empower others to act on the vision by removing barriers
  - Plan for and create short term wins and don't let up
  - Implement and organizational culture change
- Treat this as a cultural change. Create communication channels, contests, and winning culture activities around your continuous process improvement vision
- Pursue bi-directional communications and establish well-defined roles
- Create more operational visibility for technical staff of IT infrastructure status and open incidents
- Understand where you want to be by when (What can reasonably be expected?)
  - Strategic objectives
  - Tactical goals
  - Operational goals
  - When can we achieve control?
  - When can we achieve integration?
  - When can we achieve optimization?
- Identify all existing IT customers (internal and external)
  - Understand what they want by talking to them and documenting what they say
  - Determine how to measure what they want
  - Analyze negative/positive effects on customer and put a dollar value to it.
  - Determine volume (how often it occurs in the environment) of each opportunity in order to prioritize
- Create a Service Catalog that documents all services needed to support required business
  - A Service Catalog is like a lunch menu with a table of contents to communicate services to customers
- Review current Key Performance Indicators (KPI's) for appropriateness
  - Determine which ones to retain, remove and add
  - Build KPI's into processes as a way to measure success
  - Develop contests and rewards for meeting KPI's
- Define and document the interrelationships between cross-functional units so they support the business requirements and add value to the end result
- Create a staffing model to support business requirements. Identify job roles, responsibilities and advancement using a best practice framework and incorporate job descriptions, progressive skill levels and success measures.
- Prioritize services to work on first using pain/volume analysis.
  - Set clear expectations for service
    - Business requirements and capabilities
    - Negotiate Service Level Agreements (SLAs) with customer, otherwise, results are hard to measure


Eight Steps for
Managing Change
Establish a Sense of Urgency
Pull Together a Guiding Team
Create the Change Vision Strategy
Communicate for Buy-in and Understanding
Empower others to Act by Removing Barriers
Plan for and Create Short Term Wins
Don't Let Up
Create a New Culture

(John Kotter, "Our Iceberg is Melting")

5.3. Establish Roles: (these may or may not be individual people)

- **Designate an IT Service Management (ITSM) Steering Committee –**
    - Steering Committee (**SC**) members guide and oversee the entire ITSM effort and should include the Program Director, Program Manager, Process Owners, representative Customer Stakeholders, Process Architects and ITSM Subject Matter experts
- **Designate an ITSM Program Director (PD)-**
    - The primary role of the Program Director is to instill and maintain the committed organization-wide buy-in is required to successfully implement an ITSM effort
- **Designate an ITSM Program Manager (PM) –**
    - This role is responsible for all ITSM implementation activities. These activities include meeting objectives, process quality standards and timelines for delivery
    - The PM assigns and oversees "initial win" process implementation projects to Project Managers; coordinates ITSM/ITIL® Foundations training for all IT staff; regularly reports program-wide status, progress and bottlenecks to the SC for review and/or resolution; creates program-wide work plans and provides overall leadership and management of the entire implementation effort. The PM has a clearly defined escalation path to the PD
- **Designate Project Managers –**
    - Project Managers oversee the "initial win" projects assigned to them by the PM. They provide direction to project teams; regularly report project-level status, progress and bottlenecks to the PM for review and/or resolution; interface with the other Project Managers to discuss and coordinate initiatives; create project-level work plans and implementation schedules; and provide overall leadership and management of project effort, planning and deliverables. Project Managers have clearly defined escalation paths to the PM
- **Designate Process Owners –**
    - Process Owners are responsible for their assigned ITSM Processes; they coordinate and oversee all activities within the process; make changes to the ITSM process in response to feedback (Continuous Process Improvement); communicate with the other Process Owners for coordination of process decisions and activities; and evangelize process concepts and solutions to others. Process Owners have clearly defined escalation paths to the PM for resolution of issues or bottlenecks that might hinder the Process Owner's ability to maintain the integrity of the process under his/her control
- **Designate Core Team Members –**
    - Core Team Members implement ITSM solutions and communicate with the Process Owner for direction and feedback. Core Team Members also communicate with Users of the process to gather requirements; manage process documentation, metrics, develops process educational material and ensures that communication between all ITSM processes is occurring dynamically
- **Subject Matter Experts and the Process Architect –**
    - These roles provide the expertise necessary to plan, implement, evangelize and coordinate process designs and activities across the entire process architecture

APPENDIX A: CMMI Capability Levels

Capability Level 1: - Initial

"There are ad-hoc activities present, but success depends on individual skills and follow-through rather than on specific formal processes."

Maturity level 1 organizations do not have a formal documented process plan in place. At maturity level 1 the organization usually does not provide a very stable or consistent environment since IT processes are ad-hoc.

Success at maturity level 1 depends on the competence and heroics of the people in the organization and not on proven, codified processes. In spite of this ad hoc and chaotic environment, maturity level 1 organizations often produce services that work, but are prone to breakdown under duress.

Capability Level 2: - Repeatable

"We are aware of the process we are supposed to follow, but some of the elements are still incomplete or inconsistent; we have no overall measurements, reporting or controls."

At maturity level, 2 successes are repeatable for all the segments of the IT organization. Basic processes are established to track incidents.

A minimal process discipline is in place to repeat earlier successes in service restoration or resolution of the root cause of incidents that reoccur. There is still a significant risk of downtime and service interruption. The organization may use a software tool to manage incident flow and asset control, but it is often incompletely deployed and does not follow best practices or inter-relate important ITSM processes

Process discipline helps ensure that existing practices are retained during times of stress. The practices that *are* in place are usually followed, performed and managed according to their documented plans.

Capability Level 3: - Defined

"Processes are well defined, understood, implemented and measured." At maturity level 3, the organization's set of standard processes are established and improved over time. These standard processes are used to establish consistency across the organization. Tasks, roles and authorizations are well defined and communicated.

The organization's management has established process objectives, codified a set of standard processes and ensures that these objectives and process activities are appropriately addressed and followed.

A critical distinction between level 2 and level 3 is the scope of standards, process descriptions, and procedures. At level 2, the standards, process descriptions, and procedures may be quite different in each specific instance of the process (for example, for one internal organizational unit to another). At level 3, the standards, process descriptions, and procedures are tailored from the organization's set of standard processes to suit a particular project or organizational unit.

- Processes are managed and fit well with the organization objectives and goals
- Supplies desired work outputs that can be measured
- Process improvements can be derived and implemented from process measurements
- Well-defined processes include: Purpose, Inputs, Entry Criteria, Activities, Roles, Measures, Verifications steps, Outputs, Exit criteria

Capability Level 4: - Quantitatively Managed

"Inputs from processes come from other well-controlled processes; outputs from processes go to other well-controlled processes."

- Managed process statistically or quantitatively controlled
- Process quality and performance are understood quantitatively and managed
- Quantitative objectives are based on: capability of organizational standard processes, business objectives, customer needs, end users and process implementers
- Personnel performing the process are formally involved in quantitatively managing it

Using precise measurements, management can effectively control their service support effort. In particular, management can identify ways to adjust and adapt the process to particular aims without measurable losses of quality or deviations from specifications.

Quality and performance metrics transferred between processes. Sub processes are selected that significantly contribute to overall process performance. These selected sub processes are controlled using statistical and other quantitative techniques.

A critical distinction between maturity level 3 and maturity level 4 is the predictability of process performance. At maturity level 4, the performance of processes is controlled using statistical and other quantitative techniques, and is quantitatively predictable. At maturity level 3, processes are only qualitatively predictable.

Capability Level 5: - Optimizing (Nirvana)

"We have optimized, well-defined, codified and universally followed processes in place. The outputs of the processes are quantitatively managed and monitored. Processes are continuously improved based on what we learn."

Maturity level 5 focuses on continually improving process performance through both incremental and innovative technological improvements. Quantitative process-improvement objectives for the organization are established, continually revised to reflect changing business objectives, and used as criteria in managing process improvement. The effects of deployed process improvements are measured and evaluated against the quantitative process-improvement objectives. Both the defined processes and the organization's set of standard processes are targets of measurable improvement activities.

Optimizing processes that are nimble, adaptable and innovative depends on the participation of an empowered workforce aligned with the business values and objectives of the organization. The organization's ability to rapidly respond to changes and opportunities is enhanced by finding ways to accelerate and share learning.

A critical distinction between maturity level 4 and maturity level 5 is the type of process variation addressed. At maturity level 4, processes are concerned with addressing special causes of process variation and providing statistical predictability of the results.

Though processes may produce predictable results, the results may be insufficient to achieve the established objectives. At maturity level 5, processes are concerned with addressing common causes of process variation and changing the process (that is, shifting the mean of the process performance) to improve process performance (while maintaining statistical probability) to achieve the established quantitative process-improvement objectives.

APPENDIX B: ITIL® Best Practice Outlines

The Service Desk Function Best Practices Outline:

Service Desk Objective: All communication between users and support personnel should occur through the Service Desk function.

The Service Desk is a single-point-of-contact (SPOC) for users and customers for assistance with incidents and inquiries and serves like a front office for the other IT departments. Ideally, the Service Desk can deal with many customer incidents and queries without even needing to contact specialist personnel. This capability relies on the existence of a strong environment-wide online Knowledge Base.

By serving as an initial and single point of contact, the Service Desk reduces the workload on other IT departments by intercepting irrelevant questions and those, which are easily answered and resolved. The Service Desk acts as a filter that only lets calls through to second and third-line support when this is actually necessary. Service Desk personnel provide comfort to users and ensure that they do not have to search endlessly for a solution.

With access to an accurate Change Management Database (CMDB), incident tracking and management tools, the Service Desk can provide consistent service and consistent access to the resources required for satisfactory issue resolution.

Service Desk Best Practices

A mature Service Desk function incorporates:

- Policies, Processes and Procedures that are in alignment with Business objectives & ITIL
- A dedicated Service Desk Function owner
- Centralized function for incident and request handling
- Ongoing monitoring and management of customer satisfaction
- Strong levels of incident communications and ownership
- Right level of support and customer care skills among Service Desk staff and management

Critical Success Factors (CSFs)

The Critical Success Factors (CSFs) are:

- Ensure long-term Customer retention and satisfaction
- Assist in the identification of business opportunities
- Reduce support costs by the efficient use of resource and technology

Key Activities

The key activities for this function are:

- Provide advice and guidance to customers
- Communicate and promote IT services
- Manage and control service communications to customers, suppliers and the business
- Coordinate Incident Management activities
- Manage people, processes and technologies that form the contact infrastructure
- Provide management information about Service Desk quality and operations

Key Performance Indicators (KPIs)

Examples of Key Process Performance Indicators (KPIs) are shown in the list below. Each one is mapped to a Critical Success Factor (CSF).

- Ensure long-term customer satisfaction
- Percent of customers given satisfaction surveys
- Customer satisfaction rating of Service Desk
- Percent of caller hold times within service targets
- Percent of calls responded to within service targets
- Number of Incident records not yet closed
- Number of calls abandoned
- Assist in the identification of business opportunities
- Number of calls referred to sales organization
- Reduce support costs by efficient use of resources and technologies
- Percent of calls resolved at the service desk without escalation
- Staff-turnover rate
- Overall cost-per-call

Incident Management Best Practices Outline:

Incident Management Objectives: The goal of **incident** management is to restore standard service functionality as quickly as possible, while minimizing undesirable impact to productive business operations.

Incident Management Best Practices

A mature Incident Management process incorporates:

- Policies, Processes and Procedures that are in alignment with Business objectives & ITIL®
- Defined incident escalation standards and well-defined and negotiated SLA's
- A dedicated Incident Management Process Owner (with clear accountability for the entire process)
- Incident classification categories; Incident prioritization (critical, urgent, normal, information request)
- Complete, accurate and frequent Incident reports (operational summery and drill-downs)
- Ongoing process communication and education for IT staff. (ITIL® training for entire staff)

Use Key Critical Success Factors (CSFs)

- Consistent maintenance of IT Service Quality
- Consistently high Customer Experience (CE) results based on regular customer surveys
- Number of Incidents resolved and not-resolved Within Established Service Times

Key Activities

The key activities for this process are:

- Detect and record incidents
- Classify incidents
- Provide initial incident support
- Prioritize incidents based on impact and urgency
- Investigate and diagnose incidents
- Resolve incidents and recover service per agreed service levels
- Closing incidents
- Maintain ownership, monitoring, tracking and communications about incidents
- Provide management information about Incident Management quality and operations

Key Performance Indicators (KPIs)

Examples of Key Process Performance Indicators (KPIs) are shown in the list below. Each one is mapped to a Critical Success Factor (CSF).

- Maintenance and regular surveys of IT Service Quality and Customer Satisfaction
- Number of incidents in each Severity level or other category (total and by category)
- Number of incidents incorrectly categorized and/or incorrectly escalated
- Number of incidents bypassing Service Desk
- Number of incidents not closed/resolved with workarounds
- Number of incidents resolved before customers notice
- Number of incidents reopened
- Number of User/Customer surveys sent and responded to
- Average User/Customer survey score (total and by question category)
- Average queue time waiting for Incident response

Problem Management Best Practice Outline:

Problem Management Objectives: *A **problem*** is often identified as a result of identifying multiple Incidents exhibiting common symptoms. The goal of this process is to resolve the root cause of these Incidents, minimize the impact on the business and to prevent the recurrence of Incidents.

Problem Management depends on an efficient and well-executed Incident Management process.

Problem Management Best Practices

- Policies, Processes and Procedures that are in alignment with Business objectives & ITIL®
- A dedicated Problem Management Process Owner (with clear accountability for the entire process)
- Problem classification categories
- Problem trend reports
- Publicized Known Errors
- Problem analysis toolkit
- Root Cause Analysis skills and culture
- Actions to minimize impact of problems

The Critical Success Factors (CSFs) are:

- Avoiding Repeated Incidents
- Minimizing Impact of Problems

Key Activities

The key activities for this process are:

- Provide problem control
- Provide error control
- Proactively manage problems
- Conduct major problem reviews
- Provide management information about Problem Management quality and operations

Key Performance Indicators (KPIs)

Examples of Key Process Performance Indicators (KPIs) are shown in the list below. Each one is mapped to a Critical Success Factor (CSF).

- Avoiding Repeated Incidents
- Number of repeat incidents
- Number of existing Problems
- Number of existing Known Errors
- Minimizing Impact of Problems
- Average time for diagnosis of Problems
- Average time for resolution of Known Errors
- Number of open Problems; Number of open Known Errors
- Number of repeat Problems
- Number of Major Incident/Problem reviews

Change Management Best Practices Outline:

Change Management Objectives: The goal of Change Management is to minimize the impact of change-related incidents and to improve the effectiveness of day-to-day operations. A formal and strictly enforced Change Management process is a protective wall between potentially damaging Changes and the live production environment.

Changes DO NOT get released without a formal Request for Change (RFC) procedure; an adequate risk analysis made possible by a Change Advisory Board (CAB) composed if the right members and a solid Change Management Database (CMDB).

Low-risk, routine changes can be pre-approved as 'standard changes'; emergency changes (similar to Drive-by's) could be released more quickly, but would still require adherence to a formal process.

Change Management Best Practices

- Policies, Processes and Procedures that are in alignment with Business objectives & ITIL®
- Standardized methods and techniques for the efficient handling of changes
- A dedicated Incident Management Process Owner (with clear accountability for the entire process)
- A Change Advisory Board (CAB) composed of the right people to analyze and mitigate risk
- A Forward Schedule of Changes (FSC) to alert the Service Desk and to avoid scheduling conflicts
- Projected Service Availability (PSA) reports detailing changes to agreed upon SLA's and service availability due to the FSC
- A rollback plan for use if complications should arise
- No emergency change is EVER important enough to risk the integrity of service availability
- Proper levels of pre and post Change communications with customers and users
- Post Release update of the CMDB to reflect the change (very important!)

Key Critical Success Factors (CSFs)

- Controlled and risk inspected changes that protect the live environment from bad change decisions
- Consistently quick and accurate changes Based on business priorities and a rigorous risk profile
- Protection of services availability when changes are released

Key Activities

- Receive and accept (or reject) RFC's (based on strict and mandatory policies)
- Prioritize and classify changes (by potential impact and business urgency)
- Coordinate a complete change impact assessment (except for standard pre-approved changes)
- Coordinate the approval of changes
- Coordinate the scheduling of changes
- Communicate FSC to the Service Desk function
- Coordinate the implementation of changes
- Conduct post-implementation reviews and update the CMDB with changes made
- Provide management information about Change Management quality and operations

Key Performance Indicators (KPIs)

- Level of control over changes to protect live environment
- Number of RFCs processed; Number of RFCs rejected; Number of unauthorized changes detected
- Number of RFCs implemented on schedule; Number of RFCs requiring reschedules
- Making Quick and Accurate Changes Based On Business Priorities
- Number of RFCs marked as URGENT
- Number of RFCs not tested prior to implementation; Number of RFCs that failed
- Number of RFCs without business case; Number of RFCs bypassing CAB or CAB/EC
- Number of SEV1 incidents caused by RFC implementation
- Number of SEV2 incidents caused by RFC implementation
- Number of other incidents caused by RFC implementation
- Number of RFCs without a backup strategy

Configuration Management Best Practices Outline:

Configuration Management Objectives: provide a logical model of the infrastructure or a service by identifying, controlling, maintaining and verifying the versions of Configuration Items ***and the relationships between them*****.** These are stored in the Configuration Management Data Base (CMDB). A CMDB also includes all documentation: including project and Change plans, process manuals, procedures and SLA's.

Configuration Management is an IT "best practice" process that keeps up-to-date information about the IT infrastructure (hardware, software, documentation) and services. Configuration Management involves the identification, recording, and reporting of infrastructure components used by IT to deliver services. Its purpose is to enable staff to access accurate and reliable data about the equipment, software and documents used. All components of the IT infrastructure should be registered in the Configuration Management Database (CMDB).

A Configuration Management Database (CMDB) provides a common repository for IT configuration items (CI), their attributes, and relationships, offering a single source of record and a logical model of the IT infrastructure as it relates to IT services. As a proactive management tool, the CMDB can provide accountability and ownership of CI's and improved identification, verification, and management of the IT infrastructure.

Goals:

The goal is to provide a sound basis for Incident, Problem, Change and Release Management.

A best practice, mature Configuration Management process incorporates:

- Policies, Processes and Procedures that are in alignment with Business objectives & ITIL®
- Dedicated Configuration Management Process Owner (clear accountability for the entire process)
- A Configuration Management Database (CMDB) data schema
- Proper authorization and control over CMDB data
- Periodic audits and reviews of IT services and their configuration items
- Accurate information on IT services and their configuration items
- Verification of configuration records against the IT infrastructure; correct exceptions/errors found.

Critical Success Factors (CSFs);

- Managing Configuration Item information
- Providing capability to perform risk analysis of changes and releases

Key Activities

The information in the CMDB is used for five basic activities:

- Planning: Planning and defining the purpose, scope, objectives, policies and procedures, and the organizational and technical context for, Configuration Management
- Identification: Selecting and identifying the configuration structures for all the infrastructures Configuration Items (CI's), including their 'owner', their interrelationships and configuration documentation. It includes allocating identifiers and version numbers for CI's, labeling each item, and entering it on the Configuration Management Database
- Control: This gives the assurance that only authorized and identifiable CI's are accepted and recorded from receipt to disposal. It ensures that no CI is added, modified, replaced or removed without the appropriate controlling documentation e.g. approved Requests for Change of a CI, updated specification. All CIs will be under Change Management control.
- Monitoring: The status accounting and reporting of all current and historical data concerned with each CI throughout its life cycle, enables changes to CIs and tracking of their records through various statuses, e.g. ordered, received, under test, live, under repair, withdrawn or for disposal
- Verification: The reporting of all current and historical data concerned with each CI through its lifecycle. This makes changes to CI's and their records traceable. CI's also have current statuses (under development, testing, live, withdrawn)

Key Performance Indicators (KPIs)

Examples of Key Process Performance Indicators (KPIs) are shown in the list below. Each one is mapped to a Critical Success Factor (CSF).

Managing Configuration Item Information

- Number of Configuration Items logged and tracked
- Number of Configuration Items with attribute failures
- Number of changes to Configuration Item attributes
- Number of additional Configuration Items
- Number of deletions of Configuration Items
- Number and frequency of exceptions in configuration audits
- Number of incidents caused by inaccurate configuration data
- Percentage of Services tracked with Configuration Items versus known products and services

APPENDIX C: Glossary of Terms and Definitions

Processes involved in a IT Service Management Review

Process Definition
Service Desk *The Single Point of Contact (SPOC) between the service resources and Users.* A typical Service Desk manages Incidents and Service Requests, and also handles communication with the Users. Note: A Help Desk is usually more technically focused than a Service Desk and does not provide a Single Point of Contact for all interaction. The term Help Desk is often misused as a synonym for Service Desk.
Incident Management *An incident is any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service.* The first goal of this process is to restore normal service operation as quickly as possible to minimize the impact on business operations.
Problem Management *A **problem** is often identified as a result of multiple Incidents exhibiting common symptoms.* The goal of this process is resolve the root cause of incidents, minimize the impact on the business and to prevent recurrence of incidents related to these errors
Change Management *Many Problems (and the Incidents underlying them) are the result of imprecise Change Management.* A change is the addition, modification or removal of anything that could have an effect on IT Services. The goal of this process is to ensure that standardized methods and procedures are used for efficient and prompt handling of all Changes, in order to minimize the impact of any related Incidents upon service. This process incorporates **Release Management** (how changes are released into a live environment).
Configuration Management *provides a logical model of the infrastructure or a service by identifying, controlling, maintaining and verifying the versions of Configuration Items **and the relationships between them.*** These are stored in the Configuration Management Data Base (CMDB). An ITIL® CMDB includes all documentation: including project and Change plans, process manuals, procedures and SLA's. *The goal is to provide a sound basis for Incident, Problem, Change and Release Management.*

Important Terms and definitions

Term	Definition
Attribute	**(Configuration Management)** A piece of information about a Configuration Item. Examples are name, location, service tag, patches and applications. Attributes of CIs are recorded in the Configuration Management Database (CMDB).
Audit	Formal inspection and verification to check whether a Standard or set of Guidelines is being followed, that Records are accurate, or that Efficiency and Effectiveness targets are being met. An Audit may be carried out by internal or external groups.
Back-out Plan	**(Change and Release Management)** A Plan that documents the steps required to recover to a known working state if a Change or Release fails.
Baseline/Benchmark	The recorded state of something at a specific point in time, which can be created for a Configuration, Process or any other set of data. An ITSM Benchmark can be used to compare one Organization's ITSM Processes with another.
Best Practice	A proven Activity or Process that has been successfully used by multiple Organizations' (i.e. ITIL®).
Business	An overall corporate entity or Organization formed of a number of Business Units.
Business Case	Justification for a significant item of expenditure. Includes information about Costs, benefits, options, issues, Risks, and possible problems.
Business Customer	A recipient of a product or a Service from the Business.
Business Driver	Something that influences the definition of Business Objectives and Strategy. For example new legislation or the actions of competitors
Business IT Alignment (BITA)	Understanding how the IT Service Provider provides value to the Business, and ensuring that IT Strategy, Plans, and Services support the Business Objectives, and Vision.
Business Objective	The Objective of a Business Process, or of the Business as a whole. Business Objectives support the Business Vision, provide guidance for the IT Strategy, and are often supported by IT Services.
Business Operations	The day-to-day execution, monitoring and management of Business Processes.

Term	Definition
Business Perspective	An understanding of the Service Provider and IT Services from the point of view of the Business, and an understanding of the Business from the point of view of the Service Provider.
Business Process	A Business Process contributes to the delivery of a product or Service to a Business Customer.
Call	**(Service Desk) (Incident Management)** A telephone call to the Service Desk from a User. A Call could result in an Incident or a Service Request being logged.
Capability Maturity Model (CMM) **CMMI**	The Capability Maturity Model for Software (also known as the CMM and SW-CMM) is a model used to identify Best Practices to help increase Process Maturity. There are five levels of the process maturity according to Capability Maturity Model® Integration. *Predictability, effectiveness, and control of an organization's IT processes are believed to improve as the organization moves up these five levels.* Capability Maturity Model Integration
Cause / Effect Diagram	**(Problem Management)** A technique that helps a team to identify all the possible causes of an effect, such as a Problem. Originally devised by Kaoru Ishikawa and often called an Ishikawa Diagram, The output of this technique is a diagram that looks like a fishbone.
Change Advisory Board (CAB)	**(Change Management)** A group of people that assists the Change Manager in the assessment, prioritization and scheduling of Changes. This board is usually made up of representatives from all areas within the IT Service Provider, representatives from the Business, and Third Parties such as Suppliers.
Change Advisory Board / Emergency Committee (CAB/EC)	**(Change Management)** A sub-set of the Change Advisory Board who make decisions about Emergency Changes. Membership of the CAB/EC may be decided at the time a meeting is called, and depends on the nature of the Emergency Change.
Change History	**(Change Management)** Information about all changes made to a Configuration Item during its life. Change History consists of all those Change Records that apply to the CI.
Change Model	A repeatable way of dealing with a particular Category of Change. A Change Model defines specific pre-defined steps that will be followed for a change of this Category. Change Models may be very simple, with no requirement for approval (e.g. Password Reset) or may be very complex with many steps that require approval (e.g. major software release).
Change Schedule	**(Change Management)** A Document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of Change.
Classification	The act of assigning a Category to something. Classification is used to ensure consistent management and reporting. CIs, Incidents, Problems, Changes etc. are usually classified.

Term	Definition
Closure	The act of changing the Status of an Incident, Problem, Change etc. to Closed. A Closure code identifies the cause, and is intended for use in reporting and Trend Analysis.
Command, control and communications	The Processes and infrastructure that enable an Organization to effectively pass instructions and information. This enables management control of Resources.
Component CI	**(Configuration Management)** A Configuration Item that is part of an Assembly CI. For example, a CPU or Memory CI may be part of a Server CI.
Component Failure Impact Analysis (CFIA)	**(Problem Management) (Availability Management)** A technique that helps to identify the impact of CI failure on IT Services. A matrix is created with IT Services on one edge and CIs on the other. This enables the identification of critical CIs (that could cause the failure of multiple IT Services) and of fragile IT Services (that have multiple Single Points of Failure).
Configuration	A generic term, used to describe a group of Configuration Items that work together to deliver an IT Service, or a recognizable part of an IT Service. Configuration is also used to describe the parameter settings for one or more CIs.
Configuration and Change Management	An integrated approach to Planning, implementing and operating Configuration Management, Change Management and Release Management. Often referred to a C&CM
Configuration Identification	**(Configuration Management)** The Activity responsible for collecting information about Configuration Items and their Relationships, and loading this information into the CMDB. Configuration Identification is also responsible for labeling the CIs themselves, so that the corresponding Configuration Records can be found.
Configuration Item (CI)	**(Configuration Management)** Any Component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a Configuration Record within the CMDB and is maintained throughout its Lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include hardware, software, buildings, people, and formal documentation such as Process documentation and SLAs.
Configuration Management Database (CMDB)	**(Configuration Management)** A Database used to manage Configuration Records throughout their Lifecycle. The CMDB records the Attributes of each CI, and Relationships with other CIs. A CMDB may also contain other information linked to CIs, for example Incident, Problem or Change Records. The CMDB is maintained by Configuration Management and is used by all IT Service Management Processes.
Configuration Record	**(Configuration Management)** A Record containing the details of a Configuration Item. Each Configuration Record documents the Lifecycle of a single CI. Configuration Records are stored in a Configuration Management Database.

Term	Definition
Configuration Structure	**(Configuration Management)** The hierarchy and other Relationships between all the Configuration Items that comprise a Configuration.
Configuration Verification and Audit	**(Configuration Management)** The Activities responsible for ensuring that information in the CMDB is accurate and that all Configuration Items have been identified and recorded.
Continuous Improvement	Continuous Improvement continually measures achievement and modifies Processes and the IT Infrastructure to improve Efficiency, Effectiveness, and Cost Effectiveness. A Service Improvement Plan is designed to implement improvements to a Process or IT Service.
Dependency	The direct or indirect reliance of one Process or Activity upon another.
Development Environment	An Environment used to create or modify IT Services or Applications. Development Environments are not typically subjected to the same degree of control as Test Environments or Live Environments.
Diagnostic Script	**(Service Desk)** A structured set of questions used by Service Desk staff to ensure they ask the correct questions, and to help them Classify, Resolve and assign Incidents. Diagnostic Scripts may also be made available to Users to help them diagnose and resolve their own Incidents.
Effectiveness	A measure of whether the Objectives of a Process, Service or Activity have been achieved. An Effective Process or activity is one that achieves its agreed Objectives.
Efficiency	A measure of whether the right amount of resources have been used to deliver a Process, Service or Activity. An Efficient Process achieves its Objectives with the minimum amount of time, money, people or other resources.
Emergency Change	**(Change Management)** A Change that must be introduced as soon as possible. For example to resolve a Major Incident or implement a Security, patch. The Change Management Process will normally have a specific Procedure for handling Emergency Changes.
Error Control	**(Problem Management)** The Activity responsible for managing Known Errors until they are Resolved by the successful implementation of Changes.
Exception Report	A Document containing details of one or more KPIs or other important targets that have exceeded defined thresholds. Examples include SLA targets being missed or about to be missed, and a Performance Metric indicating a potential Capacity problem.
External Customer	A Customer who works for a different Business to the IT Service Provider.

Term	Definition
Failure	Loss of ability to Operate to Specification, or to deliver the required output. The term Failure may be used when referring to IT Services, Processes, Activities, and Configuration Items etc. A Failure often causes an Incident.
First-line Support	**(Service Desk) (Incident Management)** The first level in a hierarchy of Support Groups involved in the resolution of Incidents. Each level contains more specialist skills, or has more time or other resources.
Full Release	**(Release Management)** A Release that includes all Components of a Release Unit, including those that have not changed.
Functional Escalation	Transferring an Incident, Problem or Change to a technical team with a higher level of expertise to assist in an Escalation.
Help Desk	**(Service Desk)** A point of contact for Users to log Incidents. A Help Desk is usually more technically focused than a Service Desk and does not provide a Single Point of Contact for all interaction. The term Help Desk is often misused as a synonym for Service Desk.
Impact	A measure of the effect of an Incident, Problem or Change on Business Processes often based on how Service Levels will be affected. Impact and Urgency are used to assign Priority. An impact code is used to represent Impact (for example Major, Minor, Catastrophic).
Incident Record	**(Incident Management)** A Record containing the details of an Incident. Each Incident record documents the Lifecycle of a single Incident.
Integration Testing	Testing of a Build or Release to ensure that the parts work correctly together.
IT Infrastructure	All of the hardware, software, networks, facilities etc. that are required to develop, test, deliver or support IT Services. The term IT Infrastructure includes all of the Information Technology but not the associated people, Processes and documentation.
IT Operations	The Process responsible for the day-to-day monitoring and management of one or more IT Services and the IT Infrastructure they depend on. The term IT Operations is also used to refer to the group or department within an IT Service Provider responsible for IT Operations.
IT Service	A Service provided to one or more Customers by an IT Service Provider. An IT Service is based on the use of Information Technology and supports the Customer's Business Processes. An IT Service is made up from a combination of people, Processes and technology and should be defined in a Service Level Agreement.

Term	Definition
IT Service Management (ITSM)	The implementation and management of Quality IT Services that meet the needs of the Business. IT Service Management is performed by IT Service Providers through an appropriate mix of people, Process and Information Technology.
Key Performance Indicator (KPI)	A Metric that is used to help manage a Process, IT Service or Activity. Many Metrics may be measured, but only the most important of these are defined as KPIs and used to actively manage and report on the Process, IT Service or Activity. KPIs should be selected to ensure that Efficiency, Effectiveness, and Cost Effectiveness are all managed.
Knowledge Base	**(Service Desk) (Incident Management)** A Database containing information about Incidents, Problems and Known Errors. The primary purpose of Knowledge Management is to improve Efficiency by reducing the need to rediscover knowledge.
Known Error (KE)	**(Problem Management)** A Problem that has a documented Root Cause and a Workaround. Known Errors are created by Problem Control and are managed throughout their Lifecycle by Error Control. Known Errors may also be identified by Development or Suppliers and are documented in a Known Error database.
Lifecycle	The various stages in the life of a Configuration Item, Incident, Problem, Change etc. The Lifecycle defines the Categories for Status and the Status transitions that are permitted. For example: • The Lifecycle of an Application includes Design, Build, Test, Deploy, Operate etc. • The lifecycle of an Incident includes Detect, Respond, Diagnose, Repair, Recover, Restore. • The lifecycle of a Server may include: Ordered, Received, In Test, Live, Disposed etc.
Live Environment	A controlled Environment containing Live Configuration Items used to deliver IT Services to Customers.
Major Incident	**(Incident Management)** The highest Category of Impact for an Incident. A Major Incident results in significant disruption to the Business.
Management Information	Information that is used to support decision making by managers. Management Information is often generated automatically by tools supporting the various IT Service Management Processes. Management Information often includes the values of KPIs such as "Percentage of Changes leading to Incidents", or "First Time Fix Rate".
Management System	The framework of Policy and Processes that ensures an Organization can achieve its Objectives.
Manual Workaround	**(Incident Management) (Problem Management)** A Workaround that requires manual intervention.
Objective	The defined purpose or aim of a Process, an Activity or an Organization as a whole. Objectives are usually expressed as measurable targets. The term Objective is also informally used to mean a Requirement.

Term	Definition
Operational	The lowest of three levels of Planning and delivery (Strategic, Tactical, Operational). Operational Activities include the day-to-day or short term Planning or delivery of a Business Process or IT Service Management Process. The term Operational is also used to refer to a Configuration Item or IT Service being ready for use.
Optimize	Review, Plan and request Changes, in order to obtain the maximum Efficiency and Effectiveness from a Process, Configuration Item, Application etc.
Pareto Principle	A technique used to prioritize Activities. The Pareto Principle says that 80% of the value of any activity is created with 20% of the effort.
Policy	Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of Processes, Standards, Roles, Activities, IT Infrastructure etc.
Priority	A Category used to identify the relative importance of an Incident, Problem or Change. Priority is based on Impact and Urgency, and is used to identify required times for actions to be taken. For example the SLA may state that Priority2 Incidents must be resolved within 12 hours.
Proactive Problem Management	**(Problem Management)** Part of the Problem Management Process. The Objective of Proactive Problem Management is to identify Problems that might otherwise be missed. Proactive Problem Management analyses Incident Records, and uses data collected by other IT Service Management Processes to identify trends or significant problems.
Problem	The root cause of one or more incidents.
Problem Management	**(Problem Management)** The Process responsible for managing the Lifecycle of all Problems. The primary objectives of Problem Management are to prevent Incidents from happening, and to minimize the Impact of Incidents that cannot be prevented. Problem Management includes Problem Control, Error Control and Proactive Problem Management.
Process	A structured set of Activities designed to accomplish a specific Objective. A Process takes one or more defined inputs and turns them into defined outputs. A Process may include any of the Roles, responsibilities, tools and management Controls required to reliably deliver the outputs. A Process may define Policies, Standards, Guidelines, Activities, and Work Instructions if they are needed. See Business Process.
Process Control	The Activity of planning and regulating a Process, with the Objective of performing it in an Effective, Efficient, and consistent manner.

Term	Definition
Process Manager	A Role responsible for Operational management of a Process. The Process Manager's responsibilities include Planning and co-ordination of all Activities required to carry out, monitor and report on the Process. There may be several Process Managers for one Process, for example regional Change Managers or IT Service Continuity Managers for each data centre. The Process Manager Role is often assigned to the person who carries out the Process Owner Role, but the two Roles may be separate in larger Organizations.
Process Maturity	A measure of how reliable, Efficient and Effective a Process is, and of how well it is integrated with other processes. The most mature processes are formally aligned to Business Objectives and Strategy, and are supported by a framework for Continuous Improvement. There are five levels of the process maturity according to Capability Maturity Model®. *Predictability, effectiveness, and control of an organization's IT processes are believed to improve as the organization moves up these five levels.*
Process Owner	A Role responsible for ensuring that a Process is Fit for Purpose. The Process Owner's responsibilities include sponsorship, design, and change management of the Process and its Metrics. This Role is often assigned to the same person who carries out the Process Manager Role, but the two Roles may be separate in larger Organizations.
Recovery	**(Incident Management) (IT Service Continuity Management)** Returning a Configuration Item or an IT Service to a working state. Recovery of an IT Service often includes recovering data to a known consistent state. After Recovery, further steps may be needed before the IT Service can be made available to the Users (Restoration).
Relationship	A connection or interaction between two people or things. In Business Relationship Management it is the interaction between the IT Service Provider and the Business. In Configuration Management it is a link between two Configuration Items that identifies a dependency or connection between them. For example Applications may be linked to the Servers they run on, IT Services have many links to all the CIs that contribute to that IT Service.
Release	**(Release Management)** A collection of hardware, software, documentation, Processes or other Components required to implement one or more approved Changes to IT Services. The contents of each Release are managed, tested, and deployed as a single entity.
Release Management	**(Release Management)** The Process responsible for Planning, scheduling and controlling the movement of Releases to Test and Live Environments. The primary objective of Release Management is to ensure that the integrity of the Live Environment is protected and that the correct Components are released. Release Management works closely with Configuration Management and Change Management.
Release Process	The name used for the Process group that includes Release Management.
Release Record	A Record in the CMDB that defines the content of a Release. A Release Record has Relationships with all Configuration Items that are affected by the Release.

Term	Definition
Release Type	**(Release Management)** A Category that is used to classify Releases. A Release Type may be one of Full, Delta or Package Release.
Request for Change (RFC)	**(Change Management)** A formal proposal for a Change to be made. An RFC includes details of the proposed Change, and may be recorded on paper or electronically. The term RFC is often misused to mean a Change Record, or the Change itself.
Requirement	A formal statement of what is needed. For example a Service Level Requirement, a Project Requirement or the required Deliverables for a Process.
Restore	**(Incident Management)** Taking action to return an IT Service to the Users after Repair and Recovery from an Incident. This is the primary Objective of Incident Management.
Role	A set of responsibilities defined in a Process and assigned to a person or team. One person or team may have multiple Roles, for example the Roles of Configuration Manager and Change Manager be carried out by a single person.
Rollout	**(Release Management)** Synonym for Deployment. Most often used to refer to complex or phased Deployments.
Root Cause	**(Problem Management)** The underlying or original cause of an Incident or Problem.
Scalability	The ability of an IT Service, Process, Configuration Item etc. to perform its agreed Function when the Workload or Scope changes.
Scope	The boundary, or extent, to which a Process, Procedure, Certification, Contract etc. applies. For example the Scope of Change Management may include all Live IT Services and related Configuration Items; the Scope of an ISO/IEC 20000 Certificate may include all IT Services delivered out of a named data centre.
Second-line Support	**(Service Desk) (Incident Management) (Problem Management)** The second level in a hierarchy of Support Groups involved in the resolution of Incidents and investigation of Problems. Each level contains more specialist skills, or has more time or other resources.
Service	Providing something of value to a customer that is not goods (physical things with material value). Examples of services include banking and legal support. Service is also used as a Synonym for IT Service.
Service Delivery	The core IT Service Management Processes that have a Tactical or Strategic focus. In ITIL® these are Service Level Management, Capacity Management, IT Service Continuity Management, Availability Management, and Financial Management for IT Services. Service Delivery is also used to mean the delivery of IT Services to Customers.

Term	Definition
Service Level	Measured and reported achievement against one or more Service Level Targets. Service Level is sometimes used as an informal term to mean Service Level Target.
Service Manager	A generic term that can be used to mean any manager within the IT Service Provider. Most commonly used to refer to a Business Relationship Manager, a Process Manager, an Account Manager or a senior manager with responsibility for IT Services overall.
Service Request	**(Service Desk)** A request from a User for information or advice, or for a Standard Change. For example to reset a password, or to provide standard IT Services for a new User. Service Requests are usually handled by a Service Desk, and do not require an RFC to be submitted.
Service Support	The core IT Service Management Processes that have an Operational focus. These are Incident Management, Problem Management, Configuration Management, Change Management and Release Management. Service Support also includes the Service Desk.
Standard Change	A pre-approved Change that is low Risk, relatively common and follows a Procedure or Work Instruction. For example password reset or provision of standard equipment to a new employee. RFCs are not required to implement a Standard Change, and they are logged and tracked using a different mechanism, such as a Service Request.
Status	The name of a required field in many types of Record. It shows the current stage in the Lifecycle of the associated Configuration Item, Incident, Problem etc.
Strategic	The highest of three levels of Planning and delivery (Strategic, Tactical, Operational). Strategic Activities include Objective setting and long term Planning to achieve the overall Vision. A Strategic Plan designed to achieve defined Objectives.
Support Group	A group of people with technical skills. Support Groups provide the Technical Support needed by all of the IT Service Management Processes.
System	A number of related things that work together to achieve an overall Objective. For example: • A computer System including hardware, software and Applications. • A management System, including multiple Processes that are planned and managed together. For example a Quality Management System. • A Database Management System or Operating System that includes many software modules that are designed to perform a set of related Functions.
System Management	The part of IT Service Management that focuses on the management of IT Infrastructure rather than Process.
Tactical	The middle of three levels of Planning and delivery (Strategic, Tactical, Operational). Tactical Activities include the medium term Plans required to achieve specific Objectives, typically over a period of weeks to months.

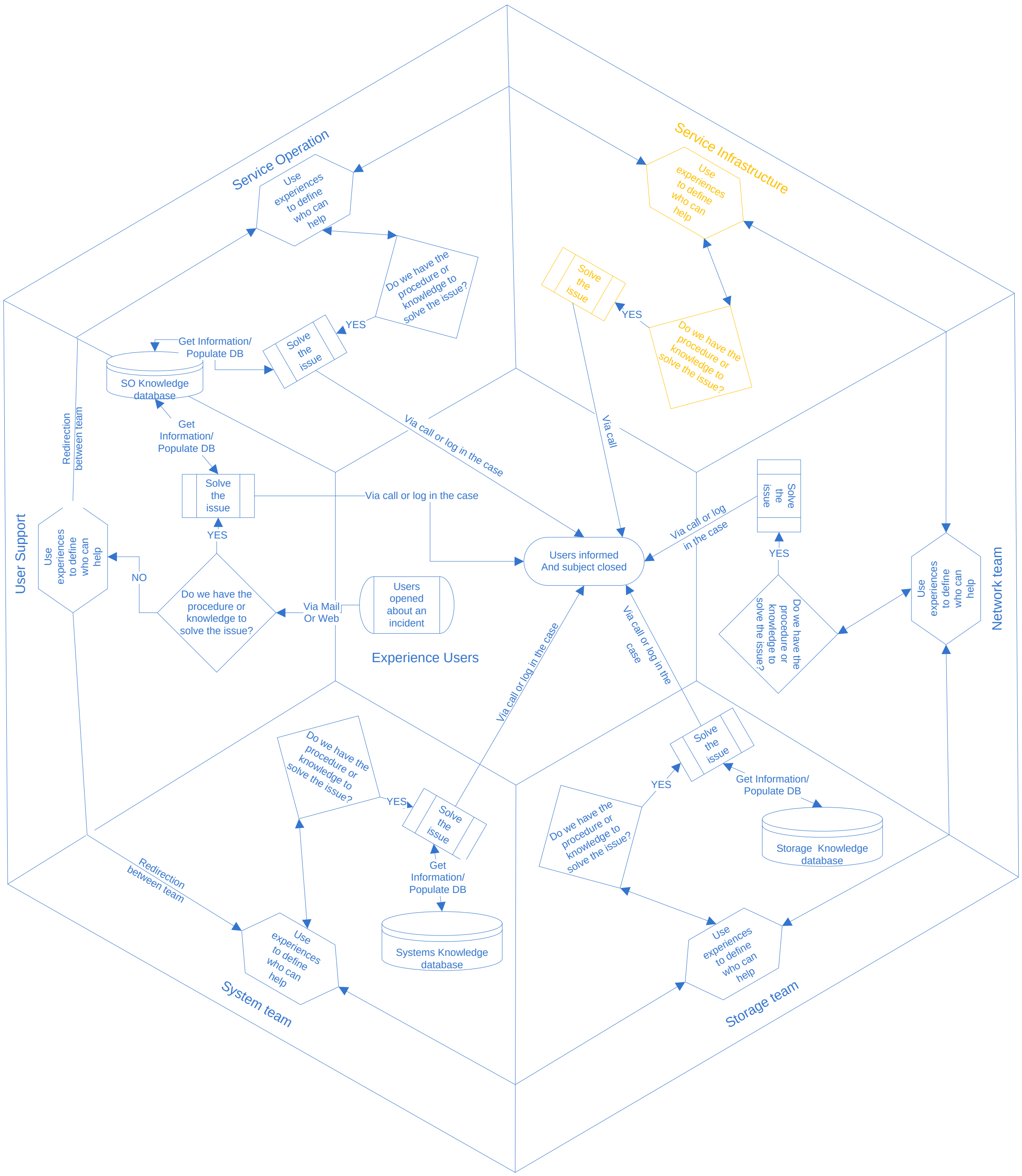
Term	Definition
Technical Observation Post (TOP)	A technique used in Service Improvement, Problem investigation and Availability Management. Technical support staff meets to monitor the behavior and Performance of an IT Service and make recommendations for improvement.
Test	A Test is used to verify that a Configuration Item, IT Service, Process etc. meets its Specification, and is able to correctly deliver specific Functional or Service Level Requirements. There should be no negative effects on other Processes or IT Services.
Test Environment	A controlled Environment used to Test Configuration Items, Builds, IT Services, Processes etc.
Third-line Support	**(Service Desk) (Incident Management) (Problem Management)** The third level in a hierarchy of Support Groups involved in the resolution of Incidents and investigation of Problems. Each level contains more specialist skills, or has more time or other resources.
Threat	A threat is anything that might exploit Vulnerability. Any potential cause of an Incident can be considered to be a Threat.
Threshold	The value of a Metric which should cause an Alert to be generated, or management action to be taken
Urgency	A measure of how long it will be until an Incident, Problem or Change has a significant Impact on the Business. For example a high Impact Incident may have low Urgency, if the Impact will not affect the Business until the end of the Financial Year. Impact and Urgency are used to assign Priority.
User	A person who uses the IT Service on a day-to-day basis. Users are distinct from Customers, as some Customers do not use the IT Service directly.
Vulnerability	A weakness that could be exploited by a Threat. For example an open firewall port, a password that is never changed, or a flammable carpet. A missing Control is also considered to be Vulnerability.
Workaround	**(Incident Management) (Problem Management)** Reducing or eliminating the Impact of an Incident or Problem for which a full Resolution is not yet available. For example by restarting a failed Configuration Item. Workarounds for Problems are documented in Known Error Records. Workarounds for Incidents that do not have associated Problem Records are documented in the Incident Record.
Workload	The resources required to deliver an identifiable part of an IT Service. Workloads may be Categorized by Users, groups of Users, or Functions within the IT Service.

APPENDIX D: Details schemas about the Incident Management processes.

The schemas are detailed schemas related to the CC-IN2P Incident Management processes. It is showing with accuracy:

- the complexity of the current processes
- how you can apply workaround
- how each team has his own independent processes and tools

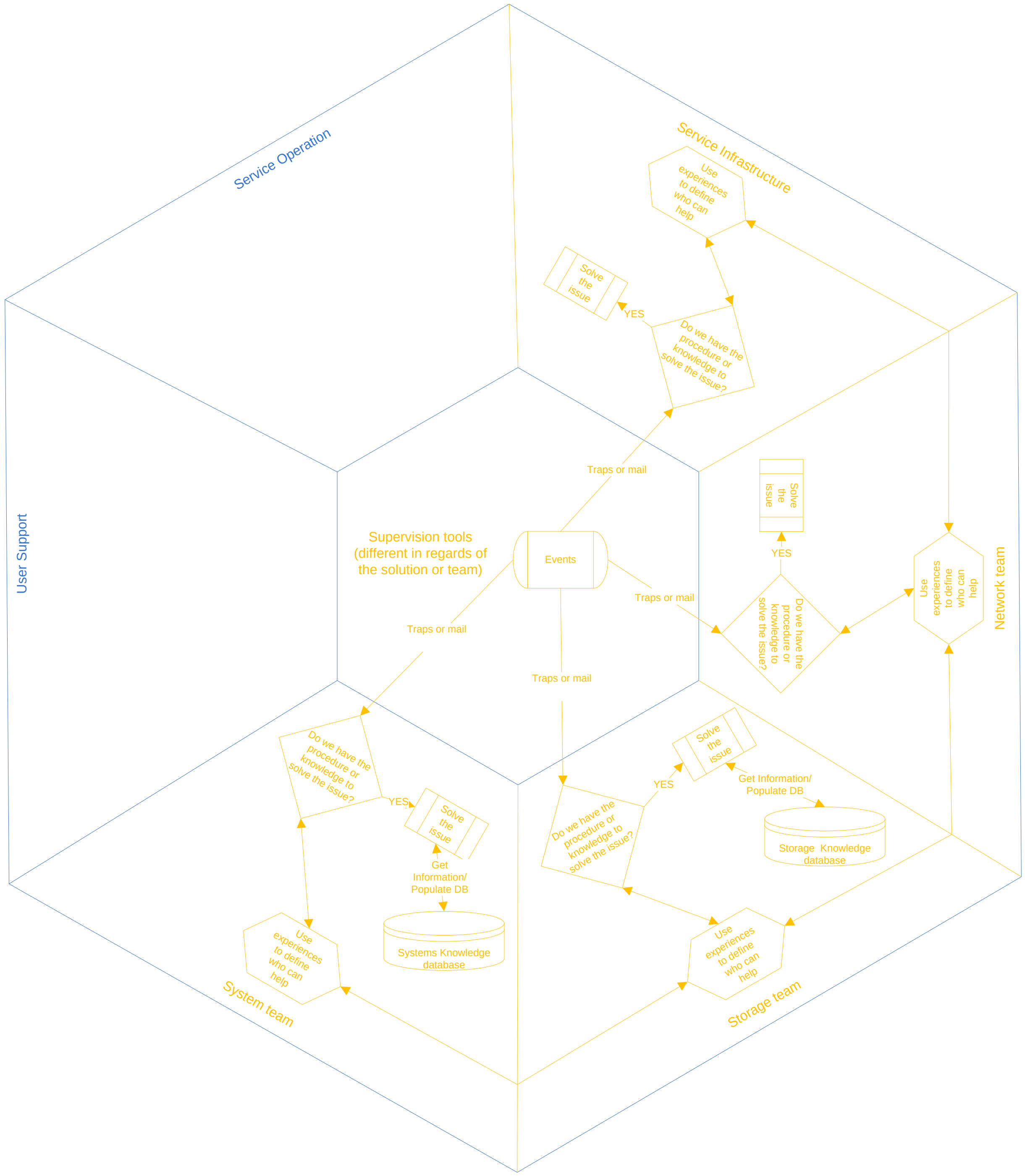
Incident Management Information flow (detail vision)


Service Operation
Use experiences to define who can help
Do we have the procedure or knowledge to solve the issue?
YES
Solve the issue
Get Information/ Populate DB
SO Knowledge database
Get Information/ Populate DB
Solve the issue
YES
Do we have the procedure or knowledge to solve the issue?
NO
Use experiences to define who can help
Redirection between team
User Support
Via call or log in the case
Via call or log in the case
Via Mail Or Web
Users opened about an incident
Experience Users
Users informed And subject closed
Service Infrastructure
Use experiences to define who can help
Solve the issue
YES
Do we have the procedure or knowledge to solve the issue?
Via call
Via call or log in the case
Solve the issue
YES
Do we have the procedure or knowledge to solve the issue?
Use experiences to define who can help
Network team
Via call or log in the case
Via call or log in the case
Do we have the procedure or knowledge to solve the issue?
YES
Solve the issue
Get Information/ Populate DB
Systems Knowledge database
Redirection between team
Use experiences to define who can help
System team
YES
Solve the issue
Get Information/ Populate DB
Do we have the procedure or knowledge to solve the issue?
Storage Knowledge database
Use experiences to define who can help
Storage team

In Blue: Use the ticketing tools

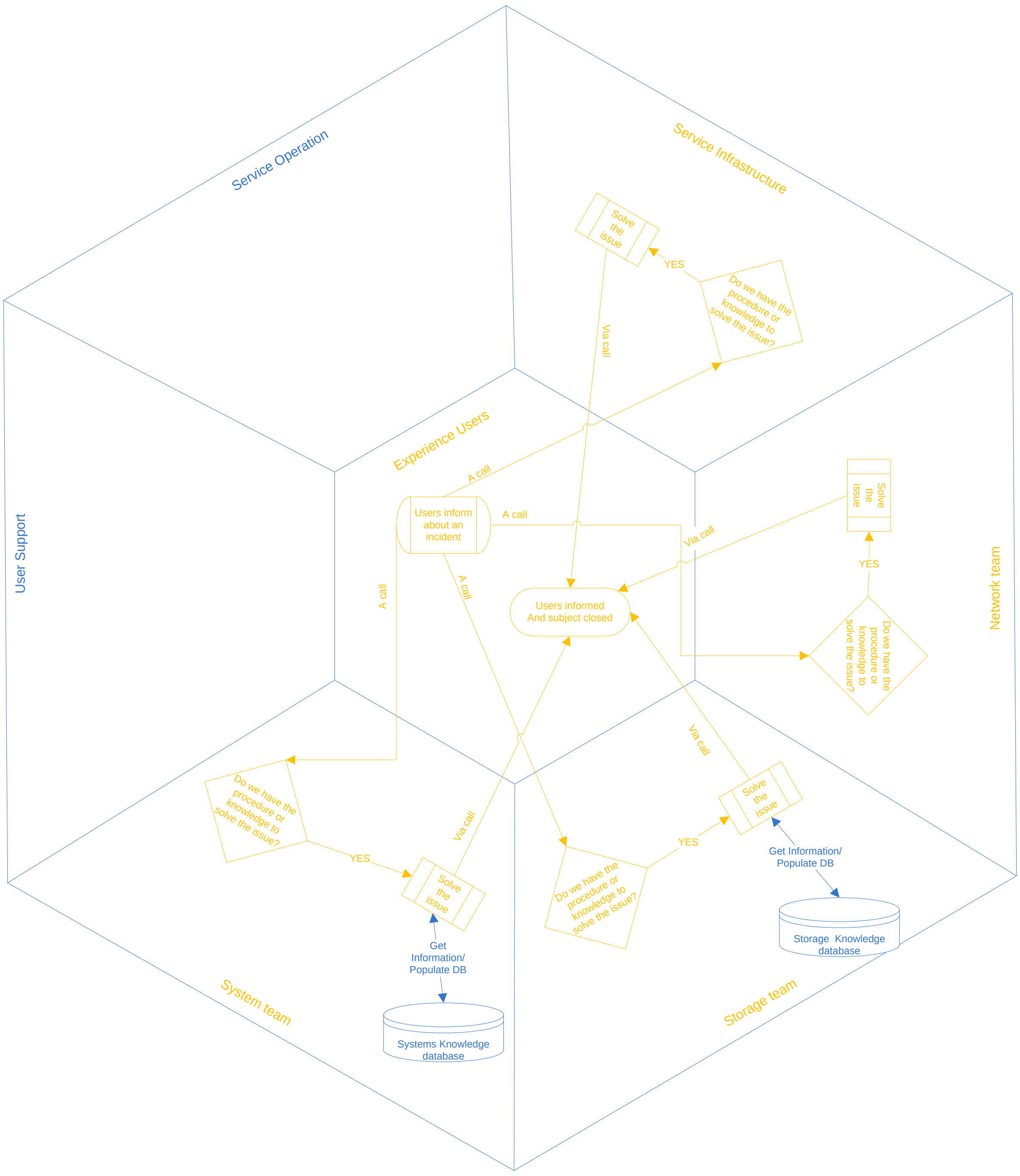
In Orange: Don't use it

Automatic event generation with supervision tools (detail vision)


Service Operation
User Support
Service Infrastructure
Network team
System team
Storage team
Supervision tools (different in regards of the solution or team)
Events
Traps or mail
Traps or mail
Traps or mail
Traps or mail
Do we have the procedure or knowledge to solve the issue?
Do we have the procedure or knowledge to solve the issue?
Do we have the procedure or knowledge to solve the issue?
Do we have the procedure or knowledge to solve the issue?
YES
YES
YES
YES
Solve the issue
Solve the issue
Solve the issue
Solve the issue
Use experiences to define who can help
Use experiences to define who can help
Use experiences to define who can help
Use experiences to define who can help
Get Information/ Populate DB
Get Information/ Populate DB
Systems Knowledge database
Storage Knowledge database

In Blue: Use the ticketing tools
In Orange: Don't use it

Possible workarounds (detail vision)


Service Operation
Service Infrastructure
User Support
Experience Users
Network team
System team
Storage team
Solve the issue
YES
Do we have the procedure or knowledge to solve the issue?
Via call
A call
Users inform about an incident
A call
Via call
Solve the issue
YES
Users informed And subject closed
A call
A call
Do we have the procedure or knowledge to solve the issue?
Via call
Do we have the procedure or knowledge to solve the issue?
YES
Solve the issue
Via call
Get Information/ Populate DB
Systems Knowledge database
Do we have the procedure or knowledge to solve the issue?
YES
Solve the issue
Get Information/ Populate DB
Storage Knowledge database

In Blue: Use a formal procedure or process
In Orange: Don't use it

APPENDIX E: How Dell can help you in relation with this study and our recommandations

Introduction

For many years, DELL has built a wide and complete offering which can be suited to the needs of an organization in respect of IT organizational and structural improvements.

The Offer contains:

- A complete hardware portfolio (server, workstation, storage) to support for example a CMDB server or a knowledge database.
- A large range of software to implement for example your asset inventory or CMDB.
- A complete set of Services which are used to train staff, structure organizations, improve IT or drill down in ITIL based on defined service package, managed services, custom services or consulting.

Main DELL offer in regards of your ITSMr assessment:

DELL education Services

URL: http://dell.training.com/microsite_content/ORG23727/ie_catalog.html

Dell is committed to "Simplify IT" for its customers reducing complexity and increasing productivity. We believe providing Dell Education Services is central to this pledge as nothing is simple until you understand the technology that you have or intend to deploy. Only when you understand the technology at your finger tips can you maximize ROI, minimize down-time and accelerate productivity. To give our customers maximum choice we have a broad range of offerings covering industry leading technologies and delivered according to your needs.

DELL education Services offers a large panel of training Professional Development and includes:

- ITIL(R) V3 Foundation Certificate in IT Service Management
- Prince2 Foundation and Practitioner (project Management)

IT Simplification

URL: http://www.dell.com/content/topics/global.aspx/services/adi/it_simplification?c=us&cs=555&l=en&s=biz

IT simplification was designed to address main pain points for a company as IT organization improvement, cost reduction or optimization and IT infrastructure improvement.

As Part of the offer, you can find:

- A full ITIL audit of your organization. The ITSMr covers 5 processes/functions of ITIL. IT Simplification are covering the overall 19 processes/functions regarding the 5 main publications which are
  - Service Strategy (Definition of your strategy and then of your portfolio)
  - Service Design (Design of your service with regards to portfolio)
  - Service Transition (Implementation of your portfolio included the change Management)
  - Service Operation (Maintenance in operational condition of your portfolio)
  - Continual Service Improvement (Consolidation and improvement of your portfolio)
- A complete Infrastructure audit (as datacenter) to address cooling, floor space or power consumption optimization.

Infrastructure Consulting Services

URL: http://www.dell.com/content/topics/global.aspx/services/adi/adi_service?c=us&cs=555&l=en&s=biz

Dell Infrastructure Consulting utilizes innovative tools, automated analysis and our own intellectual property to give customers insight into what is driving IT complexity. We can deliver a set of practical executable plans for simplifying IT infrastructure, helping reduce operating costs while freeing up resources for new business initiatives. We seek better answers than traditional service models, based on our belief that consulting should not need armies of people. Our unique approach to services gives you the flexibility to select only those point services that meet your needs or choose our end-to-end solution.

We take a practice based approach to working with customers, providing either technology focused consulting in support of specific implementation projects such as Microsoft, Storage and Virtualization; or broader issue-based consulting focused on End-User Computing, Data Center Optimization and Systems Management.

Our consulting methodology is based on intellectual property and reference architecture developed through proof of concept testing in our solution centers, rounded out with the real-world experience of supporting many customer implementations. We take advantage of innovative tools and automated analysis to avoid labor or time intensive consulting engagements to deliver rapid results.

We offer end-to-end solutions to provide a single source and point of contact for hardware, software, service and on-going support. In a time when many providers aspire to do everything, we focus on IT infrastructure services excellence. Infrastructure Consulting from Dell can help you maximize the value of your information technology investments and create an efficient, effective and scalable IT infrastructure.

Example of consulting provided following an ITSMr Assessment:

- Complete CMDB definition and implementation
- Assistance in the definition of the Service Desk
- Optimization of the datacenter in regards of cooling and power consumption.

DELL Managed Services

URL: http://www.dell.com/content/topics/global.aspx/services/saas/infrastructure_mgmt_srvcs?c=us&cs=555&l=en&s=biz

DELL provides a complete set of managed services based on onsite solution or cloud computing from 3 secure and redundant datacenters ~~in~~ across the world.

In order to participate in the Configuration Management processes definition, maintenance and consolidation, these solutions could be implemented:

Distributed Device Management Services
Dell Distributed Device Management helps you track dispersed assets, distribute software and manage patches – no matter where your PC clients are located on the Internet.

Dell Software Inventory & Usage Management
Automate asset discovery, monitor usage and simplify license compliance to help eliminate unused applications and lower support and maintenance costs.

Dell Desktop Management Solutions
Provides the ability to remotely and proactively manage your desktop infrastructure anytime, virtually anywhere. Dell provides configurable lifecycle solutions that you can configure to meet your specific needs including a 24X7 Service Desk, technician presence for on-site installation, move, add and how to support as well as complete desktop configuration management services

In order to improve your IT infrastructure and then your metrics in term of Downtime or number of incidents:

Dell Online Backup and Restore
Data loss is a serious threat to any organization. Businesses of all sizes need to protect their critical and sensitive data resources. Dell Online Backup & Restore offers rapid, intelligent offsite backup for distributed PCs – all with minimal network impact.

Email Management Services
Email is indisputably the most important business application for most organizations. Yet, managing email has always been a no-win proposition. Dell Email Management Services (EMS) are designed to help eliminate the risks of managing email with minimal maintenance, modular SaaS-enabled solutions.

Virtual Server Management - Remote Monitoring & Reporting
A managed service to help you get the most out of your virtual server environment by combining 24/7 monitoring, alerts and reporting with expert analysis and advice.

Data Center Backup Management
Helps optimize backup environments by focusing on remote reporting, monitoring, alerts, along with full remote management, freeing up IT resources.

In order to improve your overall processes of ITIL (included Service Desk):

Dell Custom Managed Solutions
Dell Custom Solutions simplify and transform IT, so that more of your time, money, and human resources can be invested in driving greater innovation in your business. Our proven best practices enable IT organizations to identify and eliminate unnecessary complexity, define and align business processes, and deliver services in new ways.

DELL Hardware Portfolio

You can find all the information on our hardware portfolio behind the URL : www.dell.fr

DELL Software Portfolio

DELL offers a large panel of Software. Some of our offer can be used in Configuration and Incident Management processes of ITIL (Supervision, management, asset inventory and control).

Dell Management Console

With the introduction of Dell Management Console powered by Altiris from Symantec, Dell is doing for systems management what we did for computer hardware, taking a complex, proprietary industry technology and transforming it by delivering a simple, streamlined, modular solution best adapted to your specific management needs

One of the strengths of the DMC product is the scalability of the solution as you can implement the complete set of Altiris options.

The features already included in the DELL Free package are:

- Discovery, Inventory, and Reporting: Holistic view of the IT environment. User can choose from device tree view, graphical reports, or exportable tables and drill into any device to see in-depth hardware inventory data.
- Hardware Monitoring: Proactive heartbeat monitoring on user-defined schedule as well as asynchronous event reception for Dell™ systems. Ability to import SNMP MIBs to receive events from non-Dell devices.
- OS Monitoring: Monitor utilization of memory, CPU, free space, and I/O. View historical reports or live graphs for monitored devices. Generate alerts based on user-defined thresholds.
- Hardware Updates: Push agent, bios , driver, and firmware updates to Dell servers. Console can be configured to download latest updates from DELL.COM on a scheduled basis.

Dell Client Manager

Dell Client Manager software helps make Dell OptiPlex desktops, Latitude notebooks and Dell Precision workstations the easiest and most cost-effective client systems you can own. The purpose of Dell Client Manager is simple: arm IT professionals with centralized, remote control and automate common tasks associated with owning client systems. The results are powerful: far fewer deskside visits and repetitive tasks, greater visibility and control of client inventory and usage, and improved consistency and compliance in the way client systems are configured.

Key Features & Benefits

Dell Client Manager Standard

Dell Client Manager Standard, a FREE product, is a powerful hardware management tool for Dell Precision workstations, OptiPlex desktops, and Latitude notebooks. From a remote management console you can:

- Identify, inventory, and add computers to the pool of managed resources
- Configure or update the BIOS of multiple computers simultaneously
- Monitor the health of key computers or computer sub components

Dell Client Manager Plus

Dell Client Manager Plus software builds upon the hardware management capabilities of Dell Client Manager Standard by adding software-level management capabilities. From the same management console you can:

- Migrate users to a new computer or operating system
- Image a new computer or re-image an existing computer
- Create software packages, distribute, and install
- Scan computers for detailed operating system and application information

DELL OpenManage

Dell OpenManage is a comprehensive set of technologies, tools, and alliances based on industry standards that meet our customers' needs for efficient systems management. Use of systems management practices can help significantly lower TCO.