INFO5991 Service Science Management Notes

Assessment Information

Assessment items	%	Group/ Individual	Due date
Assignment 1	20%	Individual	Week 6 (electronic copy)
Group Assignment	30%	Group	Final Group Presentation during lecture/tutorials in week 11/12 (electronic copy)
Final Exam	50%	Individual	To Be Announced

Book Summary: IT Governance, how top performers manage IT decision rights for superior Results.

WEEK 1

Introduction

Information technology has significantly influenced the way businesses operate in the past 4 decades. The incorporation of IT has increased the overall productivity of organisations. The scope of IT has moved from development of products into design, management and improvement of IT and business processes. Use of IT in operations management has enabled organisations to reduce costs, standardize and improve quality, and focus on customization.

General Process and Operations Management

Operations management is part of every organisation and is needed to manage the design, implementation, realization, and operationalization of its products or services a company has to offer. Operations management is concerned with managing the core purpose of a business and keep it running. All types of businesses have operations as each of them provide a product or service and operations for each of them vary for each type of business.

Information Technology and its influence

IT has disrupted our technologies. A few of these disruptive technologies are given below:

- Mobile Internet
  Increasingly inexpensive and can connect with the internet essentially connecting everyone from anywhere and having knowledge in their fingertips.
- Automation of Knowledge work
  Intelligent software systems can perform knowledge work tasks. By using Artificial intelligence, big data technologies, etc. it has varied applications in real life.
- Internet of things
  These are networks of low-cost sensors and actuators for data collection, monitoring, decision making, and process automization. It is currently being used to develop smart homes but has slowly been introduced to various other industries such as manufacturing.

- Cloud
  The use of computer hardware and software resources to deliver services over the internet or a network is what cloud is all about. It is great for scaling, and increases interconnectivity.

IT Help Desk

IT is not omnipotent. It can also break, and this might lead to various problems. Services when unavailable would lead to bad customer experience, challenges in supply chain, out-cry on social media, impact of reputation and even finances. This led to the birth of IT help desks, the technology support experts. The main role of IT help desks is to fix these problems quickly and efficiently and get the users back to their daily jobs.

The initial focus of the help desk was call logging, problem resolution, and change management. The reason for call logging was because a phone call was the primary way of contacting the help desk when it was first introduced. Now it has transformed into ticket management and incident management. Problem resolution has been the key element of help desk and now this has expanded to include not only solving and closing reported issues but also performing analysis on issues to understand and potentially prevent similar future issues. Today, using AI, focus is shifting towards the proactive prevention.

Change Management

Change management is a part of the Help desk since change may need to be implemented as part of an issue resolution. Managing change is important and yet can be difficult, particularly in large organizations because of the resistance to change, the organisational structure, and the enterprise system landscape and system dependencies. Considering this, change management involves the following:

- Understanding change
- Planning change
- Implementing change
- Communicating change

IT Service Desk

The evolution of IT help desk is IT Service Desk. The IT Service Desk includes and offers a broader range of services compared to the Help desk. It executes and operates on many aspects of IT Service Management. A service request is being managed by the IT service desk and a service request can be very versatile. It might range from answering a simple question to reserving a conference room for a meeting, etc. Today, service requests are raised not only from phone calls but through emails, self-service portals, service catalogues, etc. There are 3 types of Service desks or rather 3 different locations of the service desk, which are:

- Local Service Desk
  - Traditional model of Service desk.
  - Co-located with the users, provides for walk-up service.
  - Walk-ups can be convenient and quick way of resolving issues.
  - Walk-ups can lead to great user experience.
- Shared Service Centre
  - Centralized team provides services to multiple organisations.

    - This model is feasible now because of increase in the number of global business and commerce centres, evolution of business leader thinking, and improved technology.

- Virtual Service Desk
    - Decentralised team based on a mobile workforce concept that can be located anywhere using devices and internet.

IT Service Management

The implementation and management of quality IT services that meet the needs of the business. IT service management is performed by IT services providers through an appropriate mix of people, process, and information technology. ITSM has become synonymous with effective and efficient management of IT assets and objects. Many businesses are seeking ways to improve operational efficiency and reliability by optimizing the management of their IT operations. Dynamic scalability is key for ITSM.

It is a concept that enables an organisation to maximise business value from the use of information technology. ITSM positions IT services as the key component of delivering and obtaining value. Internal or external IT service provider work with customers to define and deliver IT services and taking responsibility for the associated costs and risks.

ITSM works across the whole lifecycle of a service from the original design to operations of the product/service. ITSM establishes a set of practices or processes to ensure sustainable and standardised quality of IT services. These set of practices are industrial, national, and international standards for IT service management. A few examples are ITIL, COBIT, ISO, etc.

Methodologies, Standards, and best practices of ITSM have been evolving since the establishment of it. IT industry is developing and is posing more challenges to all components of ITSM. The scope and details of ITSM frameworks are also quite large and can be challenging and difficult to understand. The following are 12 elements of ITSM:

- Core 12 elements
    - Service level management
    - Service requests
    - Knowledge management
    - Availability management
    - Financial management
    - Service portfolios
    - Service catalogue (Core 6 elements)
    - Incident management (Core 6 elements)
    - Problem management (Core 6 elements)
    - Release management (Core 6 elements)
    - Change management (Core 6 elements)
    - Asset and configuration management (Core 6 elements)

No single model will work for every organisation and hence needs to be customized for every organisation. The core 6 elements are mandatory and shall be available in any organisation whereas the other 6 are augmenting services and capabilities. It is how these elements are designed, implemented, and run in the organisation that can make it one of the best in class.

Service Automation

It is a cross element capability and a very dynamic topic. It enables self service capabilities and helps manage ITSM related processes effectively and efficiently. The increasing maturity of AI and ML can help to drive the use of service automation capabilities and ultimately use even further. Challenges arise in the governance of service automation and the involved establishment costs.

WEEK 2

Assigned Reading: 7 questions to ask before implementing ITIL.

ITIL is short for IT Infrastructure Library, a framework. Many organisations turn to ITIL to better manage how IT services and technology are delivered to users but needs to be customized according to the situation. There are 7 questions to ask before getting started:

- What problems are we trying to solve?
  If the answer is not clear, ITIL is not a solution.
- What's the rationale for ITIL?
  This involves identifying why you really need to change?
- What is our route to continual service improvement?
  Continual service improvement involves understanding where an organisation wants to be at a governance level.
- What is the scope and scale of this ITIL project?
  Instead of applying a sudden, across the board change, spend some time of a careful implementation strategy. Focus on the place where the impact will be the highest.
- Does it work as intended?
  Don't stop at testing and making sure the technology is working fine but use it whenever a new process is introduced. Look at the overall situation.
- Do we even need ITIL?
  Take a step back and ask is ITIL the answer after answering the previous questions. If there are different solutions to the problem, try those as well.
- What happened?
  Review and revise at regular intervals to track best how initiatives are progressing and how they are impacting the IT department.

Assigned Reading: Choose the right ITSM tool for digital era success.

Business is increasingly reliant on information technology. This has led to the development of the IT service management (ITSM) solutions market aimed at delivering IT management capabilities to help organisations to continually optimise the design, delivery, support, use and governance of IT services to cut costs, increase productivity and efficiency, and improve employee and customer satisfaction.

ITSM solutions typically include all the tools necessary to create, deploy, manage, optimise, retire, and support an IT service throughout its lifecycle. Measuring the right metrics is key to any successful management programme. In the context of ITSM, there are five key metrics that ITSM solutions should enable organisations to measure and track. These are:

- Customer satisfaction (CSAT)
- First-contact resolution (FCR) [% of contacts resolved on first contact];
- First-level resolution (FLR) [% of contacts resolved without escalation];
- Cost per ticket

- Mean time to resolution (MTTR).

There are several frameworks that organisations can use to set an ITSM strategy, create a design, manage change, handle service operation and management, and make continual improvements to ensure that the right ITSM processes, technology and skills are in place to meet business goals. Popular frameworks that provide guidance on and best practices in delivering ITSM include:

- ITIL (Information Technology Infrastructure Library)
- COBIT (Control OBjectives for Information Technologies)
- MOF (Microsoft Operations Framework)
- Six Sigma
- ISO 20000
- TOGAF (The Open Group Architecture Framework)

As a strategic approach to design, deliver, manage and improve the way businesses use information technology, ITSM is becoming essential to most businesses. Companies are increasingly looking to introduce ITSM or improve existing ITSM capabilities to drive productivity and cut costs in a competitive global market, particularly as businesses become increasingly reliant on IT. A few business benefits of ITSM are as follows:

- Better business-IT alignment and greater returns on IT investments.
- Reduced IT costs by increase in IT efficiency and reducing IT wastage.
- Predictable IT performance and cost.
- Minimal risk of disruption.
- Reduced risk of IT implementations through improved change management.
- Ability to establish well defined, repeatable, and manageable IT processes.
- Continual improvement in effectiveness and capabilities of IT services.
- Improved satisfaction of employees, customers, and IT department.
- Improved governance and reduced risk.

The future of ITSM is through AI and ML. Automation of proactive remediation and support towards tasks and workflows through AI and ML will enable organisations to:

- Provide self-service capabilities.
- Automate simple service tasks and predictive maintenance.
- Build knowledge bases to help service desk.
- Monitor IT asset performance and identify needs for replacement or upgrades.
- Proactively identify potential IT issues.
- Classify and route issues more efficiently.

The ITSM market is clearly evolving not only to respond to changing business requirements and tap into the benefits of new and emerging technologies, but also to expand beyond IT services. Many ITSM products are either being expanded to provide collaboration across service departments or re-engineered as enterprise service management (ESM) solutions. We see ESM as a major trend, with a growing number of suppliers shifting to this broader focus.

Ultimately, the selection of any ITSM solution will depend on the organisation’s particular requirements, which depend on a variety of factors. These include the size and structure of the organisation, the level of IT maturity, the demand for an ESM capability, the degree to which IT services are delivered from the cloud, and the organisation’s need for things

like cloud-based delivery, scalability, codeless workflow design, automation, mobile support and IT operations management.

Assigned Reading: ISO9000 for Software Quality Systems.

The objectives of quality management include improvement of customer satisfaction and at the same time improvement of internal processes. Quality management uses the same principles as Engineering principles. We need communication and feedback between the different levels in an organisation. The various feedback loops provide a framework for the quality management in which several elements are put together.

- Management responsibility
- Quality system
- Measurements
- Internal audits
- Management reviews
- Preventive and corrective actions

The essential requirements for a quality system are specified in a series of internationally accepted standards: the ISO 9000 standards. Implementing these requirements enables an organisation to manage and control its quality processes and the quality level of its products or services. A few of these characteristics are mentioned below:

- Characteristics of Software development
    - Great deal of emphasis is placed on design and development.
    - It is important to use design reviews and verification and validation to prevent errors or detect them as early as possible.
    - A rigorous configuration management system is needed.
    - A complete set of specifications and a clear understanding before the development is started is necessary.

There are other standards as well such as the IEEE, CMM, SPICE initiative, etc. All of them have a common objective to assist and enable an organisation to achieve better quality management of the software processes. There is also another system of audit and certification. A third-party audit means a formal investigation whether a quality system satisfies the requirements of ISO9001 or not. A successful audit may result in the certification of the organisation's quality system.

Tutorial Reading: SOX.

Originating from the scandal of the Enron company, the Sarbanes-Oxley Act was implemented. The SOX act was implemented to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes. Since the start SOX sough out the best ways and means to ensure compliance with the prescriptions of the new act.

COBIT is a framework which is compliant with SOX and is one of the most utilized frameworks by auditors. Throughout COBIT there are key processes, practices and activities, combined with a cascade of goals from Stakeholders (needs) down to Enterprise and on to IT, to ensure that the organization considers and is positioned to comply with the requirements imposed by external entities like governmental bodies, regulators, industry mandates as well as internal policies.

The internationally recognized COBIT framework helps IT, audit and finance professionals, and enterprise leaders fulfil their IT governance responsibilities while delivering

value to the business. COBIT enables information and related technology to be governed and managed in a holistic manner for the whole enterprise, taking in the full end-to-end business and functional areas of responsibility, considering the IT-related interests of internal and external stakeholders.

Assigned Reading: Compilation of research from the last 20 years.

Table 1-1: Sourcing Options

	Sourcing Options	Description
Internal	Inhouse provision, insourcing	A sourcing option in which a client owns the assets and employs their own staff.
	Shared services	A sourcing option in which a client centralizes and standardizes delivery of business services that are shared among several business units.
Hybrid	Staff augmentation, contract labor	A sourcing option in which a client buys in low to mid-level labor to supplement inhouse capabilities; the client manages the people, usually at the client site.
	Management consulting	A sourcing option in which a client buys in high-level expertise to supplement inhouse capabilities.
	Joint ventures, strategic partnerships	A specific type of arrangement entered into by two or more parties in which each agrees to furnish a part of the capital and labor for a business enterprise in a separate entity (joint venture) or under a contract (partnership).
External	Traditional outsourcing, fee-for-service outsourcing	A sourcing option in which a client pays a fee to a provider in exchange for the management and delivery of specified products or services. The client is in charge of specifying needs and the provider is in charge of managing the resources to deliver those needs.
	Cloud services	With this utility model, clients pay a usage-based fee to providers in exchange for services being delivered over the Internet.
	Crowdsourcing	A sourcing option that invites open calls to an unknown population to perform tasks; the crowd may be rewarded with financial compensation and/or personal recognition.

Table 1-2: Sourcing Location Decisions

Sourcing Locations	Provider Staff Location
Domestic	In the same country as the client's business users
Offshore	On a different continent than the client's business users
Nearshore	In a nearby country (such as a US client being serviced from a Canadian delivery center)
Rural	In a rural community.
Global	In several countries

Table 1-3: Top Motives for Sourcing Decisions

Motives	Description
Cost reduction	A client's desire or need to reduce or control costs.
Core focus	A client's desire or need to focus on its core capabilities.
Access to skills	A client's desire or need to access provider skills / expertise.
Business process improvements	A client's desire or need to help improve an organization's business, processes, or capabilities.
Technical reasons	A client's desire or need to gain access to leading edge technology available through the providers but not available inhouse.
Political reasons	A client stakeholder's desire or need to promote personal agendas such as eliminating a burdensome function, enhancing their career, or maximizing personal financial benefits.
Concern for security/ Intellectual property	A client's concerns about security of information, trans-border data flow issues, and protection of intellectual property.
Fear of losing control	A client's concerns about losing control over the business service.

Table 1-4: Transaction Attributes Affecting Sourcing Decisions

Attributes	Description
Uncertainty	The degree of unpredictability / volatility as it relates to the requirements, emerging technologies, and/or environmental factors.
Critical Role of Product or Service	The degree to which a client views the product or service as a critical enabler of business success.
Transaction Costs	The effort, time, and costs incurred in searching, creating, negotiating, monitoring, and enforcing a contract between the parties.
Business Risk	The probability that an action will adversely affect a client

Table 1-5: Influence Sources

Type	Description
Mimetic	Influences that arise from the perception that peer organizations are more successful.
Normative	Influences arising from norms of professionalism, including formal education and professional and trade associations.
Coercive	Influences that result from both formal and informal pressures exerted on a client by other organizations upon which they are dependent.

Table 1-6: Contractual Characteristics

Characteristic	Description
Contract Detail	The number or degree of detailed clauses in the outsourcing contract, such as clauses that specify prices, service levels, benchmarking, warranties, and penalties for non-performance.
Contract Duration	The duration of the contract in terms of time.
Contract Value	The contract's financial value usually measured as the total value over its duration (see Configuration Attribute #3: Financial Scale).
Price Model	A term denoting different forms of contracts used in outsourcing, predominately based on the price model (see Configuration Attribute #4: Pricing Framework).

Table 1-7: Relationship Characteristics

Characteristic	Description
Effective Knowledge Sharing	The degree to which the parties are successful in sharing and transferring knowledge.
Partnership View	The client's view of providers as trusted partners rather than as opportunistic providers.
Prior Working Relationship	The situation under which the parties have previously worked.
Communication	The degree to which parties are willing to openly discuss their expectations, directions for the future, their capabilities, and/or their strengths and weaknesses.
Trust	The confidence in the other party's benevolence.

Table 1-8: Client Capabilities

Capability	Description
Supplier management	The extent to which a client is able to effectively manage providers.
Contract negotiation	The extent to which a client is able to effectively bid, select, and negotiate effective contracts with providers.
Technical/ methodological	A client's maturity level regarding technical or process related standards (e.g. the Capability Maturity Model (CMM), Capability Maturity Model Integrated (CMMI), IT Infrastructure Library (ITIL), and best practices such as component reuse and playbook development.
Cultural distance management	The extent to which the client understands, accepts, and adapts to cultural differences between the parties.
Risk management	A client's practice of identifying, rating, and mitigating potential risks associated with outsourcing.

Table 1-9: Provider Capabilities

Capability	Description
Human resource management	A provider's ability to identify, acquire, develop, and deploy human resources to achieve both parties' organizational objectives.
Technical/ methodological	A provider's level of maturity in terms of technical or process related standards (e.g. CMM, CMMI, ITIL), and best practices such as component reuse and development of playbooks.
Domain understanding	The extent to which a provider has prior experience and/or understanding of the client's business and technical contexts, processes, practices, and requirements.

The key takeaways from this chapter were:

- Executives want to reduce costs, focus on core capabilities, and to inject organisations with provider resources such as skills, expertise, and superior technology to improve client performance.
- Executives are more likely to insource activities that have high levels of uncertainty, criticality, business risks, and transaction costs.
- Characteristics of contract, relationships, and capabilities of the client and provider need strong complementary capabilities to make outsourcing successful.
- Outsourcing has become a routine part of management.
- The benefits that outsourcing can bring, and the risks that it can harbour, requires that the CEO plays a key role.

Assigned Reading: IT governance simultaneously empowers and controls.

Firms manage many assets— people, money, plant, and customer relationships— but information and the technologies that collect, store, and disseminate information may be the assets that perplex them the most. Business needs constantly change, while systems, once in place, remain relatively rigid. Top-performing enterprises succeed where others fail by implementing effective IT governance to support their strategies.

We define IT governance as specifying the decision rights and accountability framework to encourage desirable behaviour in using IT . IT governance is not about making specific IT decisions— management does that— but rather determines who systematically makes and contributes to those decisions. “OECD Principles for Corporate Governance,” defines corporate governance as providing the structure for determining organizational objectives and monitoring performance to ensure that objectives are attained.

This definition of IT governance aims to capture the simplicity of IT governance— decision rights and accountability— and its complexity— desirable behaviours that are different in every enterprise. There are 2 sides of governance which are:

- Behavioural side

  Corporate governance encompasses the relationships and ensuing patterns of behaviour between different agents in a limited liability corporation; the way managers and shareholders but also employees, creditors, key customers, and communities interact with each other to form the strategy of the company. The behavioural side of IT governance defines the formal and informal relationships and assigns decision rights to specific individuals or groups of individuals.
- Normative side

Corporate governance also refers to the set of rules that frame these relationships and private behaviours, thus shaping corporate strategy formation. These can be the company law, securities regulation, listing requirements. But they may also be private, self-regulation. The normative side defines mechanisms formalizing the relationships and providing rules and operating procedures to ensure that objectives are met.

Effective IT governance requires a significant amount of management time and attention. There are many reasons why IT decision making should not be left to chance and thus needs good governance. A few reasons are:

- Good IT governance pays off.
- IT is expensive.
- IT is pervasive.
- New IT bombard enterprises with new business opportunities.
- IT governance is critical to organisational learning about IT value.
- IT value depends on more than good technology.
- Senior management has limited breadth.
- Leading enterprises govern IT differently.

Information Technology Infrastructure Library

ITIL is a set of prove IT best practices that can help IT organisations of all sixes to improve the delivery of IT services. It provides and ITSM structure and a collection of processes that are supported by details. ITIL can be used as a useful reference for IT organizations to improve their current ITSM performance and prepare for future ITSM challenges. ITIL can influence various processes throughout the organisation such as in Supply chain management, finance, human resources, marketing and sales, and logistics management.

ITIL has been updated through the years. It was first released in late 80s as V1 which was then upgraded to ITIL v2 around 2000. ITIL v3 was released in 2007 and the latest version was released in 2019 as v4 which makes it easier for organisations to align ITIL with DevOps, Agile, and Lean work methods.

The Service Lifecycle

The service lifecycle model is intended to provide a flexible and adaptable framework for ITIL. This is the 3rd version of ITIL. This service lifecycle model is intended to provide a flexible and adaptable framework for ITIL. IT organisations globally leverage the ITIL Service Lifecycle framework as a reference to design, realise and run their own ITSM processes and capabilities. The ITIL Service lifecycle is given below:

The 5 stages of the ITIL Service Lifecycle are:

- Service Strategy

  Figuring out what the customer wants from the service? What value should the service provide. The following are the major components of Service strategy:

  - Service portfolio management

    The main objective is to manage the service portfolio where you ensure that the service provider has the right mix of services to meet the required business outcomes for customers.
  - Financial management for IT services

    The main objective is to manage the service provider's budgeting, accounting, and charging requirements. Financial management for IT services ensures that costs are monitored and controlled to avoid unexpected budget blow outs.
  - Demand management

    The main objective is to understand, anticipate, and influence customer demand for services. Demand management works with capacity management to ensure that the service provider has sufficient capacity to meet the required demand.
  - Business relationship management

    The main objective is to maintain a positive relationship with customers. This component identifies the needs of existing and potential customers and ensures appropriate services are developed to meet those needs.
- Service Design

  Figuring out the definition of the services based on the service strategy. The design should be built around the needs of the customer and the values the service should provide. The following are the major components of Service Design:

  - Design coordination

    The main objective is to coordinate all service design activities, processes, and resources. It ensures the consistent and effective design of new or changed IT services.
  - Service Catalogue Management

    The main objective is t ensure that a service catalogue is produced and maintained, containing accurate information on all organisational services and those being prepared to be run operationally. It provided vital information for all other service management processes such as the interdependencies, details and current status.
  - Service Level Management

    The main objective is to negotiate service level agreements with the customers and to design services in accordance with the agreed service level targets. It is also responsible for ensuring that all operational agreements and underpinning contracts are appropriate.
  - Risk Management

    The main objective of this is to identify, assess, and control risks which includes analysing the value of assets to the business, identifying threats to the assets, and evaluating the vulnerability of the assets.
  - Capacity Management

    The main objective is to ensure the capacity of IT services and the IT infrastructure can deliver the agreed service level targets in a cost effective and timely manner. It considers all resources required to deliver

the IT service, plans for short-, medium-, and long-term business requirements.

- Availability Management
  The main objective is to define, analyse, plan, measure, and improve all aspects of the availability of IT services. Availability management is responsible for ensuring that all IT infrastructure, processes, tools, etc. are appropriate for the agreed available targets.
- IT Service Continuity Management
  The main objective is to manage risks that could seriously impact IT services. ITSCM ensures that the IT service provider can always provide minimum service levels by reducing risks to an acceptable level and planning for the recovery of IT services after a disaster.
- Information Security Management
  The main objective is to ensure confidentiality, integrity, and availability of an organisation's information, data, and IT services. ITSM usually forms a part of the organisational approach to security management which has a wider scope that IT service provider.
- Compliance Management
  The main objective is to ensure IT services, processes, systems comply with enterprise policies and legal requirements.
- Architecture Management
  The main objective is to define a blueprint for the future development of the technological landscape considering the service strategy and newly available technologies.
- Supplier Management
  The main objective is to ensure that all contracts with suppliers support the needs of the business and that all suppliers meet their contractual commitments.

- Service Transition
  After design the service we build and deploy it and ensure a coordinated roll-out so that the service is deployed properly without any errors. The components of Service transition are given below:
  - Change management
    The main objective is to control the lifecycle of all changes. The primary objective is to enable beneficial changes to be made with minimum disruption to the IT services.
  - Change evaluation
    The main objective is to assess major changes before those changes are allowed to proceed to the next phase in their lifecycle. Examples of these changes might include introduction of a new service or a substantial change to an existing service.
  - Project management
    The main objective is to plan and coordinate the resources to deploy a major release within the predicted cost, time, and quality measures.
  - Application development
    The main objective is to make applications and systems which provide the required functionality of IT services.
  - Release and deployment management

The main objective is to plan, schedule, and control the movement of releases. The primary goal is to ensure that the integrity of the live environment is protected, and the correct components are released.

- Service validation and testing

  The main objective is to ensure that deployed releases and the resulting services meet customer expectations and to verify that IT operations can support the new service.

- Service asset and configuration management

  The main objective is to maintain information about configuration items required to deliver an IT service, basically the documentations.

- Knowledge management

  The main objective is to gather, analyse, store, and share knowledge and information within an organisation. The primary purpose of it is to improve efficient by reducing the need to rediscover knowledge.

- Service Operation

  In this step we ensure that the IT services are delivered effectively and efficiently. The components of Service operation are given below:

  - Event management

    The main objective is to make sure services are constantly monitored and to filter and categorize the events to decide on appropriate actions.

  - Incident management

    The main objective is to manage the lifecycle of all incidents. The primary objective is to return the IT service to users as quickly as possible.

  - Request fulfilment

    The main objective is to fulfill service requests which in most cases are minor changes or request to information.

  - Access management

    The main objective is to grant authorized users the rights to use a service while preventing access to non-authorized users. The access management processes essentially execute policies defined in ISM and is also known as Rights Management or Identity Management.

  - Problem management

    The main objective is to manage the lifecycle of all problems. The primary objective is to prevent incidents from happening and to minimize the impact of incidents that cannot be prevented. It analyses incident records and uses data collected by other IT service management processes to identify trends or significant problems.

  - IT Operations control

    The objective is to monitor and control the IT services and their underlying infrastructure. The process of ITOC executes day-to-day routine tasks related to the operation of infrastructure components and applications. This includes job scheduling, backup and restore activities, print, and output management, and routine maintenance.

  - Facilities management

    The main objective is to manage the physical environment where the IT infrastructure is located. Facilities management includes all aspects of managing the physical environment. Examples: building access management, power and cooling, environmental monitoring, etc.

  - Application management

The main objective is to manage applications throughout their lifecycle of growth, maturity, and end of life.

- Technical management

  The main objective is to provide technical expertise and support for the management of the IT infrastructure.

- Continual Service Improvement

  In this step we listen to customer feedback about the service provided and review the service and optimise it via potential amendments in the previous stages. The components of CSI are given below:

  - Service review

    The main objective is to review the business services and infrastructure services on a regular basis. The aim of this process is to improve service quality where necessary and to identify more economical ways of providing a service where possible.

  - Process evaluation

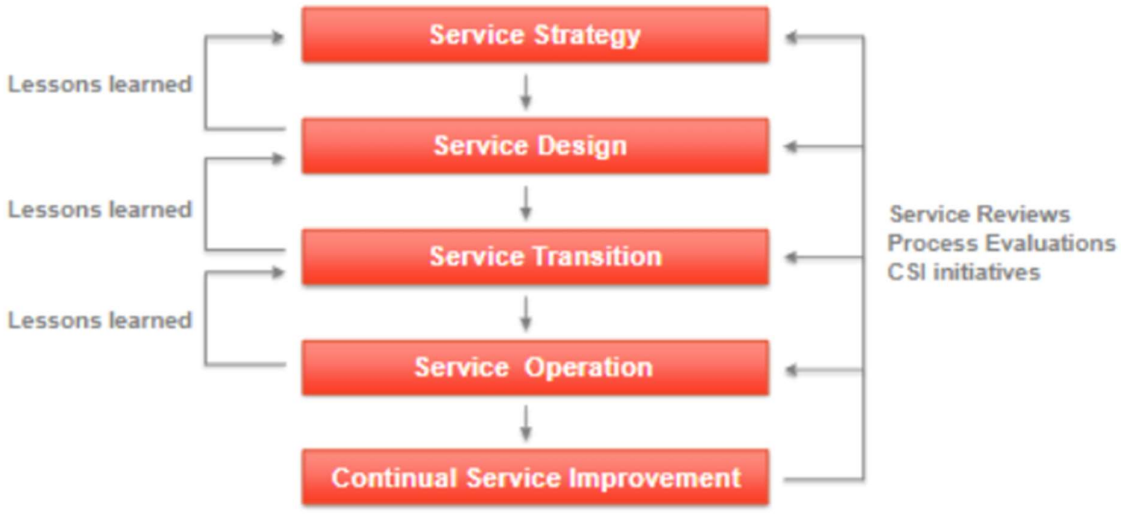
    The main objective is to evaluate the processes on a regular basis. This includes identifying key areas where the targeted process metrics are not reached and holding regular benchmarking, audits, maturity assessments, and reviews.

  - Definition of Continual Service Improvement Initiatives

    The main objective is to define the specific initiatives aimed at improving services and processes based on the results of the service improvement reviews and process evaluations. The resulting initiatives are either internal initiatives pursued by the service provider or initiatives which require customer cooperation.

  - Monitoring of CSI initiatives

    The main objective is to verify if improvement initiatives are proceeding according to plan and to introduce corrective measures where necessary.



Visualization of the Continual Service Improvement Process

ITIL v4

The Service Lifecycle was created to help organize our thoughts around ITSM. The intent of the Service Lifecycle was to help organize the processes in and components of ITIL.

Many organizations used ITIL 3 as a sequential way of working which created the following problems:

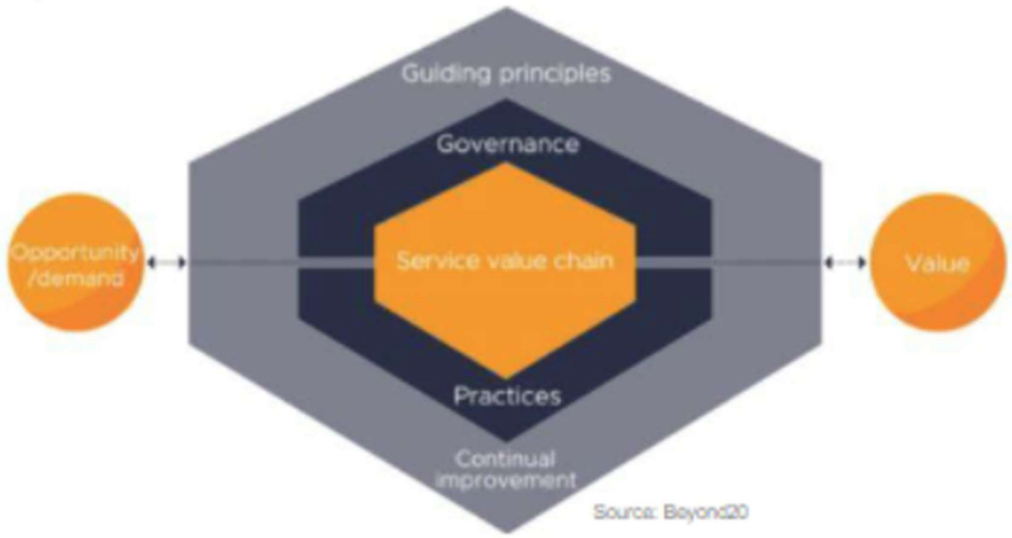
- Components of a process were considered only in this phase, but it could be relevant in other phases as well.
- ITIL teams tended to take a perfectionist approach purely focusing on dedicated aspects of ITIL while the other topics were not considered by them creating a Silo mentality.

This brings in ITIL v4 which replaces the Service Lifecycle of ITIL v3 with Service Value System and Service Value Chain. More details are given below:

- Service Value System

  The Service Value System shows the high-level forces within any organization that prevent or support our ability to deliver great products and services to our customers. These forces are:
  - Governance: How well we manage our products/services and provide guidelines and principles for them.
  - Guiding principles: The values and beliefs we live by.
  - Service Value chain: Helps to design, build, roll-out and support services.
  - Practices: There are 34 best practices/processes/capabilities of them in ITIL v4.
  - Continual Improvement: The most successful organisation are focused with continually getting better.

  The main goal of Service Value System is not to work on one area, but rather to look at how we are working as an entire organization and to examine how effectively we are going from the left-hand side of the diagram to the right-hand side of the diagram given below:

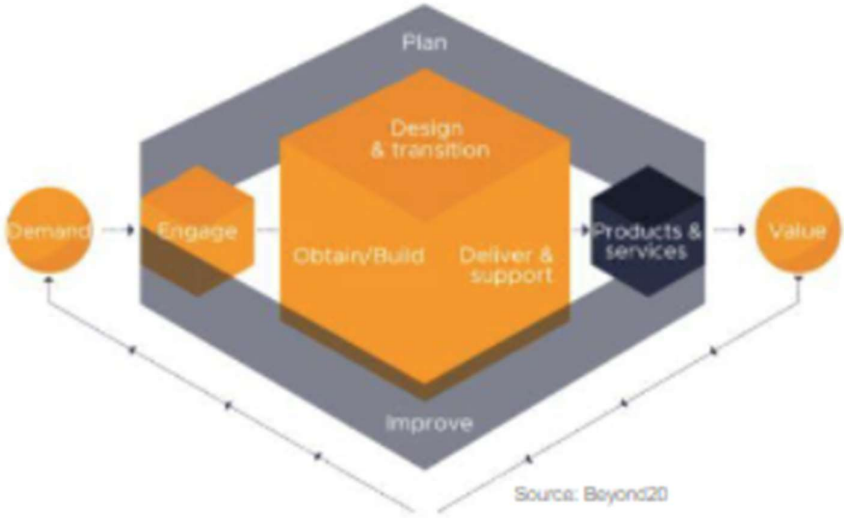


- Service Value Chain

  The Service Value Chain is a component within the overarching Service Value System that helps us to design, build, roll-out and support services. The SVC looks most like the ITIL v3 Service Lifecycle. The 6 key activities are:
  - Plan: All types of planning at all levels.
  - Engage: All interactions with people who are external to the SVC.
  - Design and Transition: Business analysis and development of new and improved services.

- Obtain/Build: Any new resource brought into the Value chain is sourced via obtain/build.
- Deliver and Support: Provisioning services and providing help and information.
- Improve: Improvements at all levels.

A diagram to display the Service Value chain is given below:



COBIT – Control Objectives for Information and Related Technology

COBIT was originally developed to address the needs of auditors focussed on technology and technology controls and has a close relationship to the Sarbanes-Oxley (SOX) act. It helps companies achieve SOX section 404 compliance and is useful for providing guidance for internal IT controls. COBIT can also be used as a reference for IT service management as it provides into IT governance and IT risk management.

COBIT framework is formed around 5 guiding principles, these are:

- An integrated IT Framework

  COBIT emphasizes the importance of aligning IT operations and services with the broader business department.
- Stakeholder Value Drivers

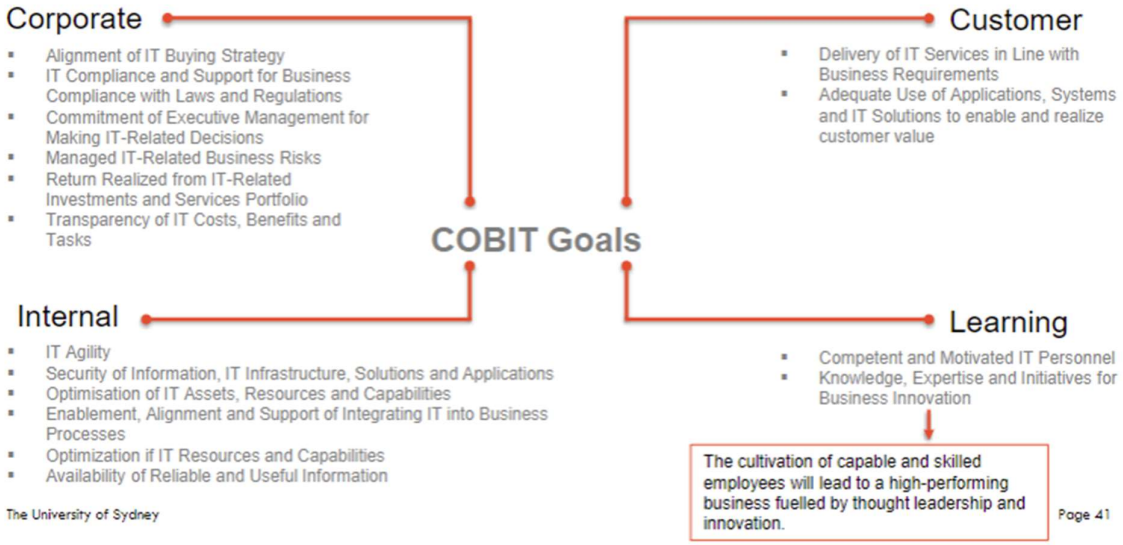
  IT operating processes should be designed to ensure the delivery of measurable value while optimizing costs through-out the lifecycle of a service or product.
- Resources focus on a Business Context

  All technology assets, information, components and people should be used to maximise the leverage of IT within the organisation.
- Risk Management

  The management team shall have a full understanding and awareness of an organisation' compliance requirements and its current risk exposure. It should also have strategies in place to manage and mitigate these risks.
- Performance Management

  Measurement and reporting processes should be implemented to ensure visibility and understanding of performance indicators supporting the primary objectives of IT.

The COBIT framework also defines goals, which help organisations to define guidelines of what they want to achieve from an ITSM perspective. These goals are distributed into 4 categories:



COBIT framework is based on 4 process groups:

- Align, Plan, and Organise
  The process group involves the following components:
  - IT Management Framework
    It recommends implementing a consistent management approach for enterprise IT governance such as organisational structures, roles and responsibilities, reliable and repeatable activities, policies and procedures, skills and competencies, and culture and behaviour.
  - Managed Strategy
    Provide a holistic view of the current business and IT environment, the future direction, and the initiatives required to migrate to the desired future environment. Assess the organization's current digital maturity and develop a road map to close the gaps. With the business, rethink internal operations as well as customer-facing activities. Ensure focus on the transformation journey across the organization.
  - Enterprise Architecture
    Establish a common architecture consisting of business process architecture, information and integration architecture, data architecture, and application and technology architecture. Architecture needs to be created aligned to the enterprise and IT Strategy.
  - Managed Innovation
    Maintain an awareness of IT and related service trends and monitor emerging technology trends. Proactively identify innovation opportunities and plan how to benefit from innovation in relation to business needs and the defined IT strategy.
  - Managed Portfolio
    Execute the strategic direction set for investments in line with the enterprise architecture vision and I&T road map. Consider the different

categories of investments and the resources and funding constraints. Evaluate, prioritize, and balance programs and services.

- Managed Budget and Costs

  Manage the IT-related financial activities in both the business and IT functions, covering budget, cost and benefit management and prioritization of spending using formal budgeting practices. Consult stakeholders to identify and control the total costs and benefits within the context of the I&T strategic and tactical plans. Initiate corrective action where needed, etc.

- Managed Human Resources

  Provide a structured approach to ensure optimal recruitment/acquisition, planning, evaluation, and development of human resources (both internal and external). Optimise human resources capabilities to meet enterprise objectives.

- Managed Service Agreements

  Align IT-enabled services and service levels with enterprise needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of IT products and services, service levels and performance indicators. Ensure that IT products, services and service levels meet current and future enterprise needs.

- Managed Relationships

  Manage relationships with business stakeholders in a formalized and transparent way that ensures mutual trust and a combined focus on achieving the strategic goals within the constraints of budgets and risk tolerance.

- Vendor Management

  Manage IT-related products and services provided by all types of vendors to meet enterprise requirements. This includes the search for and selection of vendors, management of relationships, management of contracts, and reviewing and monitoring of vendor performance and vendor ecosystem.

- Managed Quality

  Define and communicate quality requirements in all processes, applications, procedures, and related enterprise outcomes. Enable controls, ongoing monitoring, and the use of proven practices and standards in continuous improvement and efficiency efforts.

- Managed Risk

  Continually identify, assess, and reduce IT-related risk within levels of tolerance set by enterprise executive management. Integrate the management of IT-related enterprise risk with overall Enterprise Risk Management (ERM) and balance the costs and benefits of managing IT-related enterprise risk.

- Managed Security

  Define security principles, operate, and monitor a system for information security flaws. Keep the impact and occurrence of information security incidents within the enterprise's risk appetite levels.

- Managed Data

  Achieve and sustain effective data management of data assets across the data life cycle, from creation through delivery, maintenance, and

archiving. Ensure effective utilization of the critical data assets to achieve enterprise goals and objectives.

- Build, Acquire, and Implement
  The process group involves the following components:
  - Managed Programs
    Manage all programs from the investment portfolio in alignment with enterprise strategy and in a coordinated way, based on a standard program management approach. Initiate, plan, control, and execute programs, and monitor expected value from the program.
  - Managed Required Definition
    Identify solutions and analyse requirements before acquisition or creation to ensure that they align with enterprise strategic requirements covering business process, applications, information/data, infrastructure, and services requirements. Create optimal solutions that meet enterprise needs while minimizing risk.
  - Managed Solutions Identification and Build.
    Ensure agile and scalable delivery of digital products and services – ideally via DevOps and CI/CD (Continuous Integration and Continuous Delivery. Establish timely and cost-effective solutions capable of supporting enterprise strategic and operational objectives. Define guideline and principles for 'Buy vs. build'. Avoid anti-vendor sentiment/culture to keep an open mind!
  - Managed Availability and Capability
    Balance current and future needs for availability, performance, and capacity with cost-effective service provision. Include assessment of current capabilities, forecasting of future needs based on business requirements, analysis of business impacts, and assessment of risk to plan and implement actions to meet the identified requirements. Maintain service availability, efficient management of resources and optimization of system performance through prediction of future performance and capacity requirements.
  - Managed Organisational Change
    Prepare and commit stakeholders for business change and reduce the risk of failure.
  - Managed IT Changes
    Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications, and infrastructure. This includes change standards and procedures, impact assessment, prioritisation and authorisation, emergency changes, tracking, reporting, closure, and documentation. Enable fast and reliable delivery of change to the business.
  - Managed Change Acceptance and Transitioning
    Define a formalised process for new solutions, including implementation planning, system and data conversion, acceptance testing, communication, release preparation, promotion to production of new or changed business processes and IT services, early production support, and a post-implementation review. Implement solutions safely and in line with the agreed expectations and outcomes.
  - Managed Knowledge

Maintain the availability of relevant, current, validated, and reliable knowledge and management information to support all process activities and to facilitate decision making related to the governance and management of enterprise IT. Plan for the identification, gathering, organizing, maintaining, use and retirement of knowledge Provide the knowledge and information required to support all staff in the governance and management of enterprise I&T and allow for informed decision making.

- Managed Assets

  Prepare and commit stakeholders for business change and reduce the risk of failure. Manage IT assets through their life cycle to make sure that their use delivers value at optimal cost, they remain operational, and they are accounted for and physically protected. Ensure that those assets that are critical to support service capability are reliable and available. Manage software licenses to ensure that the optimal number are acquired, retained, and deployed in relation to required business usage, and the software installed is following license agreements. Account for all IT assets and optimize the value provided by their use.

- Managed Configuration

  Define and maintain descriptions and relationships among key resources and capabilities required to deliver I&T-enabled services. Include collecting configuration information, establishing baselines, verifying, and auditing configuration information, and updating the configuration repository.

- Managed Projects

  Manage all projects that are initiated within the enterprise in alignment with enterprise strategy and in a coordinated way based on the standard project management approach. Initiate, plan, control and execute projects, and close with a post-implementation review. Realize defined project outcomes and reduce the risk of unexpected delays, costs, and value erosion by improving communications to and involvement of business and end users. Ensure the value and quality of project deliverables and maximize their contribution to the defined programs and investment portfolio.

- Deliver, Service, and Support

  The process group involves the following components:

  - Managed Operations

    Coordinate and execute the activities and operational procedures required to deliver internal and outsourced IT services.

  - Managed Service Requests and Incidents

    Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate, and resolve incidents. Achieve increased productivity and minimize disruptions through quick resolution of user queries and incidents.

  - Managed Problems

    Identify and classify problems and their root causes. Provide timely resolution to prevent recurring incidents. Provide recommendations for improvements. Increase availability, improve service levels, reduce costs, improve customer convenience and satisfaction by reducing the

number of operational problems, and identify root causes as part of problem resolution.

- Managed Continuity

  Establish and maintain a plan to enable the business and IT organizations to respond to incidents and quickly adapt to disruptions. This will enable continued operations of critical business processes and required I&T services and maintain availability of resources, assets, and information at a level acceptable to the enterprise. Adapt rapidly, continue business operations, and maintain availability of resources and information at a level acceptable to the enterprise in the event of a significant disruption.

- Managed Security Services

  Protect enterprise information. Maintain and mitigate IT enterprise security risks in accordance with the security policies in place. Establish and maintain information security roles and access privileges. Perform security monitoring. Minimize the business impact of operational information security vulnerabilities and incidents.

- Managed Business Process Controls

  Define and maintain appropriate business process controls to ensure that information related to and processed by in-house or outsourced business processes satisfies all relevant information control requirements.

- Evaluate, Direct, and Monitor

  The process group involves the following components:

  - Ensured Governance Framework Setting and Maintenance

    Provide a consistent governance approach integrated and aligned with the enterprise governance approach. IT-related decisions are made in line with the enterprise's strategies and objectives, the desired value is realized and that these decisions are governed.

  - Ensured Benefits Delivery

    Optimize the value to the business from investments in business processes, IT services and IT assets. Secure optimal value from IT-enabled initiatives, services, and assets; cost-efficient delivery of solutions and services; and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.

  - Ensured Risk Optimizations

    Ensure that the enterprise's risk appetite and tolerance are understood, articulated, and communicated, and that risk to enterprise value related to the use of IT is identified and managed. Risk mitigation strategies should be in place to avoid major disruptions and potentially financial losses.

  - Ensured Resource Optimisation

    Ensure that adequate and sufficient IT-related capabilities are available to support enterprise objectives effectively at optimal cost. Ensure that the resource needs of the enterprise are met in the optimal manner, IT costs are optimised, and there is an increased likelihood of benefit realisation and readiness for future change.

  - Ensured Stakeholder Engagement

    Ensure that stakeholders are identified and engaged in the IT governance system and that enterprise IT performance and conformance measurement (e.g., via KPIs) and reporting are transparent, with

stakeholders approving the goals and metrics and necessary remedial actions. Ensure that stakeholders are supportive of the IT strategy and road map, communication to stakeholders is effective and timely, and the basis for reporting is established to increase performance.

ISO

ISO stands for International Organization for Standardization based in Geneva, Switzerland. ISO develops and publishes worldwide technical, industrial, and commercial standards. It provides a wide variety of IT industry standards such as ISO 9000 for quality management, ISO27017 for cloud security, etc. ISO9000 is defined as a set of international standards on quality management and quantity assurance. The key components of ISO9000 are:

- Keeping detailed business records.
- Implementing a continuous improvement process.
- Regular reviews of processes and quality systems to measure effectiveness.
- Monitoring productive environment for defects and implementing corrective actions.

The objectives of ISO9000 are:

- Improvement of customer satisfaction.
- Improvement of internal processes.

ISO38500 addresses the effective use of IT in an organisation. It has 3 objectives:

- Providing confidence to all stakeholders in their IT governance.
- Providing guidance to managers to help them to govern the use of IT in the organisation.
- Providing an approach for the fair and objective evaluation of IT governance within organisations.

ISO38500 helps to provide IT governance to ensure the fulfillment of the legal, ethical, and regulatory obligations of an Organisation. ISO38500 follows 6 principles for good IT governance which are:

- Responsibility: All individuals and groups withing the organisation understand and accept their responsibilities with respect to the supply and demand of the IT services and resources.
- Strategy: The execution of IT strategy must meet the projected needs of the business strategy.
- Acquisition: All IT assets and resources acquisitions should be validated with a thorough evaluation and transparent decision-making process.
- Performance: The performance of IT should be sized and scaled to the needs of the enterprise.
- Conformance: IT should be proactive in complying with all mandatory regulations and legislations and to assist with audit and governance activities.
- Human Behaviour: All IT decisions and policies should show appropriate respect for all people in the organisation.

WEEK 3

Assigned Reading: Operations Management reshaped by Robotic Automation

According to research predictable physical work, data processing, and data collection activities can be automated which describe much of the work handle in the operation centres.

Operation centres are defined as the organizations that are defined as those which manage equipment and services remotely, or that manages human forces in the field.

Robotic Process Automation has been widely adopted in organizational support functions. Environments which have standardized processes became the ripe field for introduction of RPA which when applied reduced costs and improved accuracy. It has improved further in recent years by providing high levels of quality and stability. By automating manual and repetitive tasks, successful operations centres reduce cost by 30-60% while increasing delivery quality. There are 3 differences between RPA and traditional automation technologies. These are:

- Accelerated implementation: Reduction in time and hence costs.
- Low barriers of entry: Gets overlaid on existing IT infrastructure.
- Enhanced control: RPA applications are powerful and have several features to improve efficiency.

A few things which are best to automate using RPA:

- Network monitoring
- Remote troubleshooting and resolution
- Automated dispatching
- Self-help facilities

Successful RPA-led transformations have focused on capturing value by starting small, exploring select use cases, and scaling up over time. This methodical approach has yielded a wide range of performance improvements at operations centres. Few noteworthy achievements are:

- Reduction in costs.
- Reduction in escalations and cycle time and field costs.
- Increasing quality of service.

When robotic-automation projects run into problems, a crucial reason is often misalignment between IT and business leaders—who will need a deeper level of cooperation. IT must contribute its advanced technical knowledge and experience in running production-level quality systems and ensure end-to-end performance of the bots. Close collaboration is also required whenever there is a change in the application, so that bots can be updated appropriately.

A centre of excellence (CoE) is vital both as a source of expertise and to define priorities. This central team, with responsibilities cutting across operations and other functions, leads the organization's transformation, identifies opportunities for automation, and helps scale up current automation programs. The role of the CoE evolves over time. In the short term (usually the first six months), the CoE's diverse support responsibilities will include identifying the potential for automation; prioritizing opportunities; managing early proof-of-concept testing; codification of learnings; recruitment of CoE team members; training of businesspeople; and oversight of existing transformations. In the long term, the CoE's primary role evolves. Activities include managing the entire transformation from end to end (including prioritization of initiatives and funding), providing technical support for more complex issues, and establishing best practices. The CoE also supports initiatives of varying sizes across the company, seeds subject-matter experts and advocates where needed, and provides thorough

coaching to team members. Additionally, the centre can give light support to business-led initiatives. The CoE's support should be guided by 4 main principles:

- Establish an agile way of working: Through cross-team collaboration and knowledge sharing.
- Drive standardization: By ensuring consistent automation approach and reusability of components across different sprint teams.
- Coordinate with IT: For automation delivery and execution.
- Continuously introduce emerging technologies.

For a successful transformation, a company needs a comprehensive, end-to-end view of the automation opportunity. It should prioritize automation activities by business value, ease of implementation, and risk.

Assigned Reading: TechTarget IT Service Catalogue Business Goals

CIOs are starting to redefine IT service catalogue management as a discipline that extends well beyond traditional IT support. This new service-catalogue approach allows CIOs to standardize the resolution of more types of business requests and automate more of the business.

The traditional discipline of IT service catalogue management involved resolving IT issues and fulfilling requests using an on-premises ticketing solution. Service catalogues can only streamline the business to the extent that they are used by employees. To spur catalogue adoption, one needs to educate users on how to make requests through the catalogue and prevent the fulfillment of user requests that are not made through a service catalogue.

One of the challenges with traditional service catalogues was that they placed a burden on the employee making a request, thus limiting adoption. CIOs can reduce this burden using conversational bots to automate requests. Employees simply chat with the bot, tell it what they need, and the bot uses AI to learn employees' preferences along the way. CIOs are starting to move beyond the low-hanging fruit of employee onboarding/offboarding, new equipment requests and application access requests accessed via service catalogues. The adoption of service catalogues can be daunting initially, but it gets easier over time.

One of the side benefits of well-managed ITSM processes is that they can serve as a model for other departments outside of IT. Enterprise service management (ESM) is about taking IT best practices and applying them to other service departments in the enterprise. Aside from streamlining business processes outside of IT, ESM has also given enterprises better ROI on their IT spending for tools and process automations.

Assigned Reading: The Service Revolution

The industrial revolutions started in the late eighteenth century and automated blue-collar jobs in manufacturing, thereby providing massive structural benefits to our societies. They rapidly Increased our standard of living by bringing high-quality, low-cost manufactured goods to the masses, and relieved people from laborious manual work. Robot- and AI-delivered service offers unprecedented economies of scale and scope, as the bulk of the costs are incurred in their development. Physical robots cost a fraction of adding to the headcount, and virtual robots can be deployed at negligible incremental cost.

Already, many firms are showing eager interest in experimenting with service robots. For example, hotels are introducing humanoid robots in their lobbies, where they welcome

guests, provide information and entertain guests. At airports, they scan boarding passes and help passengers to find the right departure gate. Self-moving check-in-kiosk robots detect busy areas and autonomously go there to help passengers reduce waiting time. Particularly, the outbreak of COVID-19 has increased the demand for medical service robots that check people's temperature or take over disinfection work.

Such robots in hotels, airports, and restaurants, chatbots and delivery bots are only the beginning of the service revolution. This means that, like the shift that started in the industrial revolution from craftsmen to mass production, an accelerated shift in the service sector towards robot- and AI- delivered services can be expected. The exciting prospect is that many services, including healthcare and education, are likely to become available at much lower prices and much better quality, and lead to a dramatic increase in our standard of living.

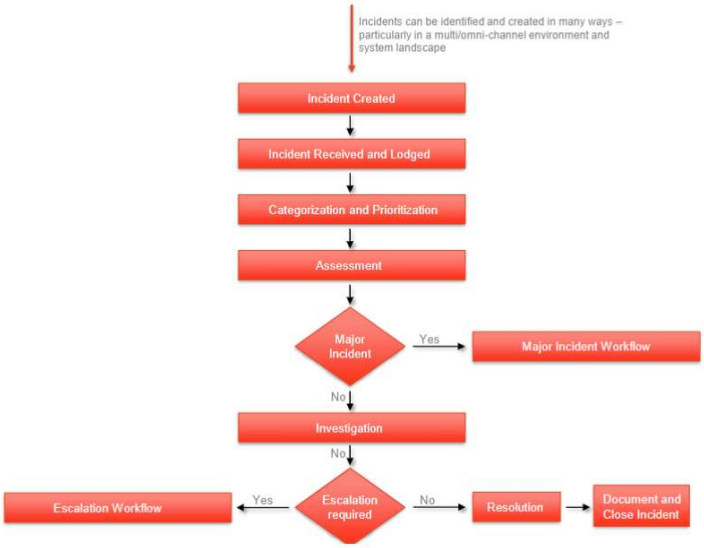
Incident Management

An incident is an instance of an event or occurrence. An incident is the trigger which creates several actions and business processes. An IT incident is usually facilitated by an IT Service desk and usually represents an interruption of the performance of an IT service. The process of managing incidents is focused on restoring the service to its normal state as quickly as possible with minimum impact on the business. It is very challenging to operate a healthy IT Service desk if a reliable and scalable incident management process is not established first.

The following facts need to be considered when setting up an IT incident management process:

- The creation of an incident is a trigger for IT Service Management.
- Rapid resolution of incidents is critical to the business.
- Critical incidents can shut down business operations and impact revenue and customers.
- Incidents can be critical to audits and governance, creating a corporate dependency on this core process.
- High performing service desks are effective and efficient at managing incidents.
- A focus on incidents and their understanding and effective management are vital components of ITSM.

Following is the Incident Management Process:



The detail of each step is given below:

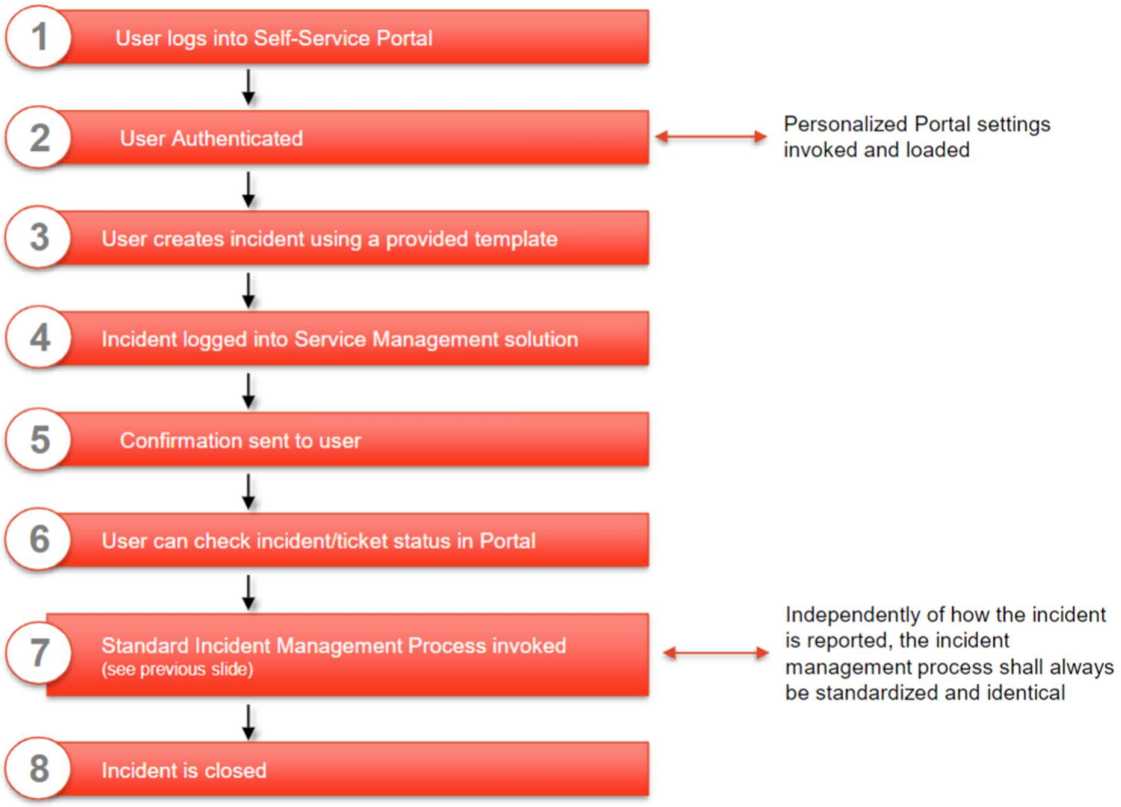
- Incident created: The incident is created with an ID to identify the incident, the user contact information of the user logging the incident, brief description of the issue, incident priority, related incidents, etc.
- Incident recorded and lodgements: Upon creation the incident is confirmed and logged in the incident management system.
- Categorization and prioritization: the incident needs to be categorized and prioritized but the priority may not represent the priority for the organisation. The categorization of incidents supports the assignment of the right resources.
- Assessment: The fundamental goal of incident management is to restore normal service as quickly as possible, once the incident is categorized and prioritized, the quick assessment is to aim for a quick error resolution. Having the knowledge base, remote control and known error logs and potential resolutions can help successful incident resolution.
- Investigation: If the quick assessment phase does not provide a fix, a full incident investigation may be triggered. Any notes of the quick assessment is used in the investigation stage. The focus of investigation is to restore service as quickly as possible, ensured restored service quality is to agree quality level. Each step of the investigation is documented, and it is important for incident escalation.
- Escalation: High priority incidents are escalated to the next level to the experts. When an incident is escalated, the issue is generally something quite serious where its high priority and has impacts which can interrupt business operations.
- Resolution: Preliminary testing is performed to verify the solution and additional use cases applied to broaden testing. Users are contacted to participate in testing or to validate the solution and then the solution is implemented.
- Document and Close: Once the incident is fixed, you need to document it along with the scenario. Incident documentation before closure should include at minimum the steps to reduce the issues, current result and expected result, timing of actions, root cause analysis and findings, applied workarounds, etc.

The way incidents were reported is changing. The phone has been the most common way to create an incident. This is changing and more convenient tools are being used such as social media, email, etc. Based on the new generation of employees and consumers, a phone call may not be the fastest and most convenient way to report an incident. Emails, social media, etc. are changing the way organisations are processing incidents. An example for email driven incident looks like the following:

- User sends email to service desk.
- Email listener receives email real time.
- Email is parsed of key words.
- An incident is automatically created.
- Workflow pushes new incident into incident process.
- Incident management begins.
- Trigger standard incident management process.
- Close incident.

A self-service model is like the email process but more bi-directional as it interacts with the user. Self-service capabilities have grown in popularity due to its ease of use, 24/7 availability, convenience, etc. Self-service portal can provide access to a variety of services such as accessing important information or knowledge, information to common questions,

management of service requests, etc. The graph below represents the incident management process via self-service:



Problem management, availability management, change management, and knowledge management are key integration and partnerships. Incident and Problem management are closely related as multiple incidents might be part of the same problem. In incident management, the focus is to resolve the issue as soon as possible whereas in problem management one wants to figure out the root cause of the problem and fix it permanently. Availability management relates to assessment of all incidents that impact service availability to determine how to prevent similar problems in the future. Change management related to working with change managers to understand and maintain visibility of changes that will address incidents and problems. Knowledge management relates to providing access to knowledge base at the time of an incident and throughout the incident lifecycle. It is also important that an organisation is proactive with knowledge management.

Following are the recommendations for successful incident management:

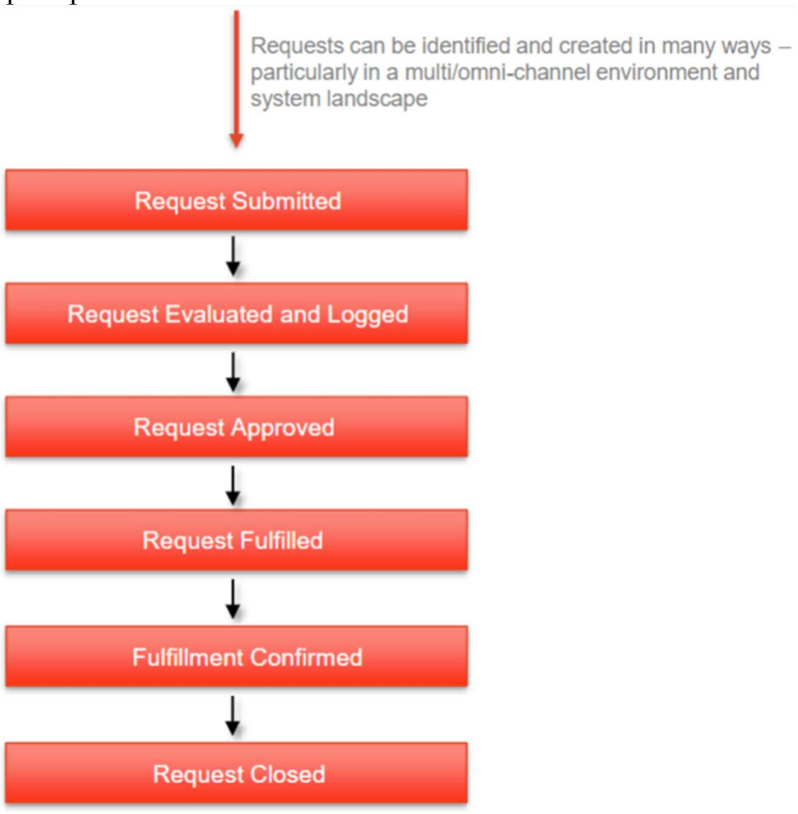
- Commitment to resolve incidents quickly with a standardized and acceptable quality level.
- Focus on speed. User satisfaction is often linked to how quickly the incident is resolved.
- Create a method to accurately measure user satisfaction.
- Leverage self-service technologies to offload the service desk and reduce costs.
- Ensure that incident workflow for major incidents is well understood, well defined, and optimized to resolve the issues with the agreed service level agreements.
- Manage escalations carefully but, when necessary, mobilize swiftly and strongly.

Service Requests

A request from a user for information, advise, a standard change, or access to a service. Service request is a trigger for a series of action designed to fulfill requests. The service request and the service fulfilment process should be flexible, agile, rapid, and standardized. Service requests broaden the scope and role of traditional tickets and incidents and move beyond break-fix model. Service requests are a necessary part of every service management process. Certain considerations when setting up IT Service Request processes are:

- A service request allows the IT Service Desk to deliver a broad range of services.
- A service request offering enables organisation to adopt quickly to changing user demands.
- Some models will mix incident management with service request management. An incident is created to resolve an issue. A service request may not necessarily solve an issue but serve the request of a customer.
- Service requests offer several benefits to organisations such as increasing speed and convenience for users to access services, easy to consume interfaces to make service request possible at any time, increase suer satisfaction by answering questions and providing access to commonly requested information, improve productivity and effectiveness of the organisation and its employees, better service fulfillment control, reduced costs, etc.

The service request process is as follows:



The process steps are:

- Service Request submission: It is the first step and should be easy and convenient to submit a service request. This is the reason why a multichannel and/or omnichannel approach is undertaken.
- Service Request Evaluation and Logging: It is the following step where the service request form should be simple and easy to understand. After a service request is logged,

the priority and category are assigned to the service request and based on the information provided, a resource assignment will be evaluated, and a fulfillment timeline can be calculated.

- Service Request Workflow: Certain service requests can be preapproved. Some service requests can also trigger an approval workflow which is usually evaluated based on the cost, risk, location, initiator, request type, etc. Approval workflow has several benefits such as approvals for higher cost requests support cost accountability, it enables us to assign costs to specific entities within an organisation and understand the cost of operations, increased visibility of the users' consuming services, and the relative demand for each service etc. Automation of this step is key as it has the potential to save cost and time making people more productive.
- Request Fulfilment: The process represents the completion of the delivery of the service request. It can be as simple as answering a question, taking feedback on user experience with existing service, or more complex workflow approvals, etc. Small things when automated will be quicker, more productive, and cost effective.
- Fulfilment confirmed: Following up with the user to ensure they have received requested service successfully and are satisfied is important and asking for feedback is important to improve service quality. A common follow up process is the 2-touch approach where the first touch is immediately after the delivery of the service request is complete and second touch is 2-4 weeks after the request is fulfilled.
- Request closed: A service request is usually closed after the first touch point. The second touch point is a scheduled task and may update the original request with value adding information. Analysing historical service requests can lead to a lot of learning outcomes.

Key integration and partnership of service requests are:

- Service Catalogue and Service Portfolios

  Coordination and collaboration to determine the set of currently active service requests and how they will be offered to users and customers. Plan for future service offerings and the potential associated service requests.
- Service Level Management

  For each service request offering, a corresponding Service Level Agreement needs to be defined and agreed on (e.g., with Service Portfolio Manager, Service Catalogue Manager, etc.). This includes service request resolution times based on priorities, responsible employees, etc.
- Non-IT Business Owners

  Develop a partnership with business domains and business owners (outside of the IT department) to determine which service requests can be defined and offered beyond IT (e.g., procurement of equipment, HR payroll updates, Facility management services to fill up fridge with drinks, etc.).

Recommendations for successful service request management is as follows:

- It should be easy to view all services available to a user.
- The service request process should be defined in a flexible way since you may not know which service request may be required in future.
- Clearly define service requests that are preapproved and those that require approval processes.
- Leverage automation for the approval and fulfilment process. Speed is essential as slow service will impact negatively on customer satisfaction.

- Evaluate user feedback and use it to improve service request process.
- Service request records must be updated with current and accurate notes. Documentation is important to analysing service requests for optimization purposes.

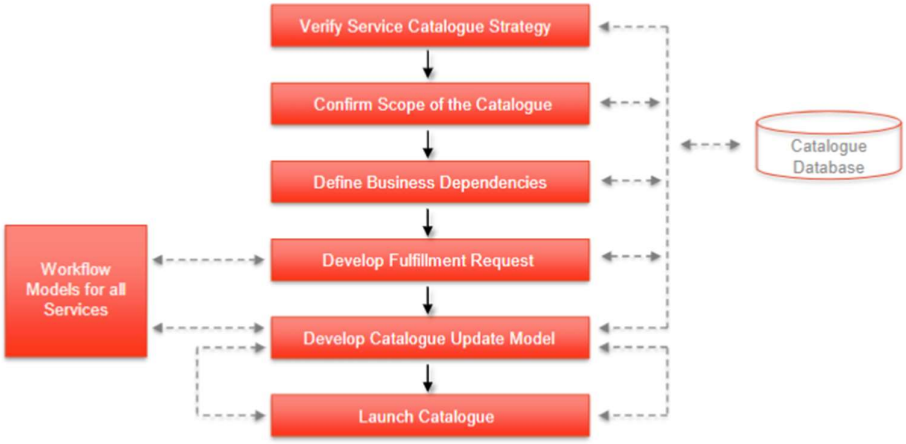
Service Catalogue

A service catalogue maintains information on all services that you currently offer to the customer. A service catalogue is produced and maintained, containing accurate information on all operational services and those being prepared to be run operations. It is a subset of the service portfolio and contains all the services from running, to inactive and future services which aren't available as well. A service catalogue is used to support the sale and delivery of IT services as it includes information about deliverables, prices, contact points, ordering and request processes.

Considerations and benefits of a service catalogue

- It provides a consistent and single view of all services currently offered.
- A correctly structured and presented service catalogue can provide a friendly and convenient way to request service across a diverse base of customers.
- It is a great opportunity to partner with non-IT departments to offer both IT and Non-IT related services making it more valuable to users and becoming a strategic asset for the organisation.
- An accurate service catalogue reduces time for users to search and order services which ultimately increases customer satisfaction.
- It can represent service dependencies and bring them to the attention of the user of other stakeholders.
- Current service catalogue solutions can provide an attractive, intuitive, convenient, and fast user experience.

The following is an overview of the service catalogue:



- Verify service catalogue strategy: before preparing a service catalogue for public launch, it would be evaluated considering which services shall be offered, have one consolidated offering or multiple service catalogues, define target users for offering, ensure all services within the catalogue are consistently defined, has a defined charge model for each service, has defined KPIs to measure performance, etc.
- Scope confirmation of the service catalogue: The service catalogue strategy will provide guidance on the service catalogue scope at the higher level. Details scope items are defined and negotiated during this phase. Close collaboration with service portfolio

manager is necessary and this phase provides and input into the required infrastructure provided to expose and offer services.

- Define business requirements: A successful operation of the service catalogue requires coordinated effort from a wide range of stakeholders. Any cross-departmental dependencies must be defined, and owners shall be identified to clarify and drive necessary actions. Actual business requirements of the tool could include search capabilities, personalization, convenient authentication, and much more.
- Define fulfilment process: Definition of details of the service fulfillment workflow/business process is necessary. Without solid service fulfilment definitions service catalogue will not go live. The offered services need to be aligned with available resources and the fulfillment process itself is usually triggered by a customer selecting a service and completing the corresponding request form.
- Develop catalogue update model: The service catalogue is a living entity changing overtime as services need to be updated. This tool needs to support the management and servicing operations accordingly. The longer a catalogue is live, the more difficult it can be to manage. Typical considerations for a service catalogue are to remember what the procedure is to add, remove, update, or how updates are being communicated to users, and how is the performance on updates being measured, etc.
- Service Catalogue Launch: Service catalogue can launch to live operations after scope, service fulfillment process, dependencies, and update model and process is defined. To mitigate the risks when launching the catalogue, try running a pilot program first, throttle request volumes via staggered go-lives, launch with a limited set of services initially then add to the list, validate the support model for the catalogue, be pro-active in getting feedback, etc.

Some key considerations and partnerships for service catalogue are:

- Service Level Management: Coordinate and define acceptable and expected service levels for a Service catalogue with involved stakeholders.
- Service Requests: Service Request Managers will be essential in providing the details for service offerings in the catalogue, their fulfilment, required workflows, etc.
- IT Leadership: the launch of a Service Catalogue usually has the attention of the CIO, CEO, and other senior executives in an organisation. Consequently, the Service Catalogue strategy should be discussed with these key stakeholders to ensure sponsorship.
- Non-IT Business Owners: Partner with business leaders in HR, facilities, marketing, sales, finance, etc. is key to offer also non-IT related services.

Recommendations for successful Service catalogues:

- User experience is key and hence the omnichannel approach.
- Consider business dependencies and try to offer a broad range of services conveniently.
- Don’t be too ambitious and start slow, whilst being simple and easy.
- Standardize integration patterns to partner services via industry standards for easier maintenance and service consumption.
- Utilize pilot periods with staggered go-lives to mitigate risks.
- Main objective of a service catalogue is to make services discoverable, available, and consumable to the end-users.

WEEK 4

Assigned Reading: Are you solving the right problems?

Most companies do not struggle with solving the problems but at figuring out the problems which exist. Most of the times, the managers tend to switch quickly to problem solving mode than try and understand the problem. Using the root cause analysis or 5 whys questioning technique makes one find themselves dig deeper into the problem than arriving at a diagnosis. Whenever faced with a problem, try to reframe the question. Identifying a different aspect of the problem can sometimes deliver radical improvements. Following are the 7 practices to reframing a problem:

- Establish legitimacy.
- Bring outsiders into the discussion.
- Get people's definitions in writing.
- Ask what's missing.
- Consider multiple categories.
- Analyse positive exceptions.
- Question the objective.

Assigned Reading: How to avoid rushing to solutions when problem solving.

Before solving a problem, one needs to know what exactly they are trying to solve. For doing this, there is a 4-step process to help get past the urge to rush to solutions. These are:

- Go and see: Understand the problem by doing close observations. Apart from the data, see the process, the world from where the data comes in.
- Frame your problem properly: It is difficult to get the right problem statement. A well framed one opens avenues of discussion and options.
- Think backwards: When facing a problem try mapping out how you got the problem in the first place. Try using a fishbone diagram, it might help.
- Ask why: Asking why repeatedly before settling on an answer is a powerful wat of avoiding jumping to conclusions or implementing weak solutions. Each question pushes you deeper and sometimes you might realise the answer is quite different from what you imagined it to be.

Assigned Reading: The knowledge creating company.

New knowledge always begins with the individual. Sometimes, one individual share tacit knowledge directly with another. An individual can also combine discrete pieces of explicit knowledge into a new whole. As new explicit knowledge is shared throughout an organization, other employees begin to internalize it—that is, they use it to broaden, extend, and reframe their own tacit knowledge. To convert tacit knowledge into explicit knowledge means finding a way to express the inexpressible.

Understanding knowledge creation as a process of making tacit knowledge explicit—a matter of metaphors, analogies, and models has direct implications for how a company designs its organization and defines managerial roles and responsibilities within it. This is the "how" of the knowledge-creating company, the structures and practices that translate a company's vision into innovative technologies and products.

Redundancy is important because it encourages frequent dialogue and communication. This helps create a "common cognitive ground" among employees and thus facilitates the transfer of tacit knowledge. Since members of the organization share overlapping information,

they can sense what others are struggling to articulate. Redundancy also spreads new explicit knowledge through the organization so it can be internalized by employees.

The main job of managers in the knowledge-creating company is to orient this chaos toward purposeful knowledge creation. Managers do this by providing employees with a conceptual framework that helps them make sense of their own experience. This takes place at the senior management level at the top of the company and at the middle management level on company teams.

Problem Management

Problem management manages the lifecycle of all problems from first identification through further investigation, documentation, and eventual removal. The main objectives of Problem management are to prevent problems and resulting incidents, eliminate recurring incidents, and minimize the impact of incidents. Problem management diagnoses the root cause of incidents and initiates actions to improve or correct the situation.

Problem management scope includes and differentiates between the following:

- Reactive Problem Management

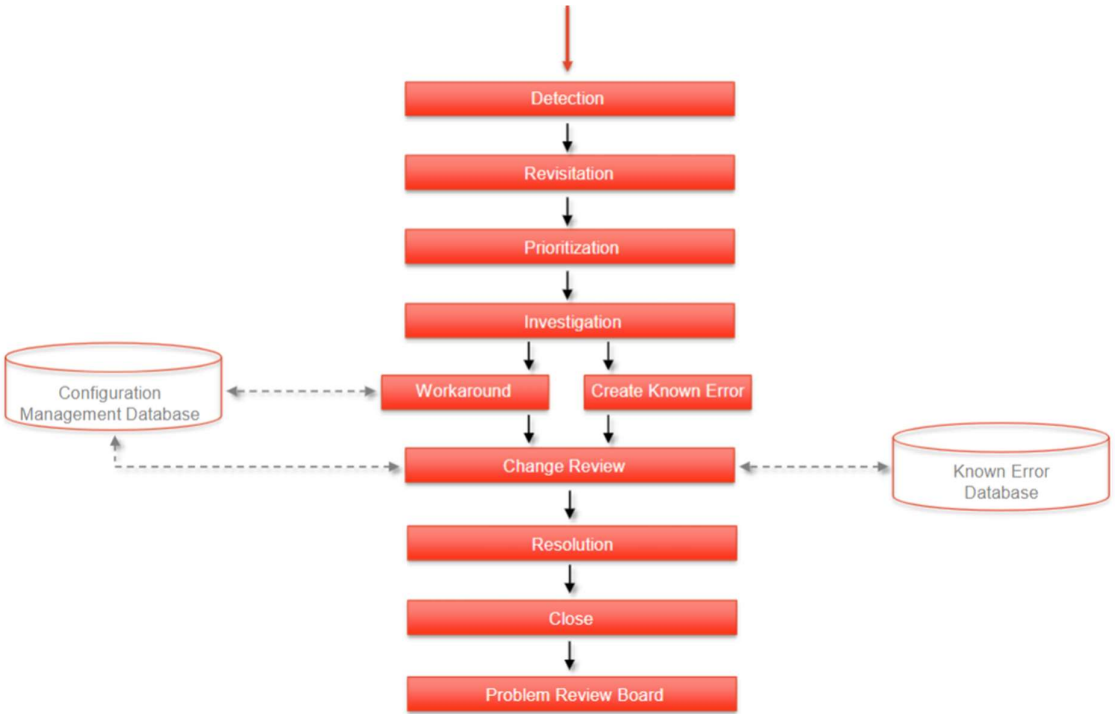
  It is as its name suggests, solving problems in response to incidents. It is executed as part of the Service Operation.
- Proactive Problem Management

  It is usually driven as part of Continual Service Improvement. Conducting reviews and analysing trends to prevent incidents. As its name suggests, it is done proactively so that incidents can be prevented.

High performing organizations have problem management as a priority and are staffed by experienced and knowledgeable people for the same. Problem management metrics are tracked and published, and the culture is focused about registering and resolving problems. Problem management increases service quality by reducing the time required to resolve incidents and by preventing future incidents through permanent solutions. This results in:

- Prevention of future incidents and problems.
- Elimination of recurring incidents.
- Reduced disruptions to business.
- Improvement in service reliability and quality.
- Accelerated resolution of incidents.
- Systematic reduction in the volume of incidents.
- Better understanding of risks related to service delivery.
- More effective workarounds for reducing incident impact.
- Creation of know error database and its utilization.
- Creation of culture of investigation and root cause analysis.

The problem management process is as follows:



- Detection

  Detection of a problem can come from several sources. Detection and identification of problems are becoming increasingly automated. Problem management needs to work together with incident management and service desk to evaluate and identify incidents, that can indicate a problem. A problem is the cause of one or more incidents and consequently an organization needs to investigate the incident and problem patterns, incident relationships, and user actions which may have caused the incidents to occur.
- Registration

  When a problem is identified, it is registered immediately. Delays should be avoided as it might lead to more incidents to occur. It is important to resolve problems quickly and quick registration is the first step to a quick problem resolution.
- Prioritization

  Not every problem must be prioritized as not all problems are equally important. A problem manager usually supports the problem prioritization. When prioritizing, multiple considerations need to be made such as:
  - Impact on the business organisation.
  - Cost to resolve the problem.
  - People required to resolve the problem.
  - Risk of additional incidents occurring.
  - Existence of any known solution.
  - Time required to execute on resolution.
- Investigation

  After the prioritization and categorization of the problem focus is shifted to investigation then finding a solution. Before starting an investigation, one should search for workarounds to buy time for your investigation. The workaround is documented and root cause analysis and investigation is required even when a workaround exists. If the root cause is identified, then a known error record is created with all the details of the problem. The known error record is then linked to the reported problem and if the

reported problem represents high risk in business, then escalation maybe required. There are multiple approaches to investigation such as:

- Kepner and Tregoe approach

  This approach asks 4 basic questions: What happened? Why did it happen? How should we act? And What the results will be? Through this approach potential future problems and side effects are anticipated and preventative actions are developed.
- Ishikawa diagram

  Ishikawa diagrams are also called as the fishbone diagram, the herringbone diagram, cause and effect diagram, or causal diagram that show the potential causes of a specific event.
- Chronological Analysis

  Chronological Analysis works by piecing together a timeline of activities working back from the point in time the problem being raised or otherwise bought to the attention of the relevant staff.
- Pain Value Analysis

  A formula is used to calculate pain value based on the number of users affected, the duration of the downtime, the impact on each user, and the cost to the business (if known). This method helps to identify when the problem started, etc.
- Brainstorming

  Brainstorming is a group creativity technique by which efforts are made to find a conclusion for a specific problem by gathering a list of ideas spontaneously contributed by its members.

- Change review

  The change review process ensures that changes to the IT environment are well-managed and controlled, reducing the likelihood of introducing new problems and improving overall IT service quality. It's an essential component of ITSM's problem management process, as it helps ensure that solutions to problems are implemented in a controlled and structured manner. The workaround and permanent solution for a problem can require the implementation of one or more changes and the problem manager must work closely with the incident and change management to plan for these changes. The early visibility of the change which can be implemented enables the speedy roll-out and implementation of the change to fix the problem. Any changes should be reviewed and approved by relevant stakeholders. Emergency changes due to high-risk issues may require very rapid deployment options into productions such as the Hot Fix System.
- Resolution

  One the root cause is identified and understood, an organisation can aim for a resolution. There are 2 options for resolving the root cause, a workaround, or a permanent solution. A preferred permanent solution may not always be feasible due to costs, technical feasibility, practicality, etc. The decision regarding the final resolution and how workarounds can be used in a final resolution is not simple and may require the judgement of the Problem Manager. The general attributes for resolution and workarounds are given below:

Resolution	Workarounds
Well understood, acceptable risk, affordable, completed within a reasonable amount of time, achievable	It is stable, low risk, low-cost option available with current IT Skills. It is a working solution for a reasonable amount

with available skills, and measurably of more value than the workaround.	of time and is understood and accepted by the customer or users.

- Close and Problem review board

  When a problem is considered resolved, a cross-function check should be performed to ensure that any changes related to the problem may have been implemented completely while ensuring that no other areas have been affected to avoid collateral damage. The Change ad release manager confirms successful implementation. Based on this, the related incidents and known errors must be closed while documentation of the root cause, key configuration and resolutions steps are made. This must also be reflected on the knowledge database. Problem review should be scheduled with the participation of the incident management team, change management team, service level team, and key business stakeholders. Problem review should focus on problem summary and date registered, final resolution and closing date, challenges encountered during resolution process, steps taken to mitigate associated risks, and the summary of follow-up actions.

A few key integrations and partnerships for problem management:

- Incident Management: Define relationships between the problem and incidents caused by it.
- Change Management: Coordinate the change request and implementation of the changes required to resolve the problem.
- Service Level Management: Investigate and assess the problem and root causes that result in the service failure and outages.
- Availability Management: Evaluate the problems impacting availability and joint planning to prevent availability issues in the future.

Recommendations for successful problem management:

- Be clear in defining the relationship between incidents and problems.
- Assign an owner to every problem and empower this role to work cross-functionally across the organisation.
- Measure and publish both incident and problem volume and resolution time metrics across the organisation to create an understanding.
- Have a plan to implement proactive problem management as a strategic investment to improve service quality and service resilience.
- Create a problem escalation model to reduce time necessary to resolve high impact problems and therefore mitigate risks.

A few common challenges faced during problem management are:

- Confusing the meaning between incidents and problems. Problems are those that occur again and again. Incidents are those which are unique and occur only once.
- Workarounds may not prevent future incidents; hence all problems must be resolved.
- During problem management, one cannot predict the resources, effort, and priority it would take to support the problem management.
- There is usually a lack of structured approach towards problems.
- There is usually insufficient information to manage and solve problems.

Knowledge Management

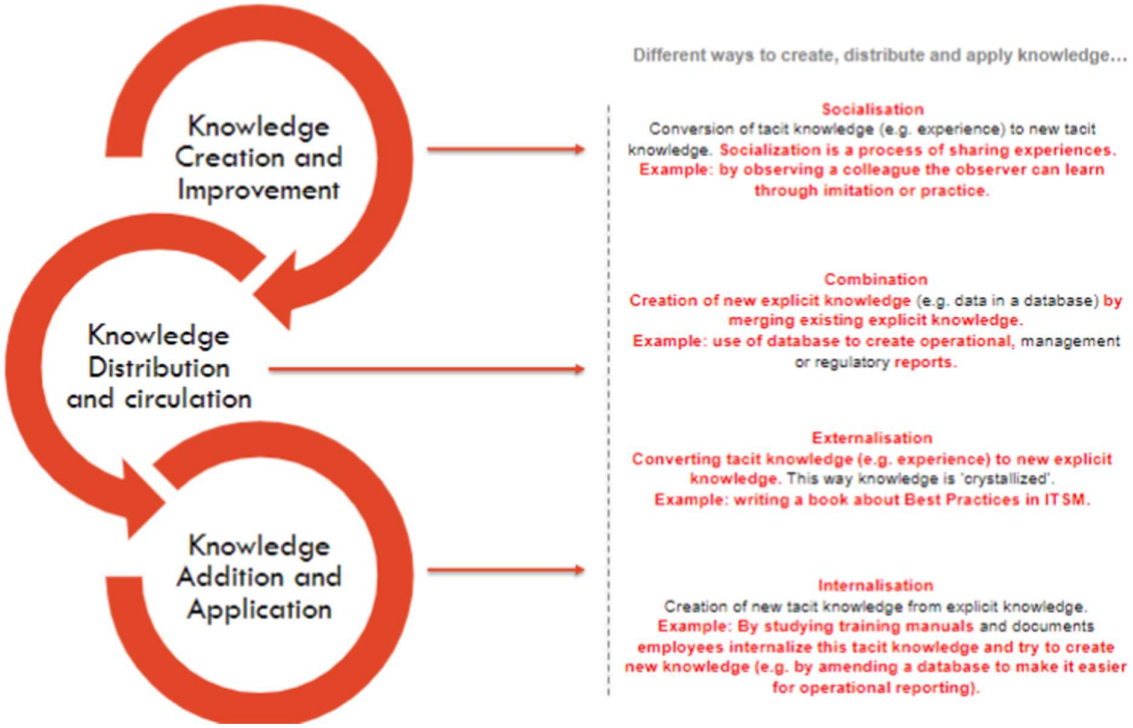
Knowledge management (KM) is a process or discipline that focuses on capturing, organizing, storing, retrieving, and sharing an organization's collective knowledge to improve

decision-making, problem-solving, and overall productivity. This is usually done to increase the quality and effectiveness of the Service Desk and all service and support channels. It involves the systematic management of both explicit knowledge (tangible and documented information) and tacit knowledge (personal insights, experiences, and expertise) within an organization. Effective knowledge management can help organizations leverage their intellectual assets, promote innovation, and enhance their competitive advantage.

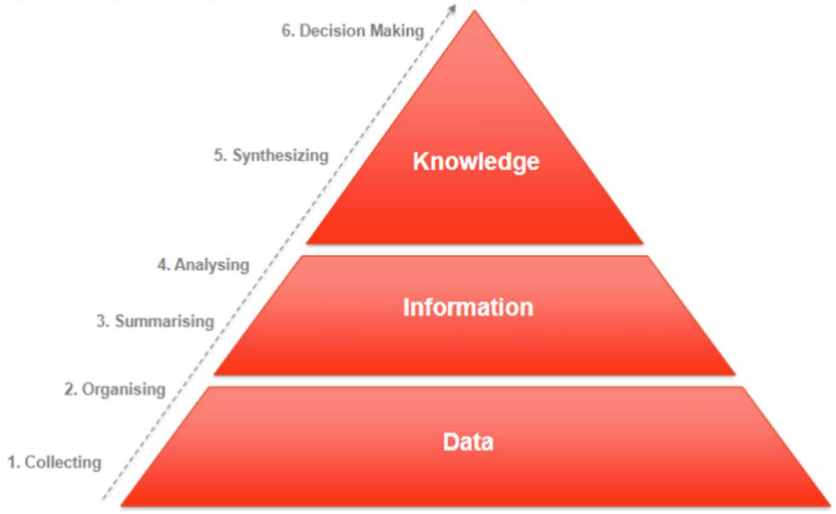
Knowledge management is part of the 12 core elements and should be part of every service management process. A few of its benefits are given below:

- More effective training of staff.
- Incident and problem information can add fundamental value to the organisation.
- Enables true- and real-life knowledge transfer process.
- Accelerates the onboarding of new staff.
- Drives improved decision making,
- Supports a higher quality of service experience.
- Empowers the service desk team with the right information at the right time.
- Reduces the time required to close an incident or a service request.

Knowledge Management is a continuous process. It starts with Knowledge Creation and improvement, followed by knowledge distribution and circulation, and finally completes the circle with knowledge addition and application.



The knowledge management process has a total of 6 steps. These are as follows:



- Collecting

  This is the most important step of knowledge management process. If irrelevant or incorrect data is collected, the resultant knowledge would not be the most accurate. Data collection process itself needs to be documented and the collection procedure defines data collection points. The data collection points maybe the summary of certain routine reports. Data extraction techniques and tools are also defined using the data collection points along with the data storage. For example, monthly sales report and daily attendance report can be resources for data collection while sales numbers entered manually into a system is also a process that needs to be defined.
- Organising

  Following the data collection step, the collected data needs to be organised. Data organisation and categorization rules are defined by an organisation based on its data strategy and its intended use and need of the data. For example, all the sales related data can be categorized together as sales data. If there is a lot of data in the data storage, then data duplication, cleaning, and compression are also to be consider. At the end of this point of the process, the data becomes information.
- Summarising

  The information gained from collection and cleaning is then summarized to make sense out of it. Information is presented in tabular or graphical format and stored appropriately. There are many tools available for this step of the process.
- Analysing

  The summarized information is then analysed to find relationships, redundancies, and patterns. An expert or an expert team is usually assigned to this part of the process as their experience plays a vital role in this step. Usually, reports are generated to report the findings, and these are the knowledge which is created.
- Synthesizing

  The results of analysis are combined to derive insights and knowledge. The organisation will have a set of knowledge elements that can be used across the organisation. This knowledge is then stored in the organisational knowledge base for further use. Usually, the knowledge base is a software implementation that can be access from anywhere through the internet.
- Decision Making

  At this stage the knowledge is used for decision making.

A few key considerations during the knowledge management process are:

- What information is available?
- Where does the information reside?
- Who needs the information and knowledge?
- How is the information used?
- How do we get the information and knowledge to the people that need it in the best possible way?
- Who are the knowledge experts?

A few key integrations and partnerships are:

- Incident Management

  Coordination on the offering of knowledge base access during the incident processing phase is necessary. This makes sure that the knowledge is received by those who need it at the right time.
- Service Request

  Determine and design the knowledge model and how it can complement the service request process. Sometimes leveraging the knowledge in service in automated ways may even lead the service request to be self-served.
- Service Catalogue

  Design the right access model with the service catalogue managers for both the internal and external users' access to knowledge. If done right, this will reflect in the continuous recognition of the service catalogue by the users.
- IT Management

  The quality of the knowledge base will be driven by consistent and ongoing access to experts and should be sponsored by the IT leadership team. Having support from the IT Management team can ensure the creating of knowledge base from different experts.

Certain recommendations for successful knowledge management:

- Take time to create a knowledge management strategy and assign an individual or team to advocate the strategy.
- Constantly reinforce that knowledge management is not about a database and collecting information but about learning and making better decisions.
- Identify, recognize, and reward knowledge experts.
- Set up a secure and scalable knowledge base. Set goals and incentives to drive growth of the knowledge base.
- Build a knowledge transfer plan and communicate it broadly. Leverage a mix of learning techniques the showcase the knowledge experts and nurture those learnings.

Service Level Management

Service Level Management (SLM) is a key process within IT Service Management (ITSM) that focuses on defining, negotiating, monitoring, and managing the levels of service that an IT service provider delivers to its customers. The primary goal of SLM is to ensure that IT services meet the agreed-upon service levels and performance expectations, as outlined in Service Level Agreements (SLAs) and other related agreements. The objectives of Service Level Management are:

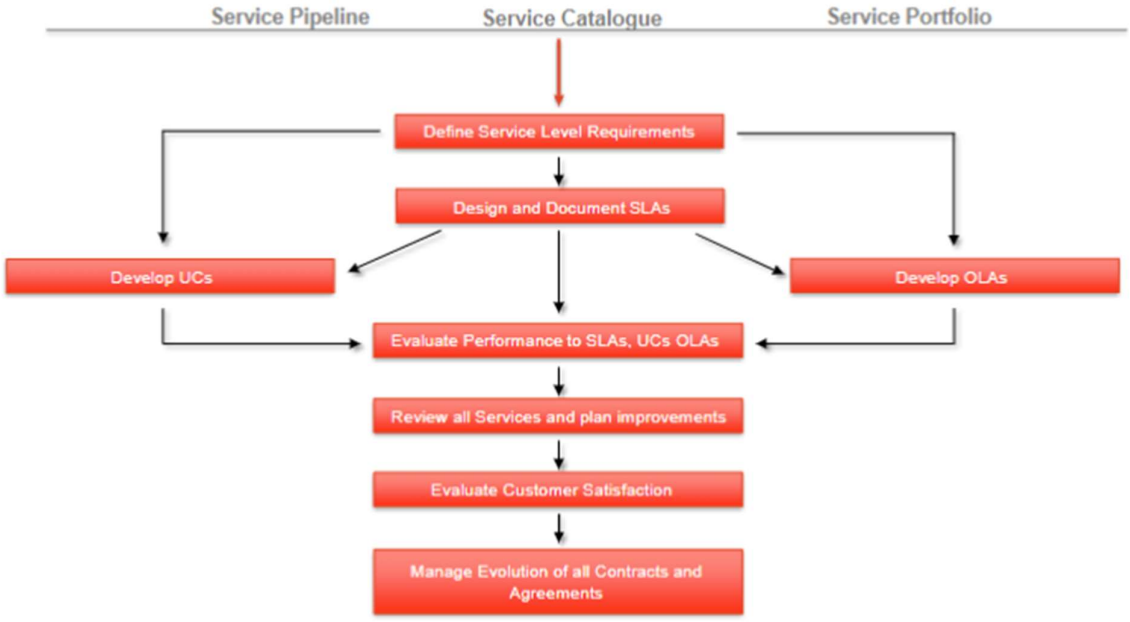
- Define, document, agree, monitor, measure, report, and review the level of IT services provided and evaluate corrective measures whenever appropriate.

- Provide and improve the relationship and communication between the customer and business in conjunction with the Business Relationship Management.
- Ensure that specific and measurable targets are developed for all IT services.
- Monitor and improve customer satisfaction with the quality of service delivered.
- Ensure all parties understand the level of service to be delivered.
- Ensure that appropriate measures to improve service quality are implemented.

Service Level Management is one of the 12 core elements of ITSM and have several benefits as given below:

- Service Level management leads the process to define the Service Level Requirement and ultimately negotiates the Service Level Agreements for all services in a structured manner.
- Expands the scope of managing to service targets to include Operational Level Agreements and underpinning contracts for all third-party suppliers.
- Works to understand service failures and develop action plans to prevent failures.
- Supports the business to understand and communicate end-to-end service performance.
- Evaluate the quality of all services relative to the Service Level Agreements and work to resolve any disagreements between involved stakeholders.

The Service Level Management Process is as follows:



- Define Service Level Requirements

  Service level management is only possible with a deep understanding of the underlying services. The requirements come from the users, and it is important to define the primary, secondary, and special use cases for services to define corresponding service level requirements. Usually creating a storyboard for each service may help define use cases. A story board uses simple diagrams, flowcharts, etc. in combination with text to explain the artifacts and related processes. A good starting point in defining Service Level Requirements is through evaluating business needs of a service and who needs to be satisfied in which way.
- Design and Document SLAs

This process starts with a discussion and negotiation around the level of service required by the customer, level of service IT can deliver, performance of each element to be measured and the metrics for each and finally the cost associated to delivering the desired level of service. The documented SLAs need to be accepted by all relevant stakeholders. The design and documentation of SLAs stage represents key aspects of how the service will run every day. Third party agreements are represented and documented in underpinning contracts and agreements between departments within the same organisation are represented and documented in Operational Level Agreements.

- Evaluate performance to SLAs

  An organisation cannot manage what they cannot measure. When a specific performance is measured, it is likely to improve and if a result is rewarded, then it is likely to repeat. All service aspects defined in the SLAs need to be measurable and the SLAs performance evaluation should be objective and not subjective. Service credits are a mechanism by which amounts are deducted from the amount to be paid under the contract to a supplier if the actual supplier fails to meet the performance standards set in the SLA. Service credits might need to be paid if the service or set of services does not meet the SLAs. In severe SLAs breaches, a cash penalty might be due to be paid.

- Review all services and plan improvements

  Continuous service improvement should be ingrained into the culture of an organisation. Service improvement can be either reactive (service is improved after problems occur) or proactive (service is improved based on knowledge and experience to avoid problems from occurring). Failures are great opportunities to improve but prevention is key. A service review should be scheduled periodically considering the following aspects:

  - Review and compare the service performance.
  - Evaluate and discuss any SLA breaches.
  - Overview of any planned service improvements.
  - Evaluation of customer feedback to experience with service.
  - Assignment of responsibilities to action items.

- Evaluate customer satisfaction

  If the customer is not satisfied with the provided service then it is likely to cost time and resources to satisfy them. Dissatisfaction of customer might lead to reputational damage and is difficult to reverse. Evaluate service metrics, communicate service levels to the customer and gather feedback frequently.

- Manage evolution of all contracts

  Business models and service offerings may change over time and it is necessary to keep up with this change. Customer expectations may also evolve during the process and needs to be accommodated for. Any service change must make sure that the investment to change should have a reasonable lifecycle of usefulness, improve value of the service, and a change in a service may require and update in its metric. Any changes to the SLAs must be drafter first and any changes to the SLAs (Service Level Agreements), UCs (Underlying Contracts), or OLAs (Operation Level Agreements) should be owned by a dedicated SLA management.

A few key integrations and partnerships involved with Service Level Management are:

- Incident and Problem management – Any and all service failures will be passing through the incident and problem management and hence SLA management need to work closely with the incident and problem management.

- Service catalogue – Coordination of the SLAs and changes to SLAs for current services active within he Service catalogue is necessary. Especially when SLAs strive for continuous evolution.
- Change management – All changes need to be ensured to be aligned with the expected SLAs.

A few recommendations for successful service level management are:

- Recognise Service Level Management as a key link between customer expectations and customer satisfaction throughout the Service Lifecyle.
- Service Level Managers are customer facing and should be in close contact with SMEs providing the service to customers.
- A service level manager should be in close contact with the service consuming customer.
- The scope of SLAs should be managed carefully. Too many metrics need to be avoided as the performance of a service need to be measurable in a clean and clear format.
- All service level requirements need to be clearly defined as poorly defined service level requirements may lead to confusion and contradicting reporting when services are live.

WEEK 5

Assigned Reading: 7 ways to improve your software release management.

To come to fruition, software projects take investment, support, nurturing and a lot of hard work and dedication. Good release management practices ensure that when your software is built, it will be successfully deployed to the people who want to use it. The seven ways to improve software release management is given below:

- Understand the current state of release management.

  You can't begin to fix something without understanding what it is, and how and where it is broken. Our first step in improving our client's release management system was to form a detailed picture of the current release process.
- Establish a regular release cycle.

  If the engineering team is the heart of the project, the release cycle is its heartbeat. Establishing a release cycle is vital because it creates an opportunity to meaningfully discuss non-functional testing that the software may need, announces a timetable for the stakeholders, create a routine which all teams can align with, and give customers confidence that they can order something and have it delivered.
- Get lightweight processes in place. Test them early and review them regularly.

  If there is one single guiding principle in engineering (or reengineering) a process, it is to do a little bit, review your results and then do some more. Repeat this cyclic approach until you get the results you want. Lightweight processes are those that do not require lengthy bureaucratic approvals or endless meetings to get agreement. They usually require only the minimum acceptable level of inputs and outputs.
- Establish a release infrastructure early.

  Your release infrastructure is anything that needs to be in place to deploy the software and to enable users to use it. Your obligation to the customer is not just that you build great software; it is that it's available for them to access and use. Crucial to getting a good release process is figuring out what you need to have in place to make it available to the customer—before the engineering team is done building the software. The release infrastructure covers the hardware, storage, network connections, bandwidth, software licenses, user profiles and access permissions. Human services and skills are part of the release infrastructure, too.

- Automate and standardize as much as you can.

  Automation enables you to do repetitive tasks without tying up valuable human resources. Standardizing ensures that your automation's inputs and outputs are consistent every time.
- Establish positive expectations.

  If getting software released is important to you, don't keep it a secret. Our teams improved their commitment to deliver the software release when they knew it was important.
- Invest in people.

  No matter how much you spend on hardware, software and fancy processes, without the commitment of team members you will not enjoy sustainable success in releasing your software.

Release management is an important part of any software project and is not often given the attention it deserves. Good release management takes hard work, resolve and great communication; however, the greatest skill is the ability to review, learn and adapt improvements.

Assigned Reading: Software asset management, a new defence against cybersecurity threats.

To combat cybersecurity threats, companies are spending millions of dollars in malware protection, firewall solutions, and security consulting. Yet even with these expensive measures, most are unaware of their greatest vulnerabilities. That's because cyber criminals are opportunists who seek the path of least resistance. Rather than wasting efforts attacking hardened firewalls, they instead snoop out the often-overlooked back doors to a company's network, such as unsupported or unapproved software, abandoned user IDs, poor password protection, or the unmanaged server under an IT analyst's desk.

Comprehensive asset management is essential to an effective IT infrastructure, service, and cybersecurity management program. SAM is a set of proven processes that delivers a comprehensive view of an organization's hardware and software inventory, usage, and risks, ultimately enabling organizations to regulate costs and resources, manage business and legal risks, and align IT investments with business needs. Effective SAM provides critical insights into the number of devices and applications deployed, along with their location and warranty status, which can significantly reduce unnecessary product costs. As a budgetary tool, SAM identifies discrepancies between software licenses owned and deployed and ensures companies are investing wisely and not paying for licenses they aren't using. From a security standpoint, SAM helps organizations identify and counter potential threats by ensuring that end-of-life products get decommissioned, and that product updates and security patches are applied in a timely way.

A SAM for cybersecurity assessment provides a comprehensive IT infrastructure analysis that covers current software/hardware deployment and usage, operational processes, and software versions to quickly determine if the right processes are in place to minimize cyber risks. In addition, it provides prescriptive cybersecurity guidance and best practices as companies move ahead. A few benefits of SAM for cybersecurity assessment includes:

- Identification of areas of potential risk, fraud, and system vulnerabilities.
- Cost savings in combatting cyberattacks and increasing efficiencies.
- More secure management of software assets and reliable cybersecurity practices.

- A roadmap for building a more resilient IT infrastructure that removes known vulnerabilities.
- More effective defence against attacks by leveraging the best industry practices and technologies available.

SAM enables organizations to set up domains by location, division, or other categories. The ability to match machines and users to specific locations helps to pinpoint security risks and ensures that inventory subsets have not been missed.

Assigned Reading: The hard side of change management.

Managing change is tough, but part of the problem is that there is little agreement on what factors most influence transformation initiatives. the different ways in which organizations combine the four factors create a continuum—from projects that are set up to succeed to those that are set up to fail. At one extreme, a short project led by a skilled, motivated, and cohesive team, championed by top management, and implemented in a department that is receptive to the change and must put in very little additional effort, is bound to succeed. At the other extreme, a long, drawn-out project executed by an inexpert, unenthusiastic, and disjointed team, without any top-level sponsors and targeted at a function that dislikes the change and must do a lot of extra work, will fail.

There are 4 factors that can be used to predict the outcomes of a project:

- Duration

  Companies make the mistake of worrying mostly about the time it will take to implement change programs. They assume that the longer an initiative carries on, the more likely it is to fail. However, contrary to popular perception, our studies show that a long project that is reviewed frequently is more likely to succeed than a short project that isn't reviewed frequently. Thus, the time between reviews is more critical for success than a project's life span.
- Integrity

  By performance integrity, we mean the extent to which companies can rely on teams of managers, supervisors, and staff to execute change projects successfully. In a perfect world, every team would be flawless, but no business has enough great people to ensure that. Since project teams handle a wide range of activities, resources, pressures, external stimuli, and unforeseen obstacles, they must be cohesive and well led. Smart executive sponsors, we find, are very inclusive when picking teams. They identify talent by soliciting names from key colleagues, including human resource managers; by circulating criteria they have drawn up; and by looking for top performers in all functions. While they accept volunteers, they take care not to choose only supporters of the change initiative. Senior executives personally interview people so that they can construct the right portfolio of skills, knowledge, and social networks.
- Commitment

  Companies must boost the commitment of two different groups of people if they want change projects to take root: They must get visible backing from the most influential executives (what we call C1), who are not necessarily those with the top titles. And they must consider the enthusiasm—or often, lack thereof—of the people who must deal with the new systems, processes, or ways of working (C2). Companies often underestimate the role that managers and staff play in transformation efforts. By communicating with them too late or inconsistently, senior executives end up alienating the people who are most affected by the changes. Organizations also underestimate their

ability to build staff support. A simple effort to reach out to employees can turn them into champions of new ideas.

- Effort

  When companies launch transformation efforts, they frequently don't realize, or know how to deal with the fact, that employees are already busy with their day-to-day responsibilities. Project teams must calculate how much work employees will have to do beyond their existing responsibilities to change over to new processes. Handing off routine work or delaying projects is costly and time-consuming, so companies need to think through such issues before kicking off transformation efforts.

As we came to understand the four factors better, we created a framework that would help executives evaluate their transformation initiatives and shine a spotlight on interventions that would improve their chances of success. We developed a scoring system based on the variables that affect each factor. Executives can assign scores to the DICE factors and combine them to arrive at a project score. The simplicity of the DICE framework often proves to be its biggest problem; executives seem to desire more complex answers. By overlooking the obvious, however, they often end up making compromises that don't work. Smart companies try to ensure that they don't fall into that trap by using the DICE framework in one of three ways:

- Track projects
- Manage portfolios of projects
- Force conversation

Asset and Configuration Management

IT Asset Management is a set of business practices that support life cycle management and strategic decision making for the IT environment. IT assets include all the software and hardware contained in the organisation's IT environment. Configuration management on the other hand is the process of managing computer systems, servers, and software in a desired consistent state. The following are the main objectives of Asset and Configuration Management:

- Controlling and optimizing the spending for IT assets.
- Support IT lifecycle management.
- Support strategic decision making for the IT environment.
- Responsible for inventory management of IT assets.
- Support contract management for IT assets within an organisation.
- Keep IT assets in a consistent and maintained state from a configuration perspective.

There are 3 main types of tasks associated to asset and configuration management. These are:

- Financial Tasks
  - Procurement of new assets.
  - Budget management.
  - Cost control.
  - Cost allocation.
  - Operational efficiencies.
- Physical Tasks
  - Inventory management.
  - IT equipment deployment.
  - Version tracking.

    - License tracking.
    - Usage monitoring.
    - IT equipment retirement/refreshment.
    - IT equipment provisioning.
- Contractual Tasks
    - License compliance.
    - Request for information/proposal.
    - Negotiation.
    - Contract maintenance.
    - Supplier management.
    - Service level management.

There are long term advantages to IT asset and configuration management, these are:

- Overall cost reduction.
- Improved software compliance.
- Empowered IT security.
- Better customer service.
- Increased control over IT assets.
- Improved communications and understanding between IT and other departments.
- Reduced governance risks from legislated requirements.
- Increased support for security and disaster recovery preparedness.
- Improved budgeting and other strategic decision-making processes.

Asset and configuration strategy needs to be aligned with an organisation's services strategy. Without the proper alignment, one would not be clear about which asset components are required and which one are optional, unclear categorization and prioritization of assets would take place, which assets are required for which services will be unclear and how these assets should be set up and configured would also be unclear. The asset and configuration management should consider reliability, resilience, performance, availability, and the lifecycle of the asset.

Asset inventory is the complete list of all currently deployed assets in an organisation. Organisations often do not know how many assets exist within the organisation and hence inventory management and the automation of corresponding inventory management processes is the key. Building up a profile including the asset attributes is helpful. This inventory information is usually stored in the Configuration Management Database. Governance processes to keep the inventory updated is key otherwise it may grow outdated very quickly.

A configuration management plan should be created to plan the configuration and maintenance of IT assets. A configuration management plan should include key requirements for current capabilities of assets, corporate policies, roles and responsibilities for assets and their configuration, tools and systems for asset and configuration management, implementation plan of assets and configuration items, key integration touchpoints, communication plan, etc. The configuration plan should be review with key stakeholders such as the IT Management team, service owners, change and release management team, and service catalogue and service portfolio managers.

Configuration identification provides details around configuration requirement for IT assets. Each configuration item should have configuration requirements attached to it. The

identification of required configuration requirements supports to plan for scheduled maintenance processes. Furthermore, dependencies between configuration items need to be considered. Understanding dependencies between configuration items also supports change management, release management, and problem management while also creating knowledge.

Configuration control establishes a process to control and govern configuration activities for configuration items. These activities include adding, modifying, or removing a configuration item. Changing the configuration of an IT asset or service can have profound contributions and impact on the business operations. Any change of configuration times needs to be aligned with change and release management. Any change of IT assets may have a significant impact on several configuration items.

A key goal of asset and configuration management is to maximise the value for IT assets in an organisation. Having status reports of all current active and inactive IT assets and their performance helps management to understand the status quo, identify areas of improvements, predict, and prepare for future spending, understand their current spending, understand and trigger strategic initiatives, and much more!

Auditing is a vital part of asset and configuration management to ensure compliance with organizational and regulatory requirements. Audits ensure that the IT inventory is updated and risks are clearly identified, classified, and mitigations strategies are in place. It also ensures that change, release, and configuration management practices and processes are established, updated, and documented accordingly. Audits can be internal or external and most corporations have a combination of both. Audit findings are assigned to the responsible stakeholder who in turn needs to evaluate and initiate potential actions. A few best practices to have a successful audit is:

- Documentation of the past, present, and planned IT assets, configuration changes and processes are key.
- Prepare reports for major production roll outs of new software and hardware.
- Document all enterprise threat detections including associated risks. This can be automated.
- Prepare reports on change success rates and failure rates.
- Prepare reports on planned new services and the process on how the organisation is planning to roll out these new changes.

From a managing perspective, IT asset and configuration management is responsible for the following:

- Efficiency

  By not having to pay for assets that are not in productive use, not assigning excessive number of resources for managing IT assets, automating processes such as data transfers, and having access to accurate information of the assets available, the organisation can increase its efficiency.
- Risk

  An organisation will be better prepared with licenses and would not have to pay unexpected license fees, and deal with possible sanctions for illegal software usage. Furthermore, the organisation will not have to invest a lot in software compliance audits and through having a proper IT asset security, will not be concerned about sensitive data being leaked.

- Cost

  Having a proper IT asset and configuration management will make sure that the organisation does not have to pay for IT assets they don't need, overspend for compliance purposes, and will be able to compare their total cost of ownership with industry standards.
- Control

  Having a proper IT asset management system will ensure that development will be proactive than reactive. Furthermore, organisation will not have to spend extra resources to ensure compliance and will have precise and effective IT asset costs and investment.
- Accountability

  The organisation will have an accurate overview of the current state of the IT assets and configuration and will be able to justify its expenses in IT assets efficiently to support business strategies.

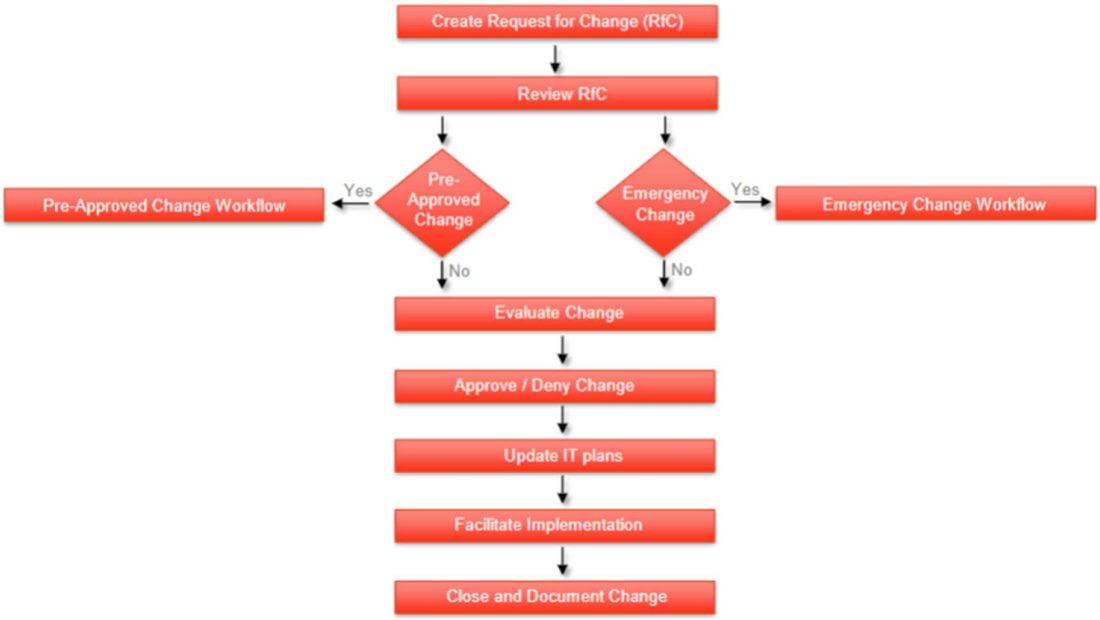
A few key integrations and partnerships are with the Incident and problem management, availability management, change management, and service catalogue and service portfolio. A few recommendations for successful asset and configuration management are:

- Take steps to ensure a strategy is in place that provides guidance on the connection and link between services, IT assets, and infrastructure.
- Build an accurate inventory of IT assets augmented by detailed IT asset information.
- Capture and understand the relationship between IT services, IT assets, and configuration items.
- Make a configuration management plan a mandatory item in the ITSM organization.
- Clearly define the owners and responsibilities for IT assets and related configurations.
- Ensure alignment between IT asset management, configuration management, change management, and release management.
- Ensure that asset and configuration plans are key to audit and governance processes.

Change Management

Change Management is a set of structured operating rules and processes that ensures all changes to a service or infrastructure are performed in a consistent manner that minimizes risks and maximises value to the business. The main purpose of change management is to control the lifecycle of all changes enabling increase in value with minimum disruption to IT services.

Change management reduces unplanned outages, enables faster recovery from service interruptions, accelerates rollout of new service offerings, enables fewer emergency changes, creates accountability for unauthorized changes, establishes a change calendar for the business, reduces the number of failed changes, enables smoother business operations, and increases employee satisfaction. The following is the change management process:



The steps are as follows:

- Create request for change.

  A change request is raised by an individual or group and needs to contain necessary information for the initial review to be completed. Request templates and required information may vary depending on the organisation. Request form should be as simple as possible and potential resources to be involved and required, should be provided to ensure accountability.

- Review Request for Change.

  Change management process should be agile and flexible to make consistently good decisions quickly and consistently. Request for change review process should be an initial quick review of the change and the RFC initiator should be notified of the review results. RFC can be qualified as pre-approved change, normal change, and emergency change.

  - Pre-approved change

    This workflow frees up time for changes that require a more detailed evaluation. Preapproved changes are usually low risk, low cost, and can be implemented with minimum resources. It is ideal for high volume change items. Some preapproved changes may still need a quick review from the manager. It is important to enforce the governance and discipline of documenting and closing preapproved changes once it is finalised.

  - Emergency change

    An emergency change is created when a risk or failure needs to be addressed quickly. It is based on the current and eminent condition that has significant impact on the business. Processes must be designed to enable the implementation of change quickly and the approval of emergency changes usually requires approval from IT leadership. Changes move immediately into implementation once the approval si received and risk evaluation is performed. An emergency change still needs to be documented and closed.

- Evaluate Change

  Normal changes need to be processed to the change evaluation state. This step includes a detailed analysis of the change. A formal risk assessment should be part of

this evaluation and every change should have a risk profile attached to it. Change evaluation criteria will focus on multiple things such as the value of the change, cost of implementation, key resources, required, etc. An objective evaluation of these criterion is important, and a potential fall-back option evaluation may be required depending on the type of change.

- Approve/Deny Change

  Risk evaluation and change evaluation criteria of previous steps are an important entry criterion for this stage. Depending on the change impact, a deeper understanding of the change is required. The change approval is usually operated by a change approval board consisting of the IT and Business experts and leaders. The change assessment process should include the priority level of the change which is used to manage and schedule the next steps in the process.

- Update IT plans

  A request for change can either be returned to the initiator for revision and resubmission, approved, or declined. In case of approval, the change needs to be incorporated into the IT plan to ensure integrity of the IT system landscape and IT infrastructure. Details of the change schedule are managed in this step. A master change calendar is a key asset! Only emergency changes can go to production outside of planned change windows.

- Facilitate implementation.

  Communication to other stakeholder is keto t ensure successful implementation of the change. Resources need to be briefed about the change requirements. Pivotal elements of a change implementation are testing plan, communication plan, remediation plan, and post implementation review. Post implementation reviews are important to evaluate to identify any variances from the expected results, time and resources necessary to implement change, any problems encountered, or any updates to test plan.

- Close and Document.

  Each change should have a defined period in test/production to see whether the change is performing as expected. Time and resources required for approving and implementing change, benefits and value received from the change, and key stakeholders and approval workflow should all be documented. In case the change is not performing as anticipated, it may be removed from test/production again. A back-out plan should follow similar steps as change request. In case of back-out any remediation activity needs to be evaluated.

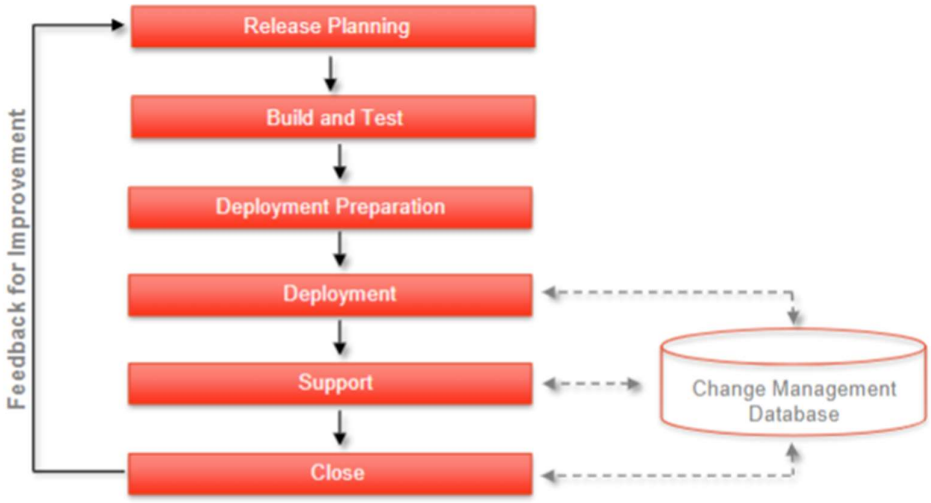
A few key integrations and partnerships involved with change management is problem management, configuration management, release management, and incident management. The following are recommendations for successful change management:

- Change management will have far reaching implications and can only be called a success when it is properly aligned with the business.
- Understand that change management is an evolutionary process and success will take time and will reshape people, processes, and technology.
- Build a strong and influential change approval board.
- Establish a goal for eliminating all unauthorized changes.
- Every change should include a back-out plan.
- Track the change success rate and review it periodically.
- Create a document that clearly outlines and describes the organisation's change management process.

Release Management

Release Management is a process that includes the management, planning, scheduling, and controlling of an IT change through every stage and environment involved, including testing, and deploying software releases. Release Management is usually only triggered by the Change Management Process. The main purpose of release management is to ensure the integrity of the live environment is protected and that correct components are released. There are several benefits of release management:

- Reduced risk of service interruptions.
- Faster execution of changes.
- Improved communication and fewer surprises.
- Reduced cost for change execution.
- Improved support for audit and compliance.
- More consistent operational performance.
- Ensure that release plans are in place.
- Supports the design of release packages.
- Drives continuous improvements to the change success rate.
- Enhances knowledge transfer to operational teams and business owners.
- A more consistent and ultimately proven implementation approach.



The following are the steps for a release management process:

- Release planning

  This is the planning stage wherein the scope of release, definition of a successful release, selection of release model, assignment of release owner, and evaluation of risks associated with the release are planned. A preliminary definition of a test plan is also required alongside a work plan for release logistics. Depending on the impact on IT assets, a validation of financial and contract models for certain releases are also required. Creation of a training plan also takes place in this step.

- Build and test

  This step captures the detailed execution of the build and test of the release. Build activities include assembling individual components and identifying the risks. Deployment and release of the changes can be piloted via quality test environment, performance environment, and preproduction environment. Deployment pilots may require additional attention if the interoperability for the release components are at significant risk.

- Deployment preparation

  A more detailed plan and documentation for deployment release is prepared in this step which also involves a final readiness check, comprehensive and updated assessment of risks, risk mitigation plan, and different checks. There are different types of deployments such as the upgrade or modification of an existing service, release of a new service, retirement of a service, merger of different services, or even transferring of service ownership.
- Deployment

  In this stage the deployment is conducted, and the deployment of release is actively monitored for any issues or warning signs. Key activities during this stage include delivery of communication, documentation, service, and decommissioning of the redundant service, assets, along with a finalization of training plan and survey to gather feedback.
- Support

  The SLAs associated with the new service is finalized. The communications and training are complete, and any initial issues are reported, logged, and resolved. Performance metrics also has been achieved.
- Close

  Document recommended improvements for the next deployment and conduct a review with the release team and business stakeholders. Conduct and audit to verify the completion of all activities and that all records and documents are up to date. Review SLAs and metrics and initiate update process if required.

A few key integrations and partnership for release management is change management, problem management, service level management, and asset and configuration management. A few recommendations for successful release management are as follows:

- Build a test plan and a pilot phase that closely mirrors an organisation's production environment.
- Assign clear owners to risks associated with the release and enforce a mitigation plan for each risk.
- Watch out for early warning signs during the deployment phase.
- Ensure that the SLA for the new service is updated and well understood.
- Take time to complete a release scorecard and recommendations for future improvements.

WEEK 6

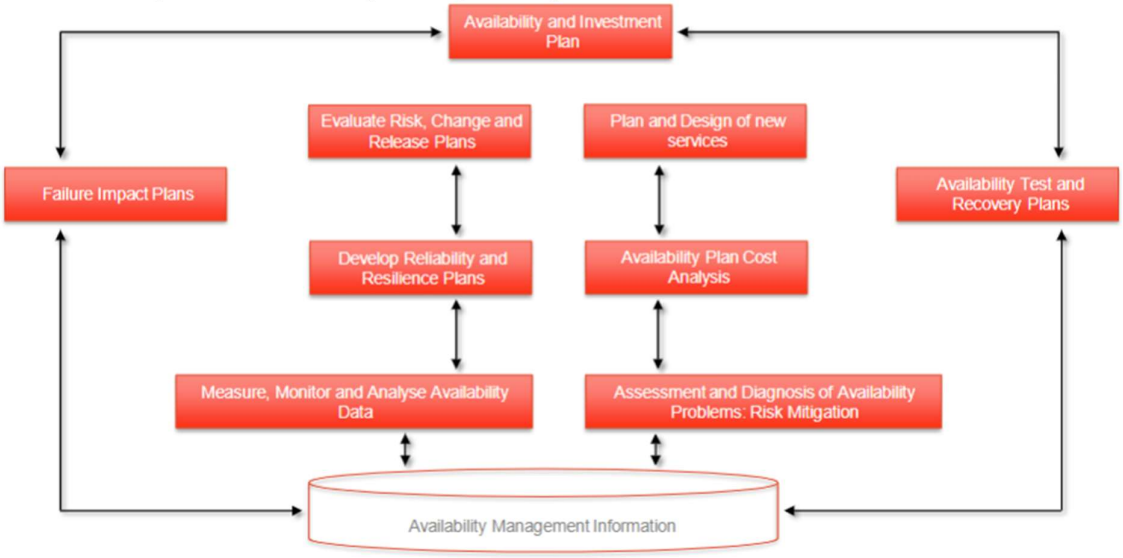
Availability Management

Availability Management will lead the planning, design, implementation, and oversight of the availability of IT services and the infrastructure components that makes these services possible and available. This process combines a view of today with what will be required in the future, including consideration of the Service Portfolio Pipeline. The main purpose of availability management is to ensure that services deliver agreed levels of availability to meet the needs of customers and users. There are several benefits of availability management such as:

- Delivering availability performance that meets or exceeds known requirements.
- Assisting in the rapid resolution of any availability related issues.
- Partnering with business to create a long term availability and investment plan.
- Working closely together with change and release management to evaluate and mitigate the risks associated with the availability of planned changes.

- Strategically evaluating the improvement of customer satisfaction through availability.
- Proactive monitoring and measurement of service performance and availability.

The following is the availability management process:



- Measure, monitor, and analyse availability data.

  Effective analysis requires a commitment to data analysis and monitoring activities. The goal of availability management is to ensure the availability of services at a level that meets or exceeds requirements. This cannot be achieved without thorough analysis of the availability data. An important consideration for data analysis is recognizing and acknowledging the different context of data such as business, users, technology, etc. Furthermore, availability data evaluation and monitoring needs to consider the aspects of availability, reliability, resilience, and maintainability.
- Assessment and diagnosis of failures

  Failures are a good source to learn from. Each failure should be thus analysed by the availability management to determine the events leading up to the failure, events during the failure and time and events to resolve the failure. In the event of a failure, effective communication and prompt response is key to avoid loss of customer satisfaction. Once a failure is understood, the recovery process and restoration of the impacted services should be initiated.
- Develop reliability and resiliency plans.

  Reliability measures how long a service can perform as expected without failure whereas resilience is the ability of a service to combat failure and in the event of failure, recover quickly and fully. Resilience can offset risks of reliability whereas reliability can offset risks of resilience.
- Availability plan cost analysis

  The goal of availability is the meeting or exceeding of customer requirements. The availability plan includes the list of services considered, available support personnel, required IT assets and components, Target Mean time between failures, and target mean time between restoration of service. Afte a draft of availability plan has been created, the associated costs need to be calculated delivering the proposed plan. The finding of the right balance between availability and associated costs may require few availability plan iterations.

- Assessment and diagnosis of failures

  Assessment of the impact of failures is critical to evaluate the risks. Failure scenarios should consider assumption of failure, capital cost of failure, impact on the user and customer requirements, last revenue, and impact to employee productivity. T
- Evaluate risk in change and release plans.

  Changes and releases can improve availability. Changes and release also present a risk, and hence the change and release management should collaborate with availability management for risk evaluation and mitigation. Availability management needs to be proactive and not reactive approaching change and release management. Redundant IT assets can support the availability and reliability of services which also affect the cost.
- Plan and design of new services

  Planning of new services is a core part of the strategic activities in IT Service Management. Service availability must be a member of the team which plans for new services. No new services can be introduced without associated SLAs for the service and planning of the agreed availability. It is pivotal to plan and design the necessary level of availability from the very beginning of the service design.
- Availability test and recovery plans

  Availability and recovery testing is part of non-functional testing and must be part of every service roll out. Proactive testing during development can reduce availability risks and improve availability performance. A few considerations to be made for the availability test plan are:
  - Testing of most common failure cases.
  - Simulate recovery risks from failures.
  - Conduct training for recovery process.
  - Identification of high-risk components.
  - Test plan to verify targeted mean time between failures.
  - Test plan to verify targeted mean time to restore service.
  - Test plan to verify recovery and repair process.
  - Publish availability test schedule.
- Availability and investment plans

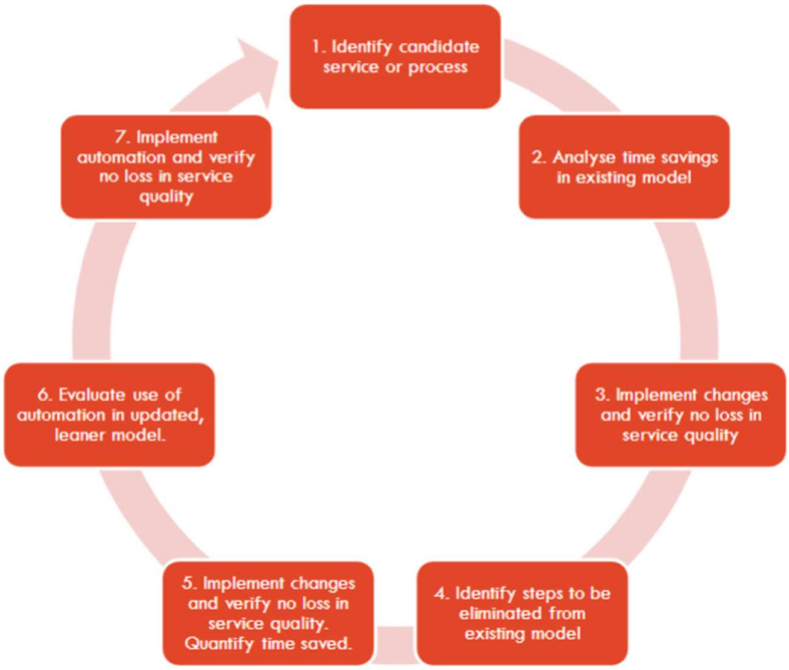
  Setting up an availability plan for all services is closely related to the availability budget and corresponding investments. Foals of an availability and investment plan are to ensure that the IT services are delivered according to the defined SLAs, ensure the availability of services required to enable the productivity of employees and leverage the plan as a platform to drive cooperation between incident, problem, change, release and financial management.

A few key integrations and partnerships to remember for availability management are incident management, problem management, change management, service catalogue, service portfolio, and financial management. A few recommendations for availability management are:

- Establish a working relationship between all key integrations.
- Make availability management a mandatory element of the planning of new services.
- The assessment of failures is as important as development of the availability plan.
- Measure and communicate defined KPIs and emphasize the importance of a speedy recovery in case of failure.
- Leverage redundancy concepts as a strategy to enhance availability.
- Work together with business department to balance costs with the required levels of availability.

Service Automation

Service Automation is the practice of an industry that enables their autonomous users to procure, manage and adjust services through self-service technology and concepts to systematically exceed user expectations. ITSM cannot scale without service automation. It is not part of the core ITSM elements but is equally if not more important. Following is a step-by-step process for achieving service automation:



Business rule objects can be used as a model for automation of a stand-alone decision or action. A business rule defines and enforces a rule of how a particular business process step operates. This business rules an be used as a building block in the construction of a multi-step workflow. An initial amount of time will be required to be invested in defining the rules, but once done, it will reduce the amount of time spent considerably. Examples of the business rule structure is given below:

The number of channels through which organisations receive requests are increasing. Phone, Emails, messages, service portal, etc. are all channels through which requests are received. Customer can experience uninterrupted user experience when given such a wide variety of options. This makes it complex for service automation. The service automation framework is more complex for variable, or less well-defined tasks. Dynamic services, services with more touch points, etc. are difficult to automate.

Service automation is an important factor for optimizing the efficiency, productivity, and user experience of an organisation but it requires investment. It ensures the successful and cost-effective delivery of IT service automation and can reshape the process and dialogue

around service automation. It can create a cultural mind-shift within the organisation toward service automation.

Service automation has 3 key integrations and partnerships. These are knowledge management, service catalogue and service portfolio, and financial management. Following are the recommendations for service automation:

- Utilize a structured approach to automation.
- Have a quantified goal defined for every automation project.
- Name an expert in the business to be the business process mentor for the project.
- Build a plan to deliver 24x7 support channels based on the omnichannel interaction and engagement approach.

Business Case

A business case is a short document that provides an overview of a potential new investment. A business case should be created for any service automation planned, this also promotes accountability and encourages a more structured and disciplined decision-making process. The business case should have an overview, costs, benefits, risks, and recommendations sections.

A well-prepared business case will not be always approved but it allows the process to be more productive and supports a better decision-making process. The business case is reviewed by the budget committee and this committee needs to make an objective and fair comparison between different business cases. Service Automation business cases with the most compelling benefits at an acceptable cost and risk level are likely to be approved.

With an approved business case, the requesting individual/group mobilizes for implementation of the service automation. The approved budget will be issued by the budget committee alongside a framework for cost control to monitor cost consumption during the lifecycle of the project.t A budget framework ensures the visibility and accountability of the spends. Meetings are better to be held to monitor actual spending against the established budget and frequent budget updates need to be made which would lead to less surprises.

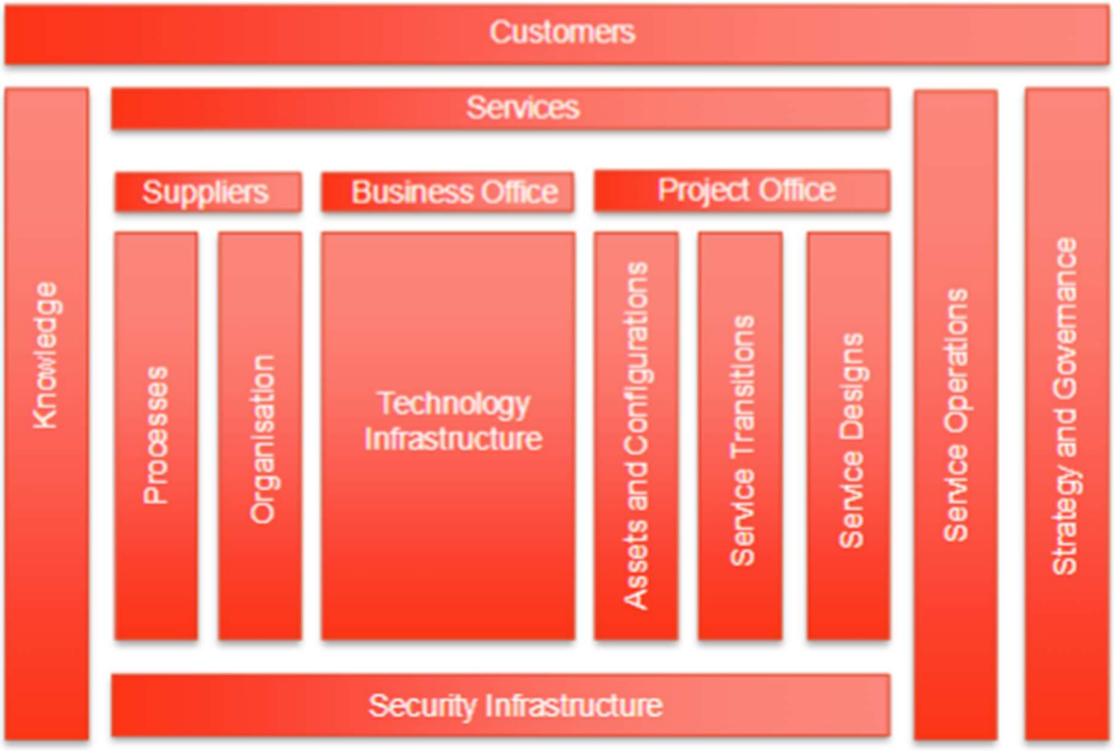
A value and investment analysis should be conducted following the completion of the implementation of the service automation project. About 3-6 months should have passed after the implementation to get a good overview of the service automation. A few of the analysis parameters are quantified value received, real value and benefit compared to the projections during business case creation, final real investment cost compared to the project investment costs, review of any setbacks, etc.

WEEK 7

ITSM Architecture Framework

IT is complex and technologies are changing rapidly. Organisations must make decisions daily and these decisions require a guideline. This guideline comes from the IT service management architecture. Without an architecture for ITSM, tools are purchased on the fly for discrete needs, decisions are made without considering the big picture, incidents happen lot more than usual, etc. An IT Service Management Architecture is the organising logic for pulling all service management processes and IT infrastructure together. It reflects and considers the integration and standardisation requirements of an organisation’s operating model.

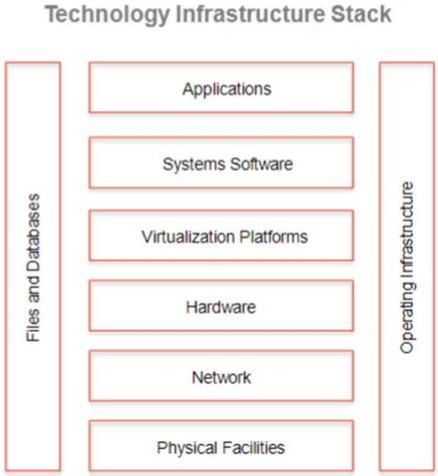
ITSM Architecture framework represents all key building blocks, components and types of configuration items that make up an IT Service Management Architecture to enable and underpin IT Services. Each block is further decomposed into several subsets. The following architecture is not a specific architecture but a typical architecture.



The main purpose of this architecture framework is to put a structure and order around all the complexities needed by a successful IT delivery organisation. The framework can also be used as a definitive reference for all the architectural elements that need to be in place to tun and operate a successful IT service delivery and support organisation.

Technology Infrastructure

The technology infrastructure block represents all the IT industry hardware and software resources used to support and deliver services. It is made up of several sub-blocks as given below:



- Physical Facilities

  Physical facilities represent actual physical locations from where IT services are delivered. Physical facilities logical items consist of building management system, air conditioning and facility cooling diagrams, facility blueprints, facility electrical safety code and plans, etc.
- Network

  Network items represent various network devices and equipment used to transport data throughout the IT infrastructure. A few networks logical items are DNS, Extranet and Intranet configurations, firewalls, IP addresses, etc.
- Hardware

  Hardware items represent processing devices and supporting hardware used throughout the IT infrastructure. A few hardware logical items are cabinets and racks, CD, DVD, Printers, scanners, laptops, etc.
- Virtualization platforms

  Virtualization platforms items represent specialized hardware and software that supports the sharing of IT physical resources among multiple applications, systems, users, and files. A few virtualizations platform logical items are virtual machine configurations, virtualization pools, virtual machine IP address, etc.
- Systems software

  System software items represent operating, middleware, the network, and hardware devices in the IT infrastructure, file and utility systems used to provide an abstraction interface to the network and hardware devices in the IT infrastructure. A few of the system software logical items are DBMS, file transfer software, messaging software, system utilities, etc.
- Applications

  Application items represent actual application softwares and development tools used within the IT infrastructure. Application logical items are application code, application code library configurations, application development softwares, APIs, etc.
- Files and Databases

  Files and databases represent the storage devices and logical file layout configurations used for data storage in the IT infrastructure. A few examples of File and database logical items are data architecture, data dictionaries, databases, files, etc.
- Operating Infrastructure

  Operating Infrastructure items represents softwares, systems, and configurations used to provide a centralized control point for managing events, incidents, problems, changes, etc throughout the IT infrastructure. A few operations management logical items are asset management software, backup and restore tools, service catalogue systems, configuration management software, change management software, etc.

Processes

Process items represent structured sequences of activities, procedures, and workflows used to manage and operate the IT infrastructure. A few processes logical items are activities, procedures, process descriptions, process architectures, process metrics, work instructions, etc.

Organisation

Organisation items represent roles, jobs, and skills that are used to describe people resources used to operate, manage, support, and deliver IT services. A few of the organisations logical items are job descriptions, organisation charts, role descriptions, etc.

Suppliers

Suppliers represent the third-party vendors used to support services delivered by the IT infrastructure. A few of the suppliers' logical items are supplier catalogues and brochures, supplier contact lists, supplier quality metrics, etc.

Business Office

Business office components represent components used to manage financial resources and transactions as well as people resources used to support and deliver IT services. A few of the business office components are budget and expenditure forecasts, purchase orders, software licenses, vendor catalogues, cost estimates, etc.

Project Office

Project office components represent components and elements used to manage projects and programs used to design, transition, and improve IT infrastructure and the services it supports. A few of the project office components are project issue lists, project portfolio, project work plans, work breakdown structure, etc.

Services

Service items represent components used to describe, measure, report, and make IT services. A few of the service components are Operational Level Agreements, Service Level Agreements, Service Dashboards, Service Quality Reports, Service metrics, etc.

Customers

Customer components represents the components used to manage relationships with customers and identify their needs and values. Customer logical components are business continuity plans, customer contact history, customer satisfaction surveys, relationship contact listings, etc.

Asset and Configurations

Asset and configuration components represent inventories, configurations, descriptions, and models for what is in the IT infrastructure and how all the parts fit together to provide IT services. A few of the Asset and configuration items are asset configuration, asset listings, asset records, configuration databases, port assignments, service models, etc.

Service Transitions

Service transitions represent elements of the infrastructure used to support build and transition activities to move new or changed IT services to a production operational state. A few of the service transition items are change approval packages, IT service continuity plans, IT service continuity test plans, IT service continuity test results, deployment plans, etc.

Service Designs

Service designs represents elements of the infrastructure used to design new or changed IT services to meet customer utility and warranty requirements. A few of the service design items are application and service sizing estimates, availability plans, capacity baselines, demand forecasts, workload characterization, etc.

Service Operations

Service operations represent elements of the infrastructure used to operate and deliver services on a day-to-day basis. Service operations items are backup schedules, event logs, event status reports, incident tickets, incident status reports, operational plans, etc.

Strategy and Governance

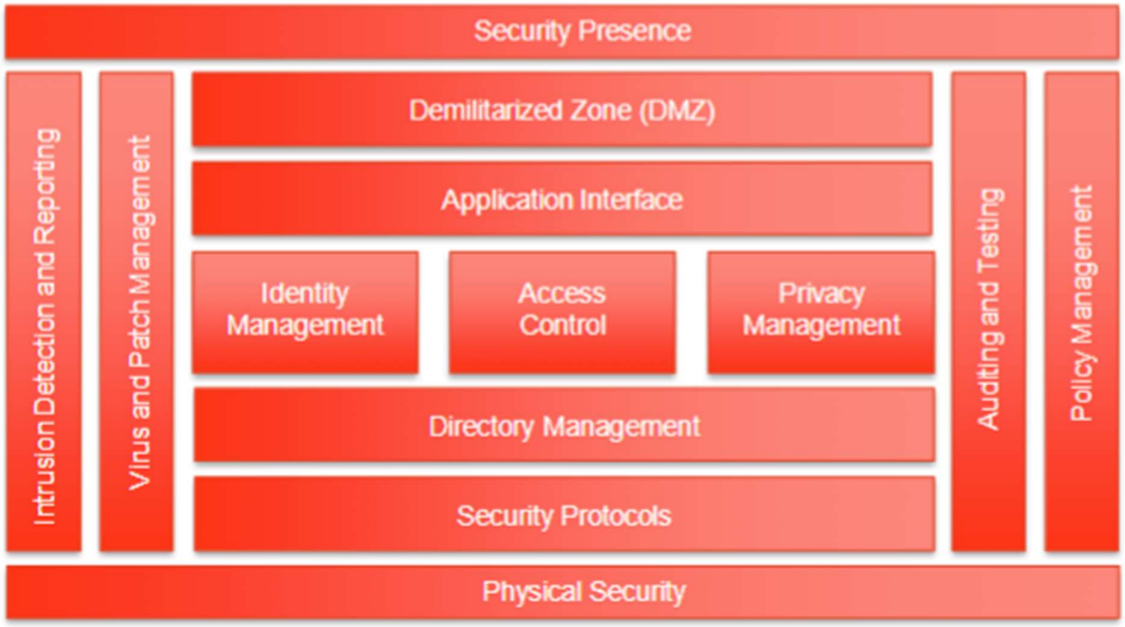
Strategy and governance components represent work artifacts used to provide strategies for services and govern their delivery. A few of the strategies and governance items are architecture standards, change policy, documentation templates, risk assessment, risk register, naming standards, etc.

Knowledge

Knowledge components represent work artifacts and repositories used for gathering, analysing, storing, and sharing knowledge and information used to operate the IT infrastructure, support, and deliver IT services. A few of the knowledge items are documentation subscription lists, IT audit results, known errors, Research reports, Training materials, training plans, etc.

Security Infrastructure

The security infrastructure building block represents all the IT technological resources and capabilities used to secure and protect service assets in the IT infrastructure. This infrastructure is used to protect confidentiality, integrity, and availability of services from unauthorized access. Security infrastructure is further subdivided into multiple blocks as given below:



- Physical Security

  Physical Security represents elements that are used to secure processing sites from unauthorized physical access. A few components of physical security are badges, biometric devices, security keypads, etc.
- Security protocols

  Security protocols are used to block access to data from unauthorized applications as it is transmitted over a network. Security protocol components are encryption schemes, secure shell controls, TLS transport layer security, etc.
- Directory Management

  Directory management represents system directories, their structures, permissions, interfaces, and management software. A few of its components are directory interfaces, directory names, directory management systems, etc.

- Identity Management

  Identity management represents systems and interfaces that restrict access to services and service assets via user ID and password protection. A few components of Identity management are Identity management applications, passwords, user ids, single sign on systems.
- Access Control

  Access control represents security profiles and access control lists to ensure only authorized users gain access to services and service assets in the infrastructure. A few of its components are access permissions, access control lists, access profiles, etc.
- Privacy and Policy Management

  Privacy and Policy Management represents policies and systems that enforce IT security policies to ensure that services and service assets are access only by those allowed to view them. A few components of these are policy enforcement systems, privacy configurations, privacy policies, etc.
- Application interfaces

  Application interfaces represent interfaces exposed by underlying backend systems and supplementing microservices accessed by production services to control or gain access to protected services, information, or service assets. A few components are web services, security appliance protocols, application IDs and control lists. Etc.
- Demilitarized Zone

  DMZ represents service assets that provide a buffer around the IT infrastructure to protect it from hostile attacks and intrusions launched over the internet. DMZ components are firewall appliance devices, firewall configurations, firewall riles, firewall servers, proxy servers, etc.
- Intrusion detection and reporting

  Intrusion detection and reporting represents security monitoring and reporting systems used to protect the IT infrastructure from hostile attacks. A few of these components are intrusion monitors, intrusion detection reports, password cracking monitors, security logs, etc.
- Virus and patch

  Virus and patch management represents patches, communications, and anti-virus updates used to proactively detect and prevent exploitation of vulnerabilities in the infrastructure. A few of its components are anti-virus patches and downloads, anti-virus subscription lists, forensics, security patches, etc.
- Auditing and Testing

  Auditing and testing based on security infrastructure are critical components to ensure the confidentiality, integrity, and availability of information and IT services. A few of its components are auditing tracking reports, testing documentation and tracking tools, test automation tools, security audit results, vulnerability testing softwares, etc.
- Security Presence

  Security presence represent the overall presence of the business organisation across the security infrastructure. This also include external security interfaces. A few of its components are external security interfaces, federated security configurations, trusted partners, etc.

Architecture and Operating Principles

There are a few principles which are used when creating the IT infrastructure. These are:

- A customer is anyone who receives a service. It is based on the customer perception that determines whether the service is of value or not.

- A service is anything of value delivered to customer.
- Customers only interact with IT in 2 ways beyond receiving their services, issue requests or report incidents.
- Customers always issue requests. These requests may change into IT change with their operating model to fulfil it.
- A request is a transaction against a service. A request is anything asked from IT that is not an incident.
- Large complex needs and activities are still requests. Larger requests like these should always be treated as requests to ensure they are properly addressed.
- IT delivers services through functions and capabilities. Services are delivered through functional organisational units.
- Suppliers support IT functions in their outcomes through goods and services. Suppliers provide goods and services to IT.
- Everything IT implements is guided by changes and implemented through releases.
- Projects exist as a mean to enhance or create new service solutions. Projects are not services, nor are they requests. They are logical units of work to provide an intended outcome.

WEEK 8

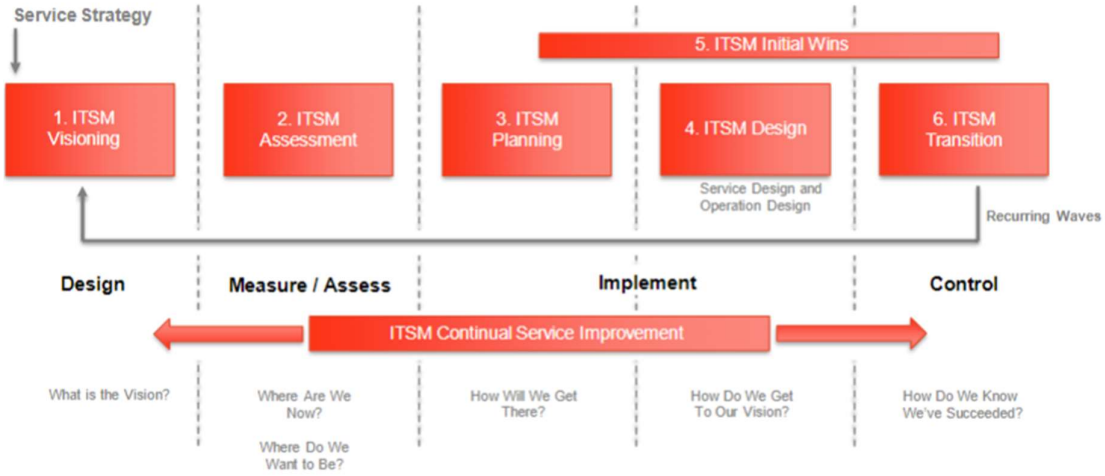
ITSM Guiding Principles

- The goal is to transform to an ITSM culture and operation and not implement individual processes.
- ITSM benefits lie in how the processes, tools, and organisation interlock and work together to meet business needs.
- ITSM transformation effort should occur in waves with achieved benefits at the end of each wave and each wave should be for 6-9 months.
- Projects that run beyond 6-9 months are harder to control in terms of scope, motivation, and management interest.
- Corporate management has little patience for major efforts that span multiple years before any return on investment can be seen.
- The effort must be driven by program of organizational change.
- Optimized processes do not happen by design and documentation. It needs to be implemented. Real benefits will come from implementing the behaviour and not new tools.
- The transformation effort must balance strategic efforts with short term gains.

ITSM Transformation

When transforming organisations towards an IT Service Management Organisation, there are two major focus areas and effort drivers, building a solid ITSM foundation core within the organisation, and taking key actions to overcome service issues and deficiencies that will be noticed and recognized by the organisation. When designing a transformational approach for ITSM, guiding principles are the key factors as they impact how the organisation was and how it will be organised and structured.

The overall transformation approach takes place in 6 high level work stages. These are given below:



- ITSM Visioning work stage

  The goal is to identify and agree on the IT service vision, Scope, and key business benefits. The outcomes of this stage are the identification of ITSM business focus, draft of ITSM vision, communication strategy, program risks, and program costs. The outcome of this stage serves as a reminder for the organisation goals and break resistance to change.
- ITSM Assessment work stage

  The mission of the work stage is to identify the gaps that exist between the current stage of organisation's ITSM practices and the planned service vision, the key actions needed to take place to close the gaps and identify the initial projects. The focus areas here are:
  - Process

    Reviewing the current state and maturity of progresses within the organisation and benchmarking them against ITSM best practices.
  - Technology

    Reviewing the technologies currently in place and assessing how well they will support the future state service vision.
  - Organisation

    Reviewing the current state organisation and assessing how well it will support and IT service culture.
  - Governance

    Reviewing current practices around IT service reporting, service governance, etc. to assess how well they will support an IT service culture.
- ITSM Planning work stage

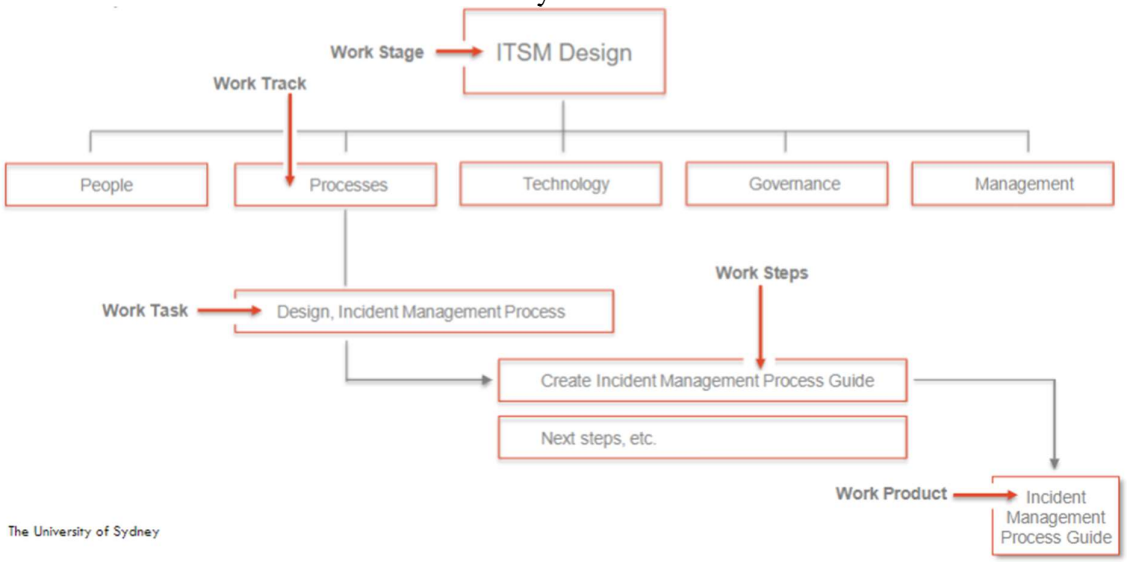
  The main goals of ITSM planning work stage are to produce detailed transformation plans and establishing the overall program infrastructure. This is the stage where everything comes together as a working program prior to the start of the ITSM transformation work. Without proper planning, resources and efforts may not be coordinated, confusion may reign, and the objectives of the transformation program may not be achieved. This stage is done in parallel with ITSM Initial Win work stage.
- ITSM Design work stage

  This is where the strategic ITSEM service vision will be designed. There are 4 focus areas for this stage as well which are process, technology, organisation, and governance. There is an important relationship between ITSM design work stage and ITSM initial win stage.

- ITSM Initial Win work stage

  The ITSM Initial Win work phase defines a series of initial win projects. Initial win projects may help and support to meet the goals of the transformation itself and make good public relationships. These are distinctive projects that provide immediate benefits. These are tactical projects with specific goals that are tangible for the stakeholders. It also has 4 focus areas, the process, organisation, technology, and governance. This stage can be done over 3-4 month, and they must have a clear sense of accomplishment at the end. It runs in parallel with ITSM planning, Design, and Transition work stage.
- ITSM Transition work stage

  The main goal of the ITSM transition work stage is to implement the processes designed in the ITSM design work stage and begin a regular cycle of reporting the process's health and state. This is where the designed and implemented processes are rolled out to the organisation and is important to focus on transitioning to necessary cultural and organisational changes to support the roll out of designed ITSM activities. This stage is usually based on a simple work breakdown model for organising work activities and tasks in a structured way. The model is as follows:



  - Work Stages

    The highest level of grouping of implementation activities. The 6 stages are vision, assessment, planning , design, initial wins, and transition.
  - Work Tracks

    All activities within a work stage are grouped into 5 work tracks, namely, process, technology, organisation, governance, and management. A few elements of a process are given below:
    - Procedure: An established method of carrying out an activity.
    - Work step: A step of work that occurs within a procedure. It is a breakdown of the long string of work to be done in a process.
    - Work instruction: A detailed breakdown of sequential steps needed to execute a work step or procedure.
    - Work products: The artifact or product produced by the work step.
    - Mission: The main objective for a given process.
    - Guiding Principles: One or more statements that have major impact on the process design or operation. These are usually derived from underlying culture or experience.

        - Scope: The description of what or who will be impacted by the process.
        - Policies: They are one or more guidelines that govern how a process will operate.
        - Critical Success Factors (CSFs): These are one or more statements describing what must happen to consider a process a success.
        - Key Performance Indicators (KPIs): These are one or more metrics that are used to measure whether CSFs have been met.
        - Supporting technologies: Tools or solutions supporting the process itself.
        - Process Owner: The organisational roll with overall or partial responsibility for process deployment and operations.
        - Roles: The representative ownership of different tasks and activities that support a process.
        - Assigned Organisation: The organisational entities within the organisation that have been assigned the service manager role.
    - Work Tasks
      These represents a key major implementation activity within a work track.
    - Work Steps
      Each work track is broken down into smaller work steps which need to proceed in a sequential order to complete a work task.
    - Work Product
      These are the ITSM implementation artifacts produced by the work steps.

RACI matrix

Ownership of each work task will be assigned to one of the 5 work tracks. A RACI matrix is used where responsibility is assigned to each stakeholder. R-Responsible, A-Accountable, C-Consulted, I-Informed.

Keep in mind when implementing ITSM in an Organization

- The effort invested for ITSM transformation needs to be treated as an Organisational Change Effort. This means that implementing new technologies and tools do not cut it, change should include the behaviour and processes as well.
- Balance strategic efforts with initial wins. If initial wins aren't present, organisations may lose motivation and the project maybe abandoned for other priorities. Hence benefits should be shown within a year or less (6-9 months).
- Implement ITSM as an operating culture and not just as a process. ITSM processes have critical dependencies on one another. Few organisations just select a few of the ITSM units while neglecting others, this may cause a huge drop in efficiency and huge increase in cost.
- Target 20% of the effort to get 80% of the benefits. Basically, do not reinvent or buy new IT solutions but focus on the existing IT solutions and perfect them. Design a new solution only when necessary. Though one must remember that overengineering and overdesigning may lead to ITSM transformation risks.
- Balance efforts with good leaders and managers. A manager is a person who have the skills to execute on ideas and tasks, whereas a leader is someone who will challenge the status quo, research new ideas, take initiative, break old habits, and company boundaries. A proper mix of both is required for a better ITSM transformation.
- Scope efforts by service and not by the geographic location of the services. The ITSM transformation should be global if customers are being served globally.
- Establish compelling business reasons for ITSM. Compelling business reasons are drivers of change for senior stakeholders and hence need to be documented, quantified,

and objectively qualified. Business reasons need to address the pain the organisation is facing and the consequences of it and shows a method of solving or addressing it. The maturity of organisation's current process can be measured via industry standards such as Capability Maturity Model Integration (CMMI).

Capability Maturity Model Integration (CMMI)

CMMI is designed to help improve performance by providing businesses with everything they need to consistently develop better products and services. Businesses can use CMMI to develop appropriate benchmarks and standards which would in turn also help to create a structure for encouraging productive, efficient behaviour throughout the organisation. CMMI was developed to combine the various maturity models into 1 framework. The CMMI model breaks down organizational maturity into 5 levels, these are:

- Maturity Level 0 – Incomplete

  At this stage the work may or may not get completed, goals have not been established and processes are only partly formed or do not meet organisational needs.
- Maturity Level 1 – Initial

  At this stage the processes are viewed as unpredictable and reactive. Work gets completed but is often delayed or over budget. This is a risky and inefficient stage to be in.
- Maturity Level 2 – Managed

  At this stage, a level of project management is achieved. Projects are planned, performed, measured, and controlled even though there are many issues to be addressed.
- Maturity Level 3 – Defined

  At this stage, the organisation is more proactive than reactive. There is a set of organisational standards that provides guidance across projects, portfolios, and programs.
- Maturity Level 4 – Quantitatively Managed

  This stage is more measured and controlled. The organisation is able to determine predictable processes that align with stakeholder needs and is ahead of risks with more data-driven insight into process deficiencies.
- Maturity Level 5 – Optimizing

  The final stage where in organisation processes are stable and flexible. This is the stage where organisational processes are in a state of continuous improvement and responsive to change over opportunities. The organisation is stable, allowing for more agility and innovation.

The CMMI has capability levels which are distinct from maturity levels. The capability levels are used to appraise an organisation's performance and process improvement. It is usually applied to individual practice areas such as process management, organisational training, peer reviews, process quality assurance, monitoring, and controlling. A process is said to be capable only if it satisfies the specified product quality, service quality, and process performance objectives. It also has got levels which are:

- Capability Level 0 – Incomplete

  The process is deemed to have inconsistent performance and has an inconsistent approach to meeting the objectives of the process.
- Capability Level 1 – Initial

  This is the phase when organisations start to address performance issues in a specific practice area but there are no set practices in place.

- Capability Level 2 – Managed

  In this stage, the progress is starting to show and there is a full set of practices in place that specifically address improvement in the practice area.
- Capability Level 3 – Defined

  It is the stage where there is focus on achieving project and organisational performance objectives and there are clear organisational standards in place for addressing projects in that practice area.

WEEK 9

Importance of ITSM metrics

Measuring IT is difficult due to various reasons. Unknown amounts of labour, how much waste is produced, how efficient IT departments are, etc. Best practices for measuring IT are available but because the IT landscape is changing and developing so rapidly, that organisations never focused on IT metrics. This has caused various issues such as the overspending on implementation of processes, inability to justify ITSM initiatives, poor decision making, etc.

Challenges with IT Metrics

Common IT KPIs are usually how many IT changes were implemented, how many incidents occurred, what was the peak utilization of resources, availability of IT assets and services, etc. These are operational metrics. These questions lead to more clarification questions. Good, value providing KPIs provide a basis for making good business decisions. Indications and decisions which can be derived from suitable KPIs are:

- Poor efficiency and effectiveness rates may indicate action is needed to reduce wasted labour when changes are being handled and processed.
- Additional operational staff may be needed if there will not be enough labour to handle the change workload created by a new application, system, solution, or impending merger.
- Incidents and problem rates may be high, but customer impact is low – therefore, IT is doing a fantastic job of protecting services but IT Services may not be able to sustain this if business volumes start to increase.

Resistance to IT metrics

Many IT decisions in terms of cloud computing, reducing IT staff, investing into new services, etc. are made with low level of facts and information. This is leading to high levels of failed IT initiatives, reactive decisions, high levels of frustrations across the organisation, erosion of IT service quality, increase in Operating costs, etc.

Benefits of using suitable ITSM metrics

ITSM metrics that matter to an organisation will provide senior executives and management with indicators which enable them to make accurate and timely business decisions. It will also provide visibility to how effectively and efficiently IT support and delivery services truly operate. Furthermore, it provides a basis for identifying and prioritising IT service improvements while the analytical information will identify service deficiencies. A set of well-defined IT metrics can also be the foundation for modelling the impacts of business and IT decisions.

Categories of IT Metrics

An ITSM metrics model uses several metric categories. These are as follows:

- Operational Metrics

  The most basic observation for operational events for each ITSM capability. They are the starting point of ITSM metric model and required to calculate the KPIs. The input for these metrics can come from the Change management system, incident management system, service desk reports, etc. A few examples of incident management operational metrics are total number of incidents, average time to resolve severity 1 and severity 2 incidents, number of incidents resolved within agreed service levels, number of major issues, etc.

- KPIs

  These are metrics that are used to indicate the performance level of an operation or process. KPIs are used to provide a basis for actionable management decisions. While operational metrics are historical in nature, KPIs are calculated or derived from one or more of these operational metrics. The results of these calculations are then compared to the tolerance thresholds to identify the acceptance level for the results. A few examples of KPIs are change efficiency rate, request processing rate, incident repeat rate, request automation rate, etc. CMMI process maturity levels can also be considered as KPIs. A few examples of incident management KPIs are number of incident occurrences, number of major incidents, incident resolution rate, customer incident impact rate, etc.

- Tolerance Thresholds

  These are the upper and lower boundaries of acceptable and non-acceptable KPI values. These are set by the Service Manager with agreement of the IT and Business Senior Management. These are critical as these indicate when the management needs to act or decide. Tolerance levels represent desired service and performance levels a business is willing to tolerate hence it will differ from business to business.

- CSFs

  These are metrics that represent operational performance requirements. It indicates whether a process or operation is performing successfully from a customer or business perspective. CSFs are calculated or derived by one or more KPIs by comparing how those KPIs performed within the tolerance range. The CSF is linked to a performance level that indicates likelihood of success as to whether the CSF was achieved or not. A few example of incident management CSFs are quickly resolving incidents, maintaining IT service quality, Maintaining user satisfaction, etc.

- Dashboards

  Dashboards are key metrics that are represented on a report or graphical interface. They indicate success or failure of a business operation. Dashboards give a quick visual summary of the current state of operation and provides information at very high levels and may include drill down capabilities to look at things in more detail. Dashboards can trigger timely actions to correct operational deficiencies and these Dashboard results are derived from the CSF results.

- Outcomes

Outcomes are key indicators of general business risk areas. Outcomes identify the success, at risk or failure of KPIs or CSFs and is used to quickly assess the level of risk created by processes or operational deficiencies. Examples of outcomes include service outages, rework, waste, security breaches, dissatisfied customers, loss of market share, etc. Each of the outcomes can be associated with an indicator such as High, medium, low that will reflect the likelihood of that outcome to occur. Outcomes are the kind of things that IT is trying to protect against.

- What Ifs

  What ifs can be characterized as use cases derived from upcoming business decisions and will be used to model the impacts of those decisions on KPIs and CSFs. For example, a use case can be: What happens if a major new application goes into production? The impact of this use case can then be modelled by raising or decreasing the values of the operational indicators related to the use case.
- Analytical

  The analytical category represents metrics more into research of an issue, incident, or service problem. These metrics are one-time only or part of a dashboard drill down feature. Typically, these metrics are usually subsets of other metrics. For example, Operational metric of total number of incidents can be further subdivided into analytical metrics such as the total number of incidents by department, geographic area, time of the day, etc.
- Other

  This category of metrics represents all the other metrics which do not fall under the earlier categories.

Balanced Scorecards

For ITSM metrics, the balanced scorecard is a good approach. It was developed around the notion that financial measures alone are not critical for business success. A balanced scorecard can be used to determine which CSFs should be used for dashboards. There are a total of 5 categories in the balanced scorecard, these are:

- Customer

  The customer category represents the customer view of the services being delivered.
- Capabilities

  The capabilities category represents the capability of the IT organisation to meet business needs.
- Operational

  The operational category represents how well the IT organisation is delivering their services on a day-to-day basis.
- Financial

  The financial category represents how well the IT organisation is managing and controlling costs as well as protecting and enhancing revenue.
- Regulatory

  The regulatory category represents how well the IT organisation is operating in a manner that protects it against regulatory risks for fines, penalties, and audit issues.

WEEK 10

Introduction

IT is always upgrading, constantly changing. The primary roles of IT have been shifting from primarily building solutions to integrating solutions and enabling business models. The traditional IT operating model of delivering IT to the business has been disrupted due to latest technological trends such as cloud computing, virtualization, outsourcing concepts, etc. This

shift gives rise to severe challenges in meeting business needs and thus IT must blend with Business.

Currently, the IT and Business within an organisation is still separated. The organisational chart is hierarchical and centralized making it harder for it to be flexible and agile. The number of IT solutions providers are increasing while the prices for these products and services are decreasing and hence IT will need to assemble services and solutions from many providers and then integrate it in an optimum manner to meet business needs. IT investments are being cut and this is because the investment decisions are being made on component level and not on a business level with the understanding of business or customer impact.

IT needs to change from traditional IT components and outputs to focus on business outcomes and values at an acceptable cost and risk. IT must be organized by services being delivered and not by technology being deployed. And for this IT transition, a service thinking approach is necessary.

Service Driven IT Organisation

A service driven organisation is one that has incorporated the concept of running IT as a business. A service driven organisation leverages ITS, capabilities to not only optimize its services but also the management of those services. This increases employee satisfaction and better business outcomes.

Consumerization of ITSM means offering a choice of high-quality services to stakeholders by leveraging rapid and agile service evolution cycle. A better service experience for customers and employees can be reached through consumerization of ITSM. The reasons mainly revolve around the fact that the IT department works directly with end-customers and hence high-quality service will lead to higher customer satisfaction. Furthermore, internal users are behaving like consumers and consumer technologies are becoming cheaper than enterprise technologies. Small number of large applications provide service to the customers today, but in the future many applications will provide services. This is how consumerization will change the IT Landscape.

Most enterprise IT departments are looking towards consumer technologies to reduce costs and improve quality as the consumer hardware and development tools are becoming cheaper along with the innovation focus being on consumers. Organisations should basically aim to combine the best of IT and business for their IT operations. This has impacted ITSM in various capabilities as well. A few of these are:

- Service Level Management: More granular services on different platforms.
- Service Requests: More frequent, but smaller requests for services.
- Knowledge management: More platforms and technologies relate to broader knowledge management capabilities.
- Service Catalogue: More services may be presented, especially with hyper personalized service offering.
- Incident and Problem Management: Number of incidents may increase and plus scaling is required.
- Release and Change Management: More frequent changes and corresponding releases to production.
- Asset and configuration Management: May become more complex!

- Financial Management: Changes from on-premises to cloud and dynamic scaling may reduce costs.
- Availability Management: May become more complex, but overall availability should increase.

A few challenges in transitioning enterprises to consumerization:

- Development Cost

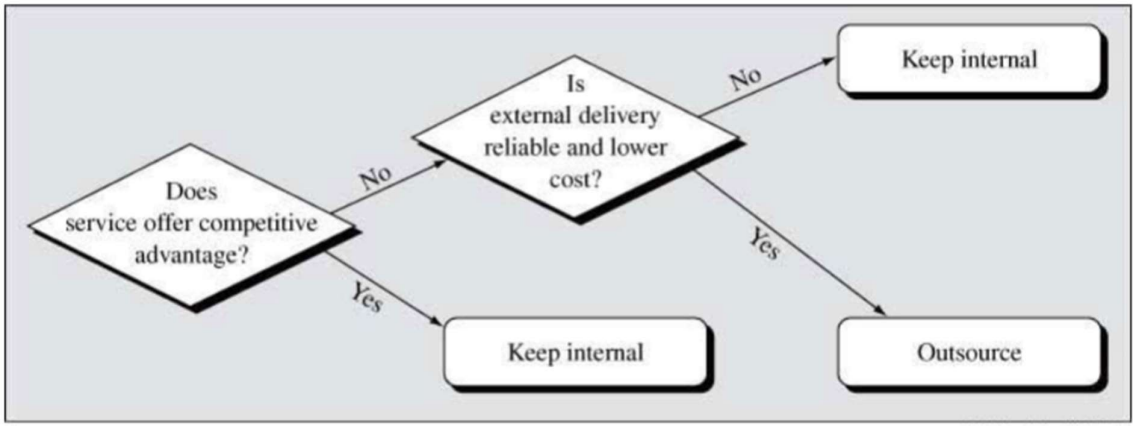
  Enterprise services and applications calculate ROI over long periods and hence need stability over such long periods. Hence there would be resistance to the usage of new technology. Enterprise services and applications are large and hence changes are difficult to make. Unless organisations make changes to the way they develop applications and services, the number of small services and applications will culminate to result in significant cost increases.
- Deployment Cost

  Enterprise services and applications are geared towards slow and careful deployment. Usually, this results in only 1 service and application being live in production at a time. If the organisation decides to deploy many small services or applications, the deployment will become complex and expensive.
- Operation Cost

  Enterprise services and applications are optimized for supporting users over many years and the ones which mature over years reduce running and operational costs. If the organisation needs to run many small services and applications together, it will make the operations management complex and expensive.

IT Outsourcing

Service driven IT organisations are outsourcing certain IT capabilities to improve service quality. Outsourcing is the use of external service providers to effectively deliver IT-enabled business process, application service, etc. 2 common types of outsourcing are total outsourcing, where an entire activity is sourced to the supplier, and selective outsourcing, where only part of the activity is outsourced to the supplier and the rest is performed in-house. The choice of which IT service to outsource is simple and the following decision tree can be used:



One could also use the following decision matrix for deciding to outsource:

IT services are unique to a company and provide significant competitive advantages over the competitors and hence tend not to be outsourced. Commodity like IT services are usually outsourced if the vendor can provide it at a reliable and low cost. There are different types of outsourcing, these are:

- Offshore outsourcing: Sending IT related work to a company in a foreign country.
- Nearshore outsourcing: Sending IT related work to a company in the country sharing borders with your company.
- Onshore (domestic) outsourcing: Sending IT related work to a company in the same country as yours.
- Cloud computing: Contracting with a 3rd party to provide IT related serviced over the internet or proprietary network. There are 3 platforms of cloud-based services, the Infrastructure as a Service which provides for IT architecture services on a pay-as-you-go basis, Platform as a Service which provides hardware and software tools over the internet, Software as a Service which provides software by a 3rd party over the internet.
- Managed services: Contracting with a 3rd party to provide network management functions such as call centres, messaging, VPNs, firewalls, etc.

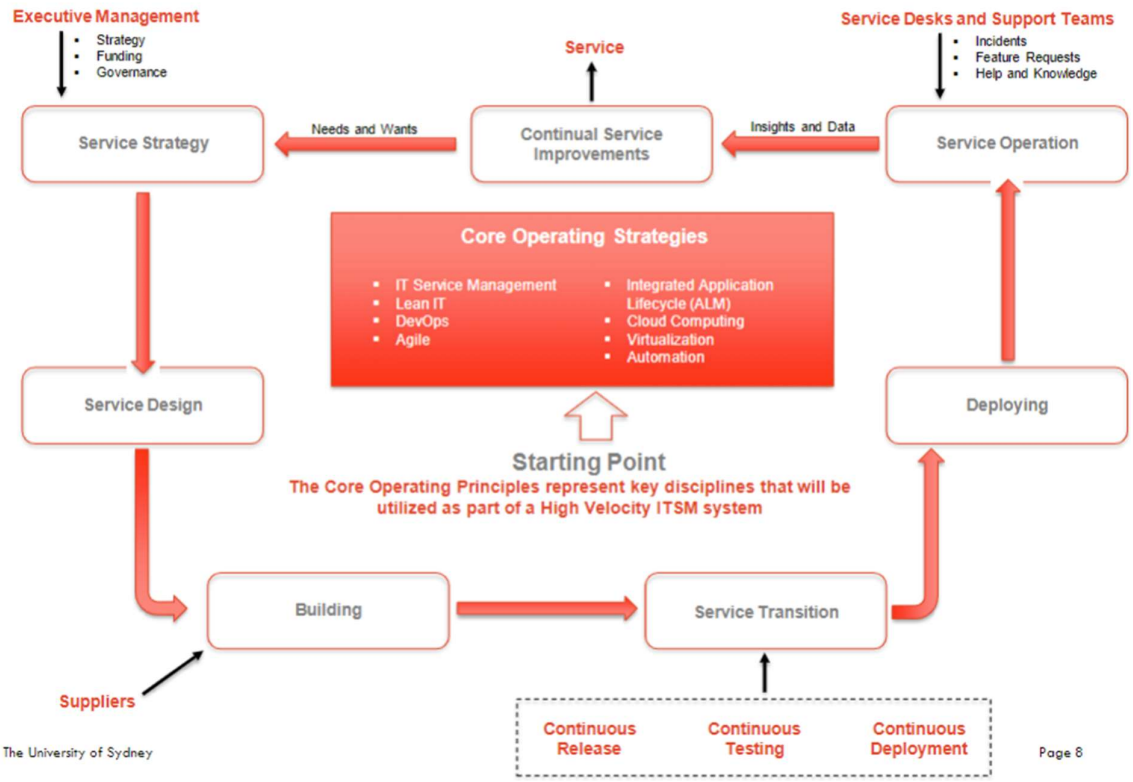
WEEK 11

High Velocity ITSM

It is operating, governing, and managing IT by services delivered with a keen focus on speed, efficiency, value, and cost. The key objectives of a high velocity ITSM are:

- The focus on service flues together development and operations.
- Continuous service improvement is always in way to make it more efficient and find more effective ways of delivering services.
- Delivery is focused on service integration and not acquiring technologies for the business.

The following is a High Velocity ITSM Operating Model:



As seen the core Operating strategies are:

- IT Service Management

  Business sees no value in IT until a service is delivered. The disciplines of ITSM are very important in high velocity ITSM operating mode. ITSM is the glue that holds everything together and forms the flow of the entire cycle.

- Lean IT

  The objective is to aggressively look at all the IT management processes and services and aggressively look for ways to improve efficiency. This can include areas such as eliminating slow and redundant steps, removing waste, automation of common redundant tasks, etc.

- DevOps

  It is a culture and practice that emphasises on the collaboration of IT operations and software developers to allow for a frequent build, test, and release of reliable software. Both the parties work in close collaboration and their main objective is to control changes and releases into the production environment but more efficiently.

- Agile

  This is a solution development practices where the requirements and solutions evolve fast and continuously improve with rapid and flexible response to change. Agile practices focus on releasing fast with small increments of change. Users get to see the product much faster and get to continuously provide feedback so that it can be quickly incorporated into each agile release. Furthermore, software defects are solved much faster in this process.

- Integrated Application Lifecycle

  The development community realized that they can't continue to build solutions by themselves without the involvement of management. Currently, activities such as version control, bug tracking, code management, etc. are being integrated alongside information across many development tasks.

- Cloud Computing

  Through using internet-based hosting services to provide on-demand access to a shared pool of computing resources, efficiencies are created. External suppliers handle all the complex task of infrastructure management of physical resources taking away majority of the risks.
- Virtualization

  Virtualization is about separating operating systems, data, and platforms from the hardware they run on. Servers, desktops, storages, data centres, etc. can be virtualized.
- Automation

  IT automation is the handling of manual tasks through scripts and software in such a way that those tasks become self-acting. Automation reduces or eliminates the need for labour and responds much faster than people, executes tasks consistently, and prevents human errors.

The following are the components of the lifecycle of a high velocity ITSM Operating model:

- Executive management

  Executive management is responsible for making every key decision and defining corporate and service strategies. These strategies are represented and governed through an IT service portfolio.
- Service strategy

  In this step the IT service portfolio is governed and managed. Executive decisions are made for the business. The output of this stage leads to projects that will build new services, modify, or enhance existing services, or remove services that are no longer needed.
- Service design

  In this step the organisations design and specify the building of IT services. With an agile approach, build activities proceed without knowing every requirement that may be ultimately needed. This stage focuses on high level things like the ITSM capabilities, user stories, and service features that will be developed.
- Building

  Solution building takes place in this step. DevOps practices are used to make sure development and operations work together to develop a comprehensive solution. Development team focuses on service utilities whereas the operations team focuses on service warranty.
- Service transition

  Activities take place to handle testing, change, release, and deployment tasks. In high velocity ITSM, these items operate in continuous matter. Releases are always in play and testing operates continuously when new releases are made. Release to the live environment occurs as soon as the testing activities have run a cycle without defects.
- Deployment

  In this step, actions take place to transfer solutions to the user. Not all deployments are immediate, some may take some time to deploy in lieu of heavy business periods of activities or when users need to be trained. Usage of technologies to automate and speed up deployment activities also take place in this step.

- Service Operation

  In this step solutions are operated every day. Typical activities include handling incidents and problems, fulfilling requests, monitoring the operation, performing admin duties, etc. This is the stage where the business receives value for their investment and this stage is also the one where lots of insights are generated.
- Service desks and support teams

  These entities exist to provide contact points for the business to interact with IT to fix defects, fulfill requests, etc. Service desks provide a valuable resource for information around service defects, how services are being used, whether the business is finding value or not, etc.
- Continuous Improvement

  In this step issues and defects are captured and analysed for improvement opportunities. Insights are gained on how to execute these services and manage supporting processes for effectively. In high velocity ITSM continuous effort needs to be made to identify opportunities to deliver faster and at a lower cost.

CHECK YOUR UNDERSTANDING QUESTIONNAIRE

1. **What are the components of the ITIL Service Lifecycle?**
2. **What are the differences and congruences between ITIL and COBIT?**
3. **Why is the importance of ITSM in a post-Covid world growing and what are some of the business benefits of ITSM?**
4. **What is the fundamental difference between an incident and a service request?**
5. **How can Service Catalogue benefit business operations fundamentally?**
6. **How does a typical Service Request process look like?**
7. **Why should organisations have a focus on service request workflow automation?**
8. **Explain the influence of robotic process automation to incident and service request management processes.**
9. **How can the solving of a problem support organisations in creating knowledge?**
10. **Why is it difficult for organisations to make a broad range of knowledge available to employees?**
11. **What are the opportunities and advantages when rephrasing problem statements?**
12. **Why are Service Level Agreements important for organisations?**
13. **What is the difference between SLA, OLA, and UC?**
14. **What is the difference between Change Management and Release Management and why are both areas so interconnected?**
15. **Why is integrity so important for change?**
16. **Why does IT Asset Management matter in the context of cyber-security?**
17. **What are common mistakes in Release Management and how can an organisation improve them?**
18. **Why is availability management important for corporations?**
19. **What is the difference between Service Level Management and Availability Management?**
20. **Which areas in corporations are ideal candidates for service automation ?**
21. **Why are service catalogues and service portfolios pivotal when assessing service automation opportunities within an organisation?**
22. **What are the key components of an ITSM Architecture Framework and how are they linked between each other?**
23. **Why is it important to have architectural principles in place that are aligned to the underlying ITSM Architecture Framework?**

24. **Why is it important to have an incident response plan for cyber security threats?**
25. **How can the ITSM Architecture Framework support organisations to be better prepared and equipped for cyber security threats?**
26. **What are the different work stages during an ITSM transformation?**
27. **What are key questions to ask in each work stage?**
28. **What is the difference between a work stage, work track, work task, work step and work product?**
29. **What are the differences between CMMI and ITIL?**
30. **Why are metrics IT been neglected for so long?**
31. **What is the difference between an Operational Metric, a Key Performance Indicator and Critical Success Factor?**
32. **What are potential consequences if no proper IT Metric Reporting capabilities are in place in an organisation?**
33. **Which perspectives are being considered within the original Balanced Scorecard approach?**
34. **What is a Service Driven Organisation and how can it leverage the consumerization of IT to its benefit?**
35. **What is the consumerization of IT and what are associated challenges?**
36. **How does outsourcing affect ITSM?**
37. **What does the future of outsourcing look like?**
38. **What is High Velocity ITSM and why are more organisations changing towards this kind of ITSM concept?**
39. **What are the main differences between conventional ITSM and High Velocity ITSM?**
40. **What is the core operating strategies that enable High Velocity ITSM?**
41. **Why could the association of the concepts of 'Agility' and 'ITSM' be considered an oxymoron?**
42. **Why is digital transformation so important for ITSM in organisation?**
43. **How can ITIL and DevOps enable digital ITSM transformation?**
44. **What barriers could occur when establishing a DevOps concept in an organisation and how can they be overcome?**