**ITIL** stands for Information Technology Infrastructure Library.It is set a detailed practices for IT service management (ITSM)that focuses on allgning IT service with the needs of business.In its current form ITIL is publiahes as a series of five core volumes,each of which cover different lifecycle stage. Although ITIL underpins [ISO/IEC 20000](https://en.wikipedia.org/wiki/ISO/IEC_20000) ([previously](https://consultantsfactory.com/verism-training-online) BS 15000), the International Service Management Standard for IT service management, there are some differences between the ISO 20000 standard and the ITIL framework. ITIL describes processes, procedures, tasks, and checklists which are not organization-specific or technology-specific, but can be applied by an organization for establishing integration with the organization's strategy, delivering value, and maintaining a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement. (It is to be noted that there is no formal independent 3rd Party Compliance Assessment available for ITIL compliance in an organisation, Certification in ITIL is only available to individuals and relates to their knowledge of the 5 books

Freamwork of ITIL:



**(1)Strategy**:

(i)Portfolo strategy: The **Service Portfolio** is described in the [ITIL](https://en.wikipedia.org/wiki/ITIL) books [*Service Strategy*](https://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library#Service_strategy) and *Service Design*. The Service Portfolio is the core repository for all information for all services in an organization. Each service is listed along with its current status and history. The main descriptor in the Service Portfolio is the [**Service Design Package**](https://en.wikipedia.org/wiki/Service_Design_Package_(ITIL)) (SDP).

The Service Portfolio consists of three parts:

**Service Pipeline**

This contains references to services that are not yet live. They may be proposed, or under development

**Service Catalogue**

This contains links to active services through their Service Design Package

**Retired Services**

Services in the process of being discontinued, before they are finally decommissioned

Of these three, only the Service Catalogue is visible to the customers and support team. Customers are excluded from the pipeline provisioning process for services under development.

(ii)Financial management:Financial management for IT services is a process inside the Service Strategy phase of an **ITIL** IT Service Lifecycle. It consists of three main processes: Budgeting – this process plans income and expenditure of money for an organization. Planning is done periodically.

(iii) **Service Portfolio Management** : The objective of **ITIL Service Portfolio Management** is to manage the **service portfolio**. This **ITIL** process ensures that the **service** provider has the right mix of services to meet required business outcomes at an appropriate level of investment.

(iv)Release management: **Release** and Deployment **Management**aims to plan, schedule and control the movement of releases to test and live environments. The primary goal of this **ITIL** process is to ensure that the integrity of the live environment is protected and that the correct components are released

**(2)Design**:

(i)Capacity Management: **Capacity management's** primary goal is to ensure that information technology resources are right-sized to meet current and future business requirements in a cost-effective manner. One common interpretation of **capacity management** is described in the **ITIL** framework.

(ii)Avilability Management:  *ITIL Availability Management* aims to define, analyze, plan, measure and improve all aspects of the availability of IT services. It is is responsible for ensuring that all IT infrastructure, processes, tools, roles etc are appropriate for the agreed availability targets.

(iii) **ITIL security management**. **ITIL security management**(originally Information Technology Infrastructure Library) describes the structured fitting of **security** into an organization. **ITIL security management** is based on the ISO 27001 standard. ... The primary goal of information**security** is to control access to information.

(iv)**Continuity Management**: This **ITIL** process ensures that the IT service provider can always provide minimum agreed Service Levels, by reducing the risk from disaster events to an acceptable level and planning for the recovery of IT services. ITSCM should be designed to support Business Continuity Management.

(v)Demand Management: According to **ITIL**, the purpose of **demand management** is to understand, anticipate, and influence customer **demand** for services. ... As a process, it is part of the **ITIL** service strategy stage of the **ITIL** lifecycle. Service strategy determines which services to offer to prospective customers or markets.

(vi) **ITIL Service Catalogue Management** aims to ensure that a **Service Catalogue** is produced and maintained, containing accurate information on all operational **services** and those being prepared to be run operationally.

**(3)Transition:**

(i) **Transition Planning** and **Support in ITIL** V3 is actually about managing service **transition** projects, so at IT Process Maps we decided to make this clear by slightly changing its name to Project Management (**Transition Planning** and **Support**). **ITIL** does not provide a detailed explanation of all aspects of Project Management.

(ii) **Service Asset** and **Configuration Management**. Objective: **ITIL Service Asset** and **Configuration Management** aims to maintain information about**Configuration** Items (CIs) required to deliver an IT**service**, including their relationships.

(iii) **Change management** is an [IT service management](https://en.wikipedia.org/wiki/IT_service_management) discipline. The objective of change management in this context is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to control [IT infrastructure](https://en.wikipedia.org/wiki/IT_infrastructure), in order to minimize the number and impact of any related incidents upon service. Changes in the IT infrastructure may arise reactively in response to problems or externally imposed requirements, e.g. legislative changes, or proactively from seeking improved efficiency and effectiveness or to enable or reflect business initiatives, or from programs, projects or service improvement initiatives. Change management can ensure standardized methods, processes and procedures which are used for all changes, facilitate efficient and prompt handling of all changes, and maintain the proper balance between the need for change and the potential detrimental impact of changes.

(iv) **Service Validation** and **Testing**. Objective: The objective of **Service Validation** and **Testing** is to ensure that deployed Releases and the resulting**services** meet customer expectations. This **ITIL**process verifies that IT operations is able to support the new **service**.

(v) **Knowledge Management: ITIL Knowledge Management** aims to gather, analyze, store and share **knowledge** and information within an organization. The primary purpose of this **ITIL** process is to improve efficiency by reducing the need to rediscover **knowledge**.

(vi) **Deployment Management**aims to plan, schedule and control the movement of releases to test and live environments. The primary goal of this **ITIL** process is to ensure that the integrity of the live environment is protected and that the correct components are released.

(vii)  Evalution:**ITIL** Change**Evaluation** aims to assess major Changes, like the introduction of a new service or a substantial change to an existing service, before those Changes are allowed to proceed to the next phase in their lifecycle.

**(4)Operation:**

(i) A **Service Desk** is a primary IT function within the discipline of IT **service** management (ITSM) as defined by the Information Technology Infrastructure Library (**ITIL**). ... A **service desk** seeks to facilitate the integration of business processes into the **service**management infrastructure.

(ii) Incident management:Failure of a configuration item that has not yet affected service is also an **incident** — for example, failure of one disk from a mirror set. The **ITIL incident management** process ensures that normal service operation is restored as quickly as possible and the business impact is minimized. **ITIL** Service Operation.

(iii)Event Manegment: **Event Management**, as defined by **ITIL**, is the process that monitors all **events** that occur through the IT infrastructure. It allows for normal operation and also detects and escalates exception conditions. **Events** are typically notifications created by an IT service, Configuration Item (CI) or monitoring tool.

(iv)Request fulfillment: **ITIL Request Fulfilment** aims to **fulfill**Service **Requests**, which in most cases are minor (standard) Changes - e.g. **requests** to change a password or **requests** for information.

(v) The primary objectives of **problem management** are to prevent **problems** and resulting incidents from happening, to eliminate recurring incidents, and to minimize the impact of incidents that cannot be prevented.

(vi) **Access management** is the process of granting authorized users the right to use a service, while preventing **access** to non-authorized users. It has also been referred to as rights **management** or**identity management** in different organizations.

(vii**) Application management**is responsible for managing applications throughout their lifecycle. This ITIL process plays an important role in the application-related aspects of designing, testing, operating and improving IT services, as well as in developing the skills required to operate the IT organization's applications. 'Application Management' is an ongoing activity, as opposed to 'Application Development' which is typically a one-time set of activities to construct applications.

(viii)  **IT Operations Management** is to monitor and control the IT services and IT infrastructure. IT Operations Management executes day-to-day routine tasks related to the operation of infrastructure components and applications.

(ix) **Technical Management** is treated in **ITIL** as a "function". It plays an important role in the**management** of the IT infrastructure. Many **Technical Management** activities are embedded in various **ITIL**processes - but not all **Technical Management**activities.

(5)Continual improvement:

(i) **The seven step process**:A change, thus implemented for the **improvement** sets a new baseline and the cycle begins again. The seven step process is the vital **process** of CSI. It enables an organizational resource to identify and understand which **process** and function of their service operations needs major enhancement.

(ii)**Quality management system**: For IT quality of service is not just for networks anymore. IT is now a service based organization. IT should follow quality management system practices and principles for the products and services it provides since they are vital to the performance of the business.

(iii)**Business Qustions for CSI**: Continual Service Improvement (CSI) uses a metrics-driven approach to identifying opportunities for improvement and to measure the impact of improvement efforts. Although CSI is a phase of the lifecycle and is documented in a separate ITIL publication, CSI can be effective only if it is integrated throughout the lifecycle, creating a culture of continual improvement. CSI should ensure that all participants in service delivery understand that identifying opportunities for improvement is their responsibility.

(iv)**ROI for CSI**: There is no true understanding of current IT capabilities or costs.

* There is limited knowledge of the business drivers, and their link with IT.
* Viable data is difficult to find in a low-process maturity, data-poor environment.
* Frequently there is limited knowledge of the cost of IT downtime to the business and IT.
* There is limited knowledge of the support at a unit level (e.g. cost of an incident, cost of a Level 2 support visit).
* There is limited experience in establishing measurement frameworks beyond simple component/system measurement.
* There is limited experience in identifying measurable benefits.
* There is a lack of understanding of the difference between benefits and ROI.
* Tangible and intangible benefits are difficult to distinguish.
* Compiling a clear and persuasive case for process improvement is difficult.
* Success criteria are inadequately identified, or a way to measure them is not clear.
* A failure to progressively measure and monitor benefits/returns.

(v)**Service Management**: IT Service Management is a general term that describes a strategic approach for designing, delivering, managing and improving the way information technology (IT) is used within an organization. The goal of every IT Service Management framework is to ensure that the right processes, people and technology are in place so that the organization can meet its business goals.

(vi) The **Service Reporting** process reports on the results achieved both operationally and strategically. It also reports on any developments related to **Service Level Agreements** such as hitting various targets, like availability.

Its purpose is to provide information to both IT and the business in order for informed decisions to be made.  IT and the business should agree the format and style of reports to suit their relevant audiences.

A **reporting framework policy** needs to be documented and agreed with the various business units as the finance department would want to see a different set of reports from the marketing department.  This would be incorporated at the **Service Design** phase.

The framework should contain as a minimum:

* Target groups and the services delivered
* Agreement of what should be measured and therefore reported upon
* The basis for calculations
* Access to the reports and what media should be used ie. Intranet, email etc.
* Regular meetings to discuss the reports and subsequent improvements