IT Service Management

Gunuganti Kiran Swathi

Wintel Server engineer, OCBC Bank, Singapore. **Email**: ks.gunuganti@gmail.com
LinkedIn: https://www.linkedin.com/in/kiran-swathi-g-87165561

Introduction

IT service management -- often referred to as ITSM -- is simply how IT teams manage the end-to-end delivery of IT services to customers. This includes all the processes and activities to design, create, deliver, and support IT services.

The core concept of ITSM is the belief that IT should be delivered as a service. A typical ITSM scenario could involve asking for new hardware like a laptop. You would submit your request through a portal, filling out a ticket with all relevant information, and kicking off a repeatable workflow.

The importance of ITSM

ITSM benefits your IT team, and service management principles can improve your entire organization. ITSM leads to efficiency and productivity gains. A structured approach to service management also brings IT into alignment with business goals, standardizing the delivery of services based on budgets, resources, and results. It reduces costs and risks, and ultimately improves the customer experience.

Benefits of ITSM to include:

- Aligning IT teams with business priorities tracked through success metrics
- Enabling cross-department collaboration
- Bringing IT teams and development teams together through streamlined project management approaches
- Empowering IT teams to share knowledge and continuously improve
- Improving request coordination for more efficient service
- Promoting customer-eccentricity with self-service and better processes
- Responding more quickly to major incidents, and preventing future ones

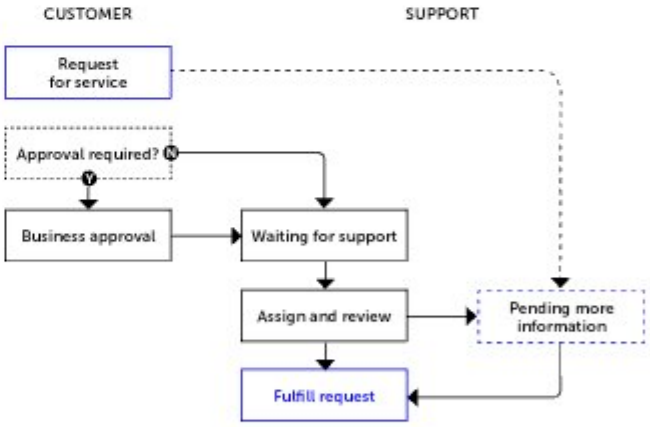
ITSM processes

What are ITSM processes? IT service teams use organizational resources and follow repeatable procedures to deliver consistent, efficient service.

A few of the core ITSM processes include:

Service Request Management

Service request management is a repeatable procedure for handling the wide variety of customer service requests, like requests for access to applications, software enhancements, and hardware updates.While there are some variations in the way a service request can be captured and fulfilled, it's important to focus on driving standardization to improve overall service quality and efficiency. The following process represents a simple request fulfillment process based on ITIL recommendations. This can be used as a starting point for adapting existing ITIL processes or defining new ones.



Knowledge Management

Knowledge management is the process of creating, sharing, using, and managing the knowledge and information of an organization

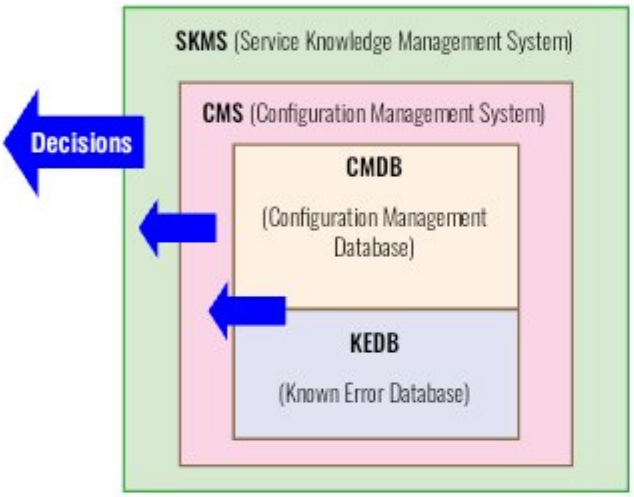
What is Service Knowledge Management

The Service Knowledge Management System (SKMS) is the central repository of the data, information, and knowledge that the IT organization needs to manage the lifecycle of its services.The SKMS is not necessarily to be a single system and usually formed by merging multiple discrete

https://doi.org/10.5281/zenodo.8250328

systems & data sources.The main purpose of SKMS is to store, analyze and present the service provider's data, information and knowledge in a structured manner.

The SKMS is closely related to CMDB, KEDB, and CMS. These act as three levels of data processing.The CMDB captures & record the configuration data and KEDB Records Known errors, the CMS arranges these records in a manageable structure and then that processed information feeds into the SKMS.Using these stored information SKMS supports delivery of the services and helps to provide relevant information for decision-making. Below Image describes the relationship among them:



Relationship between CMDB, KEDB, CMS & SKMS

IT Asset Management

IT Asset Management (ITAM) is the practice that helps your organization manage, control, and protect its IT assets and the IT services that use them. Done well, ITAM will help your organization increase value, support decision making, control costs, and effectively manage risks.

ITAM isn't just about hardware or software, and the new ITIL 4 guidance reflects this. When setting the scope for your organization's ITAM capabilities, you'll need to consider networking, cloud-based services, and client devices in addition to corporate hardware and software.

For example:

- Network infrastructure – routers, hubs, and switches
- Cloud services – Software As A Service (SaaS) offerings such as Office 365 or G-Suite, Platform As A Service (PaaS) offerings such as Microsoft Azure, and Infrastructure As A Service (IaaS) offerings such as Amazon Web Services or Google Compute Engine
- Client devices – employee personal devices that can access company systems and information.

Incident Management

Incident management is the process to respond to an unplanned event or service interruption and restore the service to its operational state.

Steps in the IT incident management process

Identify an incident and log it

An incident can come from anywhere: an employee, a customer, a vendor, monitoring systems. No matter the source, the first two steps are simple: someone identifies an incident, then someone logs it. These incident logs (i.e., tickets) typically include:

- The name of the person reporting the incident
- The date and time the incident is reported
- A description of the incident (what is down or not working properly)
- A unique identification number assigned to the incident, for tracking

Categorize

Assign a logical, intuitive category (and subcategory, as needed) to every incident. This helps you analyze your data for trends and patterns, which is a critical part of effective problem management and preventing future incidents.

Prioritize

Every incident must be prioritized. Start by assessing its impact on the business, the number of people who will be impacted, any applicable SLAs, as well as the potential financial, security, and compliance implications of the incident. Compare this incident to all other open incidents to determine its relative priority. As a best practice, define your severity and priority levels before an incident happens, making it simpler for incident managers to gauge priority quickly.

Respond

Initial diagnosis: Ideally, your front-line support team can see an incident through from diagnosis through close, but if they can't, the next step is to log all the pertinent information and escalate to the next tier team.

Escalate: The next team takes the logged data and continues with the diagnosis process, and, if this next

team can't diagnose the incident, it escalates to the next team.

Communicate: The team regularly shares updates with impacted internal and external stakeholders.

Investigation and diagnosis: This continues on until the nature of the incident is identified. Sometimes teams bring in outside resources or other department members in to consult and assist with the resolution.

Resolution and recovery: In this step, the team arrives at a diagnosis and performs the necessary steps to resolve the incident. Recovery simply implies the amount of time it may take for operations to be fully restored, since some fixes (like bug patches, etc.) may require testing and deployment even after the proper resolution has been identified.

Closure: If the incident was escalated, it is finally passed back to the service desk to be closed. To maintain quality and ensure a smooth process, only service desk employees are allowed to close incidents, and the incident owner should check with the person who reported the incident to confirm that the resolution is satisfactory and the incident can, in fact, be closed.

Problem Management

Problem management is the process of identifying and managing the root causes of incidents on an IT service.Problem management process can keep repeat incidents from happening and stop critical incidents from happening in the first place. It is a core component of ITSM frameworks.

What is the problem management process

Problem detection - Proactively find problems so they can be fixed, or identify workarounds before future incidents happen.

Categorization and prioritization - Track and assess known problems to keep teams organized and working on the most relevant and high-value problems.

Investigation and diagnosis - Identify the underlying contributing causes of the problem and the best course of action for remediation.

Create a known error record - In ITIL, a known error is "a problem that has a documented root cause and a workaround." Recording this information leads to less downtime if the problem triggers an incident. This is typically stored in a document called a known error database.

Create a workaround, if necessary - A workaround is a temporary solution for reducing the impact of problems and keeping them from becoming incidents. These aren't ideal, but they can limit business impact and avoid a customer-facing incident if the problem can't be easily identified and eliminated.

Resolve and close the problem - A closed problem is one that has been eliminated and can no longer cause another incident.

Change Management

Change management ensures standard procedures are used for efficient and prompt handling of all changes to IT infrastructure, whether it is rolling out new services, managing existing ones, or resolving problems in the code.

Types of changes

ITIL defines three types of changes.

Standard changes

Standard changes are low-risk, commonly repeated, and pre-approved. They're performed frequently and follow a documented, approved process.

For example, adding memory or storage is a standard change. Replacing a failing router with an identical working router is a standard change. Creating a new instance of a database is a standard change

For many companies, standard changes are a prime opportunity for automation. Some companies report that as many as 70% of standard changes can be automated—freeing up their teams to focus on normal and emergency changes.

Normal changes

Normal changes are non-emergency changes that don't have a defined, pre-approved process.

For example, upgrading to a new content management system is a normal change. Migrating to a new data center is a normal change. Performance improvements are normal changes. They're not standard and repeatable. There are risks involved. But they're also not emergencies. Which means they can go into the usual change management queue for risk assessment and approval.

Emergency changes

These changes arise from an unexpected error or threat and need to be addressed immediately—usually to restore service for customers or employees or secure systems against a threat.

For example, implementing a security patch is an emergency change. Dealing with a server outage is an emergency change. Resolving a major incident is an emergency change.

ITSM software and tools

There are multiple tools used in different organizations. Some of tools include Service Now, ITSM (IT service Manager), HPSM (Hewlett Packard Enterprise Service Manager) etc, Axios Systems Assyst, BMC Remedy.

Challenges of IT Service Managers in a Digital World

The main challenges IT Service Management face when seeking to transform the IT service delivery of their business and offer practical tips on how to overcome these obstacles by building a proper ITSM framework.

1. Increasing Efficiency and Performance of IT Support
2. Finding the Right Tools to Simplify and Modernize IT Processes
3. Meeting Employee and Customer Expectations

Conclusion

ITSM helps organizations to be more reliable, improve customer satisfaction, optimise service delivery, gain greater visibility of IT costs and assets, become more adaptable.

The implementation of ITSM standards provides organizations with the opportunity to differentiate their business and service offerings from their competitors. To be successful, an organization must make an honest assessment of its current position and use this as the basis for planning its future achievements.

References

[1] https://www.atlassian.com/

[2] https://www.servicenow.com/products/itsm

About the Authors

Gunuganti Kiran Swathi is a Wintel engineer at OCBC Bank Singapore. She is certified in Microsoft® Certified Solutions Expert: Server Infrastructure and Microsoft certified azure administrator associate. She has worked on Various technologies for 6 years in IT related to patch management, incident management, change management in Wintel server infrastructure. She also have worked on many migration projects according to IT standards and lead/trained the L2 teams in order to streamline and simplify the processes.